

UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
CAMPUS DE GUARATINGUETÁ

ROBERTA ALVES DO NASCIMENTO RIBEIRO

Os Códigos de Barras como Temas Geradores no Ensino de Matemática

Guaratinguetá

2021

Roberta Alves do Nascimento Ribeiro

Os Códigos de Barras como Temas Geradores no Ensino de Matemática

Trabalho de Graduação apresentado ao Conselho de Curso de Graduação em Licenciatura em Matemática da Faculdade de Engenharia do Campus de Guaratinguetá, Universidade Estadual Paulista, como parte dos requisitos para obtenção do diploma de Graduação em Licenciatura em Matemática .

Orientadora: Prof^a. Dr^a. Grasielle Cristiane Jorge

Guaratinguetá

2021

R484c	Ribeiro, Roberta Alves do Nascimento Os Códigos de barras como temas geradores no ensino de matemática / Roberta Alves do Nascimento Ribeiro – Guaratinguetá, 2021. 67 f : il. Bibliografia: f. 65-67 Trabalho de Graduação em Matemática – Universidade Estadual Paulista, Faculdade de Engenharia e Ciências de Guaratinguetá, 2021. Orientadora: Prof^ª. Dr^ª. Grasielle Cristiane Jorge 1. Código de barras. 2. Matemática (Ensino médio) 3. Matemática - Estudo e ensino. 4. Criptografia. I. Título. CDU 51
-------	---

UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
CAMPUS DE GUARATINGUETÁ

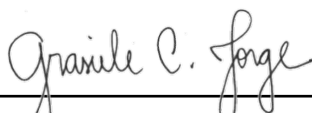
ROBERTA ALVES DO NASCIMENTO RIBEIRO

ESTE TRABALHO DE GRADUAÇÃO FOI JULGADO ADEQUADO COMO PARTE DO
REQUISITO PARA A OBTENÇÃO DO DIPLOMA DE "GRADUANDA EM
LICENCIATURA EM MATEMÁTICA "

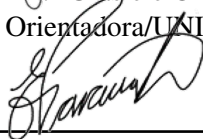
APROVADO EM SUA FORMA FINAL PELO CONSELHO DE CURSO DE GRADUAÇÃO EM
LICENCIATURA EM MATEMÁTICA

Prof^a. Dr^a. SILVIA GIULIATTI WINTER
Coordenadora

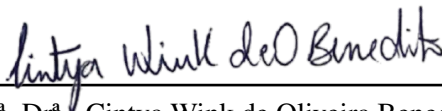
BANCA EXAMINADORA:



Prof^a. Dr^a. Graciele Cristiane Jorge
Orientadora/UNIFESP



Prof^a. Dr^a. Elisangela Pavanelo Rodrigues dos
Santos
UNESP-FEG



Prof^a. Dr^a. Cintya Wink de Oliveira Benedito
Membro Externo

Fevereiro, 2021

Dedico este trabalho aos meus pais, pelo apoio e amor incondicional.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus, porque sem Ele nada seria possível.

Agradeço à minha mãe, Tereza, por sempre acreditar em mim, até mesmo quando nem eu acredito. Agradeço ao meu pai, Carlos, por me incentivar a aprender sempre. Obrigada por todo esforço que fizeram por mim e pela minha educação.

Agradeço à minha orientadora, Prof^a. Dr^a. Grasiele Cristiane Jorge, por todo incentivo e ensinamento durante o período da minha graduação, e por ser um modelo na minha trajetória acadêmica.

Agradeço ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), pela concessão de bolsa de iniciação científica durante os anos de graduação.

Agradeço aos meus familiares, e principalmente aos meus avós: Maria (*in memorian*), Benedito, Mario (*in memorian*), Alice (*in memorian*) e Neusa. Obrigada pelas minhas melhores memórias.

Agradeço todos os professores que fizeram parte da minha formação. Agradeço à “Tia” Patrícia, que me alfabetizou e me ensinou muito além das letras e números. Agradeço à Professora Laura, por toda a motivação e carinho. Agradeço ao Professor Hélder, meu padrinho e amigo, por todo apoio, inspiração e incentivo. Espero que um dia eu seja tão importante na vida de alunos quanto vocês foram na minha.

Agradeço à Escola Ryoiti Yassuda e toda a equipe escolar. Obrigada por terem mudado a minha vida e me mostrado que é possível alcançar até os degraus mais altos da minha escada dos sonhos.

Agradeço à Universidade Estadual Paulista (UNESP) e ao corpo docente do meu curso, pela excelência do ensino.

RESUMO

Este trabalho objetiva apresentar algumas possibilidades de planejar aulas utilizando os códigos, e especialmente os códigos de barras, como temas geradores no ensino de Matemática no Ensino Médio, através de uma abordagem qualitativa na metodologia de Pesquisa Bibliográfica. A escolha do tema surgiu da percepção da presença dos códigos na vida cotidiana, desde os códigos de barras nos produtos adquiridos até os documentos de identificação, como o Cadastro de Pessoas Físicas (CPF), sua relação com a Matemática e a possibilidade de pensar neles como temas geradores nas aulas da disciplina. Com a perspectiva de promover possibilidades de ensino abrangentes e contextualizadas, o trabalho se amplia para uma abordagem dos códigos remetendo à sua história e significados diversos. As atividades desenvolvidas tratam de três subtemas, dentro do tema códigos: a criptografia, os códigos de barras e os códigos QR. Essas atividades foram pensadas à luz dos temas geradores, do Recurso à História da Matemática e da Resolução de Problemas, embora com adaptações pertinentes para cada proposta.

PALAVRAS-CHAVE: Códigos. Código de Barras. Educação. Ensino Médio.

ABSTRACT

This work aims to present some possibilities of classes using Codes, and especially Barcodes, as generating themes in the teaching and learning of Mathematics in High School, through a qualitative approach in the Bibliographic Research methodology. The choice of theme came from the perception of the presence of codes in everyday life, from barcodes in everyday products to identification documents, how it is related to Mathematics and the perspective of thinking about them as generating themes in classes. With the expectancy of promoting comprehensive and contextualized teaching possibilities, the work expands to an approach to codes referring to their history and different meanings. The developed activities deal with three sub-themes, within the theme Codes: Cryptography, Barcodes and QR Codes. These activities were planned based on the generating themes, the Resource to the History of Mathematics and the Problem Solving, although with relevant adaptations for each proposal.

KEYWORDS: Codes. Barcodes. Education. High School.

LISTA DE ILUSTRAÇÕES

Figura 1	Cítala espartana	19
Figura 2	Cifra de César com deslocamento 6	20
Figura 3	Modelo da Máquina Enigma	24
Figura 4	Patente do precursor do código de barras	26
Figura 5	Código de barras no sistema UPC	27
Figura 6	Divisões do código de barras no sistema UPC	28
Figura 7	Espessuras do código de barras no sistema UPC	29
Figura 8	Código de barras no sistema UPC	30
Figura 9	Código de barras no sistema EAN-13	32
Figura 10	Padrão de um algarismo no EAN-13	33
Figura 11	Dígito verificador do UPC	34
Figura 12	Dígito verificador	35
Figura 13	Módulos de um código QR	38
Figura 14	Modelo 1 e Modelo 2 do código QR	38
Figura 15	Versões do código QR	39
Figura 16	Estrutura do código QR	40
Figura 17	Informação da versão do código QR	41

LISTA DE TABELAS

Tabela 1 – Codificação no UPC	29
Tabela 2 – Critério de paridade no EAN-13	31
Tabela 3 – Codificação no EAN-13	32
Tabela 4 – Exemplo de Critério de Paridade no EAN-13	32

LISTA DE ABREVIATURAS E SIGLAS

BNCC	Base Nacional Comum Curricular
CEP	Código de Endereçamento Postal
CNH	Carteira Nacional de Habilitação
CNPJ	Cadastro Nacional da Pessoa Jurídica
CPF	Cadastro de Pessoa Física
DCNs	Diretrizes Curriculares Nacionais
EAN-13	European Article Number
ISBN	International Standard Book Number
NCTM	National Council of Teachers of Mathematics
PCNs	Parâmetros curriculares nacionais
QR Code	Quick Response Code
RG	Registro Geral
UPC	Universal Product Code
USPTO	United States Patent and Trademark Office

SUMÁRIO

1	INTRODUÇÃO	11
2	METODOLOGIA	14
2.1	A PESQUISA QUALITATIVA	14
2.2	A PESQUISA BIBLIOGRÁFICA	15
3	OS CÓDIGOS	17
3.1	HISTÓRIA DOS CÓDIGOS	18
3.2	O CÓDIGO DE BARRAS	25
3.2.1	Funcionamento	27
3.2.1.1	O Código UPC	27
3.2.1.2	O código EAN-13	30
3.2.2	O dígito verificador	33
3.2.3	A detecção de erros	35
3.3	O CÓDIGO QR	38
4	RESOLUÇÃO DE PROBLEMAS COMO METODOLOGIA DE ENSINO .	42
4.1	OS TEMAS GERADORES	44
4.2	A RESOLUÇÃO DE PROBLEMAS	44
4.3	O RECURSO À HISTÓRIA DA MATEMÁTICA	48
5	ATIVIDADES PROPOSTAS	50
5.1	ATIVIDADE 1 - CRIPTOGRAFIA	51
5.2	ATIVIDADE 2 - CÓDIGOS DE BARRAS	56
5.3	ATIVIDADE 3 - CÓDIGOS QR	59
6	CONSIDERAÇÕES FINAIS	63
	REFERÊNCIAS	65

1 INTRODUÇÃO

Os códigos estão presentes nas mais variadas situações do cotidiano, desde o funcionamento de celulares e computadores aos documentos de identificação, como o Cadastro de Pessoa Física (CPF), por exemplo. Uma de suas aplicações, muito recorrente, são os códigos de barras, uma representação em imagem de dados numéricos ou textuais, que tem como objetivo identificar, com segurança e numericamente, um objeto de acordo com características específicas, como sua origem e finalidade.

Os códigos de barras estão presentes em numerosas circunstâncias e cada aplicação requer um tipo diferente, por exemplo: o *European Article Numbering* (EAN-13) — Numeração Europeia de Artigos — e o *Universal Product Code* (UPC) — Código Universal de Produto —, que são utilizados no varejo e o *Quick Response Code* (QR Code) — Código de Resposta Rápida —, que possui aplicações variadas e vem apresentando, no últimos anos, crescente utilização. Seu uso promove agilidade e controle de informações, proporcionando contribuições tecnológicas tangíveis e que refletem no desenvolvimento humano.

O funcionamento dos códigos de barras envolve regras e determinações prévias que se baseiam em conceitos matemáticos variados, sendo alguns deles passíveis de serem abordados no Ensino Básico. É nesse contexto que esse tema surge como uma opção de exploração de conteúdos na disciplina de Matemática do Ensino Fundamental e Médio, com uma vasta possibilidade de tratamento.

No início desse século, os Parâmetros Curriculares Nacionais para o Ensino Médio (Bases Legais) já afirmavam ser possível prever que “(...) nas próximas décadas, a educação vá se transformar mais rapidamente do que em muitas outras, em função de uma nova compreensão teórica sobre o papel da escola, estimulada pela incorporação das novas tecnologias.” (BRASIL, 1998, p.6).

Isso evidencia a necessidade de se pensar educação — e aqui especificamente Educação Matemática — incluindo as tecnologias nas aulas, explorando suas funcionalidades, história e contribuições para o mundo globalizado. É imprescindível considerar que as ciências, assim como as tecnologias, são construções humanas situadas historicamente. De acordo com Krasilchik, “Os alunos não serão adequadamente formados se não correlacionarem as disciplinas escolares com a atividade científica e tecnológica e os problemas sociais contemporâneos.” (KRASILCHIK, 2000, p.90).

Levando isso em conta, esse trabalho não se limitará a abordar apenas os códigos de barras, mas também outras formas de códigos, como a criptografia e, em particular, as cifras, pois:

Para além do uso prático e imediato, é também possível relacioná-los à história e desenvolvimento da humanidade tendo em vista seu papel de destaque na preservação do conhecimento, relações entre os povos e, notadamente, conflitos. Estudando a presença de códigos durante algumas guerras percebemos uma estreita relação com a criptografia, chegando ao ponto de muitas vezes confundir-se quanto ao significado de cada uma. (SOUSA, , p.1)

Por essa razão, abordar os códigos de forma abrangente, considerando a criptografia, proporciona um tratamento mais completo e situado historicamente. No caso deste trabalho, as possibilidades de

ensino se ampliam vantajosamente, possibilitando o desenvolvimento de atividades que utilizem o Recurso à História da Matemática.

Dessa forma, este trabalho será desenvolvido visando à elaboração de propostas de atividades a serem abordadas no Ensino Médio que utilizem os códigos, e principalmente os códigos de barras, como temas geradores e que abranjam recursos de ensino diversificados, como o Recurso à História da Matemática, utilizando a Resolução de Problemas como metodologia de ensino. A Matemática deve ser um instrumento que auxilie na compreensão do mundo e, por isso, os códigos oferecem uma aproximação oportuna de competências e habilidades contempladas na disciplina.

Inicialmente, esse trabalho foi planejado para o desenvolvimento de uma sequência didática a ser desenvolvida em sala de aula. Contudo, o ano de 2020 sofreu consequências drásticas e inimagináveis em todos os quesitos, incluindo na educação, por conta da pandemia da Covid-19. O ensino passou a ser remoto, trazendo novos desafios para professores e alunos, e impossibilitando que o planejamento deste trabalho fosse colocado em prática. Por essa razão, um novo planejamento foi realizado, e este trabalho contém apenas os aspectos teóricos do tema escolhido.

Tal proposta será guiada pela pergunta “Como os códigos, especificamente os códigos de barras, podem ser utilizados como temas geradores no ensino de Matemática para o Ensino Médio?”, desenvolvendo a partir disso uma análise que possibilite a resposta desse questionamento, o aperfeiçoamento dessa abordagem e a reflexão acerca dos resultados obtidos com esse trabalho. Essa pergunta busca esclarecer quais as possíveis contribuições que podem ser alcançadas no ensino da Matemática no Ensino Médio, através dos códigos como temas geradores, especificamente os códigos de barras, tão frequentemente utilizados em nosso cotidiano.

Considerando a contribuição da Matemática como uma possibilidade para a compreensão do mundo, se faz necessário que os professores busquem situações-problema que tratem desse tema. A percepção da constante presença dos códigos na vida cotidiana, de sua correlação com a Matemática e das possibilidades de ensino que oferece, suscitou a curiosidade em investigar o desenvolvimento de atividades que contemplem esse tema no Ensino Médio. É nesse contexto que surge a proposta deste trabalho, buscando desenvolver atividades nessa perspectiva e investigar as possíveis contribuições que esse tema pode viabilizar aos educadores e educandos.

Para isso, a abordagem adotada será a qualitativa, através da pesquisa bibliográfica. Uma de suas principais características, de acordo com Tozoni-Reis (2009), é que a coleta de dados é realizada na própria bibliografia do tema que se quer investigar. No entanto, como salientam Marconi e Lakatos (2003), a pesquisa bibliográfica não se limita a repetir o que já foi escrito ou dito sobre um determinado tema, mas possibilita o exame desse assunto sob um novo ângulo, chegando em novas conclusões.

O trabalho foi dividido da seguinte forma: o Capítulo 2 trata da metodologia de pesquisa adotada no trabalho, caracterizada pelo modo de pesquisar qualitativo com a abordagem da pesquisa bibliográfica; o Capítulo 3 é destinado a abordar os códigos, focando na história dos códigos, estendendo para a criptografia, nos códigos de barras e no código QR; o Capítulo 4 justifica a abordagem pedagógica escolhida para as atividades a serem propostas, considerando os temas geradores, o recurso à História da Matemática e a metodologia de ensino da Resolução de Problemas, trazendo os códigos à luz da Educação Matemática com ajuda dos documentos oficiais norteadores da educação; em seguida,

o Capítulo 5 desenvolve as três atividades propostas pela autora; e, por fim, o Capítulo 6 traz as considerações finais acerca de todo o trabalho realizado.

2 METODOLOGIA

Ao falar de pesquisa, logo são suscitados alguns questionamentos quanto ao seu objetivo, motivação, público alvo, objeto de investigação e metodologia, por exemplo. Quanto à metodologia de pesquisa, existem duas opções: a quantitativa e a qualitativa. Neste texto, será discutida a pesquisa qualitativa, com considerações gerais e abordagem específica em relação à Educação Matemática.

2.1 A PESQUISA QUALITATIVA

O modo de pesquisar qualitativo, quando realizado por meio de princípios reguladores, é tão confiável quanto o quantitativo e, por isso, devemos negar o pensamento de que apenas a quantificação permite validade e confiabilidade. Esses princípios reguladores dizem respeito aos parâmetros que uma comunidade, após discussões, estabelece em relação à avaliação de uma investigação, e aos critérios que direcionem as ações do pesquisador. É necessário se atentar para a diferença entre regular e regulamentar, e podemos entender que “‘Regular’ diz do sujeitar a regras, dirigir, regerar, estabelecer e facilitar por meio de disposições. ‘Regulamentar’ fala da sujeição a regulamentos.” (GARNICA, 2001, p.38). É necessário distinguir esses termos pois, algumas vezes, em busca de moldes que guiem a pesquisa qualitativa e a protejam de críticas, abre-se mão do regular para aderir aos regulamentos.

Mas o que é pesquisar qualitativamente? Segundo Bicudo, as pesquisas que se voltam para o método qualitativo

São pesquisas que permitem compreender características do fenômeno investigado e que, ao assim procederem, oferecem oportunidade para possibilidades de compreensões possíveis quando a interrogação do fenômeno é dirigida a contextos diferentes daquele em que a investigação foi efetuada. (BICUDO, 2012, p.19)

Isso nos diz que, nesse modo de fazer pesquisa, o contexto do fenômeno investigado tem de ser levado em consideração, explorando as suas manifestações sem, no entanto, poder generalizá-las e aplicá-las em diferentes conjunturas. Além disso, a pesquisa qualitativa não possui moldes e parâmetros fixos, pois, como tratado acima, apesar de possuir princípios reguladores, não se caracteriza por regulamentações. Tal desprendimento se dá pela compreensão de que o mundo não se revela imutável aos nossos olhos sem que haja um processo que envolve nossa percepção e interpretação, suscitando diferentes interrogações e preocupações. Aqui cabe o destaque para a interrogação no modo de pesquisar qualitativo.

Conforme Bicudo (2012), a interrogação e seu esclarecimento são vistos como pontos cruciais para a pesquisa qualitativa, influenciando na definição de questionamentos indispensáveis para o desenvolvimento da investigação, como no “o quê” e no “como”. Isso faz prevalecer o processo em detrimento do produto, ou seja, o decurso da investigação, as interações estabelecidas, a metodologia realizada e os passos definidos para responder a interrogação inicial são mais valorizados do que o produto e o resultado obtido.

Há, ainda, outras regulações que permeiam o pesquisar qualitativo, como a prevalência de processos indutivos no momento de análise, a predominância de dados descritivos, o consentimento da comunidade quanto aos critérios de avaliação e a responsabilidade dirigida ao pesquisador sobre sua pesquisa.

Quanto à Educação Matemática, que possui suas pesquisas majoritariamente efetuadas de modo qualitativo, todos os aspectos anteriormente citados são aplicáveis. Sendo esta uma área teórico-prática que objetiva estudar ações e reações humanas na esfera da educação, não convém projetar resultados e expectativas quanto às investigações realizadas, e sim empreender um estudo preocupado com os processos desenvolvidos nessa pesquisa. Quanto aos possíveis temas de pesquisa nessa área:

Podemos apontar em um grande leque de possibilidades de temas de pesquisa, por exemplo, aquelas que buscam por compreensões de modos pelos quais os alunos constroem suas aprendizagens (de matemática), individualmente, com os colegas, com a mídia, em contextos específicos; de atividades de ensino, da realidade escolar, dos textos que servem de mediadores ao ensino, mas que não são entendidos como neutros ideológica e cientificamente, donde atentar-se pelo que dizem além do dito. O mesmo ocorre com os documentos que sustentam instituições e a própria Educação Pública. (BICUDO, 2012, p.24)

Desse modo, ao pesquisar em Educação Matemática, é necessário considerar o diálogo entre as áreas Matemática e Educação, sem que estas sejam tomadas isoladamente ou que de modo que haja sobreposição de uma a outra. Outra preocupação primordial está relacionada ao dever de os educadores matemáticos delimitarem suas fronteiras de ação prática e de pesquisa.

A pesquisa qualitativa possui uma miríade de abordagens, como a Fenomenologia, a Hermenêutica, a Pesquisa Participante, a Pesquisa Ação, a Pesquisa Etnográfica, a Análise de Conteúdo, o Experimento de Ensino e a Pesquisa Bibliográfica. No desenvolvimento desse trabalho, se optou pela abordagem da Pesquisa Bibliográfica.

2.2 A PESQUISA BIBLIOGRÁFICA

Tal abordagem se caracteriza pela busca “(...) nos autores e obras selecionados, os dados para a produção do conhecimento pretendido. Não vamos ouvir entrevistados, nem observar situações vividas, mas conversar e debater com os autores através de seus escritos” (TOZONI-REIS, 2009, p.25). A sua principal vantagem, conforme em Gil (2002), reside no fato de possibilitar ao investigador a cobertura de uma variedade de fenômenos muito mais ampla do que poderia pesquisar diretamente.

A pesquisa bibliográfica é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos. Embora em quase todos os estudos seja exigido algum tipo de trabalho dessa natureza, há pesquisas desenvolvidas exclusivamente a partir de fontes bibliográficas. (GIL et al., 2002, p.44)

Dada uma hipótese, a pesquisa bibliográfica busca a resolução de um problema através de referenciais teóricos publicados, utilizando-se das contribuições científicas prévias, a fim de proporcionar recursos para o tema que está sendo pesquisado. Segundo Lima e Miotto (2007) uma pesquisa bibliográfica bem feita é capaz de gerar a postulação de hipóteses e interpretações que poderão servir de ponto de partida para outras pesquisas.

O procedimento dessa metodologia não é aleatório, pois “(...) implica em um conjunto ordenado de procedimentos de busca por soluções, atento ao objeto de estudo” (LIMA; MIOTTO, 2007, p.38). De acordo com Tozoni-Reis (2009), existem etapas para uma pesquisa bibliográfica, sendo elas: delineamento da pesquisa; revisão bibliográfica; coleta de dados; organização dos dados; análise e interpretação dos dados; e redação final. Apesar de esses passos serem essenciais para qualquer tipo de pesquisa, os procedimentos metodológicos da pesquisa bibliográfica são bastante específicos, caracterizando principalmente a leitura, análise e interpretação de texto como etapas determinantes nesse processo.

Por exemplo, a leitura a ser realizada no processo da pesquisa bibliográfica não é a leitura comum, como estamos habituados. Segundo Gil (2002) são recomendáveis quatro momentos de leitura, sendo eles: leitura exploratória (verifica em que medida a obra consultada interessa à pesquisa); leitura seletiva (seleção do material pertinente); leitura analítica (organizar e sintetizar as informações que possibilitem a obtenção de respostas); e leitura interpretativa (objetiva relacionar as asserções do autor com o problema para o qual se propõe uma solução).

Assim, a produção de conhecimentos, que resulta do trabalho de investigação científica que toma a pesquisa bibliográfica como modalidade e não se reduz a uma apresentação das ideias de diferentes autores acerca do tema estudado. (...) Concordar, discordar, discutir, problematizar os temas à luz dos autores lidos são os procedimentos dessa modalidade de pesquisa. (TOZONI-REIS, 2009, p.27)

Nesse trabalho, intencionando atender aos objetivos e justificativas dados, será realizada a pesquisa bibliográfica desenvolvida com base nos referenciais teóricos pertinentes, como livros, dissertações e artigos científicos, inicialmente através de um levantamento bibliográfico e seguindo as demais etapas recomendadas nessa metodologia. Não há um “problema” a ser resolvido no trabalho, mas sim uma proposta do uso de um tema pertinente em sala de aula e, dessa forma, a pesquisa bibliográfica será uma ferramenta para a apresentação desse tema, da sua justificativa pedagógica com base nos documentos educacionais oficiais e das propostas de atividades. Reiterando isso, “A bibliografia pertinente oferece meios para definir e resolver não somente problemas já conhecidos, como também explorar novas áreas” (MANZO, 1971 apud LAKATOS; MARCONI, 2001).

Propostas de aulas serão desenvolvidas acerca das possibilidades de se utilizar os códigos, especificamente os códigos de barras e os códigos QR, como temas geradores nas aulas de Matemática, com base em todo o conhecimento procedido da pesquisa prévia, através da Resolução de Problemas.

Assim compreendido, entendemos que o trabalho que nos propomos a desenvolver nesta pesquisa poderá ser desenvolvimento mediante a abordagem qualitativa da Pesquisa Bibliográfica.

3 OS CÓDIGOS

No decorrer de sua evolução social e intelectual, o homem sentiu a crescente necessidade de registrar e comunicar suas ideias, assim como de transmitir informações de naturezas diversas. Alguns dos primeiros registros que mostram a realização desses feitos consistem nos registros rupestres pré-históricos, formas gráficas de comunicação utilizadas por grupos pré-históricos que habitaram determinadas regiões do mundo. Os hieróglifos egípcios, considerados a escrita mais antiga da humanidade, datando de 3000 a.C., também são exemplos de registros primitivos com a finalidade mencionada.

Essas formas de registros evoluíram e se aperfeiçoaram conforme o homem se desenvolvia em sociedade e se adaptava às novas necessidades que encontrava, além de avanços relacionados ao alcance e simplicidade das formas de comunicação, atingidos pelos seus esforços intelectuais.

Por exemplo, para escrever esse texto, está sendo utilizado o alfabeto latino, que consiste em 26 símbolos diferentes, cada um representando uma unidade básica de som da língua portuguesa, nesse caso. Esses símbolos, quando organizados de maneira apropriada, formam as palavras, que são dotadas de significado. Isso permite que informações sejam registradas de forma duradoura, com maior alcance, precisão e formalidade.

No entanto, nem sempre essa facilidade de acesso à informação é desejada ou conveniente ao comunicante. Algumas situações requerem privacidade na comunicação ou no armazenamento de informações, ou até mesmo maior simplicidade na sua apresentação.

Nesta Seção intencionamos apresentar os códigos, desde seus usos primários, seus destaques históricos no desenvolvimento da humanidade e, principalmente, seus usos atuais, com amplas aplicações e finalidades. Essa breve contextualização histórica busca criar paralelos entre o desenvolvimento de determinadas ciências e os aspectos sociais que as influenciaram, como forma de minimizar a fragmentação intelectual, inserindo o objeto de estudo desse trabalho em um panorama mais amplo.

Antemão, é necessário delinear o que são os códigos. As definições são amplas e há divergências entre o uso popular e o uso técnico. Ao consultar um dicionário encontram-se, entre outros, os seguintes significados:

“6 Linguagem, secreta ou não, em que entram palavras, às quais, convencionalmente, se dão significações diferentes das que normalmente possuem. 7 Coleção sistemática de sinais, números ou abreviações, destinados a possibilitar brevidade de expressão ou economia de palavras, para vários fins. 8 INFORM Regras usadas para converter instruções ou dados de uma forma para outra. 9 COMUN, LING Sistema de signos devidamente organizados e convencionados, a fim de permitir a elaboração e transmissão de mensagens.” (MICHAELIS, 2015)

Um dos objetivos desse trabalho é abordar os códigos de barras, que melhor se encaixam na definição oito. Antes disso, porém, serão abordados os códigos em sua definição mais técnica, conjuntamente com o que se entende por cifras. “Tecnicamente um código é definido como uma

substituição de palavras ou frases, enquanto cifra é definida como uma substituição de letras.” (SINGH, 2020, p.47), ou, ainda, “(...) enquanto que os códigos são um conjunto de sinais, um vocabulário, utilizado em comunicações, podendo ou não ser secretos, a criptografia está interessada em um conjunto de técnicas para transformar a escrita ininteligível para aqueles que originalmente não façam parte da comunicação.” (SOUSA, , p.2).

Dessa forma, o trabalho se expande para essas definições, objetivando a visão ampla e histórica do tema, com sua evolução e novas aplicações conforme desenvolvimento da sociedade.

3.1 HISTÓRIA DOS CÓDIGOS

Em alguns momentos da história, o homem se deparou com situações que demandavam discrição e privacidade na transmissão de mensagens. Tais situações podem ter sido as mais variadas e datadas de períodos muito primordiais, como o contato entre chefes militares numa guerra, comandos de reis, faraós ou imperadores para seus soldados, descobertas importantes entre estudiosos ou ainda cartas entre casais que compartilhavam um amor proibido. Muitas podem ter sido as circunstâncias para o desejo de manter suas informações em sigilo, e aqui serão tratadas as principais de que se tem registros.

De acordo com Singh (2020), o que motivou a criação das cifras foi a ameaça de interceptação inimiga, mostrando a necessidade do desenvolvimento de técnicas que ocultassem uma mensagem para expectadores indesejados. Ainda segundo o autor, a história dos códigos e cifras é, também, a história das batalhas entre os codificadores e os codificantes através dos séculos, uma batalha de esforço intelectual e que impactou grandiosamente a história da humanidade.

Este capítulo possui como principal referencial teórico o livro “O Livro dos Códigos”, de Simon Singh (2020).

Alguns dos primeiros registros da utilização de meios secretos para transmitir mensagens remetem dos conflitos entre a Grécia e a Pérsia, no século V a.C. Um dos registros mostra como a escrita secreta foi responsável por salvar os gregos de serem conquistados pelos persas, quando estes deram início ao plano secreto de formar um exército para conquistar os territórios gregos. O elemento surpresa era vital para o sucesso do ataque, mas um grego exilado, Demarato, testemunhou os preparativos e decidiu avisar a sua nação.

Para enviar o aviso à Esparta, de maneira a evitar a interceptação dos guardas persas, Demarato raspou a cera de um par de tábuas de madeira e escreveu a mensagem embaixo, cobrindo-a com cera novamente. Foi uma estratégia esperta e bem sucedida, mas que exigiu um pouco de sorte, pois os gregos também não sabiam como descobrir a mensagem. Foi uma mulher, Gorgo, que adivinhou o “segredo” e enfim passou a mensagem aos outros. Isso permitiu que os gregos se preparassem para o ataque formando uma estratégia de defesa poderosa e que garantiu a vitória sobre a potente força militar da Pérsia.

Outro relato interessante sobre a transmissão de mensagens através da sua ocultação é a história de Histaeu: para encorajar uma revolta contra o rei persa, ele escreveu as instruções no couro cabeludo de um mensageiro e esperou que seu cabelo crescesse até enviá-lo em viagem. Como ele não carregava nada suspeito, não teve problemas atravessando as fronteiras e chegou ao seu destino bem, podendo contatar o destinatário da mensagem e, após raspar o cabelo, exibir a mensagem desejada.

Quando a comunicação é realizada como nos casos mencionados, de maneira a ocultar uma mensagem, ela é conhecida como esteganografia, “(...) nome derivado das palavras gregas *steganos*, que significa coberto, e *graphein*, que significa escrever” (SINGH, 2020, p. 21). Essa forma de ocultação foi amplamente utilizada nos dois milênios que se seguiram aos relatos anteriores, com diversas formas, materiais e finalidades. No entanto, sua fraqueza é óbvia, pois podem ser facilmente descobertas e as mensagens que intencionavam ser ocultas, serem reveladas.

Com a necessidade de transmitir mensagens com segurança, paralelamente à esteganografia se desenvolveu a criptografia. Nesse caso, a intenção não é ocultar a mensagem, mas sim o seu significado, o que é feito através de um processo de encriptação, onde “Para tornar a mensagem incompreensível, o texto é misturado de acordo com um protocolo específico, que já foi estabelecido previamente por ambos transmissor e receptor.” (SINGH, 2020, p. 22), criando dificuldade ou até mesmo impossibilidade de compreensão caso ela seja interceptada.

A criptografia pode ser dividida em duas partes: os casos em que são usados transposição e os casos em que são usados substituição. No primeiro caso, trata-se de um rearranjo das letras da palavra, resultando no que conhecemos com anagrama.

Existem muitas formas de se fazer essa transposição, e quanto maior a mensagem a ser cifrada, maiores as possibilidades para tal. No entanto, essa técnica não é vantajosa se aplicada para cifrar palavras curtas, pois nesse caso pode ser decifrada facilmente. Por exemplo, a palavra *sim* pode ser arranjada de seis formas diferentes (*sim*, *smi*, *msi*, *mis*, *ism*, *ims*), pois possui apenas três letras. Enquanto isso, a palavra *matemática* tem mais de 151 mil maneiras de ser rearranjada, e esse número seria maior não fossem as letras repetidas na palavra.

O primeiro aparato criptográfico militar, datado do século V a.C., consistia em uma forma de criptografia de transposição, chamado *cítala espartana*. O objeto é um bastão de madeira no qual se enrola uma tira de pergaminho ou couro e se escreve a mensagem desejada, como na Figura 1.

Figura 1 – Cítala espartana



Fonte: Wikipédia (sem indicação de autor) (2021).¹

Ao desenrolar a tira, serão apenas letras aleatórias por seu comprimento. Dessa forma, é seguro viajar com ela e o mensageiro pode carregá-la sem suspeitas. O destinatário deverá apenas ter um bastão de madeira de mesmo diâmetro, e quando receber a tira, deverá enrolá-la em torno dele, revelando a mensagem.

¹ Disponível em: <<https://upload.wikimedia.org/wikipedia/commons/5/51/Skytale.png>>

Enquanto a cifra de transposição mantém a identidade de cada letra e apenas altera suas posições nas palavras, a cifra de substituição age de forma oposta, mantendo a posição, mas alterando a identidade das letras. As maneiras de se realizar a substituição são inúmeras.

Júlio César, o imperador romano, foi o responsável por usar uma cifra de substituição pela primeira vez em um documento para propósitos militares. Nesta ocasião, tentando contatar Cícero, ele substituiu as letras do alfabeto romano por letras gregas, impossibilitando que, caso interceptada, os inimigos a compreendessem. Júlio César utilizava métodos de escrita secreta muito frequentemente, e seu método mais famoso é conhecido a partir dos relatos contidos em documentos do século II, onde ele substituíria cada letra do alfabeto pela letra que estivesse três posições à frente.

A chamada cifra de César consiste em substituições com qualquer deslocamento de posições das letras do alfabeto e, portanto, possibilita a criação de 25 cifras diferentes. Por exemplo, seja o caso em que o deslocamento escolhido é o de seis posições. As correspondências passarão a ser como mostrado na Figura 2.

Figura 2 – Cifra de César com deslocamento 6

Alfabeto original →	a	b	c	d	e	f	g	h	i	j	k	l	m
Alfabeto cifrado →	G	H	I	J	K	L	M	N	O	P	Q	R	S

Alfabeto original →	n	o	p	q	r	s	t	u	v	w	x	y	z
Alfabeto cifrado →	T	U	V	W	X	Y	Z	A	B	C	D	E	F

Fonte: Produção da própria autora (2021).

Por exemplo, seja a frase “*A Matemática é linda*”. Se para cifrar esta frase for utilizada a Cifra de César com o deslocamento de seis posições como mostrado acima, a mensagem obtida será “*G SGZKSGZOIG K ROTJG*”.

Para definir um método geral de codificação, temos o algoritmo e a chave, que especificam em detalhes quais os procedimentos para uma determinada codificação. Cada cifra pode ser considerada nesse sentido, onde o algoritmo consiste na substituição de cada letra do alfabeto original (em letras minúsculas) por uma letra do alfabeto cifrado (em letras maiúsculas), enquanto a chave define exatamente qual o alfabeto cifrado. No caso exibido na Figura 2, a chave é dada pelo deslocamento de seis posições das letras do alfabeto.

A segurança de um sistema de código deve ser garantida por alguns fatores, como o número de chaves possíveis para codificação, por exemplo. Um interceptador pode conhecer o algoritmo da mensagem, mas se ele não conhecer a chave, não poderá decifrá-la, e por isso o número de chaves possíveis é um fator determinante para a segurança do sistema.

No caso da Cifra de César, são apenas 25 chaves em potencial, o que não garante segurança na transmissão de mensagens, pois é relativamente fácil testar cada uma delas. No entanto, “(...) se o remetente da mensagem usar um algoritmo de substituição mais geral, que permite que o alfabeto cifrado consista

em qualquer rearranjo do alfabeto original, então existem 400.000.000.000.000.000.000.000.000 de chaves possíveis para se escolher.” (SINGH, 2020, p.28).

A cifra de substituição é simples de implementar e oferece um alto nível de segurança, o que motivou que ela fosse amplamente utilizada para os fins da escrita secreta durante o primeiro milênio. Dada sua adesão e aparente indecifrábilidade para os estudiosos antigos, não foram desenvolvidos novos métodos de comunicação secreta e segura. Os quebradores de códigos passaram todo esse tempo buscando atalhos para decifrar as mensagens e descobrir as chaves utilizadas, e foi no Oriente que essa descoberta foi realizada.

Muitas evidências documentais mostram que os árabes, desde o século X, utilizavam a criptografia rotineiramente, tanto em comunicações secretas para assuntos do Estado, quanto para a proteção de registros administrativos. Mas eles não eram apenas proficientes no uso das cifras de substituição monoalfabética, como também foram os responsáveis por quebrá-las, criando assim a criptoanálise, a ciência que possibilita a decifração de uma mensagem sem conhecer a sua chave.

Os estudiosos islâmicos, com esforços em diversas áreas de conhecimento, observaram que algumas letras são mais comuns que outras nos idiomas, caracterizando uma frequência que pode ser analisada. Essa técnica, conhecida como análise de frequência, consiste em observar textos normais num determinado idioma e estabelecer a frequência com que cada letra aparece, e repetir o processo com um texto cifrado (no mesmo idioma). É provável que as letras mais frequentes do texto cifrado correspondam às letras mais frequentes no texto normal, podendo estabelecer relações. É claro que a análise oferecerá apenas médias, e as correspondências podem não ser certas, mas esse processo pode auxiliar o criptoanalista para a decifração de mensagens que antes pareciam impossíveis de serem compreendidas.

Enquanto isso, na Europa, os avanços eram muito mais lentos. Foi apenas por volta dos séculos XIII e XIV que seu uso se tornou difundido, impulsionado pelo Renascimento. Pode ser que a criptoanálise, junto com outras descobertas na ciência e Matemática, tenha sido importada do mundo árabe, mas é provável que ela tenha sido desenvolvida independentemente.

Muitas histórias interessantes se desenvolveram nesse período de crescente emprego da comunicação secreta. Com o tempo e os avanços dos criptoanalistas, a percepção de que novos modos de cifragem deveriam ser criados suscitou invenções engenhosas.

A introdução das palavras-código foi uma dessas tentativas de reforçar a segurança das cifras de substituição, e consistia na representação de palavras inteiras por símbolos ou outras palavras. Para seu uso, remetente e destinatário precisam combinar previamente quais serão essas palavras, frequentemente dispondo de um documento que registre isso e possa ser usado para conferir. Sua aplicação oferece infinitas possibilidades, mas não é prático a seus usuários, pois é muito trabalhoso.

Como mencionado anteriormente, trataremos principalmente dos códigos, mas falamos majoritariamente das cifras até aqui. Vale ressaltar que “(...) um código é definido como uma substituição de palavras ou frases, enquanto a cifra é definida como uma substituição de letras.” (SINGH, 2020, p.47), mas é importante abranger todos esses aspectos para a ampliação da contextualização histórica e das vindouras propostas pedagógicas apresentadas.

Para fins de envio de mensagens secretas, as cifras sempre foram as preferidas dos criptógrafos,

pois as fraquezas dos códigos eram muito mais evidentes e difíceis de se contornar.

As cifras de substituição, apesar de oferecerem grandes números de chaves, foram enfraquecidas pela descoberta da análise de frequências. Por isso, surgiu a necessidade do desenvolvimento de um novo tipo de cifra, mais segura e que contornasse as estratégias utilizadas na análise de frequência.

Dessa forma, de acordo com Singh (2020), com os esforços dos criptógrafos foram criadas novas e mais potentes cifras nos séculos seguintes, tais como a cifra de Vigenère, do francês Blaise de Vigenère e a Grande Cifra, dos Rossignol, utilizada pelo rei Luís XIV da França. Consequentemente, os criptoanalistas tiveram bastante trabalho para decifrar as novas tentativas de manter mensagens em segredo. Em determinados casos, seus usos e tentativas de quebra tiveram participação no desenvolvimento de eventos históricos, como diz a teoria de que Charles Babbage, intelectual britânico, foi obrigado a ocultar sua descoberta sobre a quebra da cifra de Vigenère para dar vantagem à Inglaterra na guerra da Criméia, por exemplo.

No entanto, a criptografia não era utilizada apenas em contextos militares e diplomáticos. Com a invenção do telégrafo e seu extenso uso, a criptografia passou a ter interesse público e comercial, pois as pessoas sentiam a necessidade de proteger suas mensagens. As cifras utilizadas pelo grande público geralmente não eram complexas e poderiam ser facilmente compreendidas por criptoanalistas profissionais, mas serviam ao objetivo de manter as correspondências ocultas contra possíveis curiosos.

A partir disso, os códigos e cifras passaram a aparecer como desafios em jornais, na literatura – em obras de Júlio Verne, Sir Arthur Conan Doyle e Edgar Allan Poe, por exemplo – e em documentos e registros pessoais. Ao mesmo tempo, não haviam avanços significativos da parte dos criptógrafos na criação de cifras mais poderosas, uma vez que a segurança das cifras conhecidas estava destruída pelos criptoanalistas.

Com a invenção do rádio, no fim do século XIX pelo físico italiano Guglielmo Marconi, e o consequente interesse dos militares, a necessidade de uma codificação confiável se fez ainda mais evidente. O rádio possuía como maior vantagem a facilitação da comunicação, pois não necessitava de fios, como o telégrafo, e permitia o contato direto entre dois pontos quaisquer no globo. No entanto, sua maior desvantagem residia na facilidade com que essa comunicação poderia ser interceptada.

Com o início da Primeira Guerra Mundial, os esforços para a criação de uma cifra segura foram intensificados, mas todas as alternativas criadas fracassaram eventualmente. Mesmo assim a criptografia foi amplamente utilizada pelos países, ocasionando além das tentativas de criação de novas cifras, o emprego de criptoanalistas para a interceptação e quebra dos códigos utilizados pelos inimigos.

Um importante caso dessa utilização foi o “Telegrama Zimmermann”, uma mensagem cifrada escrita pelo Ministro das Relações Exteriores da Alemanha, Arthur Zimmermann, que definia uma ampla estratégia de ataque aos Estados Unidos, até então neutro no conflito, cuja interceptação e decifração pelos ingleses finalmente levou os estadunidenses a tomarem lado na guerra e enviarem suas tropas à Europa.

As dificuldades na criação de novas cifras não foram superadas nos anos seguintes à Primeira Guerra, mas os criptógrafos não interromperam seus esforços e passaram a considerar uma nova abordagem, deixando o lápis e papel e passando a explorar as possibilidades oferecidas pela tecnologia. Foi em 1918 que o inventor alemão Arthur Scherbius criou uma máquina criptográfica poderosa e que

teria um grande impacto no futuro: a Enigma.

Com um funcionamento mecânico e intrincado, a Enigma consistia em três elementos básicos: um teclado para a entrada do texto a ser cifrado, um misturador para cifrar a mensagem e um mostrador para exibir o texto cifrado. Seu funcionamento não é complexo, mas é detalhado:

A unidade de cifragem era composta por três cilindros móveis, que podiam alternar a sua posição dentro da máquina, e um fixo, que se chamava espelho. Cada um dos cilindros contem as vinte e seis letras do alfabeto. Entre o teclado e o primeiro cilindro existe um painel de ligação, que permite a troca de seis pares de letras das vinte e seis do alfabeto. O que eleva bastante o número de chaves que se pode utilizar. Por cada letra cifrada, o primeiro cilindro roda um sexto sempre no sentido directo, quando dá uma volta completa, o segundo cilindro roda também um sexto, após seis voltas do primeiro cilindro, o segundo dá uma volta completa e o terceiro roda um sexto. Ou seja, por cada seis letras cifradas, o segundo cilindro move-se e por cada 36 letras move-se o terceiro, o que permite o uso de 17576 alfabetos de cifra diferentes. (FIARRESGA, , p.22)

No entanto, o número de alfabetos de cifras não corresponde ao total de chaves possíveis na máquina Enigma. Esse cálculo se dá da seguinte forma:

- Os 3 cilindros permutam entre si, logo: $3! = 6$;
- Cada cilindro pode ser regulado de vinte e seis maneiras diferentes, logo: $26^3 = 17.576$;
- No painel de ligação seis pares de letras podem ser trocados a partir das vinte e seis do alfabeto, e esse cálculo é dado, simplificadamente, por:

$$\frac{(26 \times 25) \times (24 \times 23) \times (22 \times 21) \times (20 \times 19) \times (18 \times 17) \times (16 \times 15)}{2^6 \times 6!} = 100.391.791.500;$$

- O número total de chaves é dado considerando esses totais de maneiras diferentes de cada componente da máquina, sendo:

$$6 \times 17576 \times 100391791500 = 1.058.691.676.442.400$$

A escolha de colocação dos cilindros, seu posicionamento e o conhecimento da troca dos seis pares de letras determinam a chave que deve ser usada. Para salientar o poder de cifrar uma mensagem na Enigma, basta dizer que ela possui mais de 10.000.000.000.000.000 chaves possíveis, e: “(...) um criptoanalista persistente, capaz de testar um ajuste a cada minuto, precisaria de mais tempo do que a idade total do universo para checar cada ajuste.” (SINGH, 2020, p.155).

A Enigma sofreu diversas alterações durante os anos, e em 1925 Scherbius começou a produzir as máquinas em massa para que fossem usadas pelos militares, pelo governo e pelas empresas estatais. Nas duas décadas seguintes, os militares alemães compraram por volta de 30 mil máquinas Enigas.

Quando a Segunda Guerra Mundial se iniciou, a Enigma proporcionou aos alemães o sistema de criptografia mais seguro do mundo, e eles pensaram que ela garantiria que o fiasco de segurança nas comunicações presenciado na Primeira Guerra não se repetisse.

Figura 3 – Modelo da Máquina Enigma



Fonte: Dorotheum GmbH & Co KG (2020).²

Para decifrar as mensagens alemãs cifradas pela Enigma foram necessários anos de dedicação, que se iniciaram bem antes do início da Segunda Guerra. Esse trabalho se iniciou na Polônia e além da dedicação dos criptoanalistas poloneses, contou com a traição de um alemão buscando vingança de sua pátria e de seu irmão, espões, e da contribuição da França fornecendo acesso aos documentos alemães.

Um dos principais criptoanalistas envolvidos nessa operação foi o polonês Marian Rejewski, e seus esforços levaram ao surgimento das “bombas”, máquinas que auxiliavam na decifração das mensagens da Enigma. No entanto, em 1939, alterações na Enigma tornaram os avanços poloneses insuficientes para a continuidade do trabalho. Com esperanças que os aliados pudessem dar continuidade nessa operação, a Polônia revelou aos franceses e britânicos os seus avanços durante a última década, deixando-os chocados e admirados. O progresso polonês evidenciou que a Enigma não era uma cifra perfeita, como eles pensavam, e deu novas esperanças aos aliados.

Em Londres foi criada uma operação para a quebra de códigos da Enigma, localizada em Bletchley Park, que iniciou empregando uma equipe de 200 pessoas, mas em cinco anos alojou mais de 7 mil homens e mulheres. Os operadores alemães mudavam a chave da Enigma diariamente, e diariamente os britânicos se lançavam na missão de descobrir essa chave e decifrar as mensagens alemãs, garantindo que os aliados tivessem uma boa visualização dos planos do inimigo e pudessem planejar estratégias bem sucedidas.

Muitos atalhos foram utilizados na decifração diária da Enigma explorando suas fraquezas, mas foi Alan Turing que obteve o feito de identificar uma fraqueza capaz de possibilitar avanços extraordinários. Turing era um matemático já renomado e foi convidado a trabalhar na operação militar, contribuindo no árduo trabalho dos quebradores de cifras britânicos.

Assim como Rejewski, Turing abordou o problema através da mecanização do processo de decifração, e por semelhanças com a máquina polonesa, a máquina britânica também foi nomeada como

² Disponível em: <<https://www.dorotheum.com/en/l/6711042/>>

“bomba”. As bombas de Turing enfraqueceram a Enigma e garantiram maior rapidez e efetividade nas atividades de decifração britânicas. Em “O Livro dos Códigos”, Singh afirma: “Tem sido defendido, embora com controvérsias, que as conquistas de Bletchley Park foram um fator decisivo para a vitória aliada. O que é certo é que os quebradores de códigos de Bletchley Park encurtaram a guerra de modo significativo.” (SINGH, 2020, p.209).

Apesar da importância das bombas de Turing para a história do mundo e no desenvolvimento da criptografia, foi o Colossus, outro aparelho decifrador desenvolvido em Bletchley Park, que determinou o desenvolvimento da criptografia na segunda metade do século XX. Este aparelho foi criado para combater a cifra Lorenz, utilizada por Hitler para se comunicar com seus generais, e que possuía semelhanças com a Enigma, mas era ainda mais forte.

O Colossus era uma máquina capaz de se adaptar a problemas diversos, um requisito para decifrar a Lorenz, e sua realização proporcionou o precursor do moderno computador digital. Contudo, sendo parte da estratégia de guerra, o Colossus, as bombas de Turing e suas respectivas plantas foram destruídos depois do fim do conflito, além de que seus desenvolvedores foram proibidos de falar sobre o assunto, deixando que outros cientistas levassem o crédito pela invenção do computador no futuro.

No entanto, essas experiências evidenciaram aos criptoanalistas a vantagem de se empregar a tecnologia dos computadores para a quebra das mais variadas cifras, obtendo como benefício a velocidade e a flexibilidade oferecida. A partir disso, o computador se tornou um personagem central na batalha entre codificadores e decodificadores.

Com a popularização dos computadores e seu uso comercial, a criptografia novamente surgiu como uma necessidade pública. Isso incentivou a criação de códigos padronizados para a troca de mensagens entre empresas e bancos, por exemplo, controlados por agências nacionais e internacionais. Buscando superar as eventuais dificuldades apresentadas, as cifras foram se aperfeiçoando cada vez mais.

Uma dificuldade que sempre esteve presente na cifragem de mensagens era a distribuição das chaves e as complicações de logística e segurança que esse fator oferecia. Para vencer esse empecilho, foram criados conceitos como a criptografia de chave pública (ou troca de chaves Diffie-Hellman-Merkle) e a criptografia RSA, considerados dois dos maiores avanços da criptografia na história.

Até aqui falamos apenas da necessidade de trocar informações confidenciais e as alternativas que foram desenvolvidas para alcançar esse objetivo, conjuntamente com as tentativas de interceptação e compreensão de tais mensagens. No entanto, como mencionado inicialmente, os códigos não estão restringidos a este único uso.

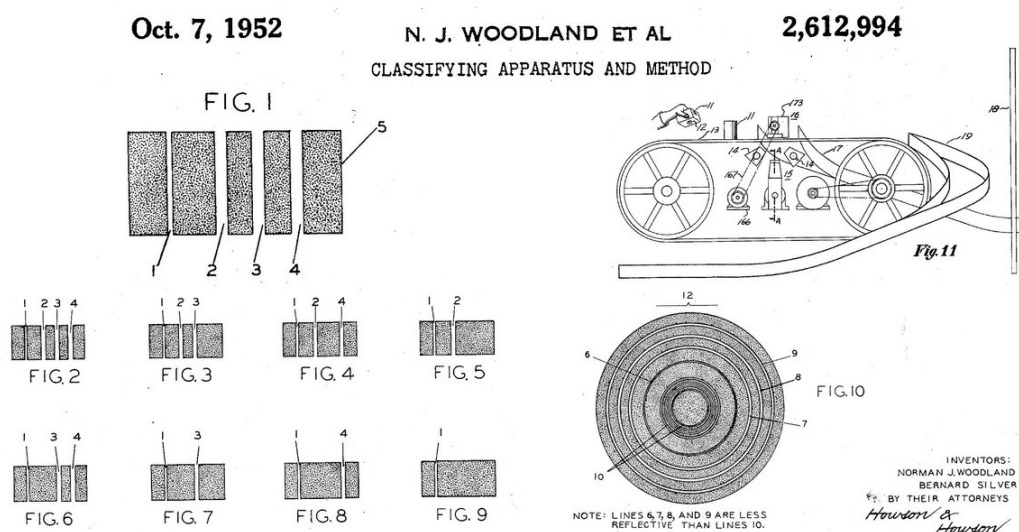
3.2 O CÓDIGO DE BARRAS

Com os avanços tecnológicos ocasionando no crescimento da automação e na expansão comercial, consequentemente um novo problema surgiu: como ler milhões de dados rapidamente e com custos reduzidos? De acordo com GS1 Brasil (2019), inicialmente, esse problema era resolvido manualmente: os produtos eram identificados de acordo com normas de cada empresa e registrados pelos funcionários para manter o controle do estoque, por exemplo. Conforme o volume de serviços e mercadorias aumentava, esse se mostrou um trabalho difícil de manter atualizado. Era necessário encontrar uma forma de identificar os produtos em larga escala, com rapidez e de forma padronizada.

De acordo com Drexel (2012), em 1948, o dono de uma rede de supermercados local foi até o Instituto de Tecnologia da Universidade de Drexel, em Filadélfia, Pensilvânia, Estados Unidos, solicitar uma pesquisa sobre um método automático de ler as informações de produtos durante a venda. Bernard Silver, um estudante de engenharia elétrica, tomou conhecimento dessa conversa e relatou o problema para um colega, Norman Joseph Woodland, estudante de engenharia mecânica na universidade.

O problema fascinou Woodland, que passou a se dedicar integralmente à pesquisa para uma solução. Depois de algumas tentativas frustradas, a dupla de colegas chegou num protótipo promissor em 1949, classificado como um “classificador de artigos através da identificação de padrões”. Em 1952 eles obtiveram a patente pela invenção de um “Aparato e Método de Classificação”.

Figura 4 – Patente do precursor do código de barras



Fonte: Página oficial do United States Patent and Trademark Office (USPTO) no Twitter (2021).³

O código criado pela dupla de engenheiros consistia em um padrão de circunferências concêntricas com espessuras variáveis, como visto em Figura 4. No entanto, essa versão inicial não teve sucesso comercial, pois apesar de ter sido utilizada em alguns casos, ainda não havia a tecnologia que tornasse a implementação do método viável. Somente em 1970 a empresa IBM desenvolveu a versão popular do código de barras, com listras verticais pretas e brancas e funcionando com leitura óptica, tendo Woodland como funcionário e colaborador no projeto e o engenheiro George J. Laurer como autor.

Essa nova versão foi patenteada e ficou conhecida como UPC, e consistia em uma sequência de 12 dígitos, traduzidos para barras seguindo um padrão estabelecido. Foi formalmente aceito em 1973 e adotado nos Estados Unidos e Canadá. Posteriormente, novas versões sucederam ao UPC, apenas com pequenas alterações para ampliar o alcance do sistema.

Como afirma Fini (2009), a vantagem de utilizar números nos sistemas de identificação reside na maior eficiência em armazenar e transmitir dados do que os nomes, além de superar as barreiras dos idiomas. Baseado no UPC, Laurer criou um novo código com 13 dígitos, o EAN-13, atualmente adotado por alguns países, com nomenclaturas diferentes.

Com os avanços tecnológicos possibilitando maior acessibilidade aos aparatos necessários – escâneres e computadores, por exemplo –, os códigos de barras passaram a ser amplamente utilizados

³ Disponível em: <<https://twitter.com/uspto/status/910955917734236161?s=20>>

nas mais diversas empresas. Seu uso proporciona diversas vantagens, tais como a rastreabilidade dos produtos, o controle e melhor gestão de estoques, a otimização no fluxo de informações, agilidade na identificação de itens, redução dos custos e o combate às fraudes (GS1 BRASIL, 2017). Hoje em dia, os códigos de barras estão presentes na maioria dos estabelecimentos comerciais e existem órgãos reguladores para os seus usos em cada país ou região.

3.2.1 Funcionamento

O código de barras tem duas formas de representação: a gráfica e a numérica. A representação gráfica se dá pelas barras verticais paralelas e com larguras variadas, enquanto a representação numérica se dá por dígitos do sistema de numeração decimal. Cada código de barras associa uma única representação gráfica a uma única representação numérica, caracterizando um único item.

É importante destacar que este trabalho abrange, até aqui, apenas os códigos de barras mais conhecidos, presentes nos artigos que consumimos regularmente e que são vendidos em supermercados, por exemplo. No entanto, os códigos de barras possuem aplicações diversas e podem ser utilizados para simbolizar não somente dados numéricos como também podem armazenar dados como letras e símbolos ortográficos, desde que seguindo normas estabelecidas. Apesar de existirem várias versões do código de barras verticais, vamos focar em duas delas: o UPC e o EAN-13.

3.2.1.1 O Código UPC

O código UPC, ou Código Universal de Produtos, foi o pioneiro no uso comercial e permanece até hoje sendo utilizado nos Estados Unidos e Canadá. Sua representação numérica é composta por 12 dígitos, enquanto sua representação gráfica se dá por listras brancas e pretas alternadas, de espessuras variadas, que podem ser classificadas como finas, médias, grossas ou muito grossas (MILIES, 2008).

Todos as representações numéricas do sistema UPC têm os 12 algarismos dispostos na forma $x\text{-}xxxx\text{-}xxxx\text{-}x$, como é possível ver na Figura 5, que mostra o código de barras da embalagem de um *pack* com 12 unidades de Coca-Cola.

Figura 5 – Código de barras no sistema UPC



Fonte: Barcode Lookup (2021).

Além disso, cada algarismo tem um significado específico para a descrição dos itens, onde:

O primeiro algarismo do sistema UPC indica um “sistema numérico” que, de certa forma, especifica o tipo de produto classificado. Por exemplo, os começados por 0 são códigos atribuídos aos produtos de consumo usuais; o 1 está reservado para uso futuro, já os começados por 2 correspondem a artigos a serem pesados na loja e os começados por 3 são remédios e outros produtos relacionados com a saúde. Os seguintes cinco algarismos do sistema são utilizados para identificar o fabricante e os outros cinco para identificar o produto em si. (MILIES, 2008, p.47).

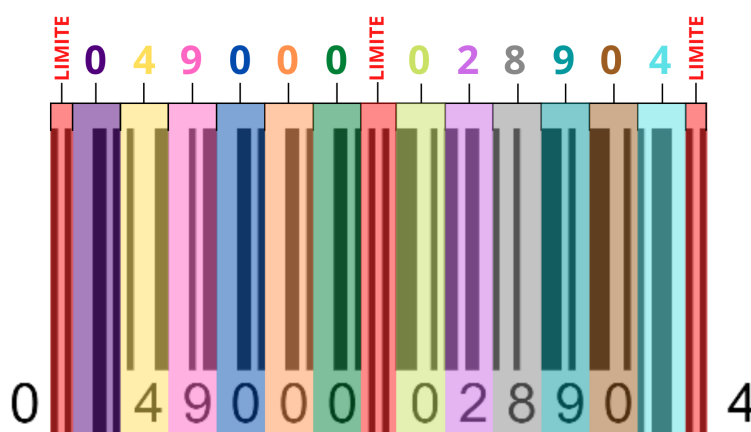
No código de barras, cada algarismo da sua representação numérica de 0 a 9 refere-se a um espaço de tamanho fixo correspondente a 7 barras finas. Duas barras finas da mesma cor geram uma barra média, três barras finas da mesma cor geram uma barra grossa e quatro barras finas da mesma cor geram uma barra super grossa.

Todas as listras são associadas a uma sequência de dígitos ‘0’ ou ‘1’, de acordo com sua cor e a espessura, seguindo um padrão estabelecido, onde o símbolo 0 indica uma listra branca fina, o símbolo 00 uma listra branca média, 000 uma listra branca grossa e 0000 uma listra branca muito grossa. Analogamente, 1, 11, 111 e 1111 representarão uma listra preta fina, média, grossa ou muito grossa, respectivamente (MILIES, 2008). O último algarismo é chamado de dígito de controle e serve para a detecção de erros, que será abordada na Seção 3.2.3.

As extremidades e o meio do código possuem listras mais compridas que servem para determinar os seus limites e consistem em três listras (preta fina, branca fina e preta fina) que indicam seu início e fim e cinco listras centrais (branca fina, preta fina, branca fina, preta fina e branca fina) que indicam sua separação entre direita e esquerda. Essas listras limitadoras não estão associadas aos algarismos da representação numérica do código.

A Figura 6 exibe uma exemplificação de como é feita essa divisão da representação gráfica de um código de barras no sistema UPC. Na figura, cada dígito da representação numérica corresponde a uma cor, e essas cores indicam na representação gráfica qual a "área" associada a cada um desses dígitos. As áreas sombreadas com vermelho indicam as listras limitadoras

Figura 6 – Divisões do código de barras no sistema UPC



Fonte: Produção da própria autora (2021).

A Figura 7 mostra como é feita a divisão de espaço no código UPC para as listras. São 95 posições, cada uma correspondendo a um dígito ‘1’ ou ‘0’, que é traduzido para uma barra fina preta ou branca. Nesta imagem, por exemplo, tem-se a ordem de listras: preta fina, branca fina, preta fina, branca grossa, preta média, branca fina, ..., e assim por diante.

Figura 7 – Espessuras do código de barras no sistema UPC



Fonte: Produção da própria autora (2021).

Cada configuração de dígitos 0's e 1's corresponde a um único número, mas cada número é representado por duas configurações de dígitos, uma para o lado esquerdo do código e o outro para o lado direito, como representado na Tabela 1.

Tabela 1 – Codificação no UPC

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

Fonte: Milies (2008).

Note que a codificação de um dado número, à direita, se obtém da sua codificação à esquerda, trocando cada 0 por 1 e reciprocamente. Agora, o mecanismo de reconhecimento fica claro se notarmos que cada sequência do lado esquerdo tem um número ímpar de dígitos iguais a 1 e, conseqüentemente, cada uma das que estão à direita tem um número par. Assim, verificando a paridade de cada sequência de sete dígitos, a máquina “sabe” imediatamente de que lado está lendo o código. (MILIES, 2008, p.48).

Ou seja, dessa forma, o leitor é capaz de identificar a orientação do código de barras, pois consegue distinguir se os dígitos fazem parte do lado direito ou esquerdo. É por isso que ao passar um produto em um escâner é possível fazer sua leitura mesmo que esteja “de cabeça para baixo”.

Para compreender esse funcionamento, seja o código de barras da Figura 8. As primeiras quatro listras da figura (excluindo as três listras que servem de limite), da esquerda para a direita, são uma listra branca grossa (000), uma preta média (11), uma branca fina (0) e uma preta fina (1), que ao juntar resulta na sequência 0001101. Como essas barras estão no lado esquerdo do código, conferindo a Tabela 1, essa sequência representa o número 0. De fato, o primeiro número do código de barras em questão é o número 0.

Agora sejam as primeiras listras do lado direito desse código, depois das listras limitadoras centrais: uma preta grossa (111), uma branca média (00), uma preta fina (1) e uma branca fina (0), que ao juntar resulta na sequência 1110010. Como essas barras estão no lado direito do código, conferindo o 1, essa sequência representa o número 0 e, de fato, o primeiro número do lado direito do código de barras em questão é o número 0. Observa-se que nas duas situações o número codificado é 0, mas assumindo representações diferentes em razão de suas posições no código de barras — primeiro, no lado esquerdo, depois, no direito.

Figura 8 – Código de barras no sistema UPC



Fonte: Produção da própria autora (2021).

3.2.1.2 O código EAN-13

O código EAN-13, posterior ao UPC, tem um funcionamento muito parecido com seu predecessor. Com os objetivos de identificar o país de origem do produto e permitir que a mesma máquina leitora pudesse ler indistintamente os códigos UPC e EAN-13, apenas um novo dígito foi adicionado a cada código. É claro que esse único dígito não permite que todos os países sejam identificados, pois existem muito mais que apenas dez países no mundo. Na realidade, o país de registro do fabricante é representado pelos dois ou três primeiros dígitos do código. Os quatro ou cinco dígitos seguintes

(dependendo de quantos já foram empregados para identificar o país) indicam o produtor enquanto os cinco restantes indicam o próprio artigo produzido. O último dígito, por sua vez, é um dígito de controle, assim como no sistema UPC.

Os códigos EAN deveriam ser lidos pelas mesmas máquinas que liam os códigos UPC, dessa forma, eles deveriam manter as mesmas dimensões e, conseqüentemente, a mesma quantidade de algarismos a serem codificados. A solução para esse problema é muito engenhosa e envolve uma padronização simples. Os treze algarismos desse sistema são sempre dispostos da forma $x\text{-}xxxxxx\text{-}xxxxxx$, e o segredo para cumprir com os requerimentos está no fato de que o primeiro algarismo não possui representação gráfica, mas define implicitamente como os próximos algarismos serão representados graficamente:

Isso foi conseguido utilizando-se diversos padrões de paridade, na codificação do lado esquerdo, que variam, dependendo do dígito inicial. Por outro lado, não foi modificada a codificação do lado direito, em que todos os dígitos continuam codificados empregando-se um número par de posições iguais a 1 (permitindo assim que as leitoras continuassem a identificar o lado correspondente). (MILIES, 2008, p.50)

No código UPC, os algarismos à esquerda eram codificados com um número ímpar de dígitos iguais a 1. No EAN, se o primeiro dígito é 0, então ele representa os países que já haviam adotado o UPC – Canadá e EUA –, e para manter o mesmo padrão do sistema antecessor, todos os dígitos do lado esquerdo são codificados utilizando-se sempre um número ímpar de posições iguais a 1, tal como antes. Dessa forma, a representação gráfica de um produto registrado nesses países é a mesma nos dois sistemas de códigos de barras abordados aqui, apenas com a adição de um algarismo 0 no início do código EAN-13.

Para cada dígito inicial há um padrão de paridade específico, onde cada algarismo do lado esquerdo pode ser codificado com um número ímpar ou par de posições iguais a 1, de acordo com a Tabela 2:

Tabela 2 – Critério de paridade no EAN-13

Dígito inicial	1º	2º	3º	4º	5º	6º
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

Fonte: Milies (2008).

Isso quer dizer que se o dígito inicial do código for 7, o critério a ser seguido é ímpar - par - ímpar - par - ímpar - par, então o primeiro algarismo a ser codificado (o segundo algarismo na representação numérica, mas o primeiro na representação gráfica) tem que ser codificado com uma quantidade ímpar de posições iguais a 1, enquanto o segundo deve ser codificado com uma quantidade par de posições

igual a 1, e assim por diante. Essa quantidade de posições igual a 1 e as posições em si não são aleatórias, mas seguem uma simbologia estabelecida, como mostra a Tabela 3:

Tabela 3 – Codificação no EAN-13

Dígito	lado esquerdo ímpar	lado esquerdo par	lado direito
0	0001101	0100111	1110010
1	0011001	0110011	1100110
2	0010011	0011011	1101100
3	0111101	0111101	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

Fonte: Milies (2008).

Por exemplo, seja o código de barras da Figura 9, referente a um pacote de sulfite A4 da marca Chamequinho:

Figura 9 – Código de barras no sistema EAN-13



Fonte: Online Barcode Generator (2021).

Esse é um código de barras registrado no Brasil, pois tem 789 como algarismos iniciais. Sua representação gráfica é obtida através de sua codificação, que obedece às regras apresentadas acima. Como seu algarismo inicial é 7, então deve seguir o critério ímpar - par - ímpar - par - ímpar - par, visto na Tabela 2. Os algarismos da esquerda são 891173, e serão codificados seguindo o critério de paridade e a simbologia da Tabela 3, assim:

Tabela 4 – Exemplo de Critério de Paridade no EAN-13

Dígito	paridade	simbologia
8	ímpar	0110111
9	par	0010111
1	ímpar	0011001
1	par	0110011
7	ímpar	0111011
3	par	0100001

Fonte: Produção da própria autora (2021).

Isso quer dizer que as barras verticais desse código serão, para o algarismo 8: listra branca fina (0), preta média (11), branca fina (0) e preta grossa (111), como é possível visualizar na Figura 10, e analogamente para cada um dos seguintes algarismos.

Figura 10 – Padrão de um algarismo no EAN-13



Fonte: Produção da própria autora (2021).

Os algarismos do lado direito são codificados da mesma forma que no sistema do UPC. Dessa maneira, a máquina leitora ainda é capaz de identificar qual lado do código ela está lendo, a partir da paridade observada na representação dos algarismos: o lado direito continua mantendo uma quantidade par de posições 1 para todos os algarismos, enquanto o lado esquerdo varia conforme mostrado.

Além disso, a máquina é capaz de identificar qual é o dígito inicial de cada código através da identificação do padrão de paridade do lado esquerdo. Por exemplo, se ela identifica que em um determinado código o critério seguido é ímpar - ímpar - par - par - ímpar - par, então ela sabe que o dígito inicial é o 2, pois ele é representado por esse padrão de paridade.

3.2.2 O dígito verificador

Ao falar sobre o UPC e o EAN-13, foi mencionado que em ambos os sistemas, o último dígito tem a função de dígito verificador, mas não foi definido o que isso significa. Imagine que um funcionário de supermercado precise digitar manualmente os algarismos do código de barras, ou seja, digitar a sequência numérica única que representa um determinado produto. Qualquer erro nesse registro pode causar um problema, pois pode ser que um produto diferente seja identificado ou que não se tenha registro de nenhum produto com tal representação. Como o sistema pode identificar esse erro e impedir o registro equivocado desse código?

É justamente por esse problema que um dígito verificador foi estabelecido para esses sistemas. Para compreender como funciona o processo de determinação desses dígitos, o algoritmo cuja função é atribuir um dígito verificador será apresentado para cada um dos sistemas já mencionados.

O código UPC possui 12 algarismos, e sejam eles $(a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10} a_{11} x)$. Cada um dos 11 primeiros algarismos tem um significado específico, como abordado nas seções anteriores, enquanto o último algarismo, aqui denotado por x , é o dígito verificador. A fim de facilitar a compreensão do algoritmo, a sequência será escrita como um vetor:

$$\alpha = (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, x).$$

O sistema UPC usa em seu algoritmo para detecção de erros um vetor fixo, que será denominado

por vetor de pesos e é dado por:

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

O algoritmo pode ser descrito como segue:

1. Converter a representação numérica $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}x$ do código de barras para o vetor $\alpha = (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11})$ — o dígito verificador x não é considerado no vetor;
2. Calcular o produto escalar P entre os vetores α e ρ ;
3. Calcular o resto R da operação $P \div 10$;
4. Calcular x tal que $R + x = 10$, em que x é o dígito verificador.

No passo 3 o resto da operação indicada corresponde ao algarismo das unidades de P .

Por exemplo, seja o código da Figura 11, cujo último dígito foi ocultado. Para descobrir qual é esse dígito desconhecido, basta aplicar o algoritmo descrito.

Figura 11 – Dígito verificador do UPC



Fonte: Produção da própria autora (2021).

1. Converter a representação numérica $88491226839x$ do código de barras para o vetor $\alpha = (8, 8, 4, 9, 1, 2, 2, 6, 8, 3, 9)$;
2. Calcular o produto escalar P entre os vetores α e ρ :

$$\begin{aligned} P &= \alpha \cdot \rho = (8, 8, 4, 9, 1, 2, 2, 6, 8, 3, 9) \cdot (3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3) \\ &= 3 \cdot 8 + 1 \cdot 8 + 3 \cdot 4 + 1 \cdot 9 + 3 \cdot 1 + 1 \cdot 2 + 3 \cdot 2 + 1 \cdot 6 + 3 \cdot 8 + 1 \cdot 3 + 3 \cdot 9 \\ &= 24 + 8 + 12 + 9 + 3 + 2 + 6 + 6 + 24 + 3 + 27 \\ &= 124; \end{aligned}$$

3. Calcular o resto R da divisão $124 \div 10$:

$$124 \div 10 = 10 \cdot q + R$$

$$124 \div 10 = 10 \cdot 12 + 4.$$

Isso quer dizer que, ao dividir 124 por 10 o resto obtido é 4;

4. Calcular x tal que $R + x = 10$, em que x é o dígito verificador.

$$4 + x = 10$$

$$x = 10 - 4$$

$$x = 6.$$

De fato, o dígito verificador desse código de barras é o algarismo 6, aqui representado por uma listra preta fina, uma branca fina, uma preta fina e uma branca super grossa (Figura 12).

Figura 12 – Dígito verificador



Fonte: Produção da própria autora (2021).

Existem diversas formas de escrever esse algoritmo, como usando a aritmética modular de restos, por exemplo. Dessa maneira, o terceiro e último passo do algoritmo seria:

3. Calcular $124 \equiv x \pmod{10}$, em que x é o dígito verificador.

Isso quer dizer que o dígito verificador é aquele que torna o produto escalar entre os 11 primeiros algarismos do código de barras e o vetor de pesos ρ um múltiplo de 10. Em outras palavras, o dígito verificador é o número que somado ao produto escalar em questão, resulta em um múltiplo de 10.

Para o código EAN-13 o processo é similar, com a alteração do vetor de pesos, que passa a ser $\rho = (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3)$, já que nesse sistema os códigos são compostos por 13 algarismos. O restante do algoritmo é realizado da mesma forma, multiplicando os vetores e encontrando o número que torna o resultado da operação um múltiplo de 10.

3.2.3 A detecção de erros

O método de identificação de erros nos sistemas UPC e EAN-13 é muito útil. Se por alguma razão a máquina leitora não consegue escanear o código de barras de um produto, então ele deve ser registrado manualmente, abrindo margem para erros de digitação. Se um dígito é registrado erroneamente, então o sistema identifica o erro ao aplicar o algoritmo pertinente e receber a informação que o resultado obtido não é um múltiplo de 10 — basta conferir se o algarismo da unidade é o 0.

Vários erros podem ser cometidos nesse processo de digitar um código de barras, como o erro de um único dígito ou a transposição, por exemplo. Segundo Polcino Milies (2009), autores como D.F. Beckley e J. Verhoeff investigaram a ocorrência desses tipos de erros cometidos por operadores humanos, registrando que os tipos de erros mais frequentes são o erro único — o operador comete

um erro de digitação, trocando um algarismo do código por um número qualquer —, com 79% das ocorrências, e o erro de transposição — o operador digita todos os algarismos do código corretamente, mas inverte a ordem de dois algarismos vizinhos —, com 10,2% das ocorrências.

O algoritmo definido para a detecção de erros consegue identificar todos os erros únicos, pois define uma situação em que qualquer alteração modifica o resultado final da operação. Seja o algoritmo do sistema UPC, onde

$$\alpha \cdot \rho = 3a_1 + 1a_2 + 3a_3 + 1a_4 + 3a_5 + 1a_6 + 3a_7 + 1a_8 + 3a_9 + 1a_{10} + 3a_{11} + 1a_{12} = 10k,$$

com k inteiro não-negativo, e a_{12} o dígito verificador. Suponha que um a_i qualquer, com $1 \leq i \leq 12$, tenha sido digitado errado, passando a ser um d qualquer, com $0 \leq d \leq 9$. Cometer esse erro é o mesmo que no lugar de a_i digitar $a_i + c$, onde $1 \leq |c| \leq 9$, tal que o produto escalar passe a ser igual a:

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

caso i seja par. Ou, ainda, igual a:

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

caso i seja ímpar.

Ambas situações são possíveis, dependendo da paridade da posição em que o erro ocorreu. O importante é que nos dois casos o produto escalar não será um múltiplo de 10, pois o segundo membro da igualdade será igual a $10k + c$ ou a $10k + 3c$, e c e $3c$ não são múltiplos de 10. O fato de que 3 e 10 são primos entre si, ou seja, $\text{mdc}(3, 10) = 1$ é importante para essa afirmação. De fato, se no vetor de pesos o 3 fosse substituído por qualquer outro número inteiro positivo e primo com 10, o mesmo resultado seria obtido e, neste caso, o número 3 foi escolhido por ser o menor número com essas propriedades. O mesmo é válido para o sistema EAN-13.

Quanto aos erros de transposição, nem sempre eles podem ser identificados. Por exemplo, seja um código no sistema EAN-13, onde $\alpha = (a_1, \dots, a_i, a_{i+1}, \dots, a_{13})$ e $\rho = (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$, obtendo

$$\alpha \cdot \rho = (1a_1 + \dots + 1a_i + 3a_{i+1} + \dots + 1a_{13}) = 10k,$$

com k inteiro não-negativo. Supondo que houve um erro de transposição entre algarismos adjacentes a_i e a_{i+1} no momento que o código numérico foi digitado e que i seja ímpar, então o vetor da sequência numérica passa a ser, sem perda de generalidade, $\beta = (a_1, \dots, a_{i+1}, a_i, \dots, a_{13})$ e

$$\beta \cdot \rho = (1a_1 + \dots + 1a_{i+1} + 3a_i + \dots + 1a_{13}).$$

Admitindo que esse erro não tenha sido identificado pelo sistema, então $\beta \cdot \rho$ também é um múltiplo de 10, assim, é possível escrever $\beta \cdot \rho = (1a_1 + \dots + 1a_{i+1} + 3a_i + \dots + 1a_{13}) = 10m$, com m inteiro não-negativo. Subtraindo $\beta \cdot \rho$ de $\alpha \cdot \rho$ tem-se:

$$2a_i - 2a_{i+1} = 10k - 10m \iff 2(a_i - a_{i+1}) = 10(k - m) \iff a_i - a_{i+1} = 5q,$$

com $q = k - m$, onde k , m e q são inteiros. Ou seja, o erro de transposição de adjacentes não é identificado se, e somente se, $|a_i - a_{i+1}| = 5$. Aqui se evidencia a importância do vetor de pesos ter pesos intercalados, pois um vetor de pesos todos iguais a 1 seria capaz de identificar erros únicos, mas não seria eficiente na identificação de erros de transposição.

Por exemplo, seja o código numérico 7894721832865 correspondente a um código de barras no sistema EAN-13. Ao digitar esse código, o operador comete um erro de digitação, trocando um o algarismo 1 por 2 e registrando a sequência 7894722832865. Ao aplicar o algoritmo — considerando o dígito verificador —, com $\alpha = (7, 8, 9, 4, 7, 2, 2, 8, 3, 2, 8, 6, 5)$, obtém-se:

$$\alpha \cdot \rho = (1 \times 7 + 3 \times 8 + 1 \times 9 + 3 \times 4 + 1 \times 7 + 3 \times 2 + 1 \times 2 + 3 \times 8 + 1 \times 3 + 3 \times 2 + 1 \times 8 + 3 \times 6 + 1 \times 5) = 131.$$

Logo, o sistema identifica que há um erro, pois 131 não é múltiplo de 10. Qualquer erro dessa natureza – erro único – seria identificado pelo sistema do computador e emitiria um sinal ao operador, indicando que há algo errado. Agora, supondo que o operador digite novamente o código, mas dessa vez cometa um erro de transposição de adjacentes, e usando o mesmo código como exemplo, digite 7894271832865, trocando a ordem do 5º e 6º algarismos. Ao aplicar o algoritmo, com $\alpha = (7, 8, 9, 4, 2, 7, 2, 8, 3, 2, 8, 6, 5)$, obtém-se:

$$\alpha \cdot \rho = (1 \times 7 + 3 \times 8 + 1 \times 9 + 3 \times 4 + 1 \times 2 + 3 \times 7 + 1 \times 1 + 3 \times 8 + 1 \times 3 + 3 \times 2 + 1 \times 8 + 3 \times 6 + 1 \times 5) = 140.$$

Ou seja, houve um erro de digitação, mas ainda assim o resultado da operação do algoritmo é um múltiplo de 10, o que impede que o computador reconheça a falha. Isso ocorre porque os algarismos transpostos foram 2 e 7, e $|2 - 7| = 5$. Se por acaso os algarismos adjacentes transpostos fossem 3 e 2, então o computador reconheceria o erro, uma vez que $|3 - 2| \neq 5$.

Além disso, se o operador cometer mais de um erro em uma mesma digitação, é possível que o resultado do algoritmo seja um múltiplo de 10 porque os erros podem “se compensar”.

Há ainda outras formas de detecção de erros aplicadas em outros tipos de códigos. Por exemplo, o código International Standard Book Number (ISBN), não foi apresentado anteriormente, mas é um código de barras internacional para identificar livros e softwares e que os classifica por título, autor, país, editora e edição. Atualmente são emitidos com 13 algarismos, mas até 2007 eram compostos por apenas 10, e são identificados por ISBN-10 e ISBN-13.

O ISBN-13 possui um algoritmo de detecção de erros igual ao do EAN-13 mas o ISBN-10 possui algumas diferenças: o processo é o mesmo, mas o vetor de pesos é dado por $(10, 9, 8, 7, 6, 5, 4, 3, 2, 1)$ e o produto escalar deve ser um múltiplo de 11. Se por acaso o dígito verificador corresponder ao número 10, ele será representado pela letra X.

Outros exemplos de códigos numéricos que possuem um dígito verificador são o Cadastro de Pessoas Físicas (CPF), o Cadastro Nacional da Pessoa Jurídica (CNPJ) e o Cadastro Nacional de Habilitação (CNH) (CAMPUS CODE, 2020).

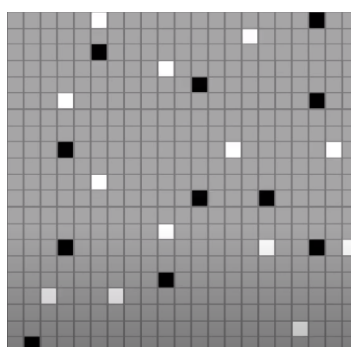
3.3 O CÓDIGO QR

Nesta Seção, o Quick Response Code (QR Code) — ou Código de Resposta Rápida (código QR), em português — será apresentado. Antes de iniciar, porém, é importante salientar que, por conta da complexidade do preenchimento dos códigos QR, o seu funcionamento não será abordado detalhadamente para não sair do propósito do uso em sala de aula.

O código QR é um tipo de código de barras bidimensional. Foi criado em 1994, no Japão, pela Denso-Wave, uma empresa do grupo Toyota, com o engenheiro japonês Masahiro Hara sendo o líder do projeto. Com o propósito inicial de facilitar a classificação de peças de carros, buscava-se um código mais compacto e abrangente do que os códigos de barras. Quando ficou pronto, esse código mostrou uma capacidade de armazenamento muito superior aos códigos de barras convencionais e a possibilidade de ser lido até 10 vezes mais rápido que outros códigos.

Enquanto os códigos de barras originais armazenam informação apenas horizontalmente, os códigos QR podem armazenar informações horizontal e verticalmente. Além disso, eles podem ser lidos a partir de qualquer direção, pois possuem padrões de detecção de posições. Seu formato é característico, sendo um quadrado maior subdividido por quadrados menores, chamados de módulos. A Figura 13 mostra uma subdivisão de um quadrado maior em 21×21 módulos e alguns destes coloridos em preto e branco para exemplificar o preenchimento.

Figura 13 – Módulos de um código QR



Fonte: Captura de tela do vídeo “How QR Codes Are Built?”, do canal *James Explains* no Youtube (2021).⁴

Existem diversos modelos de códigos QR, mas os mais comuns são o Modelo 1 e Modelo 2, exemplificados na Figura 14:

Figura 14 – Modelo 1 e Modelo 2 do código QR



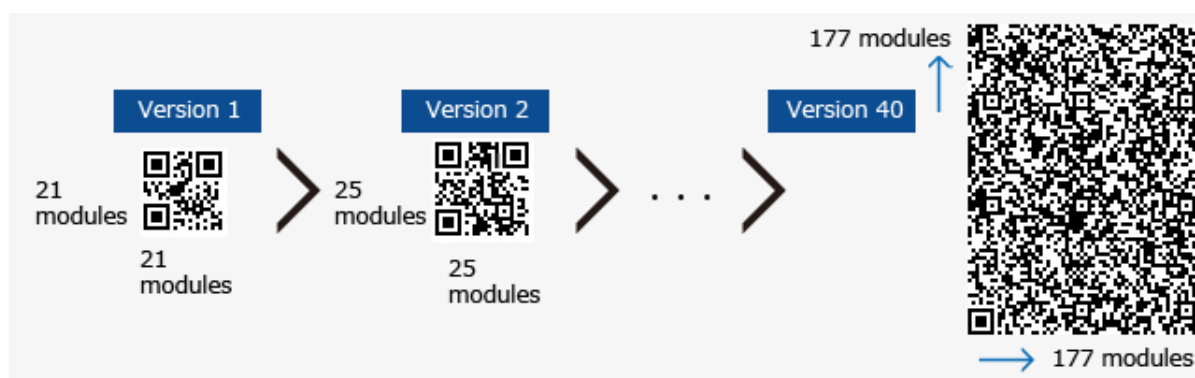
Fonte: Denso Wave (2021).⁵

⁴ Disponível em: <<https://youtu.be/142TGhaTMtI>>

⁵ Disponível em: <<https://www.qrcode.com/en/codes/model12.html>>

O Modelo 1 é o código QR original, com a capacidade de codificar 1.167 numerais e possui 14 versões diferentes, sendo que a versão máxima tem a configuração de 73 x 73 módulos. O Modelo 2 surgiu a partir de uma melhoria do Modelo 1, visando a possibilidade de leitura até mesmo com distorções de ângulo e visibilidade. É capaz de codificar 7.089 numerais e sua versão máxima é a 40 (177 x 177 módulos). As “configurações de módulo” dizem respeito ao número de módulos que cada símbolo (código) contém, variando de acordo com sua versão, como pode ser visto na Figura 15:

Figura 15 – Versões do código QR



Fonte: Denso Wave (2021).⁶

Segundo Law e So (2010), os códigos QR podem armazenar 7089 caracteres numéricos, 4296 caracteres alfanuméricos, 2953 bytes binários e 1817 caracteres Kanji (ideogramas, caracteres da língua japonesa) ou uma mistura destes. Existem outros códigos bidimensionais, tais como o *DataMatrix* e o *Maxi Code*, mas nenhum possui tamanha capacidade de armazenamento de dados.

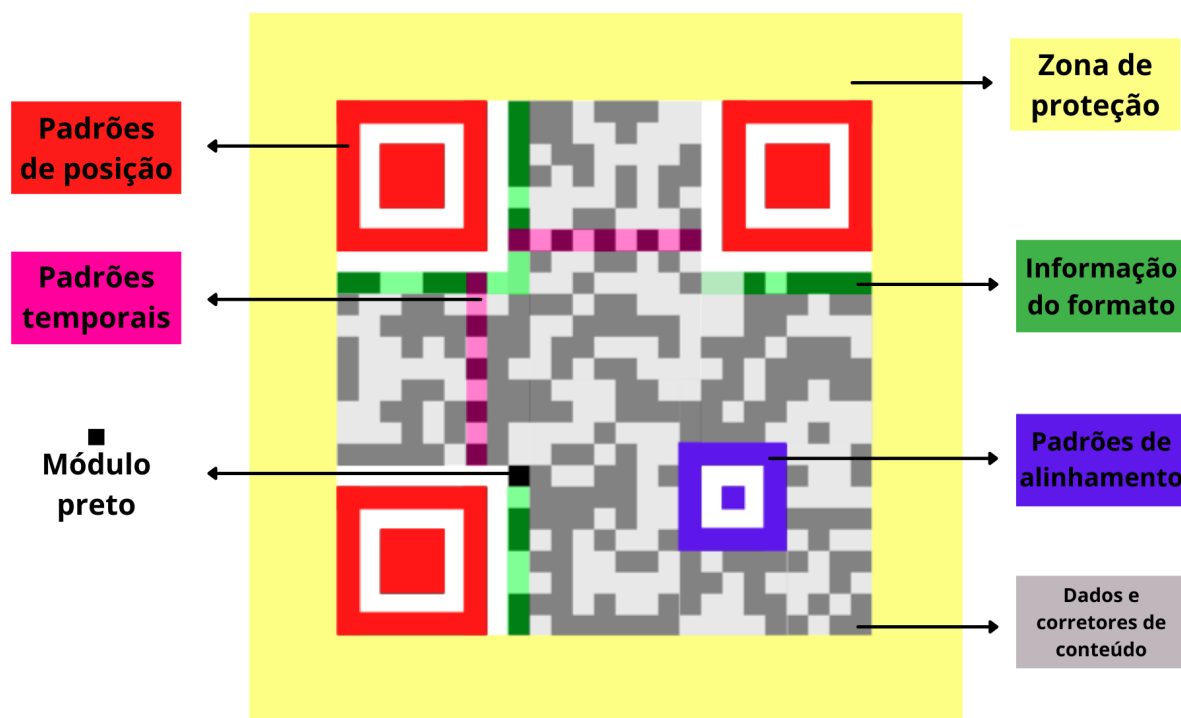
Os códigos QR têm um funcionamento complexo, onde os módulos possuem agrupamentos diversos para representar distintos componentes, conforme a Figura 16.

Cada um desses componentes tem um significado:

1. **Padrões de posição:** Geralmente, os códigos QR têm três quadrados pretos nos cantos inferior esquerdo, superior esquerdo e superior direito — sempre tem tamanho 7x7—, e eles servem para informar ao leitor a orientação do código e seus limites externos;
2. **Zona de proteção:** Margem branca vazia ao redor da célula. Serve para que o leitor de QR determine o que está, de fato, contido no código, sem interferência de elementos externos;
3. **Padrões temporais:** Módulos pretos e brancos intercalados que auxiliam na percepção do posicionamento das linhas e colunas do código e na determinação da dimensão do símbolo;
4. **Informação do formato:** Informa o nível de correção de erros e a máscara de codificação usada no código. Um código QR usa o algoritmo de correção de erros Reed-Solomon com quatro níveis de correção (7, 15, 25 e 30%) e a máscara é usada na codificação para alterar setores que possam confundir o leitor, como muitos módulos da mesma cor reunidos ou setores que pareçam com áreas reservadas;

⁶ Disponível em: <<https://www.qrcode.com/en/about/version.html>>

Figura 16 – Estrutura do código QR



Fonte: Produção da própria autora (2021).

5. **Módulo preto:** Um único módulo preto que sempre ocupa a mesma posição, localizado ao lado do padrão de posição do canto esquerdo inferior;
6. **Dados e corretores de conteúdo:** Onde está codificada a mensagem armazenada e os campos de correção de erro. O modo de codificação da mensagem pode assumir o formato de bytes, numérico, alfanumérico e kanji — cada um possuindo uma padronização de codificação diferente.
7. **Padrões de alinhamento:** Orientador de posição para a leitura. Um código QR pode ter vários padrões de alinhamento, de acordo com a versão, mas todos eles possuem tamanho 5x5;
8. **Informação da versão:** Não consta na versão da Figura 16, pois aparece apenas da versão 7 em diante do código QR — nesse exemplo, a versão utilizada é a 2, com 25x25 módulos. É um campo destinado a informar qual a versão do código, e é colocado em dois lugares, no formato 6x3, como visto na Figura 17.

A capacidade de armazenamento de dados de cada versão do código QR varia de acordo com a quantidade de dados, o tipo de caractere e o nível de correção de erros utilizado, ou seja, conforme a quantidade de dados aumenta, mais módulos são necessários para a codificação e, consequentemente, requer símbolos maiores (DENSO WAVE, 20—).

Todas essas informações contidas se dão pelo posicionamento dos quadradinhos pretos ou brancos, sendo que os dados são traduzidos através de um padrão binário, podendo ser o padrão de bytes, numérico, alfanumérico ou kanji.

O código QR não possui nenhuma licença, ou seja, pode ser usado por qualquer pessoa e para quaisquer fins, ao contrário dos códigos de barras originais que requerem regulação no uso e agências

Figura 17 – Informação da versão do código QR



Fonte: Produção da própria autora (2021).

de controle de registro e distribuição. Este fator contribuiu muito para a sua popularização, como mencionam Law e So (2010). Atualmente, com o aumento do acesso à tecnologia e avanços tecnológicos evidentes, é muito fácil acessar um código QR no cotidiano. Muitos celulares possuem um leitor desses códigos embutido — e, dependendo do sistema operacional, se não tiver, é possível baixar um aplicativo que habilite a função —, então basta que o usuário aponte sua câmera para um deles e tenha acesso à internet para que acesse a informação contida no código.

As informações que podem ser armazenadas no código QR são as mais variadas: ele pode direcionar o usuário para um site da internet que contenha imagens, vídeos, textos, mapas, aplicativos etc. Ou seja, é possível embutir as mais variadas informações em um código QR, atendendo às mais variadas necessidades. Ademais, como mencionado, qualquer pessoa pode gerar um código QR, sendo este um processo simples e realizado gratuitamente por sites e aplicativos.

Dessa forma, os códigos QR possuem uma ampla aplicabilidade. É cada vez mais comum vê-los em embalagens de produtos, anúncios publicitários, informativos, atalhos para transações bancárias e para fins de rastreamento, por exemplo. Os usos são numerosos e diversificados, chegando até mesmo às artes e ao entretenimento. Os códigos QR contribuem para a facilitação ao acesso à informação e estão presentes no cotidiano de muitas pessoas e, por isso, configuram como uma possibilidade de conteúdo a ser desenvolvido na educação nas mais diversas aplicações.

4 RESOLUÇÃO DE PROBLEMAS COMO METODOLOGIA DE ENSINO

No século XXI a sociedade desenvolve-se intrinsecamente conectada à tecnologia e informação, conferindo um ritmo acelerado e mudanças contínuas no cotidiano, provocando impactos diversos em nossas vidas, e essa ainda recente constituição de mundo promove novas reflexões e desafios quanto à compreensão da realidade nos âmbitos mais variados, inclusive na Educação e, em especial, na Educação Matemática, fazendo necessário reconhecer que as “(...) transformações nos contextos nacional e internacional atingem diretamente as populações jovens e, portanto, o que se demanda de sua formação para o enfrentamento dos novos desafios sociais, econômicos e ambientais, acelerados pelas mudanças tecnológicas do mundo contemporâneo.” (BRASIL, 2018, p.462).

Ainda segundo Brasil (2018), em função do desenvolvimento das tecnologias, os meios de produção sofreram mudanças, configurando um novo sistema organizacional de trabalho, e “(...) as incertezas relativas às mudanças no mundo do trabalho e nas relações sociais representam um grande desafio para a formulação de políticas e propostas de organização curriculares para a Educação Básica, em geral, e para o Ensino Médio, em particular.” (BRASIL, 2018, p.462).

A partir dessa perspectiva, torna-se indispensável o estudo de possibilidades de ensino que ofereçam uma educação tecnológica, que sensibilize os alunos para

a compreensão e a utilização dos conceitos e teorias que compõem a base do conhecimento científico, e dos procedimentos metodológicos e suas lógicas; o reconhecimento da necessidade de continuar aprendendo e aprimorando seus próprios conhecimentos; a apropriação das linguagens das tecnologias digitais e a fluência em sua utilização; a apropriação das linguagens científicas e sua utilização na comunicação e na disseminação desses conhecimentos. (BRASIL, 2018, p.466)

Dado esse contexto social, surgem inquietações quanto à abordagem que se deve realizar da Matemática no Ensino Básico, contemplando as recomendações dos documentos que explicitam a base da educação e dos que orientam a pesquisa de educadores matemáticos. Tais inquietações promovem um esforço para adequar as tecnologias aos objetivos da educação, buscando propostas de aprendizagem que sejam instigantes e prazerosas aos alunos e os levem à construção de conhecimento.

Ao refletir sobre essa questão buscando temas do cotidiano, surgem, entre outros, os códigos: o Registro de Certidão de Nascimento, o Cadastro de Pessoa Física (CPF), o Registro de Identidade (RG), o Código de Endereçamento Postal (CEP), os números de telefone, placas de carros, códigos de barras e diversos outros códigos de identificação frequentes em nossas vidas. O principal objetivo de um código, como mencionado no Capítulo 3, é identificar, com segurança e numericamente, um objeto ou artigo, de acordo com características específicas, como sua origem e finalidade, por exemplo.

Apenas recentemente este passou a ser um tema considerado viável ao trabalho em aulas, pois suas aplicações matemáticas não eram exploradas ou eram com pouca ênfase ou como exceção. Os códigos apresentam grandes possibilidades de abordagem no ensino, trazendo-o para uma perspectiva

da Aritmética no Ensino Fundamental e da Álgebra, no Ensino Médio, ambos inseridos na Teoria dos Números. Segundo Sousa (), através do estudo dos códigos

(...) podemos estimular e aprimorar a leitura e interpretação de tabelas, fórmulas e dos próprios códigos. Ainda podemos reforçar e destacar propriedades básicas de operações como soma, multiplicação e divisão, potenciação, cálculos mentais e linguagem algébrica para escrever algoritmos. (SOUSA, , p. 45)

O estudo dos códigos permite uma abordagem histórica da Matemática, salientando que a “(...) percepção da unidade da Matemática, além da diversidade de suas práticas, serve também para mostrar que o desenvolvimento da disciplina é fruto da experiência humana ao longo da história.”(BRASIL, 2018, p.522).

Essa abordagem é reforçada por Sousa (), que afirma, quanto aos códigos, que, “para além do uso prático e imediato, é também possível relacioná-los à história e desenvolvimento da humanidade tendo em vista seu papel de destaque na preservação do conhecimento, relações entre os povos e, notadamente, conflitos.” (SOUSA, , p.1). Os temas a serem estudados são amplos, incluindo não somente os códigos, mas também as cifras e a criptografia.

Dessa maneira, vê-se a necessidade de se desenvolver conteúdo do currículo de Matemática na Educação Básica que valorize o estudo dos códigos. Mais especificamente, alguns temas oferecem possibilidades favoráveis à aprendizagem, como a investigação do padrão de formação do número de CPF que utiliza, entre unidades temáticas mais básicas, a Aritmética Modular dos Restos; o código de barras, refletindo sua utilidade e estrutura de formação e do QR Code, um código de barras bidimensional, explorando como realizar a sua leitura e geração.

O desenvolvimento desse conteúdo deve primar por uma proposta que proporcione um ambiente criativo e investigativo, visto que possibilita “(...) fazer conexões entre diversos conceitos matemáticos, suas diferentes formas de pensamento com outras áreas do saber e com as aplicações na atualidade.” (TAKAHASHI, 2015, p.288).

Por fim, atento às recomendações educacionais, o estudo dos códigos possibilita o desenvolvimento de competências e habilidades presentes nos documentos oficiais da educação, como os PCNs e a Base Nacional Comum Curricular (BNCC), alguns deles relativos “a leitura e interpretação de textos em representações matemáticas como tabelas, gráficos, equações, fórmulas e muitas outras, além da possibilidade de estimular o trabalho em equipe e cooperação por meio das atividades propostas.” (SOUSA, , p.66).

É a partir dessas noções, geradas com base nos estudos e documentos mencionados, que as atividades propostas serão desenvolvidas, com embasamento em pesquisas elaboradas previamente, mas buscando uma abordagem diferenciada quanto à sua possibilidade de desenvolvimento em sala de aula, com ênfase na utilização da História da Matemática como recurso auxiliador, através da Resolução de Problemas.

4.1 OS TEMAS GERADORES

As discussões acerca de uma formação integral, que desenvolva as atitudes para além das habilidades e competências técnicas, são cada vez mais comuns. O mundo contemporâneo exige uma postura diferente no ensino, visando que os alunos se tornem mais críticos sobre os fenômenos que cercam seu contexto. Isso desperta a necessidade de educadores com posturas diferenciadas, que abandonem o posto de mero reprodutor de conhecimento e assumam a postura de transformador da realidade (COSTA; PINHEIRO, 2013).

Dessa forma, as práticas de ensino inflexíveis, cujos princípios recaem na repetição para memorização e na presença do professor como transmissor e dos alunos como meros receptores, devem ser repensadas a fim de promover as transformações necessárias. Os temas geradores, desenvolvidos como uma proposta de método de ensino por Paulo Freire, educador brasileiro de reconhecimento internacional, surgem como uma possibilidade de educar e promover uma escolarização cumpridora de seu papel social.

Os temas geradores se caracterizam partir da adoção de situações que cercam a realidade de educandos e educadores a serem abordados em sala de aula, onde não precisam apenas ser apreendidos, mas refletidos, a fim de que ocorra a tomada de consciência dos indivíduos sobre eles. Assim, o ensino baseado na proposta de temas geradores parte da contextualização de um assunto presente no dia a dia dos educandos e do educador, destacando que “O ponto de partida é a experiência concreta do indivíduo, em seu grupo ou sua comunidade. (...) As palavras e os temas mais significativos deste universo são escolhidos como material para (...) a elaboração do novo conhecimento, partindo da problematização da realidade vivida” (ANDREOLA, 1993, p.33).

Ao trabalhar com os temas geradores, é necessário que educador e educandos assumam uma postura problematizadora. Essa postura deve começar a partir da escolha dos temas, onde o educador deve refletir a pertinência de cada tema e suas possibilidades de abordagem nas aulas. Isso refletirá diretamente na interação dos alunos com a prática, pois também assumirão a postura problematizadora durante as aulas, partindo, principalmente, de situações desafiadoras.

“Quanto mais se problematizam os educandos, como seres no mundo e com o mundo, tanto mais se sentirão desafiados. Tão mais desafiados, quanto mais obrigados a responder ao desafio. Desafiados, compreendem o desafio na própria ação de captá-lo. Mas, precisamente porque captam o desafio como um problema em suas conexões com outros, num plano de totalidade e não como algo petrificado, a compreensão resultante tende a tornar-se crescentemente crítica, por isto, cada vez mais desalienada”. (FREIRE, 2011, p.33).

4.2 A RESOLUÇÃO DE PROBLEMAS

A utilização de problemas no ensino de Matemática não é uma prática incomum. Segundo Allevato e Onuchic (2009), eles ocupam um lugar central no currículo da disciplina desde a Antiguidade, com registros na história antiga egípcia, chinesa e grega, por exemplo. Geralmente, os problemas eram

criados, resolvidos e apresentados, para que então os alunos recebessem uma lista com problemas semelhantes para resolver. Ainda hoje é possível encontrar esse tipo de dinâmica em livros didáticos e em salas de aula, onde a ênfase está voltada aos procedimentos a serem reproduzidos na resolução de um problema.

A Resolução de Problemas como metodologia de ensino é um conceito mais recente na Educação Matemática, e é o foco deste trabalho. De acordo com Allevato e Onuchic (2009), foi por volta da década de 1950 que a resolução de problemas começou a ser discutida, tendo George Poyla, Herbert F. Spitzer e Luis Alberto S. Brasil como principais referências. No entanto, nos anos seguintes a Educação Matemática se preocuparia com outros tópicos, sendo que as investigações sistemáticas sobre a resolução de problemas e as suas implicações curriculares se desenvolveram apenas no início da década de setenta.

A importância dada à resolução de problemas é, portanto, recente e somente nessa década é que os educadores matemáticos passaram a aceitar a idéia de que o desenvolvimento da capacidade de resolver problemas merecia mais atenção. A caracterização da Educação Matemática em termos de resolução de problemas reflete uma tendência de reação a caracterizações passadas, que a configuravam enfatizando a memorização de um conjunto de fatos, o domínio de procedimentos algorítmicos ou um conhecimento a ser obtido por rotina ou por exercício mental. (ALLEVATO; ONUCHIC, 2009, p.136)

A década de oitenta foi marcada pela preocupação em dar destaque à resolução de problemas nas aulas de Matemática e, com o objetivo de tornar a resolução de problemas o ponto central das aulas, muitos recursos foram desenvolvidos para auxiliar os professores. No entanto, o significado de resolução de problemas e sua presença na sala de aula tinha concepções discordantes, o que influenciou para o insucesso do trabalho nessa década. Foi apenas nos anos 1990 que a Resolução de Problemas se tornou objeto de pesquisas e estudos como uma Metodologia de Ensino, e o ensino através dela passou a ser fortemente recomendado pelos estudiosos e documentos de ensino, por exemplo. No Brasil, os Parâmetros Curriculares Nacionais, elaborados no fim da década de 1990, expõem essa necessidade, salientando as vantagens que o ensino através da Resolução de Problemas pode proporcionar.

“Não somente em Matemática, mas até particularmente nessa disciplina, a resolução de problemas é uma importante estratégia de ensino. Os alunos, confrontados com situações-problema, novas mas compatíveis com os instrumentos que já possuem ou que possam adquirir no processo, aprendem a desenvolver estratégia de enfrentamento, planejando etapas, estabelecendo relações, verificando regularidades, fazendo uso dos próprios erros cometidos para buscar novas alternativas; adquirem espírito de pesquisa, aprendendo a consultar, a experimentar, a organizar dados, a sistematizar resultados, a validar soluções; desenvolvem sua capacidade de raciocínio, adquirem autoconfiança e sentido de responsabilidade; e, finalmente, ampliam sua autonomia e capacidade de comunicação e de argumentação.” (BRASIL, 1998, p.52).

Dessa forma, vem se intensificando o interesse por essa Metodologia de Ensino nos últimos anos, atentando-se às novas demandas e tendências mundiais no que diz respeito ao ensino e à aprendizagem de Matemática.

Ao falar dessa metodologia, sempre é mencionado que o ensino de Matemática é feito *através* da Resolução de Problemas, pois ela age como o ponto inicial de todo o processo, o problema é o elemento que desencadeia um processo de construção do conhecimento. Todavia, outras duas possibilidades de conceber a resolução de problemas surgem: ensinar sobre resolução de problemas e ensinar para resolução de problemas. A primeira utiliza o problema como objetivo, ensinando-se Matemática para resolver problemas — é o uso mais comum, ainda muito utilizada nas salas de aula —, e a segunda utiliza o problema como processo, enfatizando as estratégias utilizadas na resolução.

Antes de apresentar a metodologia em si, é importante definir o que é um “problema”. O termo “problema” é muito utilizado no cotidiano, podendo assumir significados diferentes de acordo com o contexto de utilização. Em Matemática, e especificamente em Educação Matemática, também existem diferentes concepções de problemas.

Para o documento de referência produzido e publicado pelo National Council of Teachers of Mathematics (NCTM) — Conselho Nacional de Professores de Matemática — em 1991, denominado “Normas para o currículo e a avaliação em matemática escolar”, “(...) um problema genuíno é uma situação em que, para o indivíduo ou para o grupo em questão, uma ou mais soluções apropriadas precisam ainda de ser encontradas. A situação deve ser suficientemente complicada para constituir um desafio, mas não tão complexa que surja como insolúvel.” (NCTM, 1991).

Van de Walle (2009) define problema como qualquer tarefa ou atividade que não possibilite que os alunos empreguem regras ou métodos memorizados na resolução, ou ainda que desperte nos estudantes a percepção de que existe um modo correto e específico de solução. Para Allevato e Onuchic, um problema “é tudo aquilo que não se sabe fazer, mas que se está interessado em fazer.” (ONUCHIC; ALLEVATO, 2011, p.81).

Existem diversas outras definições para os problemas, de acordo com diferentes estudiosos e documentos, mas aqui, de acordo com as definições mencionadas, a concepção assumida é a de que um problema é aquilo que os alunos não possuem os meios necessários para a resolução, mas que estão motivados a resolver.

Com isso definido, é possível partir para a Resolução de Problemas como Metodologia de Ensino. Para este trabalho, o principal referencial teórico são os estudos e pesquisas realizados por Allevato e Onuchic, com o conceito da “Metodologia de Ensino-Aprendizagem-Avaliação de Matemática através da Resolução de Problemas”. O emprego da palavra composta ensino-aprendizagem-avaliação confere uma nova abordagem à Metodologia, pois

Ao considerar o ensino-aprendizagem-avaliação, isto é, ao ter em mente um trabalho em que estes três elementos ocorrem simultaneamente, pretende-se que, enquanto o professor ensina, o aluno, como um participante ativo, aprenda, e que a avaliação se realize por ambos. O aluno analisa seus próprios métodos e soluções obtidas para os problemas, visando sempre à construção de conhecimento. Essa forma de trabalho do aluno é consequência de seu pensar matemático, levando-o a elaborar justificativas e a dar sentido ao que faz. De outro lado, o professor avalia o que está ocorrendo e os resultados do processo, com vistas a reorientar as práticas de sala de aula, quando necessário.(ONUCHIC; ALLEVATO, 2011, p.81)

Ainda segundo as autoras, nessa metodologia “(...) o problema é ponto de partida e, na sala de aula, através da resolução de problemas, os alunos devem fazer conexões entre diferentes ramos da Matemática, gerando novos conceitos e novos conteúdos.” (ONUCHIC; ALLEVATO, 2011, p.81).

Não existe uma forma rígida para se ensinar Matemática através da resolução de problemas em sala de aula, configurando ao professor e aos alunos posturas e atitudes diferentes. O professor deve assumir a responsabilidade do preparo ou escolha de problemas pertinentes ao conteúdo ou conceito que deseja desenvolver nas aulas e promover uma dinâmica em que deixa de ser o foco das aulas, passando esse papel aos alunos, e estes devem assumi-lo conscientemente.

Allevato e Onuchic (2011) desenvolveram um roteiro de apoio para o desenvolvimento mais proveitoso da metodologia. Nesse roteiro, seguem-se algumas etapas:

- Preparação do problema: Escolha do problema gerador, ou tema gerador, visando o conceito que o professor quer desenvolver com os alunos. O conteúdo necessário para a resolução do problema não deve ter sido previamente apresentado aos alunos;
- Leitura individual;
- Leitura em conjunto: releitura do problema, mas agora em grupos. Se surgirem dificuldades na leitura, o professor pode auxiliar os alunos;
- Resolução do problema: os alunos devem trabalhar cooperativamente para resolver o problema proposto. Esse momento conduzirá os alunos para a construção do conteúdo planejado pelo professor através do problema gerador;
- Observar e incentivar: o professor deve observar, analisar o comportamento dos alunos e incentivar o trabalho cooperativo dos alunos, deixando seu papel de “transmissor” do conhecimento de lado. É um momento de mediação e orientação para que os alunos usem seus conhecimentos prévios, busquem caminhos alternativos, explorem possibilidades e lidem com possíveis problemas secundários;
- Registro das soluções na lousa: os alunos devem fazer esse registro, mesmo que a resolução esteja incorreta;

- Plenária: os alunos devem discutir as soluções apresentadas, argumentando e esclarecendo suas dúvidas. Mais uma vez, o professor age como mediador, incentivando que os alunos participem ativamente;
- Busca do consenso: após discussões, os alunos, com auxílio do professor, tentam chegar a um consenso sobre o resultado correto;
- Formalização do conceito: O professor registra na lousa uma apresentação formal do conteúdo abordado, de forma organizada e estruturada na linguagem matemática.

É importante ressaltar que a avaliação é realizada durante todo esse processo, considerando o envolvimento e desenvolvimento dos alunos.

Essa metodologia de ensino promove uma abordagem diferente e que pode causar estranhamento tanto nos alunos quanto nos professores. Entretanto, ela pode promover diversas vantagens ao ensino-aprendizagem, dentre as quais, segundo Van de Walle (2009), configuram:

- Os alunos passam a dar atenção às ideias e no sentido das mesmas, ao invés de instruções e procedimentos;
- Os alunos desenvolvem a convicção de que são capazes de fazer matemática e, a partir disso, encontram sentido nela;
- Há continuidade na avaliação dos alunos, contribuindo para a análise do professor, para a evolução dos alunos e para o envolvimento dos pais e responsáveis;
- Os alunos se deparam com diversos caminhos e alternativas para desenvolver a resolução de um problema, contribuindo para a diversidade de ideias, criatividade e argumentação;
- Os alunos são envolvidos na disciplina e são ativos no próprio processo de aprendizagem;
- O “potencial matemático” se desenvolve: resolver problemas, argumentar, comunicar, conectar e representar;
- É divertida e envolvente tanto para os professores quanto para os alunos.

4.3 O RECURSO À HISTÓRIA DA MATEMÁTICA

A Matemática, como toda ciência, possui um processo histórico. Seu desenvolvimento reflete as necessidades sociais, políticas e históricas, e conhecer esses contextos é de extrema importância para sua própria compreensão. De acordo com Ubiratan D'Ambrosio, “Em todos os momentos da história e em todas as civilizações, as ideias matemáticas estão presentes em todas as formas de fazer e de saber.” (D'AMBROSIO, 1999, p.97) e “A Matemática tem, como qualquer outra forma de conhecimento, a sua dimensão política e não se pode negar que seu progresso tem tudo a ver com o contexto social, econômico, político e ideológico.” (D'AMBROSIO, 2021, p.43).

Dessa forma, é primordial que, ao discutir Educação Matemática, tais recursos sejam considerados, e que a Matemática não seja desvinculada das outras atividades humanas — isto, segundo D'Ambrosio

(1999) é um dos maiores erros que se pratica em educação. As Diretrizes Curriculares Nacionais da Educação Básica (DCNs) afirmam que é importante “(...) romper com a centralidade das disciplinas nos currículos e substituí-las por aspectos mais globalizadores e que abranjam a complexidade das relações existentes entre os ramos da ciência no mundo real.” (BRASIL, 2013, p.183).

A Base Nacional Comum Curricular (BNCC) apresenta como uma competência geral da Educação Básica a necessidade de “Valorizar e utilizar os conhecimentos historicamente construídos sobre o mundo físico, social, cultural e digital para entender e explicar a realidade, continuar aprendendo e colaborar para a construção de uma sociedade justa, democrática e inclusiva.” (BRASIL, 2018, p.9) .

Assim sendo, é fundamental que haja uma preocupação com um ensino contextualizado historicamente e, quanto à Matemática, posicioná-la de forma que os alunos possam vê-la como uma disciplina integrada nesse objetivo, relacionando etapas da história da Matemática com a evolução da humanidade e trabalhando isso como uma competência e habilidade a ser desenvolvida na disciplina, afirmando que a relevância do aprendizado da História da Matemática transcende a relação social, pois também ilustra o desenvolvimento e a evolução dos conceitos a serem aprendidos.

Quanto aos seus objetivos pedagógicos, segundo Miguel (2009), a História da Matemática pode contribuir para que os alunos percebam a Matemática como criação humana; compreendam as razões pela qual se faz Matemática; entendam as necessidades sociais, históricas, políticas e econômicas como estímulo para o desenvolvimento da Matemática; entre outros fatores importantes para o desenvolvimento da aprendizagem da Matemática não apenas como disciplina, mas também como uma presença constante em nossas vidas.

Compreendendo a necessidade de se pensar Educação Matemática aliada à História da Matemática, cabe a reflexão sobre o preparo dos educadores. Para além dos conhecimentos óbvios da disciplina e dos quais o professor teve acesso durante sua formação, é necessário que, visando a prática de ensinar Matemática historicamente contextualizada, se conheça a História da Matemática. Essa não é uma tarefa simples, e “Para se adotar essa prática, a formação do professor é essencial. (...) A preparação que permite ao professor fazer uma abordagem histórico-crítica exige um aprendizado permanente.” (D’AMBROSIO, 2021). No entanto, o próprio autor afirma que o professor não precisa ser especialista no assunto para que utilize o recurso, bastando estudar o tema que for abordar em suas aulas.

Por fim, com base nesses princípios, se justifica a utilização da História da Matemática como um recurso metodológico capaz de auxiliar no processo de construção do conhecimento.

5 ATIVIDADES PROPOSTAS

Neste capítulo serão apresentadas três propostas de atividades a serem realizadas com turmas do Ensino Médio, onde os códigos, e principalmente os códigos de barras, serão os temas geradores. Essas atividades foram planejadas para aplicação em sala de aula, mas devido às mudanças causadas pela pandemia da Covid-19 no ensino no ano de 2020, isso não foi possível. Entretanto, espera-se que essas atividades ofereçam possibilidades de aplicação, auxiliando professores e alunos no processo de ensino e aprendizagem dos conteúdos, conceitos e procedimentos pertinentes.

A primeira atividade proposta não tem como tema gerador o código de barras, mas sim as cifras e a criptografia. Como salientado no Capítulo 3, a história dos códigos frequentemente se confunde com a história da criptografia, tornando relevante abordar os dois conceitos conjuntamente. A segunda atividade terá como tema gerador o código de barras tradicional, com as barras verticais, visto na Seção 3.2. Por fim, a terceira proposta abordará os códigos QR, da Seção 3.3, como um tema gerador para o conceito de progressão aritmética.

Essas atividades estão interligadas e podem ser aplicadas em sequência, contribuindo para a compreensão geral dos alunos sobre os códigos, e apresentando um aumento gradativo no nível de dificuldade das propostas. Entretanto, cada atividade também pode ser desenvolvida individual e independentemente das outras, atendendo às necessidades específicas de cada turma, professor e planejamento escolar. Além disso, cada uma delas pode ser adaptada de acordo com as demandas que podem surgir nos diferentes contextos - por exemplo, a duração das aulas pode ser adaptada ao contexto de cada turma, considerando a disponibilidade de aulas, a familiaridade com os temas e as alterações pertinentes em cada atividade.

Cada atividade apresentará, inicialmente, uma justificativa, a fim de localizar a prática pretendida nas recomendações de ensino dos principais documentos de referência da educação no Brasil, como a BNCC (2018), e no Estado de São Paulo, como o Currículo do Estado de São Paulo (2020a). Em seguida, a atividade será descrita, salientando os principais procedimentos em busca dos objetivos propostos em cada uma delas. As três atividades propostas são pensadas tendo a adoção de temas geradores e a Metodologia Ensino-Aprendizagem-Avaliação de Matemática através da Resolução de Problemas como principais parâmetros.

As atividades não preveem em qual ano específico do Ensino Médio serão desenvolvidas, pois possuem passibilidade de aplicação durante toda a etapa — as próprias habilidades consideradas aqui não determinam um ano para que sejam desenvolvidas. Ademais, é importante que, em todas as atividades e etapas, os alunos estejam cientes de que as propostas exigem uma postura ativa, pois apresentarão problemas cujos conteúdos ainda serão desconhecidos ou pouco explorados na disciplina e, por isso, não existem respostas erradas — o importante é que eles se envolvam em todos estágios da atividade. Isso também caracterizará a avaliação proposta, que deve ser realizada pelo docente durante todo o procedimento das atividades, considerando o envolvimento e desenvolvimento dos alunos.

5.1 ATIVIDADE 1 - CRIPTOGRAFIA

Como visto na Seção 4.2, é fundamental que haja uma preocupação com um ensino contextualizado historicamente e, quanto à Matemática, posicioná-la de forma que os alunos possam vê-la como uma disciplina integrada nesse objetivo. Essa atividade busca cumprir com essa necessidade, recorrendo à História da Matemática como um recurso de ensino, cujo tema gerador são os códigos, criptografia e as cifras.

São muitas as possibilidades de desenvolvimento nessa temática, mas esta atividade se fundamenta no enfoque ao tema da Segunda Guerra Mundial e a presença da criptografia como uma estratégia de guerra e suas consequências nos eventos históricos. Tal perspectiva não é arbitrária, mas se alicerça nas orientações dadas pelo Currículo do Estado de São Paulo (2020b) de que no nono ano do Ensino Fundamental, a disciplina de História desenvolva, com os estudantes, o tema da Segunda Guerra Mundial, e de que no Ensino Médio, a disciplina preze por abordar as revoluções na ciência e os impactos dos avanços técnico-científicos informacionais. Uma vez que essas atividades são pensadas para aplicação no Ensino Médio, o tema surge como uma continuidade na aprendizagem dos alunos e na viabilidade de aprofundamento, valendo-se da interdisciplinaridade.

Para além dessa finalidade, a atividade propõe abordar os seguintes conteúdos matemáticos: operações básicas, combinatória e criação de algoritmos — uma sequência de instruções que podem ser executadas mecanicamente por uma pessoa ou máquina. Em relação aos algoritmos, seu ensino é fortemente recomendado pelos documentos educacionais que alicerçam este trabalho. Na BNCC, duas habilidades de Matemática para o Ensino Médio mencionam o conceito:

(EM13MAT315) Reconhecer um problema algorítmico, enunciá-lo, procurar uma solução e expressá-la por meio de um algoritmo, com o respectivo fluxograma. (...)
 (EM13MAT406) Utilizar os conceitos básicos de uma linguagem de programação na implementação de algoritmos escritos em linguagem corrente e/ou matemática.
 (BRASIL, 2018, p.529-531).

Já no Currículo do Estado de São Paulo (2020a), além de habilidades voltadas para o desenvolvimento do tema, os algoritmos surgem também como objetivos de conhecimento para a modelagem de problemas e de soluções.

Desenvolvimento

Duração total: 10 aulas de 50 minutos.

Etapa 1

Duração: duas aulas.

Organização da turma: quartetos.

Orientações:

Os alunos serão organizados em grupos, e cada um receberá uma folha com o seguinte texto, e serão orientados a realizarem a *leitura individual*.

“Dois reinos vizinhos estão em conflito diplomático há anos, mas a situação ameaça escalar para uma guerra violenta em breve. O Reino do Norte deseja encerrar o conflito em paz, mas não consegue convencer o Reino do Sul de suas intenções. A rainha do Reino do Norte teme que o rei do Reino do Sul esteja planejando atacar seu território de surpresa e que esteja usando espiões entre seus conselheiros. Ela precisa, urgentemente, de um espião que acesse as informações do reino rival, pois só assim poderá se defender. Ela tem um candidato perfeito para esse papel: você! Será uma tarefa fácil, pois o rei é seu tio e ele não faz ideia que você é leal ao Reino do Norte — você sabe como seu tio pode ser perverso, também teme o desenrolar de uma guerra e tem como melhor amigo o filho da rainha, por isso aceita ajudá-la. Mas existe um problema. Assim que você começar a espionar o rei, não poderá retornar ao Reino do Norte, pois isso seria arriscado demais. No entanto, a rainha exige que você envie relatórios a cada três dias contando tudo o que descobrir. Você pode enviar cartas, mas existe o risco de que elas sejam interceptadas e seu conteúdo seja revelado e, bom, isso significaria o fim da linha pra você. Você precisa surgir com uma solução rápida, pois logo partirá para o sul. De que formas você pode resolver esse problema?”

Em seguida, deverão fazer uma leitura em grupo (*leitura em conjunto*). Nesse momento, todas as dúvidas devem ser expostas e esclarecidas pelo professor — significado de palavras, interpretação, comando etc. Quando todos os alunos compreenderem a proposta, devem partir para a resolução do problema, discutindo as possibilidades em grupo e registrando a resposta nas folhas (*resolução do problema*). O papel do professor é de observador e incentivador, agindo de forma a deixar que os alunos sejam os protagonistas da resolução, auxiliando apenas se necessário, e nunca cedendo a resposta (*observar e incentivar*).

Quando todos os alunos tiverem resolvido o problema, cada grupo escolherá um representante para expor a resposta para o resto da turma (*registro das soluções na lousa*). Posteriormente, a turma, orientada pelo professor, deve discutir qual a melhor proposta para resolver o problema e chegar em um consenso (*plenária e consenso*).

Resultados esperados: Espera-se que os alunos, em algum momento, proponham a utilização de um “código secreto” como alternativa para a comunicação da situação analisada. Se não for o caso, o professor deve incentivar que os alunos pensem essa possibilidade. Esse é um momento propício para que o docente promova questionamentos que aprofundem os alunos na utilidade, funcionamento e possibilidades dos usos de códigos.

Etapas 2

Duração: uma aula.

Orientações:

Após as discussões, abordar a criptografia — apresentá-la como sendo um tipo de código —, o que ela significa e de onde veio a necessidade de utilizá-la, iniciando uma breve contextualização histórica, tal como vista na Seção 3.1. Mencionar as diversas formas de comunicação ao longo da história e as circunstâncias que desencadearam na necessidade de manter tais comunicações em segredo. Nessa

proposta, o foco é que a criptografia na Segunda Guerra Mundial seja o principal tema histórico abordado.

Nessa etapa, é interessante que haja um trabalho conjunto entre professor de Matemática e História, planejando a melhor forma de conectar as duas disciplinas aproveitando-se da proposta dessa atividade.

Etapa 3

Duração: duas aulas.

Organização da turma: quartetos.

Orientações:

O professor pode optar por focar em determinados tipos de criptografia, de acordo com suas intenções de planejamento — esta é uma das vantagens em utilizar a criptografia como tema gerador, pois ela possibilita uma gama de alternativas interessantes e pertinentes, como a combinatória, a divisibilidade, as sequências alfanuméricas e até mesmo a probabilidade. Neste caso, optando por abordar a combinatória, a Cifra de César é um tema ideal. Para isso, promovendo uma dinâmica semelhante ao que foi descrito na Etapa 1, entregar aos alunos o seguinte texto:

“Você, trabalhando como espião para a rainha do norte, acabou se deparando com algumas mensagens secretas enviadas ao rei do sul. Em uma delas, lia-se o seguinte: X ANQVX MX VXACN MNEN BNA JCJLJMX JX JVXQCNLNA MX YAQUNQAX MQJ MN QVENAVX. Você suspeita que a mensagem está escrita utilizando uma cifra de substituição, com deslocamento do alfabeto.

- *Descubra o que a mensagem diz.*
- *Escreva, detalhadamente, os procedimentos para descobrir a mensagem.*
- *Sabendo como a mensagem foi cifrada, descreva, detalhadamente, os procedimentos para que qualquer mensagem seja cifrada dessa forma.”*

Dar tempo suficiente para que eles possam ler individualmente e em grupo, e discutir, testar e propor soluções. Promover, novamente, o momento do registro das soluções na lousa e da plenária, incentivando que revelem as estratégias utilizadas para decifrar a mensagem — “O reino do norte deve ser atacado ao anoitecer do primeiro dia de inverno”. Quanto aos tópicos de descrição do procedimento, incentivar que sejam bem rigorosos, de modo que qualquer pessoa compreenda e realize os passos descritos. Este momento é a introdução do conceito de algoritmo, que deve ser formalizado pelo professor.

Prosseguir a aula com a proposta de mais um problema, seguindo a mesma dinâmica de organização e desenvolvimento. O seguinte texto deve ser entregue aos alunos, ainda seguindo a situação imaginária proposta na Etapa 1:

“A mensagem que você interceptou anteriormente foi fácil de decifrar. Por quê? O que mudaria se, ao invés de seguir o deslocamento fixo no alfabeto, as letras pudessem ser substituídas aleatoriamente?”

- *Seguindo a “Cifra de César”, quantas são as possibilidades para cifrar uma mensagem?*
- *Ainda utilizando uma cifra de substituição, mas dessa vez substituindo as letras aleatoriamente, quantas são as possibilidades para cifrar uma mensagem?”*

Resultados esperados: Espera-se que os alunos proponham soluções que considerem todas as possibilidades envolvidas, mesmo que não cheguem em resultados exatos. Depois da plenária e do consenso, o professor deve formalizar os conceitos de chave, relacionados à criptografia, e de combinatória, da forma que for mais pertinente.

Etapa 4

Duração: uma aula.

Orientações:

Apresentar aos alunos a história da máquina Enigma, desde sua criação, sua adoção pelo exército alemão e todo o trabalho desempenhado para a quebra do seu código. O principal foco desse conjunto de aulas deve recair sobre o papel da criptografia na Guerra e o envolvimento da Matemática. É ideal que os alunos participem ativamente desse momento e discutam o papel das ciências no desenvolvimento da sociedade.

Etapa 5

Duração: duas aulas.

Organização da turma: quartetos.

Orientações:

Uma vez que o conceito de combinatória está formalizado, os alunos já possuirão as ferramentas necessárias para lidar com situações mais complexas. Nessa etapa, a máquina Enigma será analisada do ponto de vista matemático.

Retomar a apresentação da máquina, dessa vez destacando seu funcionamento, mostrando cada um de seus componentes e suas funções. Se possível, levar os alunos para lidarem com softwares que simulam a Enigma — existem opções gratuitas e de fácil acesso na internet. Por fim, propor questionamentos envolvendo combinatória considerando o funcionamento da máquina, tais como:

- O que acontece se adicionarmos mais um misturador? E se retirarmos um?
- Se os decodificadores britânicos soubessem a disposição dos rotores, mas não conhecessem a disposição dos misturadores, com quantas possibilidades de codificação ainda teriam que trabalhar?

Quanto ao total de cifragens possíveis pela Enigma, é recomendado que seja um cálculo realizado com o acompanhamento do professor, devido à sua complexidade.

Resultados esperados: É esperado que os alunos compreendam a combinatória através dos exemplos abordados, podendo aplicar esse conhecimento em outras situações e problemas posteriores. Além disso, espera-se que através dessa abordagem os discentes entendam o impacto da matemática e tecnologia no decorrer da história e a importância de sua aplicação em contextos reais.

Etapas 6

Duração: duas aulas.

Organização da turma: quartetos.

Orientações:

Agora que os alunos conhecem a criptografia, os conceitos de chave e algoritmo e a combinatória, a fim de finalizar esse conjunto de aulas e consolidar esses conceitos, será proposto que eles criem seu próprio código, retornando à situação imaginária das etapas anteriores. Entregar o texto:

“Agora você sabe que, para se comunicar com a rainha do norte, devem utilizar algum tipo de código. Por isso, você deve criar um código, diferente dos que você já conhece, que seja eficiente e possível de ser trocado entre vocês. Descreva, na forma de um algoritmo, o código que foi criado. Depois, escreva uma mensagem utilizando seu código avisando à rainha sobre o ataque anunciado na mensagem que você interceptou anteriormente. Por fim, responda às perguntas:

- *Quantas chaves tem seu código?*
- *Como vocês conhecerão as chaves do código?*
- *Você acha que seu código é seguro?”*

Solicitar que os grupos troquem os algoritmos e as mensagens, e decifrem as mensagens uns dos outros. Se tiverem dificuldades, isso significa que o algoritmo e o código podem não estar bem elaborados. Propor que os grupos apresentem seus códigos para a turma e promover a plenária, discutindo cada possibilidade criada, possíveis falhas e melhorias. Por fim, decidir por um código “vencedor” — a competição não deve ser incentivada, apenas a argumentação para a decisão da melhor escolha considerando o contexto criado na atividade.

Resultados esperados: A expectativa é que os alunos compreendam a utilidade da criptografia e estejam aptos para criar o próprio código para comunicação segura. É uma atividade que envolve tanto o aprendizado teórico desenvolvido na proposta quanto a criatividade e a capacidade de solucionar um problema, mesmo que fictício.

Sugestões

Existem outras possibilidades de abordagem a partir desse tema gerador, tais como a abordagem da Criptografia RSA e a divisibilidade, por exemplo. A criptografia oferece oportunidades ricas e pertinentes para o estudo de Matemática, permitindo que o professor seja criativo em suas escolhas de temas e abordagens.

5.2 ATIVIDADE 2 - CÓDIGOS DE BARRAS

Essa atividade será desenvolvida tendo como tema gerador o código de barras tradicional, com as barras verticais. Mais uma vez, o tema gerador proposto abrange possibilidades diversas de aplicação na sala de aula, podendo ser modificado de acordo com as finalidades desejadas. Nessa atividade, os principais conceitos a serem desenvolvidos são: operações básicas, divisibilidade, representações binárias e algoritmos.

Desenvolvimento

Duração total: 8 aulas de 50 minutos.

Etapa 1

Duração: uma aula.

Organização da turma: quartetos.

Orientações:

Os alunos, organizados em grupos, recebem o texto:

“O mundo está enfrentando uma pandemia de uma doença causada por um vírus pouco conhecido — o SARS-CoV-2, ou mais popularmente, a COVID-19. Depois de meses de esforços científicos, uma vacina foi produzida e deve começar a ser aplicada na população em breve. Em uma cidadezinha do interior de um país, a prefeitura está preocupada com a logística dessas vacinas que estão para chegar, pois não sabe como organizar a vacinação. O comitê de vacinação dessa cidade decide que a embalagem de cada vacina deve identificar algumas características, para que haja um controle dos grupos vacinados, uma vez que há certos critérios de prioridade. Primeiro, eles decidem esses critérios, e são eles:

- *Idade;*
- *Profissão;*
- *Grupo de risco — se a pessoa possui doenças que caracterizam complicações em caso de infecção ou idosos que vivem em instituições de longa permanência;*
- *Bairro em que reside na cidade.*

Em seguida, é acordado que cada vacina deve conter todos esses dados. Entretanto, não é possível que todas essas informações sejam escritas, pois ocupariam muito espaço. O comitê não sabe como proceder para resolver esse problema.

- *Se você fosse parte desse comitê, como resolveria o problema?”*
- *As informações dadas são suficientes?*

Solicitar aos alunos que criem esse código da forma que acharem ideal, considerando todos os

critérios. Não é esperado que os códigos sejam eficientes ou que se pareçam com um código de barras, mas eles devem se aproximar à ideia de armazenamento de dados através de um código.

Resultados esperados: Espera-se que os alunos, durante a resolução, proponham a criação de um tipo de etiqueta ou código. Se não for o caso, o professor pode incentivar essa linha de pensamento. Com o momento de plenária e consenso, a turma deve optar pela criação de um código. É imprescindível que, neste ponto, as discussões propostas pelo professor e alunos envolvam questionamentos acerca do formato desse código (numérico ou alfabético, por exemplo), de sua extensão, da finalidade dos algarismos escolhidos etc. Além disso, os alunos devem problematizar a decisão do comitê do texto, questionando, por exemplo, quais idades e profissões são consideradas como prioridade, quantos e quais são os grupos de risco e, por meio de pesquisas em fontes confiáveis, propor soluções para esses problemas secundários.

Etapa 2

Duração: duas aulas.

Orientações:

A aula deve se iniciar com a introdução dos códigos de barras através de discussões e exemplos. O professor deve questionar se os alunos os conhecem e sabem o que eles significam, como funcionam, onde podem encontrá-los etc. Nesse momento, exemplos de códigos de barras devem ser mostrados para a turma e estes são convidados a fazer observações acerca de suas características e formato.

A fim de contextualizar historicamente o assunto e salientar o papel da matemática e tecnologia no desenvolvimento da sociedade, o professor deve falar sobre a história dos códigos de barras, destacando as condições que motivaram seu surgimento. A partir desse momento, os dois principais códigos de barras — UPC e EAN-13 — serão os objetos de estudo do conjunto de aulas.

É imprescindível que seja mostrado como esses códigos funcionam, assim como visto na subseção 3.2.1. O uso de representações gráficas e tabelas é fundamental para que os alunos compreendam o funcionamento desses códigos, pois eles são detalhados e padronizados.

Resultados esperados: Os alunos devem chegar ao final dessa etapa compreendendo o funcionamento dos códigos de barras UPC e EAN-13, abrangendo conceitos como representações binárias e codificação padronizada. É importante que ao final dessa etapa os alunos saibam reconhecer as representações numéricas e gráficas do código de barras — o porquê das listras de espessuras diferentes, o que cada uma delas representa e como “traduzi-las”.

Etapa 3

Duração: uma aula.

Organização da turma: quartetos.

Orientações:

Essa etapa é destinada a tratar da correção de erros presente nos códigos de barras mencionados. Novamente, seguindo a Metodologia de Ensino-Aprendizagem-Avaliação de Matemática através da Resolução de Problemas — com algumas adaptações —, a aula deve se iniciar com a proposta de um problema:

O comitê de vacinação decidiu usar o código que você elaborou, criou um programa de computador que interpreta esses dados e a vacinação já começou! Mas ocorreu um problema... Uma das enfermeiras, ao registrar os códigos manualmente, inserindo os números no programa de computador, cometeu alguns erros: mais de uma vez ela digitou um número errado, e o computador registrou que essas vacinas foram destinadas a outros grupos ou descartadas. Isso não pode acontecer! A cidade está preocupada em seguir o calendário de vacinação à risca, e um erro desses pode atrapalhar toda a logística. Para piorar, ela não notou esses erros imediatamente, e quando se deu conta, já era tarde demais para consertar... Ela não sabe o que fazer! Você consegue pensar em um modo de ajudar a enfermeira? Existe uma forma de evitar que esses erros sejam cometidos? Ou então, é possível evitar que o computador aceite um código incorreto? Como isso pode ser feito?

Resultados esperados: O conceito de detecção de erros, como feito nos códigos de barras, não é uma ideia trivial e, portanto, é improvável que os alunos surjam com essa ideia independentemente. Possivelmente, as propostas serão voltadas para a *ideia* de um método para detectar erros, e dificilmente para o método em si. A expectativa dessa etapa é que os alunos compreendam a necessidade de um método como esse e que proponham soluções diversas e criativas, mesmo que não sejam corretas ou se aproximem do tema pretendido.

Etapa 4

Duração: duas aulas.

Organização da turma: quartetos.

Orientações:

Essa etapa deve ser usada para formalizar a determinação dos dígitos verificadores que ocorre nos códigos de barras, tratado em na Subseção 3.2.2, mas sem definir os algoritmos, apenas exemplificando como o procedimento é feito.

Em seguida, o professor deve solicitar que, em grupos, os alunos resolvam o seguinte:

“Um colega está tentando explicar ao outro como faz para detectar um erro no código UPC:
João: *É bem fácil, primeiro você pega os números e multiplica por 1 e 3.*
Ana: *Que números? E se eu multiplicar por 1, não vai mudar nada, né?*
João: *Você entendeu errado, é pra multiplicar alternando, primeiro por 1, depois por 3, aí...*
Ana: *Multiplicar quem? Não estou entendendo nada...*
O diálogo continua, mas João continua dando explicações confusas, deixando Ana cada vez mais perdida. Ajude-os escrevendo todos os procedimentos para a detecção de erros nos códigos de barras UPC.”

Neste momento, os alunos estarão lidando com a criação de um algoritmo. É necessário que o professor oriente sobre a necessidade de tornar essa descrição a mais detalhada e compreensível possível. Seguem-se os momentos de plenária, consenso e formalização do conceito — nesse caso, algoritmos e, especificamente, o algoritmo para a detecção de erros no UPC. Se possível, repetir o

mesmo desenvolvimento, mas dessa vez com o EAN-13. Ademais, é possível que o professor enfatize outros conceitos nessa mesma etapa, tais como divisibilidade, números primos, etc, dependendo de seu interesse.

Resultado esperado: Espera-se que os alunos saibam descrever o algoritmo adequadamente, possibilitando que qualquer leitor compreenda o procedimento da detecção de erros.

Etapa 5

Duração: duas aulas.

Organização da turma: quartetos.

Orientações:

Agora que os alunos conhecem exemplos de códigos de barras, é necessário retornar à proposta da Etapa 1, retomar a leitura do texto proposto e os códigos que já haviam sido criados pelos grupos. O professor deve propor que os alunos aperfeiçoem seus códigos de acordo com o que aprenderam até aqui, procurando erros que possam atrapalhar no objetivo da proposta e criando um método de detecção de erros que auxilie na identificação de possíveis inconstâncias no momento de registrar esses códigos manualmente. Por fim, esse método deve ser escrito como um algoritmo. Não é o foco dessa proposta, mas como uma alternativa, se for viável, o professor pode propor que esses algoritmos sejam testados através de softwares adequados, como o Excel, por exemplo.

Sugestões

Ao trabalhar com os códigos de barras, surgem, além do conteúdo proposto nessa atividade, outras possibilidades, das quais é possível citar: conceitos de divisibilidade com os dígitos verificadores, combinatória na análise do armazenamento de dados nos códigos e até mesmo o desenvolvimento de aulas na disciplina de Física acerca do funcionamento dos leitores ópticos dos códigos de barras. Essas possibilidades oferecem ao docente a oportunidade de refletir acerca dos códigos de barras como temas geradores e como desenvolver esses temas da melhor forma, visando um ensino integral e compromissado com seu papel social de formador.

5.3 ATIVIDADE 3 - CÓDIGOS QR

A última atividade proposta tem como tema gerador os códigos QR. Nesta atividade, a aplicação da Metodologia de Ensino-Aprendizagem-Avaliação de Matemática através da Resolução de Problemas sofre uma pequena alteração em relação ao que vinha sendo desenvolvido nas atividades anteriores: os alunos já terão conhecimento sobre o código QR antes dos problemas serem propostos, ou seja, os alunos não lidarão com o código QR *como* problema, mas sim com problemas diretamente ligados ao que os alunos aprenderam sobre esses códigos. Os códigos QR ainda serão temas geradores para o desenvolvimento dos conteúdos e conceitos, mas com a dinâmica diferenciada. O tema a ser desenvolvido são as progressões aritméticas.

Desenvolvimento

Duração total: 6 aulas de 50 minutos.

Etapa 1

Duração: duas aulas .

Orientações:

O docente deve iniciar a aula questionando se os alunos conhecem os códigos QR e incentivando que falem sobre tudo que sabem acerca do tema — onde está presente, como é lido, pra quê serve, como funciona etc. É provável que os alunos já tenham visto e usado esse tipo de código, sem compreender a fundo sua funcionalidade. A partir disso, o professor deve incentivar que os alunos opinem livremente sobre como imaginam seu funcionamento, desde sua formatação até sua leitura por dispositivos móveis.

Em seguida, é importante promover uma discussão acerca de sua origem e necessidade, relatando aos discentes a história do surgimento dos códigos QR, mesmo que brevemente. É o momento de destacar, mais uma vez, a importância dos desenvolvimentos científicos e tecnológicos para a humanidade, salientando o impacto dessa invenção e seus usos mais comuns na sociedade atual. Os alunos devem se envolver nessa discussão, questionando e opinando quando for pertinente.

Para dar prosseguimento, o professor deve explicar o funcionamento dos códigos QR. Esse tipo de código não é simples e envolve conceitos que não são interessantes para o desenvolvimento no Ensino Médio — não se encaixam em nenhuma exigência dos documentos de ensino, tampouco configuram um nível de dificuldade adequado à etapa. Assim, cabe ao professor desenvolver esse tema o suficiente para a compreensão da turma, mas sem aprofundamentos inoportunos. A Seção 3.3 aborda o funcionamento dos códigos QR em um nível de explicação suficiente para esse fim.

É importante que nessa etapa o docente use muitas figuras de exemplificação ou até mesmo vídeos disponíveis online — desde que sejam adequados para a proposta. Os códigos QR são uma representação gráfica bidimensional, portanto, valer-se de recursos visuais para sua apresentação é imprescindível.

Etapa 2

Duração: duas aulas.

Organização da turma: quartetos.

Orientações:

Para isso, iniciar a etapa entregando o seguinte texto e perguntas:

“Os códigos QR possuem diversas versões, cada uma com uma quantidade de módulos diferente — os módulos são cada uma das unidades de codificação, ou seja, cada ‘quadradozinho’. São 40 versões, onde a versão 1 possui 21x21 módulos ou, como vamos nos referir aqui, configuração 21; a versão 2 possui configuração 25; a versão 3 possui configuração 29...”

- *Você observa algum padrão na formação dessas versões?*
- *Qual será a configuração da versão 4? E da versão 5? E da versão 8?*
- *É possível descrever, matematicamente, a configuração de cada versão?*
- *Escreva uma fórmula matemática para encontrar a configuração para a versão n .*

- *Teste sua fórmula para as versões 1, 2, 3 e 4 e confira se os resultados estão corretos.*
- *Escreva, na forma de sequência numérica, as configurações das 10 primeiras versões.*
- *Usando sua fórmula, descubra qual a configuração para a versão 40.*

Prosseguir a aula com os momentos previstos na metodologia adotada: leitura individual, leitura em conjunto, resolução de problemas, registro das soluções na lousa, plenária e busca do consenso. Todos esses momentos devem exigir do professor a postura de observador, incentivador e mediador.

Resultados esperados: Espera-se que os alunos desenvolvam um método para calcular as configurações solicitadas, utilizando-se de linguagem matemática e aplicando a fórmula pensada por eles mesmos para a conferência dos resultados.

Etapas 3

Duração: duas aulas.

Organização da turma: quartetos.

Orientações:

Essa etapa deve ser desenvolvida para consolidar a aprendizagem do tema, dessa vez com a generalização do conceito da progressão aritmética — razão pela qual a etapa anterior não contou com formalização do conceito. Para dar início a essa etapa, entregar o texto e as questões:

Agora seja um outro modelo — fictício — de códigos QR, onde a versão 3 possui configuração 35 (ou seja, 35x35 módulos), a versão 5 possui configuração 47 e a versão 8 possui configuração 65.

- *Você observa algum padrão na formação dessas versões?*
- *Qual será a configuração, em módulos, da versão 4? E da versão 6? E da versão 1?*
- *Escreva uma fórmula matemática para encontrar a configuração de módulos para a versão n .*
- *Usando sua fórmula, descubra qual a configuração para a versão 15.*
- *Escreva, na forma de sequência numérica, as configurações das 10 primeiras versões.*
- *Compare essa fórmula com a fórmula desenvolvida na atividade anterior. Quais semelhanças você observa? E quais diferenças?*
- *Generalize essa fórmula para descobrir um **termo** de qualquer sequência dada.*

Mais uma vez, prosseguir a aula com os momentos previstos na metodologia adotada. Nessa etapa é possível que surjam dúvidas durante as leituras do texto, pois os alunos podem ter dificuldade em compreender a pergunta “Generalize essa fórmula para descobrir um **termo** de qualquer sequência dada”. O professor, como observador e mediador, deve esclarecer essas dúvidas, sem, no entanto, revelar as respostas do problema. Por fim, após o desenvolvimento da proposta e os alunos compreenderem

bem o que se espera, o conceito — progressão aritmética — deve ser formalizado.

Resultados esperados: Assim como na etapa anterior, espera-se que os alunos obtenham as respostas dos problemas e, através das relações entre as duas etapas, notem a possibilidade de generalização para determinar os termos de quaisquer sequência numérica. Depois dos momentos propostos, é esperado que eles compreendam o conceito de progressão aritmética e a aplicabilidade da sua fórmula para facilitar os cálculos. Vale destacar que a intenção não é que a fórmula seja memorizada, mas sim entendida, possibilitando que os alunos possam deduzi-la a partir de um raciocínio lógico (pensando em exemplos simples, por exemplo).

Sugestões

Apesar da complexidade do funcionamento dos códigos QR, pensá-los como temas geradores no ensino de Matemática proporciona algumas abordagens interessantes e relevantes para a sala de aula. Do ponto de vista conceitual, é possível abordar, além da progressão aritmética aqui citada, a combinatória, as bases numéricas e até mesmo a probabilidade.

Ademais, um uso interessante e frequentemente citado em trabalhos acadêmicos, se configura pelo uso dos códigos QR como *ferramenta* de ensino, criando dinâmicas em que os alunos têm contato com esses códigos em ambientes diversos, como no espaço escolar, atividades em sala de aula e até mesmo nas provas. Uma proposta feita em Sousa () é muito interessante: o professor pode desenvolver uma espécie de “caça ao tesouro”, utilizando os códigos QR como armazenadores das pistas. Cada pista contém um problema diferente — e aqui a vantagem é que o professor pode desenvolver qualquer conteúdo matemático através desses problemas —, e a resolução de cada problema oferece aos alunos as dicas para a próxima etapa através de uma carta-código, onde alguns números (neste caso, as respostas para as pistas) são associados à frases ou palavras).

6 CONSIDERAÇÕES FINAIS

Os códigos configuram um tema de interesse antigo, cuja longevidade favorece uma história rica e diversa, desde seus usos em variados contextos sociais e históricos até as diferentes possibilidades de aplicação — ocultar o conteúdo de mensagens, ou facilitar o armazenamento e a privacidade de dados, por exemplo. No ensino de Matemática, essa caracterização proporciona abordagens múltiplas, pois a partir dela é possível desenvolver práticas pertinentes aos planejamentos escolares, tanto na procedência de conteúdos específicos quanto na demonstração de que as ciências, assim como as tecnologias, são construções humanas situadas historicamente.

A partir dessas possibilidades, a proposta desse trabalho era a elaboração de situações de aprendizagem que tivessem os códigos como temas geradores. Como visto, os temas geradores contemplam o diálogo entre a educação e a realidade, partindo da contextualização de um assunto presente no cotidiano dos educandos, o que justifica a escolha do tema principal do trabalho, dada a presença massiva dos códigos no mundo contemporâneo.

O desenvolvimento dessas propostas se deu através do aprofundamento na parte teórica acerca dos códigos, incluindo, para fins de ampliação do tema e contextualização, a Criptografia. O estudo desenvolvido — origem, usos primitivos, desenvolvimento, funcionalidade e evolução — contribuíram para uma compreensão global do tema, e possibilitaram o planejamento inicial das propostas, definindo as possibilidades pedagógicas de cada “subtema”, sendo eles a história dos códigos (incluindo a criptografia); o código de barras; e o código QR.

Essa etapa do trabalho promoveu reflexões importantes acerca do papel do docente no planejamento de propostas de ensino, pois os conteúdos que podem ser oferecidos por cada tema não se revelam sem um estudo cuidadoso e uma análise meticulosa. Para essa análise, a metodologia de pesquisa adotada foi fundamental, pois o trabalho se guiou através da Pesquisa Bibliográfica. Com o auxílio de produções literárias pertinentes, foi possível desenvolver os temas escolhidos à luz das recomendações educacionais e estudos teóricos de autores conceituados. As atividades foram elaboradas preocupando-se, principalmente, em atender duas exigências propostas: o trabalho com temas geradores e a Metodologia de Ensino-Aprendizagem-Avaliação de Matemática através da Resolução de Problemas, além, é claro, dos conteúdos didáticos presentes no Ensino Médio.

Dessa forma, através desse trabalho, foram propostas situações de aprendizagem articulando temas geradores apropriados para a realidade de alunos do Ensino Médio, possibilitando a abordagem de conteúdos necessários nessa etapa de ensino, atentando para o desenvolvimento de uma metodologia de ensino que ganha cada vez mais destaque e proporcionando ambientes de argumentação, investigação e criatividade. No desenvolvimento de todas as atividades há o empenho de possibilitar conexões entre a Matemática e outras áreas do saber, bem como temas atuais.

O processo de elaboração desse trabalho não foi isento de dificuldades. As mudanças causadas no ensino no ano de 2020 obrigaram que os rumos iniciais fossem alterados e, portanto, as propostas pedagógicas não puderam ser desenvolvidas em sala de aula, impossibilitando a observação e análise de suas possibilidades e limitações, diretamente com os alunos.. Uma inquietação constante em todas

as etapas foi a incerteza do nível de dificuldade das atividades, aliado ao tempo previsto de execução. Esses são fatores que poderiam ser aperfeiçoados através da prática na sala de aula, mas nesse trabalho ficaram restritos apenas às nossas suposições baseadas em experiências prévias e, portanto, podem apresentar inconsistências durante a aplicação.

Ademais, as propostas aqui apresentadas não devem ser entendidas como rígidas e finais, pelo contrário. Cada uma das propostas pode — e deve — ser vista como um *ponto de partida* para os conteúdos planejados, exigindo do professor a interpretação acerca das demandas de cada realidade escolar. Os próprios conteúdos pensados para cada atividade não caracterizam abordagens únicas, podendo ser desenvolvidos a partir de diferentes metodologias de ensino, tratamento e desenvolvimento nas aulas. Além disso, cada tema gerador conta com múltiplas alternativas de conceitos e conteúdos, mais uma vez delegando ao docente o trabalho de reflexão, escolha e análise dessas possibilidades, acordando com suas reivindicações.

Dessa forma, evidencia-se a potencialidade dos códigos como temas geradores, permitindo a exploração de propriedades aritméticas e algébricas, da História da Matemática, dos debates do papel das Ciências e Tecnologias nos avanços da sociedade e outros, dependendo da intenção e adaptação por parte de cada docente.

Por fim, o que se espera ao fim desse trabalho é que o leitor — especialmente os professores — sinta-se motivado para realizar as sugestões de atividades, apropriando das particularidades de cada necessidade pedagógica. Para os alunos que vivenciarem a prática, espera-se que o trabalho os auxilie a buscar objetos codificados e se aproximar a matemática abstrata a algo simples e agradável, para ser observado, compreendido e valorizado não apenas no contexto escolar, mas na vida, afinal, a Matemática está em *tudo*. Em tempo, esperamos que as propostas possam alcançar resultados positivos, de melhora no rendimento apresentado pelos alunos do Ensino Médio, sendo um aspecto incentivador e auxiliador no processo de ensino e aprendizagem de Matemática.

REFERÊNCIAS

- ALLEVATO, N. S. G.; ONUCHIC, L. D. L. R. Ensinando matemática na sala de aula através da resolução de problemas¹. **Boletim Gepem**, Rio de Janeiro, v. 33, n. 55, p. 133 – 156, 2009.
- ANDREOLA, B. A. O processo do conhecimento em paulo freire. **Educação e realidade**, Faced/UFRGS Porto Alegre, v. 18, n. 1, p. 32–34, 1993.
- BICUDO, M. A. V. A pesquisa em educação matemática: a prevalência da abordagem qualitativa. **Revista Brasileira de Ensino de Ciência e Tecnologia**, Paraná, v. 5, n. 2, 2012. Disponível em: <https://periodicos.utfpr.edu.br/rbect/issue/view/93>. Acesso em: 01 fev. 2021.
- BRASIL. Secretaria de Educação Fundamental. **Parâmetros Curriculares Nacionais Ensino Médio: Bases Legais**, Brasília, DF: MEC, 1998.
- BRASIL. Conselho Nacional de Educação. **Diretrizes Curriculares Nacionais da Educação Básica**, Brasília, DF: MEC, 2013.
- BRASIL. Ministério da Educação. **Base Nacional Comum Curricular: Ensino Médio**, Brasília, DF: MEC, 2018.
- CAMPUS CODE. **O cálculo do dígito verificador do CPF e do CNPJ**. 2020. Disponível em: <https://campuscode.com.br/conteudos/o-calculo-do-digito-verificador-do-cpf-e-do-cnpj/>. Acesso em: 01 fev. 2021.
- COSTA, J. de M.; PINHEIRO, N. A. M. O ensino por meio de temas-geradores: a educação pensada de forma contextualizada, problematizada e interdisciplinar. **Imagens da Educação**, v. 3, n. 2, p. 37–44, 2013.
- D’AMBROSIO, U. A história da matemática: questões historiográficas e políticas e reflexos na educação matemática. In: BICUDO, M. A. V. (Ed.). **Pesquisa em Educação Matemática: Concepções e Perspectivas**. São Paulo, SP: Editora UNESP, 1999. cap. 5, p. 97–115.
- D’AMBROSIO, U. A interface entre história e matemática: Uma visão histórico-pedagógica. **Revista história da matemática para professores**, Natal, v. 7, n. 1, p. 41 – 64, 2021. Disponível em: <http://rhmp.com.br/index/index.php/rhmp/article/view/137>. Acesso em: 01 jul. 2021.
- DENSO WAVE. **What is a QR Code?** 20–. Disponível em: <https://www.qrcode.com/en/about/>. Acesso em: 01 fev. 2021.
- DREXEL, U. **Barcode 60th Anniversary**. 2012. Disponível em: <https://drexel.edu/now/archive/2012/October/Barcode-60th-Anniversary/>. Acesso em: 01 fev. 2021.
- FIARRESGA, V. M. C. **Criptografia e matemática**. 2010. Lisboa, Portugal. 161 p. Tese (Mestrado) - Faculdade de Ciências, Universidade de Lisboa. Disponível em: <http://hdl.handle.net/10451/3647>. Acesso em: 01. fev. 2021.
- FINI, M. I. Controle dos códigos de identificação. **Revista do Professor - Atualidades, SEESP**, São Paulo, SP. 2 Ed., p. 70–75, 2009.
- FREIRE, P. **Pedagogia do oprimido**. Rio de Janeiro, RJ: Paz e Terra, 2011. 256 p.

- GARNICA, A. V. M. Pesquisa qualitativa e Educação (Matemática): de regulações, regulamentos, tempos e depoimentos. **Mimesis**, Bauru, v. 22, n. 1, p. 35–48, 2001.
- GIL, A. C. et al. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2002. v. 4. 175 p.
- GS1 BRASIL. **Código de barras: conheça sua história de evolução**. 2017. Disponível em: <https://blog.gs1br.org/codigo-de-barras-conheca-sua-historia-de-evolucao/>. Acesso em: 01 fev. 2021.
- GS1 BRASIL. **Como era o comércio antes do código de barras?** 2019. Disponível em: <https://blog.gs1br.org/comercio-antes-do-codigo-de-barra/>. Acesso em: 01 fev. 2021.
- KRASILCHIK, M. Reformas e realidade: o caso do ensino das ciências. **São Paulo em perspectivas**, São Paulo, v. 14, n. 1, p. 85–93, 2000.
- LAKATOS, E. M.; MARCONI, M. d. A. **Metodologia do Trabalho Científico**. São Paulo: Atlas, 2001. 219 p.
- LAW, C.; SO, S. QR Codes in Education. **Journal of Educational Technology Development and Exchange (JETDE)**, China, v. 3, n. 1, p. 85–100, 2010.
- LIMA, T. C. S. d.; MIOTO, R. C. T. Procedimentos metodológicos na construção do conhecimento científico: a pesquisa bibliográfica. **Revista Katálysis**, Florianópolis, v. 10, n. SPE, p. 37–45, 2007.
- MARCONI, M. d. A.; LAKATOS, E. M. **Fundamentos de Metodologia Científica**. 5. ed., São Paulo, SP: Atlas, 2003. 311 p.
- MICHAELIS. **Dicionário Brasileiro da Língua Portuguesa Michaelis**. 2015. Disponível em: <https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/codigo/>. Acesso em: 01 fev. 2021.
- MIGUEL, A. As potencialidades pedagógicas da história da matemática em questão: argumentos reforçadores e questionadores (primeira parte). **Zetetiké**, Campinas, v. 5, n. 2, p. 73–89, 2009. Disponível em: <https://periodicos.sbu.unicamp.br/ojs/index.php/zetetike/article/view/8646848>. Acesso em: 01 fev. 2021.
- MILIES, F. C. P. A matemática dos códigos de barras. **Revista do Professor de Matemática**, Rio de Janeiro, v. 65, p. 46–53, 2008. Disponível em: <https://www.rpm.org.br/cdrpm/65/9.html>. Acesso em: 01 jul. 2021.
- MILIES, F. C. P. A matemática dos códigos de barras: detectando erros. **Revista do Professor de Matemática**, Rio de Janeiro, v. 68, p. 38–42, 2009. Disponível em: <https://www.rpm.org.br/cdrpm/68/12.html>. Acesso em: 01 jul. 2021.
- NCTM. **Normas para o Currículo e a Avaliação em Matemática Escolar** - tradução portuguesa dos Standarts do National Council of Teachers of Mathematics. Lisboa, Portugal: Associação dos Professores de Matemática, Instituto de Inovação Educacional, 1991. 304 p.
- ONUCHIC, L. D. L. R.; ALLEVATO, N. S. G. Pesquisa em resolução de problemas: caminhos, avanços e novas perspectivas. **Bolema: Mathematics Education Bulletin**, p. 73–98, 2011.
- São Paulo, (Estado). Secretaria de Educação do Estado de São Paulo. **Currículo Paulista: Etapa Ensino Médio**, São Paulo, SP, p. 301, 2020.
- São Paulo, (Estado). Secretaria de Educação do Estado de São Paulo. **Currículo Paulista: Etapa Ensino Fundamental**, São Paulo, SP, p. 526, 2020.

SINGH, S. **O livro dos códigos**. 11. ed., Rio de Janeiro, RJ: Editora Record, 2020. 446 p.

SOUSA, D. P. **Dos Hieroglifos ao QR Code: Códigos como ferramenta na sala de aula**. 2016. 79 p. Tese (Mestrado) - Departamento de Ciências Exatas e Tecnológicas, Universidade Estadual do Sudoeste da Bahia. Vitória da Conquista, BA. 2016. Disponível em: http://www2.uesb.br/ppg/profmat/wp-content/uploads/2018/11/Dissertacao_DEIVISON_PORTO_DE_SOUSA.pdf. Acesso em: 01. fev. 2021.

TAKAHASHI, C. R. dos S. Ensinando matemática através dos códigos de barras. **Ciência e Natura**, Universidade Federal de Santa Maria, v. 37, n. 3, p. 278–288, 2015.

TOZONI-REIS, M. F. C. **Metodologia da Pesquisa**. 2. ed., Curitiba, PR: IESDE Brasil SA, 2009. 136 p.

WALLE, J. A. Van de. **Matemática no Ensino Fundamental: Formação de Professores e Aplicação em Sala de Aula**. 6. ed., Porto Alegre, RS: Penso Editora, 2009. 577 p.