Teoria dos números e criptografia: uma estratégia para o ensino e aprendizagem ativa da Matemática

NUMBER THEORY AND CRYPTOGRAPHY: A STRATEGY FOR TEACHING AND ACTIVE LEARNING IN MATHEMATICS

TEORÍA DE NÚMEROS Y CRIPTOGRAFIA: UNA ESTRATEGIA PARA LA ENSEÑAZA Y EL APRENDIZAJE ACTIVO EN MATEMÁTICAS

Daiane Soares Veras
Instituto Federal de Goiás (IFG)
daiane.veras@ifg.edu.br

Resumo

Este trabalho é fruto de uma análise sobre ações planejadas de forma a possibilitar ao aluno a oportunidade de processar, aplicar e compartilhar suas experiências como parte do processo educacional, a fim de trazer benefícios para a aprendizagem e despertar o interesse pela Matemática, apresentando uma estratégia de ensino e aprendizagem baseada em problemas gerados pelo tema criptografia. Apresentamos ainda os dados de pesquisa desenvolvida como parte de um projeto de iniciação científica do IFG – Câmpus Valparaíso, direcionada a professores que lecionam disciplinas da área de Ciências Exatas a alunos do curso de Licenciatura em Matemática e da educação básica, sobre o uso dessa estratégia, sua contribuição para o ensino e a aprendizagem da Matemática e sua aceitação por parte de alunos e professores. Os resultados sugerem que essa abordagem pode despertar o interesse dos alunos e trazer grandes benefícios para o ensino e a aprendizagem da Matemática.

Palavras-chave: criptografia. Ensino da Matemática. Aprendizagem por meio de problemas.

Abstract

This paper is the result of an analysis of planned actions in order to provide students with the opportunity to process, apply and share their experiences as part of the educational process, in order to bring benefits to learning and arouse interest in Mathematics, presenting a strategy of teaching and learning based on problems generated by the subject of cryptography. We also present research data developed as part of a scientific initiation project by the IFG - Campus Valparaíso, aimed at teachers who teach disciplines in the area of Exact Sciences to students of the Degree in Mathematics and of the basic education, on the use of this strategy, its contribution to the teaching and learning of Mathematics and its acceptance by students and teachers. The results suggest that this approach can arouse students' interest and bring great benefits to the teaching and learning of Mathematics.

Keywords: Cryptography. Teaching mathematics. Learning through problems.

Resumen

Este trabajo es el resultado de un análisis de acciones planificadas con el fin de brindar a los estudiantes la oportunidad de procesar, aplicar y compartir sus experiencias como parte del proceso

educativo, con el fin de traer beneficios al aprendizaje y despertar el interés por las Matemáticas, presentando una estrategia de enseñanza y aprendizaje basada en problemas generados por la asignatura criptografía. También presentamos datos de investigación desarrollada como parte de un proyecto de iniciación científica del IFG - Campus Valparaíso, dirigido a docentes que imparten disciplinas en el área de Ciencias Exactas a estudiantes de la Licenciatura en Matemáticas y de la educación básica, sobre el uso de esta estrategia, su aporte a la enseñanza y aprendizaje de las Matemáticas y su aceptación por parte de estudiantes y docentes. Los resultados sugieren que este enfoque puede despertar el interés de los estudiantes y aportar grandes beneficios a la enseñanza y el aprendizaje de las Matemáticas.

Palabras clave: Criptografía. Enseñanza de las Matemáticas. Aprendiendo a través de problemas.

Introdução

O esforço para modernizar as metodologias de ensino e assim, proporcionar aos alunos maiores possibilidades de aprendizagem e aperfeiçoamento da construção do seu conhecimento tem trazido a necessidade de muita pesquisa e atualização constante de professores e alunos. Contudo, a implementação de sistemas de ensino que são capazes de formar profissionais em sintonia com tempos de mudanças tecnológicas é um grande desafio no ensino da Matemática.

Quando uma disciplina não desperta o interesse dos alunos, e isso é bem recorrente no caso da Matemática, cabe ao professor procurar ferramentas para motivá-los e tornar o processo de ensino e aprendizagem prazeroso e efetivo. Para Haydt (1995, p. 145), o professor deve considerar, ao escolher uma técnica de ensino, os seguintes aspectos básicos:

> a) adequação aos objetivos estabelecidos para o ensino e a aprendizagem;
> b) a natureza do conteúdo a ser ensinado e o tipo de aprendizagem a efetivar-se;
> c) as características dos alunos, como, por exemplo, sua faixa etária, o nível de desenvolvimento mental, o grau de interesse, suas expectativas de aprendizagem;
> d) as condições físicas e o tempo disponíveis.

O perfil atual dos alunos exige novas metodologias, posturas pedagógicas diferenciadas e visões da relação ensino e aprendizagem mais consistentes. Nessa situação, a expressão "aprendizagem ativa", ou "métodos ativos de aprendizagem", vem recebendo atenção por constituir uma resposta possível às novas demandas educacionais (VILLAS-BOAS *et al.*, 2012).

Um conjunto de ações, ou eventos, planejados de forma que os participantes se sintam motivados a processar, aplicar, interagir e compartilhar suas experiências, como parte do processo educacional podem ser considerados metodologias ativas de ensino e aprendizagem. Assim, pode-se dizer que qualquer método instrucional que incorpore os estudantes no processo de aprendizagem, o que requer, portanto, que eles executem atividades significativas de aprendizagem e raciocinem sobre o que estão fazendo, é considerada uma aprendizagem ativa (VILLAS-BOAS *et al.*, 2012).

Numa perspectiva de formação integral e contínua de discentes e docentes, este trabalho foi motivado por experiências exitosas do uso da criptografia como tema gerador de problemas de Matemática básica, e propõe colaborar como um espaço de observação, avaliação e experimentação de práticas pedagógicas a partir da implantação de métodos ativos no ensino e aprendizagem de Matemática: a aprendizagem baseada em problemas relacionados às técnicas de criptografia.

Uma vez que há um número razoável de alunos que demonstram desinteresse por essa disciplina, sendo a dificuldade um dos principais fatores relatados pelos alunos que contribuem para esse desinteresse, incluir novas estratégias de ensino pode ser uma forma de motivá-los ou tornar a disciplina de Matemática mais interessante, possibilitando que alunos se tornem autônomos, criativos e protagonistas do próprio processo de aprendizagem.

Existem vários trabalhos enveredados pela análise do uso da criptografia no ensino de Matemática nos níveis de educação básica, por meio de exemplos de utilização prática dos conteúdos matemáticos do currículo base da Educação Básica como forma de visualização da amplitude dos caminhos matemáticos no processo de ensino e aprendizagem dentro do ambiente escolar, dentre os quais podemos citar as obras “criptografia e o currículo de Matemática no ensino médio” e “criptografia: um tema gerador para os conteúdos matemáticos no ensino fundamental”, das autoras Clarissa Olgin e Claudia Groenwald. Neste artigo abordaremos o ensino de Matemática por meio de problemas (Problem Based Learning/Aprendizagem Baseada em Problemas) relacionando as técnicas de envio de mensagens criptografadas com o ensino de funções. Tudo isso possui como principal ponto de ancoragem a construção de um significado mais amplo de alguns conteúdos matemáticos que muitas vezes são

apresentados de forma crua e sem nenhum atrativo que motive os alunos a desenvolverem conhecimentos em torno do que é ensinado.

Para finalizar, apresentaremos ainda o resultado de uma pesquisa realizada por meio de um questionário on-line respondido por alunos e professores, e desenvolvido como parte de um Projeto de Iniciação Científica, com a participação de três alunas do curso de Licenciatura em Matemática do IFG Campus Valparaíso, sob minha orientação. O objetivo desse questionário era avaliar a aceitação do tema criptografia como ferramenta para o ensino da Matemática entre alunos e professores. Com os dados coletados buscamos responder a perguntas como: o professor acha que o uso dessa metodologia ativa auxilia no processo de aprendizado dos alunos? Esse tipo de metodologia é capaz de despertar um maior interesse dos alunos pela Matemática?

1 Metodologias ativas e o favorecimento do aprendizado

Segundo Morán (2015), a maior parte do tempo – na educação presencial e a distância – ensinamos com materiais e comunicações escritos, orais e audiovisuais, previamente selecionados ou elaborados. São extremamente importantes, mas a melhor forma de aprender é combinando equilibradamente atividades, desafios e informação contextualizada. Desafios e atividades podem ser dosados, planejados, acompanhados e avaliados com apoio de tecnologias. Os desafios bem planejados contribuem para mobilizar as competências desejadas, intelectuais, emocionais, pessoais e comunicacionais.

Nas etapas de formação, os alunos precisam de acompanhamento de profissionais mais experientes para ajudá-los a tornar conscientes alguns processos, estabelecer conexões não percebidas, superar etapas mais rapidamente, confrontá-los com novas possibilidades. Quanto mais aprendamos próximos da vida, melhor (MORÁN, 2015). Neste contexto, as metodologias ativas são uma nova maneira de pensar o ensino tradicional. Isso porque um dos princípios da Base Nacional Comum Curricular (BNCC) é a promoção do aluno como protagonista de seu processo de ensino-aprendizagem. Assim, essas metodologias são ponto de partida para processos mais avançados de reflexão, integração cognitiva, generalização e reelaboração de novas práticas de ensino, de forma a incentivar os alunos a aprender de forma autônoma e participativa, a partir de problemas e situações

reais, fazendo com que eles estejam no centro do processo de aprendizagem, participando ativamente e sendo responsáveis pela construção de conhecimento.

O objetivo das atividades desenvolvidas nas instituições de ensino vai além da transmissão do conhecimento. O diferencial na formação do aluno é o desenvolvimento de capacidades como, por exemplo, autonomia, reflexão, criatividade, autoaprendizagem (aprender a aprender), pensamento estratégico – que possibilitem a inovação social e tecnológica. Desse modo, todos os envolvidos no processo de ensino e aprendizagem são considerados sujeitos da educação e podem contribuir para o desenvolvimento de soluções de problemas apresentados, tanto na escola quanto fora dela. As Metodologias Ativas de Aprendizagem favorecem este tipo processo de ensino e aprendizagem e podem corresponder às mudanças que o ensino vem necessitando.

Essas metodologias são revolucionárias porque promovem uma aprendizagem que é realizada de forma ativa, coletiva e colaborativa, utilizando diversos recursos e contribuindo para o aumento da qualidade do ensino, com professores mais articuladores e, claro, para a formação de alunos mais críticos, participantes e conscientes. É preciso refletir e registrar as experiências, em sala de aula/instituição de ensino, sobre as propostas das Metodologias Ativas de Aprendizagem, discutindo, avaliando, comparando, reinventando, exercitando a práxis educativa, e registrando os seus resultados para que seja efetiva a formação de cidadãos autônomos, criativos e críticos.

Em sua obra "A prática educativa: como ensinar", Antoni Zabala (1998) destaca que os conteúdos é que determinam os métodos, pois cada conteúdo exige o uso de determinados procedimentos mentais. Dessa forma, a escolha de qual metodologia utilizar vai de acordo com as especificidades de cada conteúdo.

1.1 A aprendizagem baseada em problemas

Freire (1997) afirmava que o educador precisa saber que "ensinar não é transferir conhecimento, mas criar as possibilidades para a sua produção ou a sua construção". Essa afirmação contrapõe-se ao tradicionalismo implementado pelas escolas, onde o professor, com sua experiência em áreas especificas, transmite este saber em aulas expositivas e pouco interativas. O processo tradicional de formação de conhecimento baseia-se apenas na orientação cognitiva, com teoria e prática repassada por um

professor, esse como principal agente, tornando assim o estudante, um agente passivo. Neste modelo não há incentivo, nem espaço, para desenvolver o autoaprendizado. A resolução de um problema deve ser encontrada em um padrão de informações compostas previamente para "facilitar" a aprendizagem. O método é desenvolvido em três etapas: formulação, resolução e discussão do problema.

Tratando-se de Matemática, em especial, "o ponto principal do processo de ensino e aprendizagem deve ser a abordagem de assuntos que despertem o interesse do aluno, estimulando a curiosidade e permitindo a construção de novos conhecimentos" (GROENWALD; FRANKE, 2007).

Em 2017, o Ministério da Educação publicou a BNCC (BRASIL, 2017), que define o conjunto de aprendizagens essenciais que os estudantes devem desenvolver ao longo da educação básica. De acordo com esse documento:

> No Ensino Médio a área de Matemática e suas Tecnologias tem a responsabilidade de aproveitar todo o potencial já constituído pelos estudantes no Ensino Fundamental para promover ações que ampliem o letramento matemático iniciado na etapa anterior. Isso significa que novos conhecimentos específicos devem estimular processos mais elaborados de reflexão e de abstração, que deem sustentação a modos de pensar que permitam aos estudantes formular e resolver problemas em diversos contextos com mais autonomia e recursos matemáticos. Para que esses propósitos se concretizem nessa área, os estudantes devem desenvolver habilidades relativas aos processos de investigação, de construção de modelos e de resolução de problemas.
> Para tanto, eles devem mobilizar seu modo próprio de raciocinar, representar, comunicar, argumentar e, com base em discussões e validações conjuntas, aprender conceitos e desenvolver representações e procedimentos cada vez mais sofisticados (BRASIL, 2017, p.528).

Assim, a aprendizagem baseada em problemas é capaz de promover o desenvolvimento de várias competências, principalmente as que envolvem raciocinar, além de proporcionar uma maior interação entre aluno e professores e construir uma visão integrada da Matemática, aplicada à realidade, em diferentes contextos.

2 A criptografia como tema gerador de problemas envolvendo conteúdos de Matemática básica

O artigo "Criptografia e o currículo de Matemática no Ensino Médio" apresenta o tema criptografia como motivador e gerador de situações didáticas que permitem o

aprofundamento da compreensão de conceitos matemáticos, possibilitando ao aluno perceber a utilização do conhecimento matemático em situações práticas, visando salientar a importância da utilização de atividades didáticas que possibilitem aos alunos resolver problemas, levantar hipóteses e trabalharem em grupo e cooperativamente (GROENWALD; OLGIN, 2011).

Outras pesquisas são enveredadas pela análise do uso da criptografia no ensino de Matemática nos níveis fundamentais e médio como exemplos de utilização prática dos conteúdos matemáticos do currículo da Educação Básica e como forma de visualização da amplitude dos caminhos matemáticos no processo de ensino-aprendizagem dentro do ambiente escolar (DANTAS, 2016).

De acordo com a professora Bini (2016), em sala de aula, o maior desafio enfrentado atualmente é conquistar os alunos para que sejam reais parceiros na construção do conhecimento. Portanto, o tema criptografia pode trazer inúmeras maneiras de abordar conteúdos de forma a atrair os alunos para esse processo construtivo dos conhecimentos matemáticos. A seguir detalharemos um pouco mais alguns exemplos desse tipo de abordagem, mas, antes disso, falaremos um pouco mais sobre a criptografia.

Primeiramente, vamos diferenciar criptografia de *Criptoanálise*. Segundo Coutinho (2000), em grego, *cryptos* significa secreto, oculto. A *criptografia* estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. É a arte dos "códigos secretos". Já a *Criptoanálise* é o processo inverso, a ciência que estuda as formas de se decifrar essas informações. Ambas sempre estiveram fortemente relacionadas à Matemática, em especial à Teoria dos Números, e o desenvolvimento de métodos mais sofisticados vem acompanhando os avanços dessa durante os séculos.

Durante a Segunda Guerra Mundial os alemães criaram uma máquina, chamada Enigma, para enviar mensagens de forma segura, indecifráveis pelos inimigos que tentassem interceptá-las. Este foi um grande passo para o avanço da criptografia. A Enigma foi decifrada por uma equipe inglesa, liderada pelo Matemático e Cientista da Computação Alan Turing. Nessa época a criptografia estava subordinada a fins militares, porém nos dias de hoje está fortemente

inserida no contexto das transações bancárias e comerciais entre computadores em rede. Tal mudança de contexto tornou necessária a criação de um novo conceito de criptografia, o da chave-pública, em contraste com a criptografia clássica, de chave-privada. Segundo Coutinho (2000, p.9):

> O mais conhecido dos métodos de criptografia de chave pública é o RSA. Este código foi inventado em 1977 por R. L. Rivest, A. Shamir e L. Adleman, que na época, trabalhavam no Massachussets Institute of Technology (M.I.T.), uma das melhores universidades americanas. As letras RSA correspondem às iniciais dos inventores do código. Há vários outros códigos de chave pública, mas o RSA continua sendo o mais usado em aplicações comerciais.

Para criptografar uma mensagem é necessário, antes, de uma etapa chamada pré-codificação. Para simplificar, utilizaremos um texto onde não há números, apenas palavras, e sem fazer distinção de letras maiúsculas e minúsculas e considerando o espaço entre as palavras. Na etapa de pré-codificação convertemos as letras em números usando a seguinte tabela de conversão:

Tabela 1 – Valor numérico de cada letra utilizada na etapa da pré-codificação

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
10	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
23	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**

Fonte: Elaborada pela autora.

O espaço entre duas palavras será substituído pelo número 99, quando for feita a conversão. Por exemplo, de acordo com a tabela acima, a frase ***"AMO APRENDER"*** seria convertida na sequência numérica ***10222499102527142313142 7.***

2.1 Criptografia no Ensino médio: uma experiência de ensino e aprendizagem

Em maio de 2019, ofereci uma oficina intitulada "Criptografia RSA", na programação da Semana de Integração Acadêmica do IFG – Câmpus Uruaçu. Cerca de 25 alunos dos cursos Técnicos Integrados ao Ensino Médio participaram das atividades propostas e a aceitação foi muito boa. Os alunos participaram ativamente do processo de construção dos conteúdos utilizando computadores conectados à internet e mesmo seus aparelhos celulares para auxiliar nos cálculos propostos. Esse tipo de abordagem está de acordo com a BNCC, que, além de destacar a importância da utilização de recursos tecnológicos e digitais para desenvolver o pensamento computacional dos alunos, prevê que:

> Novos conhecimentos devem estimular processos mais elaborados de reflexão e de abstração, que deem sustentação a modos de pensar que permitam aos estudantes formular e resolver problemas em diversos contextos com mais autonomia e recursos matemáticos (BRASIL, 2017, p.529).

A oficina começou com uma breve apresentação do que é a criptografia e onde ela é aplicada no nosso cotidiano. Para melhor compreensão das técnicas de Codificação e Decodificação, isto é, tornar uma mensagem ininteligível e, depois, ser capaz de recuperar a mensagem original, utilizamos um dos primeiros métodos criptográficos conhecidos historicamente: a Cifra de César. Essa cifra consiste basicamente em deslocar as letras do alfabeto três casas para a direita, conforme a Tabela 2:

Tabela 2 – Cifra de César

A	B	C	D	E	F	G	H	I	J	K	L	M
D	E	F	G	H	I	J	K	L	M	N	O	P
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Fonte: Elaborada pela autora.

Como exemplo, se aplicássemos a Cifra de César para Criptografar a palavra "**ESTUDAR**", obteríamos "**HVWXGDU**".

Após a familiarização com a Cifra de César, fizemos uma analogia com o processo de pré-codificação apresentado na seção anterior. Demonstramos para os alunos que aplicar a Cifra de César equivale a "somar 3" aos valores de cada letra da Tabela 1 e associar o resultado, outro número, à letra correspondente. Por exemplo: para descobrir qual a letra correspondente à letra "P" na Cifra de César, consultamos a Tabela 1 e vimos que a letra "P" está associada ao número 25. Somando-se 3 a esse número obtemos 28 que, de acordo com a mesma tabela, corresponde à letra "S", conforme a *Tabela 2*.

Vale ressaltar que o processo de criptografar uma mensagem não é apenas o ato de tornar uma mensagem ininteligível. No processo escolhido deve haver garantia de que é possível recuperar a mensagem original por meio da mensagem codificada, sem alterá-la. Desse modo, para o bom funcionamento do nosso método foi fundamental o fato de que para cada letra do alfabeto existia um único número correspondente a ela.

Essa observação vai ao encontro do conceito de funções. A chave de criptografia utilizada na Cifra de César nada mais é do que a função $f(x) = x + 3$, em que x assume um dos valores apresentados na Tabela 1. Esse conjunto de valores é chamado de Domínio da função e os resultados obtidos, também chamados de valor numérico da função, formam o conjunto Imagem.

Ao receber uma mensagem criptografada precisamos ser capazes de recuperar a mensagem original. Esse é o objetivo da *Criptoanálise*, que é a Ciência que estuda as formas de decifrar mensagens criptografadas.

Para facilitar a compreensão, suponha que tenhamos recebido uma mensagem com a palavra **"HVWXGDU",** criptografada com a Cifra de César. A princípio essa palavra não tem sentido nenhum. No entanto, podemos fazer uma analogia entre a *Criptoanálise* e a inversão de funções da seguinte maneira: primeiro precisamos transformar a mensagem recebida em números usando a pré-codificação (Tabela 1), conforme a Tabela 3.

Tabela 3 – Etapa de pré-codificação

H	V	W	X	G	D	U
17	31	32	33	16	13	30

Fonte: Elaborada pela autora.

Como vimos, a Cifra de César equivale a somar 3 aos valores da pré-codificação e, portanto, os números da tabela acima foram obtidos somando-se 3 aos valores das letras da palavra original. Isso nos leva a concluir que, para decifrar a mensagem acima, devemos subtrair 3 dos valores da tabela 3, e associar o resultado às letras da Tabela 1. Nesse raciocínio, após efetuarmos os cálculos $17 - 3 = 14, 31 - 3 = 28, \dots, 30 - 3 = 27$, obtemos a Tabela 4:

Tabela 4 – Etapa de decodificação

14	28	29	30	13	10	27
E	S	T	U	D	A	R

Fonte: Elaborada pela autora.

Em termos matemáticos, nada mais fizemos do que encontrar a função inversa de $f(x) = x + 3$, determinada por $f^{-1}(x) = x - 3$. Note que, para esse passo, foi fundamental o fato de que dois números distintos, no processo de pré-codificação, correspondem a duas letras distintas. Por esse motivo, podemos dizer que essa regra é injetora. Note ainda que, para cada número de 10 a 35, existe uma letra no alfabeto que corresponde a ele, de acordo com a Tabela 1, e por isso essa regra é também chamada de sobrejetora. Uma regra de associação (função) que é bem definida e é ao mesmo tempo injetora e sobrejetora, é chamada de bijetora.

Após a compreensão desses conceitos os alunos foram estimulados a enviar mensagens criptografas uns para os outros. Para isso, foi utilizada a função $f(x) = 2x + 3$ como chave de criptografia. O domínio da função continuou sendo o conjunto de valores da Tabela 1. Desse modo, para enviar as mensagens os alunos tiveram que calcular valor

numérico da função e, para decifrar as mensagens recebidas, precisavam encontrar a inversa da função que criptografou a mensagem, que equivale à chave de decriptação.

Note que, com essa abordagem, o estudo de funções se tornou algo interessante e atrativo para os alunos, promovendo a integração dos conteúdos, relacionando conceitos e proporcionando o aprendizado de forma interativa, já que os alunos trabalhavam pelo menos em duplas para a troca de mensagens.

2.2 Encaminhamentos Metodológicos

Para se desenvolver um trabalho metodológico significativo na sala de aula, os conteúdos propostos para os alunos da educação básica, em especial os do Ensino Médio, devem ser abordados de modo a explorar as competências Matemáticas elencadas na BNCC, por meio de tendências metodológicas que possibilitem a utilização de estratégias, conceitos e procedimentos matemáticos para interpretar situações em diversos contextos, sejam atividades cotidianas, sejam fatos das Ciências da Natureza e Humanas, das questões socioeconômicas ou tecnológicas, divulgados por diferentes meios, de modo a contribuir para uma formação geral, das quais destacamos :

- *Modelagem Matemática*: possibilita que os estudantes desenvolvam habilidades relativas aos processos de investigação, de construção de modelos e de resolução de problemas, conforme prevê a própria BNCC;
- *A resolução de problemas:* proporciona o desenvolvimento de competências que envolvem raciocinar. Para isso é necessário que os estudantes possam, em interação com seus colegas e professores, investigar, explicar e justificar as soluções apresentadas para os problemas, com ênfase nos processos de argumentação Matemática;
- *Utilização de instrumentos/mídias tecnológicas:* favorecem as experimentações Matemáticas ajudando na resolução de problemas e favorece o desenvolvimento do pensamento computacional;
- *Investigações Matemáticas:* explora as competências que estão diretamente associadas a representar e pressupõem a elaboração de registros para evocar um objeto matemático. Levam o aluno a formular conjecturas a

respeito do que está investigando e verificar qual a mais adequada, realizando provas e refutações; articulação de diferentes tendências.

Consideramos que o uso da criptografia como ferramenta de ensino explora as competências elencadas acima, mas, para além dela, podem ser utilizados diversos recursos didáticos e/ou tecnológicos como: jogos; calculadora, vídeos, softwares, Internet; livros didáticos, jornais, sólidos geométricos, quadro e giz, entre outros que podem variar de acordo com a realidade de cada ambiente escolar.

Com o objetivo de obter algumas informações sobre o tema "criptografia como ferramenta de ensino", foi elaborado um questionário com sete perguntas e mais um espaço para sugestões ou comentários. Essa pesquisa foi amplamente divulgada por meio da página do IFG/Valparaíso, como pode-se verificar pelo link: https://www.ifg.edu.br/component/content/article/190-ifg/campus/valparaiso/noticias-campus-valparaiso/19671-professor-voce-acredita-que-a-criptografia-pode-auxiliar-no-ensino-da-matematica-e-voce-aluno?highlight=WyJjcmlwdG9ncmFmaWEiXQ==. Além disso, contamos com a colaboração de professores que fizeram a divulgação por meio das suas salas das suas disciplinas na plataforma Moodle.

Devido ao objetivo da pesquisa, as perguntas foram mais direcionadas para o ensino, mas foram coletadas respostas tanto de professores quanto de alunos. Ao todo, 104 pessoas responderam ao questionário e esse formulário foi parte de um trabalho de Iniciação Científica intitulado "Teoria dos Números e a criptografia RSA" desenvolvido no IFG - Valparaíso, sob minha orientação, que contou com a participação de três alunas do Curso de Licenciatura em Matemática: Bruna da Costa Mesquita, como bolsista, Sabrina de Castro Pereira Lima e Laís dos Santos Souza, como voluntárias.

2.3 Análise e discussão dos dados obtidos no questionário

A seguir, apresentaremos alguns dos resultados obtidos na pesquisa citada no tópico anterior. Os dados coletados apresentados durante o 13º Seminário de Iniciação Científica e Tecnológica do IFG. Do total de participantes, 33 eram estudantes do Ensino Fundamental II e Médio, 35 professores de Matemática e 36 estudantes do ensino superior, conforme pode-se observar no Gráfico 1.

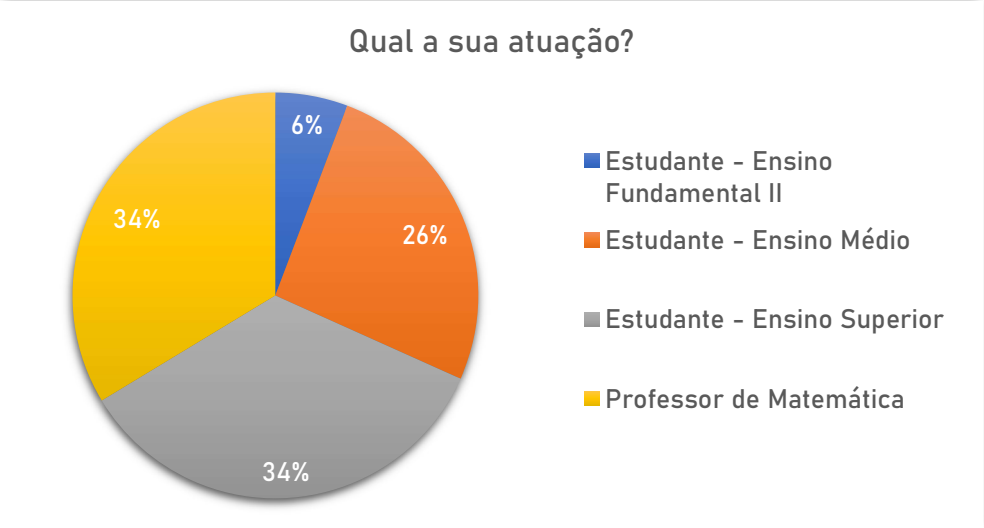

Gráfico 1 – Resultado da pesquisa "Teoria dos Números e a criptografia RSA" por questionário do Google Formulários

Fonte: Elaborado pela autora.

Buscamos entender, do ponto de vista do aluno e do professor, qual a relevância desse tipo de aplicação no ensino e aprendizagem da Matemática, visto que essa ferramenta pode ajudar o aluno a "visualizar" melhor alguns conceitos matemáticos até então puramente abstratos. De acordo com Duval, "não há entendimento sem visualização. E é por isso que a visualização não deve ser reduzida à visão, ou seja: a visualização torna visível tudo o que não é acessível à visão." (DUVAL, 1999, p. 13).

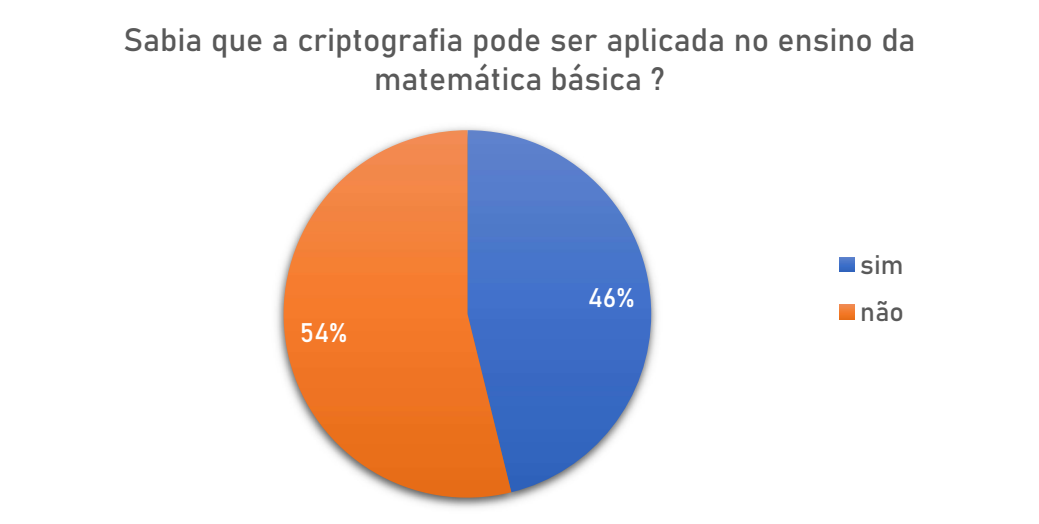

Gráfico 2 – Resultado da pesquisa "Teoria dos Números e a criptografia RSA" por questionário do Google Formulários

Fonte: Elaborado pela autora.

Como podemos observar no Gráfico 2, mais da metade dos respondentes não sabiam que a criptografia pode ser utilizada como ferramenta de ensino da Matemática básica. Esse resultado pode sugerir que há uma demanda emergente no campo da formação continuada de professores da Educação Básica. As lacunas que existem no campo do conhecimento da Matemática podem fazer com que grande parte dos professores se sinta inseguros quanto à sua prática pedagógica, limitando-os ao uso do livro didático como ferramenta de ensino e impedindo-os de explorar novas metodologias mais dinâmicas.

Vários debates relacionados à qualidade da Educação Básica no Brasil têm abordado o conhecimento matemático do professor, constatando-se que formação continuada é um aspecto fundamental na sua carreira, tendo em vista a necessidade de que esse profissional esteja constantemente em processo de atualização para desenvolver sua prática pedagógica. Assim, o que o professor aprende em sua formação acadêmica inicial não pode ser considerado como objeto final a ser usado em sala de aula. O conhecimento está em constante evolução e as formas de ensinar devem acompanhar estas mudanças.

Os diferentes tipos de conhecimento do conteúdo necessários à prática docente são classificados por Shulman (1986) ao desenvolver o "knowledge base for teaching" (base de conhecimentos para o ensino), a saber, o conhecimento do conteúdo, do curricular, do pedagógico, do conteúdo, do cognitivo dos estudantes, entre outros. O conhecimento integra, além da capacidade do professor de apresentar aos estudantes as verdades aceitas na área, a capacidade de explicar o porquê de um determinado resultado ser considerado verdadeiro, como ele se relaciona com outros resultados ou porque é pertinente conhecê-lo (CARVALHO *et al.*, 2019).

Além disso, conforme Carvalho et al. (2019), a formação de professores é um processo complexo iniciado na sua formação durante a graduação, refletido ou não no desenvolvimento profissional, concretizado, desenvolvido e significado em sala de aula a partir das inúmeras experiências advindas do ambiente escolar, e os conhecimentos construídos ao longo dessa trajetória são determinantes para o ensino e aprendizagem dos estudantes.

No formulário mostramos como relacionar criptografia ao estudo de funções por meio do seguinte exemplo: "Para comunicar-se de forma secreta, um mensageiro e seu amigo decidiram usar uma função $f(x) = 2x + 1$ para cifrar as mensagens e construíram

uma tabela para codificar cada palavra, de acordo com a qual $A = 0, B = 1, C = 2, D = 3, E = 4, F = 5$. O mensageiro deseja enviar a palavra "FÉ". Sabendo que $F = 5, E = 4$ e utilizando a função escolhida para codificar a mensagem temos: $f(5) = 2 \cdot 5 + 1 = 11$ e $f(4) = 2 \cdot 4 + 1 = 9$. Pronto! A palavra "FE", criptografada, será representada por 11 - 9. Seguindo esse mesmo raciocínio você consegue criptografar a palavra CAFE?"

Os resultados apresentados nos gráficos a seguir sugerem que o exemplo é de fácil assimilação e reprodução.

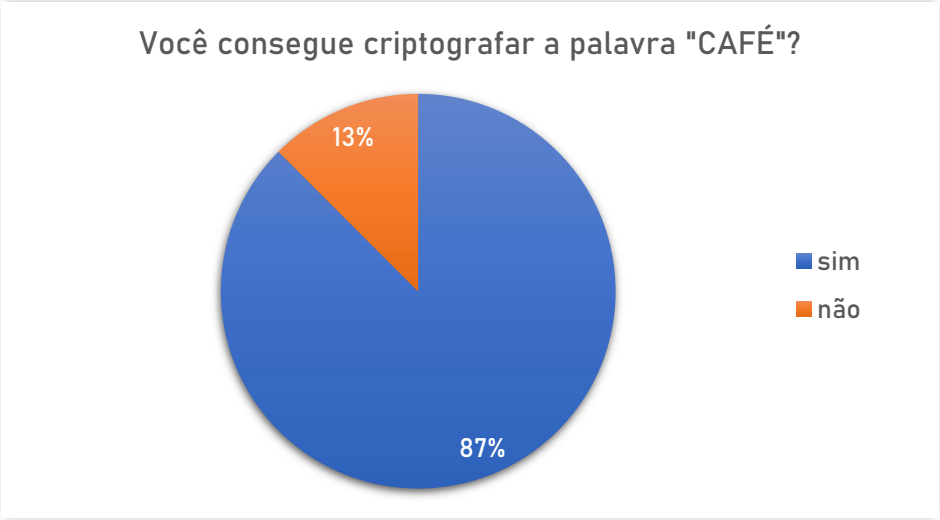

Gráfico 3 – Resultado da Pesquisa "Teoria dos Números e a criptografia RSA" por questionário do Google Formulários

Fonte: Elaborado pela autora.

De acordo com os dados do gráfico acima podemos notar que os alunos foram capazes de reproduzir um raciocínio matemático que foi apresentado na forma de um problema contextualizado. Esse tipo de abordagem favorece o aprendizado, uma vez que, de acordo com Cifuentes (2005, p. 66):

> Contextualizar [no sentido de identificar o contexto de] um objeto é dar um referencial espaço temporal ao objeto, de modo que, do ponto de vista estético, o contexto passa a formar parte do próprio objeto como sugerido por Aristóteles, embora a "realidade" do contexto possa ser diferente da realidade do objeto.

Vale ressaltar que, além da contextualização, trazendo para o aluno um problema "real", com esse tipo de abordagem o professor pode ainda apresentar o conceito de modelagem matemática, uma alternativa pedagógica para o ensino e aprendizagem da Matemática. Segundo Bassanezi (2002, p. 16), modelagem matemática pode ser entendida

como “a arte de transformar problemas da realidade em problemas matemáticos e resolvê-los, interpretando suas soluções na linguagem do seu contexto de origem”.

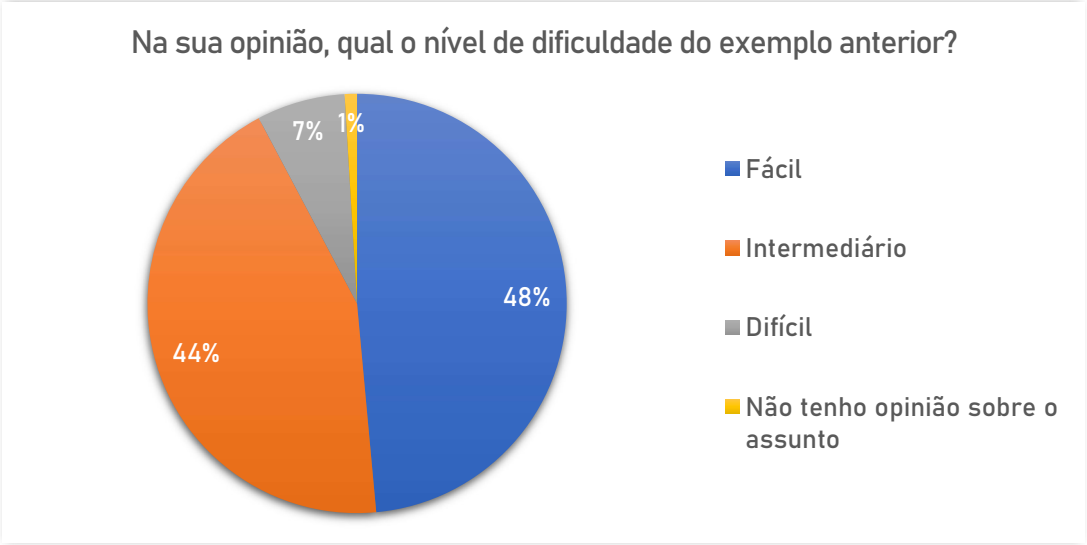

Gráfico 4 – Resultado da Pesquisa “Teoria dos Números e a criptografia RSA” por questionário do Google Formulários

Fonte: Elaborado pela autora.

Para finalizar a pesquisa perguntamos sobre o nível de interesse sobre esse tipo de abordagem em sala de aula, tanto por parte dos alunos quanto dos professores, e o resultado pode ser observado no gráfico a seguir.

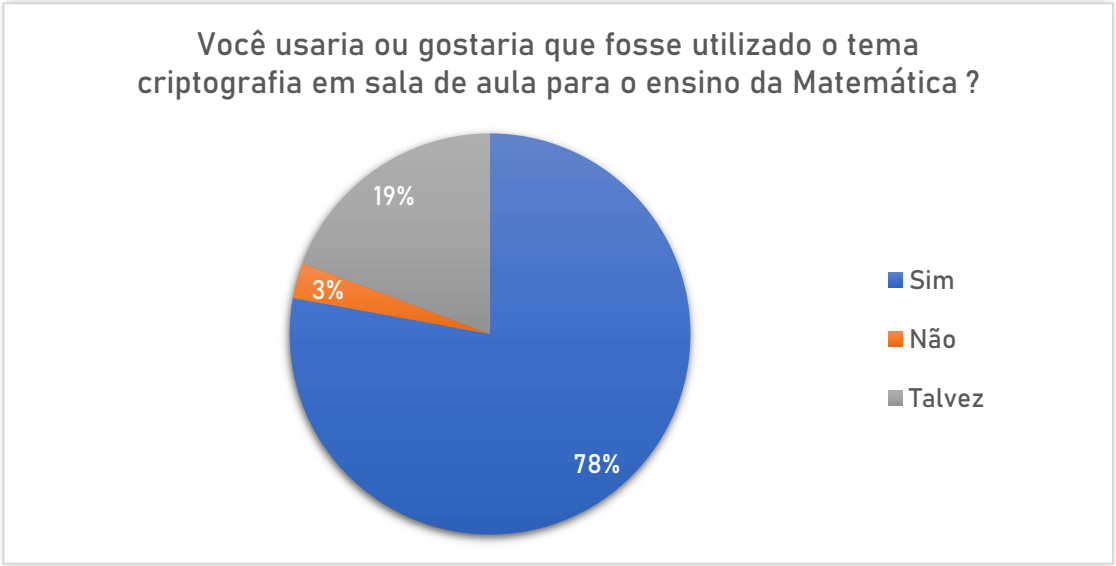

Gráfico 6 – Resultado da Pesquisa “Teoria dos Números e a criptografia RSA” por questionário do Google Formulários

Fonte: Elaborado pela autora.

Como podemos observar, 78% responderam que utilizaria essa abordagem em sala de aula ou gostaria que ela fosse utilizada. Isso nos mostra que abordagem pode despertar o interesse de alunos e professores, estimulando a curiosidade e permitindo a construção de novos conhecimentos (GROENWALD e FRANKE, 2007) e colocando a Matemática com um caráter integrador junto às demais Ciências, o que vai ao encontro do que diz a BNCC.

Considerações finais

Além do conhecimento do professor, o uso de ferramentas e metodologias capazes de tornar o aluno sujeito da educação pode contribuir para o seu desenvolvimento, tanto na escola quanto fora dela. Assim, o uso metodologias ativas de ensino e aprendizagem, como abordagem de conteúdos de Matemática básica por meio de conceitos relacionados à criptografia, podem favorecer este tipo processo de ensino e aprendizagem e, quem sabe, integrar as mudanças que o ensino vem necessitando.

Como um espaço de observação, avaliação e experimentação de práticas pedagógicas a partir da implantação de métodos ativos no ensino e aprendizagem de Matemática, motivado por experiências exitosas com aprendizagem baseada em problemas relacionados às técnicas de criptografia, este trabalho tem uma perspectiva de contribuir com a formação integral e contínua de docentes e tentar atrair a atenção dos discentes, uma vez que é grande o número de alunos que demonstram desinteresse pela Matemática.

É importante observar que as respostas obtidas no questionário sobre o uso da criptografia como instrumento de ensino e aprendizagem não determinam uma conclusão precisa, visto que existe um distanciamento (físico e social) entre os respondentes que deve ser considerado e que um recurso/instrumento de trabalho pedagógico pode não ser tão atraente em um primeiro momento e depois passar a ser. Em geral, o bom aproveitamento desses recursos está relacionado com o nível de entusiasmo do aplicador, que muitas vezes, pela própria escassez de condições adequadas em sala de aula, não se sentem estimulados para aplicar novas

metodologias e preferem manter a forma corriqueira com que tratam o processo de ensino e aprendizagem.

Vale destacar que há uma pressão intensa para que Escolas e IES (Instituições de Ensino Superior) sejam mais atraentes, mais flexíveis, com currículos mais atualizados, muito mais centrados na experimentação, em competências e valores, combinando os espaços físicos e digitais. Há também um movimento de transformação no Brasil, com resultados muito díspares: escolas muito interessantes ao lado de outras bastante convencionais. No entanto, sabemos que as mudanças dependem de políticas públicas educacionais nacionais consensuadas e coerentes, com diretrizes claras e ações para valorização de escolas, gestores, docentes e alunos e adaptadas regional e localmente (MORÁN, 2020).

Por fim, a importância do papel do professor de Matemática na sala de aula é amplamente reconhecida e, apesar das diferenças culturais, econômicas e geográficas existentes em cada ambiente de ensino, é consensual o reconhecimento da necessidade de melhorar a qualidade dos recursos educacionais nas escolas.

Referências

BASSANEZI, R. C. *Ensino-aprendizagem com modelagem Matemática*: uma nova estratégia. São Paulo: Contexto, 2002.

BINI, M. B. Carta código: uma atividade para a sala de aula. *Revista do professor de Matemática*, n. 76, 2016.

BRASIL. *Base Nacional Comum Curricular.* Brasília: MEC, 2017. Disponível em: http://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf Acesso em: 8 jul. 2021.

CARVALHO, R. O. *et al*. O conhecimento matemático como fator determinante no ensino e na aprendizagem: percepções de professores brasileiros que ensinam Matemática. *In*: CONFERENCIA INTERAMERICANA DE EDUCACIÓN MATEMÁTICA, 15., 2019, Medellin. *Anais* [...]. Medellin, Colombia: Universidad de Medellin, 2019.

CIFUENTES, J. C. Uma via estética de acesso ao conhecimento matemático. *Boletim GEPEM*, v. 46, 55-72, 2005.

COUTINHO, S. C. *Números inteiros e criptografia RSA*. 2.ed. Rio de Janeiro: IMPA, 2000.

DANTAS, A. A. *A criptografia no Ensino Fundamental e Médio*. Trabalho de Conclusão de Curso (Especialização em Matemática para o Ensino Médio) – Universidade Federal do Rio Grande do Norte, Caicó, 2016.

DUVAL, R. Representation, vision and visualization: Cognitive functions in mathematical thinking. Basic issues for learning. *In*: NORTH AMERICAN CHAPTER OF THE INTERNATIONAL GROUP FOR THE PSYCHOLOGY OF MATHEMATICS EDUCATION, 21., 1999, Morelos. *Proceedings* [...]. Morelos, 1999. p. 3-26.

FREIRE, P. *Pedagogia da autonomia*: saberes necessários à prática educativa. São Paulo: Paz e Terra, 1997.

GROENWALD, C. L. O.; FRANKE, R. F. Currículo de Matemática e o tema criptografia no Ensino Médio. *Educação Matemática em Revista*, n. 8, p. 51-57, 2007.

GROENWALD, C. L. O. OLGIN, C. de A. Criptografia e o currículo de Matemática no Ensino Médio. *Revista de Educação Matemática*, v. 13, n. 15, p. 69-78, 2011.

HAYDT, R. C. *Curso de didática geral*. 2. ed. São Paulo: Ática, 1995.

MORÁN, J. *Educação trasnformadora*: como acelerar mudanças na educação. 2020. Disponível em: http://www2.eca.usp.br/moran. Acesso em: 8 jul. 2021.

MORAN, J. Mudando a educação com metodologias ativas. *In*: SOUZA, C. A. de; MORALES, O. E. T. (org.). *Convergências midiáticas, educação e cidadania*: aproximações jovens. Ponta Grossa: Foca Foto-PROEX/UEPG, 1995.

OLGIN, C. de A.; GROENWALD, C. L. O. Criptografia: um tema gerador para os conteúdos matemáticos no ensino fundamental. *In*: SEMINÁRIO INTERNACIONAL DE PESQUISA EM EDUCAÇÃO MATEMÁTICA, 5., 2012, Petrópolis. *Anais* [...]. Brasília: SBEM, 2012. Disponível em: http://sbem.iuri0094.hospedagemdesites.ws/files/v_sipem/PDFs/GT02/CC00720610060_A.pdf Acesso em: 8 jul. 2021.

PRINCE, M. J; FELDER, R. M. Inductive Teaching and Learning Methods: Definitions, Comparisons, and Research Bases. *Journal of Engineering Education*, 2006.

SHULMAN L. S. Those who understand: knowledge growth in teaching. *Educacional Researcher,* v. 15, n. 2, p. 4 -14, 1986.

VILLAS-BOAS, V. *et al.* Aprendizagem ativa na educação em engenharia. *In*: *Desafios da educação em Engenharia:* vocação, formação, exercício profissional, experiências metodológicas e proposições. Brasília, DF: Abenge, 2012.

ZABALA, A. *A prática educativa*: como ensinar. Trad. Ernani F. da F. Rosa. Porto Alegre: ArtMed, 1998.