Matemática: Ciência e Aplicações 3

Annaly Schewtschik
(Organizadora)

Atena Editora
Ano 2019

Annaly Schewtschik
(Organizadora)

Matemática: Ciência e Aplicações 3

Atena Editora
Ponta Grossa - 2019

Editora Chefe: Profª Drª Antonella Carvalho de Oliveira
Diagramação e Edição de Arte: Lorena Prestes e Geraldo Alves
Revisão: Os autores

Dados Internacionais de Catalogação na Publicação (CIP)
(eDOC BRASIL, Belo Horizonte/MG)

M376 Matemática: ciência e aplicações 3 [recurso eletrônico] / Organizadora Annaly Schewtschik. – Ponta Grossa (PR): Atena Editora, 2019. – (Matemática: Ciência e Aplicações; v. 3)

Formato: PDF
Requisitos de sistema: Adobe Acrobat Reader
Modo de acesso: World Wide Web
Inclui bibliografia.
ISBN 978-85-7247-123-7
DOI 10.22533/at.ed.237191402

1. Matemática – Estudo e ensino. 2. Professores de matemática – Prática de ensino. I. Schewtschik, Annaly. II. Série.

CDD 510.7

Elaborado por Maurício Amormino Júnior – CRB6/2422

APRESENTAÇÃO

A obra "Matemática: ciências e aplicações" aborda uma série de livros de publicação da Atena Editora publicado em três volumes. O Volume III em seus 27 capítulos apresenta resultados de pesquisas que trataram dos diferentes recursos que podem ser utilizados para o ensino e a aprendizagem da matemática, assim como na formação de professores.

Os trabalhos evidenciam inferências sobre as experiências de uso de recursos manipuláveis, didáticos, paradidáticos e tecnológicos incluindo softwares, na Educação Básica e no Ensino Superior. Veremos entre os recursos didáticos: mapas conceituais e o uso de livros didáticos; os paradidáticos: o uso de Edições Especiais de Paradidáticos de Matemática, Anuais e Manuais promovidas por diferentes entidades, inclusive religiosas; o tecnológico: criptografias, softwares educativos de geometria, programação computacional, aplicativos e redes sociais; e, os manipuláveis: uso de diferentes jogos e dobraduras na aprendizagem da matemática.

A Matemática como Ciência é pensada nos trabalhos que enfocam os objetos matemáticos no contexto de aprendizagem, e como aplicações do conhecimento matemático ligados ao uso de diversos recursos, principalmente no que diz respeito aos recursos tecnológicos.

A Educação Matemática é revelada nas análises referente as práticas de sala de aula – contanto com discussões inclusivas, enfatizando o uso de recursos para o ensino e a aprendizagem, tanto na Educação Básica como na Educação Superior.

Este volume é direcionado para todos os educadores que acreditam que a matemática poder ser ensinada a partir de diversos recursos, contribuindo para uma aprendizagem bem mais prazerosa.

Annaly Schewtschik

SUMÁRIO

CAPÍTULO 7

CRIPTOGRAFIA E SUAS POTENCIALIDADES NA EXPLORAÇÃO DAS IDEIAS ASSOCIADAS À FUNÇÃO AFIM

Beatriz Fernanda Litoldo
Universidade Estadual de Campinas – UNICAMP (Brasil)
Rio Claro – São Paulo

Arlete de Jesus Brito
Universidade Estadual Paulista – UNESP (Brasil)
Rio Claro – São Paulo

RESUMO: O objetivo desse texto é apresentar alguns resultados advindos de uma pesquisa de mestrado que buscou evidenciar as potencialidades que uma sequência pedagógica de tarefas envolvendo problemas de Criptografia pode proporcionar durante seu desenvolvimento. Na investigação buscamos compreender em que uma sequência pedagógica de tarefas de caráter criptográfico auxilia os alunos na exploração das ideias associadas à função afim. Alguns dos resultados apontaram o desenvolvimento de atitudes autônomas sobre os próprios processos de aprendizagem por parte dos alunos. As tarefas possibilitaram que eles assumissem posturas mais investigativas, o que propiciou a criação de diferentes estratégias e etapas de resolução e refletiu nas explorações e investigações realizadas por eles acerca das ideias associadas ao conceito de função afim, bem como as maneiras que os alunos organizavam e exteriorizavam tais ideias. Assim, conclui-se que esse tipo de tarefa contribuiu para que os alunos adquirissem atitudes ativas e indagativas em seus procedimentos de resolução, incidindo na exploração do conceito de função afim.

PALAVRAS-CHAVE: Educação Matemática; Ensino Médio; Cifras; Sequência Pedagógica; Criptoanálise.

ABSTRACT: The purpose of this text is to present some results from a master's research that sought to highlight the potentialities that a pedagogical sequence of tasks involving Cryptography problems can provide during its development. The objective of the investigation was to try to understand in which a pedagogical sequence of tasks of cryptographic character assists the students in the exploration of the ideas associated with the related function. Some of the results pointed to the development of autonomous attitudes about students' own learning processes. The tasks enabled them to take on more investigative positions, which led to the creation of different strategies and stages of resolution and reflected in the explorations and investigations carried out by them on the ideas associated with the concept of related function, as well as the ways the students organized and exteriorized such ideas. Thus, it is concluded that this type of task contributed to the students acquiring active and questioning attitudes in their resolution procedures, focusing

on the exploration of the concept of related function.

KEYWORDS: Mathematics Education. High school. Cipher. Pedagogical Sequence; Cryptanalysis.

1 I INTRODUÇÃO

Os Parâmetros Curriculares Nacionais para o Ensino Médio – PCNEM (BRASIL, 2000) e a Base Nacional Comum Curricular – BNCC (BRASIL, 2018) destacam em suas ementas a necessidade de se buscar alternativas metodológicas variadas para o ensino e aprendizagem da Matemática. O trabalho com a resolução de problemas é uma das estratégias de ensino destacadas por esses documentos como sendo um dos possíveis processos matemáticos pelos quais os alunos constroem a aprendizagem (BRASIL, 2000; BRASIL, 2018).

Ambos os documentos, citados acima, tecem orientações a respeito da importância do trabalho do professor quanto ao planejamento das atividades. Promover aos alunos tarefas que proporcionam problemas desafiadores que podem partir de problemas estimulantes e contextualizados em situações de investigação. Tais atividades podem desencadear situações desafiadoras que os alunos se sintam motivados e encorajados a realizar. Aulas que favoreçam o desenvolvimento da curiosidade, da imaginação e do processo de investigação, contextualizadas sempre que possível, contribuem para a formação das visões da matemática, da sociedade e do mundo BNCC (BRASIL, 2018).

Buscando situações em que é possível desenvolver tarefas nesse sentido, recorremos ao tema Criptografia. Considerando que essa temática tem como principal característica de não ser dependente de um único método de decifração de uma mensagem, tarefas envolvendo problemas criptográficos possibilitam um leque de possibilidades de estratégias de resolução, além de despertar a curiosidade e as atitudes investigativas dos alunos. Groenwald, Franke e Olgin (2009) destacam que a utilização dos recursos de cifração e decifração dispostos pelo tema Criptografia a configura como sendo um agente motivador e gerador de situações didáticas que permitem o "aprofundamento da compreensão dos conceitos matemáticos, possibilitando ao aluno perceber a utilização do conhecimento matemático em situações práticas" (GROENWALD, FRANKE E OLGIN, 2009, p. 42). Corroborando as ideias de Groenwald, Franke e Olgin (2009), Fiarresga (2010) destaca que esse tema permite ao professor elaborar problemas que busquem desenvolver nos alunos capacidades de concentração e persistência em relação a problemas matemáticos, além de estimular a vontade de estudar matemática e de colaborar para o desenvolvimento de diferentes estratégias para a resolução das tarefas.

Fincatti (2010) e Groenwald e Olgin (2011) também tecem considerações sobre a possibilidade de contextualização desse tema em sala de aula, partindo da concepção de que a Criptografia está presente no cotidiano da sociedade, por exemplo, nas atividades *on-line*, como compras e vendas, transações bancárias, auditorias eletrônicas, senhas de e-*mail*, de *Facebook*, dentre outras. Munido com as ideias de cifração e decifração –transformações de origem matemática ou não, utilizada para se modificar uma mensagem, advindos da Criptografia e da Criptoanálise (SINGH, 2008) – o professor dispõe, então, de várias possibilidades de elaboração de tarefas que concatenam alguns dos conteúdos matemáticos permeados pelos padrões e regras de codificação e decodificação, por exemplo, números pares e ímpares, sequência numérica e funções, buscando, sempre em última instancia, o aprendizado dos alunos (OLGIN; GROENWALD, 2011; TAMAROZZI, 2001).

Em nossas investigações, objetivamos buscar reflexões sobre as possíveis possibilidades de utilizar o tema Criptografia aliado ao conceito de função afim. Para atingir tal objetivo, desenvolvemos um material didático na forma de uma sequência pedagógica de tarefas envolvendo problemas criptográficos. Posto isso, analisamos suas potencialidades para explorar as ideias associadas ao conceito de função afim. Esse texto tem como finalidade apresentar alguns dos resultados advindos dessa pesquisa.

2 I A CONCEPÇÃO CONSTRUTIVISTA E A RESOLUÇÃO DE PROBLEMAS

Na concepção construtivista, a aprendizagem do aluno é mediada pela representação pessoal sobre o objeto ou conteúdo a ser aprendido e pela construção dos conceitos por meio de espaços de aprendizagens significativos (SOLÉ; COLL, 2009). As representações construídas pelos próprios alunos fazem parte do desenvolvimento deles à mediada que elas auxiliam nas organizações, exteriorizações e compreensões relacionadas às ideias matemáticas (PONTE; SERRAZINA, 2000). Independente das representações serem mais ou menos sofisticadas, Ponte e Serrazina (2000) afirmam que, a partir delas, podem derivar situações valiosas uma vez que “apoiam a compreensão e solução de problemas, fornecem formas significativas de registro de um método ou de uma solução e fornecem um ponto de partida do qual os alunos podem desenvolver uma apreciação de outras representações” (PONTE; SERRAZINA, 2000, p. 43).

O suporte aos novos conteúdos, representados por meio dos diversos tipos de linguagens estão fundamentados sobre experiências matemáticas, os conhecimentos prévios e as disposições e ações entre os alunos e o professor (SOLÉ; COLL, 2009). Durante o envolvimento do aluno com os novos conteúdos matemáticos estudados, seus significados e conhecimentos matemáticos anteriores podem assumir dois processos: ou eles se mantêm, servindo como embasamento para a interpretação do “novo”, ou se modificam, considerando que o “novo” realmente requer alterações quanto aos novos significados e conhecimentos das informações apresentadas.

Solé e Coll (2009) afirmam que no segundo processo, "não só modificamos o que já possuímos, mas também interpretamos o novo de forma peculiar, para poder integrá-lo e torná-lo nosso" (SOLÉ; COLL, 2009, p. 20).

A concepção construtivista, parte do pressuposto que o ensino e a aprendizagem estão imbricados por processos conjuntos e compartilhados entre alunos e professor, sendo eles dispostos e fundamentados na e para a construção do conhecimento por meio da mediação do professor, que por sua vez, exerce papel importante no desenvolvimento dos aspectos de competência e autonomia dos alunos na resolução das tarefas, focando sempre a aprendizagem dos conteúdos matemáticos abordados.

Nesse sentido, consideramos que a construção de significados, por parte do aluno, na aprendizagem está relacionada com aspectos que envolvam sentimentos e crenças sobre sua competência e pro atividade, autoestima e de respeito mútuo, além da concatenação com o desenvolvimento e a exploração do domínio das representações e procedimentos, a criação, aceitação e negociação de atitudes e da compreensão de determinados conceitos matemáticos.

Considerando a teia de conexões que se estabelece entre os procedimentos, atitudes e conceitos em uma perspectiva construtivista, tem-se em consideração o ato de aprender dos alunos imersos em suas próprias relações de aprendizagem, fundamentados em seus próprios conhecimentos, e das relações de ensino entre o professor, em uma situação que considera o aluno como o centro da intervenção (MAURI, 2009, LITOLDO, 2016). As relações de aprendizagem interligam tanto conceitos, quanto procedimentos e atitudes.

Relativamente aos conceitos, Mauri (2009) destaca que os conhecimentos conceituais prévios, quando são organizados e oportunos, propiciam a concatenação entre os conhecimentos anteriores com as novas informações. Concernente aos procedimentos, a autora considera que o conjunto de técnicas, regras, algoritmos, habilidades motoras e cognitivas, bem como as estratégias de resolução devem possibilitar ao aluno a capacidade de "realizar ou executar, em algum grau, as operações de procedimentos necessárias para lograr a meta proposta e, também, possuir uma representação ou ideia do procedimento em si mesmo" (MAURI, 2009, p. 111).

Os procedimentos são considerados processos a serem utilizados para se resolver um problema, podendo eles se modificarem a cada situação (ECHEVERRÍA; POZO, 1998). Os procedimentos, atrelados às etapas de resolução, se fazem presentes ao aluno à mediada em que ele busca caminhos para resolver o problema –, na retomada de conceitos anteriores, na organização e explicação desses conhecimentos para os colegas e professor, na construção dos novos conhecimentos e na autonomia no próprio processo de aprendizagem (ECHEVERRÍA; POZO, 1998; MAURI, 2009).

A ação atuante e investigativa do aluno em seu próprio processo de aprendizagem tem relações muito próximas com o tempo e as condições propiciadas a eles para a resolução das tarefas propostas –, a exploração de seus conhecimentos prévios, a liberdade de investigação relacionada aos seus próprios procedimentos e o espaço aberto para o compartilhamento de ideias (PONTE; BROCADO; OLIVEIRA, 2009). Esses quesitos se refletem na independência e pro atividade do aluno, ocasionando espaços coletivos interessantes, à mediada em que os alunos desenvolvem trabalhos em grupo, momento importante em que expressam suas opiniões e ideias. O trabalho em grupo contribui para a construção e organização de outras ideias e procedimentos incidindo no desenvolvimento de sua autonomia (ECHEVERRÍA; POZO, 1998; MAURI, 2009). Portanto, considerando os alunos como construtores ativos de seus próprios conhecimentos, para a aprendizagem de conceitos, é necessário que os procedimentos e as atitudes sejam trabalhados e desenvolvidos, não em contextos disjuntos, mas sim em tarefas que explorem e construam significados para cada um desses elementos.

Desse modo, para que os alunos possam ser protagonistas de suas aprendizagens, é importante proporcionar-lhes contextos em que explorem a resolução de problemas, visto que tais cenários possibilitam aos alunos aulas diferenciadas, nas quais eles investigam o problema e seus diferentes procedimentos de resolução. Sobre a resolução de problemas, Ponte e Serrazina (2000) afirmam que essa metodologia possibilita desenvolver a compreensão das ideias matemáticas anteriormente enraizadas e também a explorar e consolidar novas ideias matemáticas. Aqui, assumimos a definição de que, uma determinada questão só se torna um problema a um aluno se ele não depender de nenhuma regra procedimental, permitindo assim, que o aluno reflita, explore e desenvolva processos de resolução (ECHEVERRÍA; POZO, 1998; PONTE; SERRAZINA, 2000).

Seguindo essa perspectiva, um problema deve ser envolto por situações investigativas que coloquem-nos em uma posição de verdadeiros exploradores e investigadores (PONTE; BROCADO; OLIVEIRA 2009). Tais problemas não permitem uma forma ou um caminho explicito para a sua resolução. Esse tipo de problema deve desafiar, motivar e convidar os alunos a se debruçarem sobre ele, resgatando seus conhecimentos prévios, os procedimentos (estratégias), os conhecimentos conceituais e as atitudes que lhes possibilitem explorar as informações do problema, conjecturando e explorando as estratégias de resolução. Essas caraterísticas do problema contribuem para aguçar a motivação dos alunos para resolve-lo e dar sentido à realização do estudo a ser promovido (ECHEVERRÍA; POZO, 1998).

Aliada à resolução de problemas, alguns autores destacam as possíveis etapas de sua investigação, e consequentemente, sua resolução (ECHEVERRÍA; POZO, 1998; PONTE; BROCADO; OLIVEIRA, 2009). De modo geral, essas etapas estão atreladas à compreensão do problema, à explorações iniciais, ao levantamento de conjecturas permeadas pelas suas verificações ou refutações, à argumentação e organização das informações, e por fim, à demonstração e avaliação do trabalho realizado (entre os alunos). Nesse ponto é importante ressaltar que tais etapas não seguem uma lineariedade, os alunos transitam entre as fases de acordo com as necessidades encontradas por eles, sendo que todo esse conjunto de etapas constitui o processo de investigação e resolução dos problemas.

3 I UM BREVE RELATO DA CRIPTOGRAFIA E SUA EVOLUÇÃO

Derivado das palavras gregas *kriptós* que significa escondido, oculto e *gráphein* que significa escrever, a palavra Criptografia pode ser definida como sendo a arte ou a ciência de escrever mensagens em cifras ou em códigos, com a finalidade de ocultar mensagens a terceiros, possibilitando exclusivamente apenas à pessoa autorizada a decifrar e ler as mensagens (TAMAROZZI, 2001).

A Criptografia vem permeando a história da humanidade sempre com o intuito de garantir, de maneira sigilosa, as trocas de mensagens humanas, podendo ser considerada tão antiga quanto à própria escrita hieroglífica dos egípcios (SINGH, 2008). Os meios de comunicação secretos sempre fizeram parte da história, especialmente para governantes, que dependiam de meios de comunicação sigilosos para governar seus territórios, comandar seus exércitos entre outros. Em tempos de guerras, a Criptografia configura-se como um aliado dos comandantes, pois a necessidade de garantir a eficiência e o sigilo nas comunicações exerce papel fundamental nas estratégias de batalhas. Sua importância durante a história impeliu o desenvolvimento de técnicas eficientes de cifragem de modo que as mensagens criptografadas transitassem seguras pelos meios de comunicação com a garantia de que apenas o destinatário pudesse ler seu conteúdo.

A busca por desenvolver cifras cada vez mais seguras é resultado de uma disputa entre os Criptográficos e os Criptoanalistas. Enquanto que os criadores de cifras buscam cifras cada vez mais eficientes, os decifradores procuraram meios de quebrar tais cifras. Essa tarefa dos decifradores é conhecida como a Criptoanálise, a qual é definida com sendo a "ciência da dedução do texto original a partir do texto cifrado, sem o conhecimento da chave [cifradora]" (SINGH, 2008, p. 423).

Os primeiros resquícios registrados da utilização de cifras para troca de mensagens militares correspondem a *Cifra de César* e a cifra de Vigenère, que pode ser considerada uma evolução da *Cifra de César*. A partir dessas duas cifras, muitas outras se originaram (cifra *ADFGVX*, cifra do *Chiqueiro,* cifra *Lucifer* entre outras). Com o surgimento dos aparelhos eletrônicos, as comunicações começaram a fluir de maneira mais rápida, no entanto, esses meios também apresentavam ineficiência quanto a sua segurança de interceptação. Essa vulnerabilidade impulsionou o primeiro grande salto no desenvolvimento de cifras seguras. Esse momento é marcado pelo surgimento da máquina *Enigma* (1918) durante a Primeira Guerra Mundial. Tal invenção pode ser considerada como sendo a mais promissora e desafiadora de toda a evolução da Criptografia. A decifração das mensagens produzidas pela *Enigma* foi realizada com sucesso por Alan Turing, em 1940, que finalizou o projeto de máquinas que seriam utilizadas para quebrar os códigos das *Enigma*.

O segundo momento da história da Criptografia em relação à proteção das mensagens ocorreu por volta de 1977 com os cientistas de computação Rivest e Shamir e do matemático Adleman. Esses três pesquisadores investigaram por meio da matemática um método de garantisse, mesmo com interceptações, trocas seguras de informações. Foi buscando funções de mão única, que fossem condizentes com os critérios exigidos para uma cifra assimétrica[5], que o sistema conhecido como RSA (Rivest, Shamir e Adleman) se desenvolveu.

O sistema, chamado RSA, é então um sistema de Criptografia assimétrico, também conhecido como *criptografia de chave pública*. Nos dias de hoje a Criptografia RSA é extremamente empregada nos meios de comunicação que necessitam de trocas de informações seguras. Esse tipo de cifra pode ser encontrado, por exemplo, em quase todos os sistemas que envolvem o ciberespaço, como os sistemas de correios eletrônicos, compras e vendas *on-line*, transições bancárias, senhas de *sites* comerciais entre outros.

4 I CONTEXTO E MÉTODO

Esta investigação faz parte de uma pesquisa de mestrado que buscou refletir sobre as potencialidades de uma sequência pedagógica de atividades envolvendo problemas criptográficos para o desenvolvimento do conceito de função afim. Nossa pesquisa teve por fundamentação teórico-metodológica uma intervenção de caráter qualitativo. Aqui temos como foco apresentar e discutir alguns dos resultados advindos do trabalho com os alunos a partir da sequência pedagógica elaborada. Por conta do espaço e objetivo da investigação, não apresentaremos as tarefas desenhadas para a sequência pedagógica, no entanto, elas podem ser encontradas em Litoldo (2016).

O contexto dessa investigação ocorreu uma escola pública da cidade de Rio Claro/ SP, onde propusemos a sete alunos, nomeados aqui por nomes fictícios, do primeiro ano do Ensino Médio, o desenvolvimento de uma sequência pedagógica. Essa sequência era composta por oito tarefas sendo elas estruturadas na forma de enigmas envolvendo contos baseados no personagem Sherlock Holmes, de Sir Arthur Conan Doyle. Tais tarefas envolviam a definição de função afim e suas particularidades como, função linear, função identidade e função constante; suas respectivas funções inversas e seus gráficos.

Os encontros entre os sete alunos e a pesquisadora para o desenvolvimento das tarefas ocorreram na própria escola (em sala de vídeo ou em sala de aula), entre os meses de maio a setembro de 2014, ocorrendo um ou dois encontros por semana e tendo como duração duas horas cada encontro, totalizando ao final 18 encontros. As tarefas da sequência pedagógica eram desenvolvidas em duplas ou trios de alunos, sendo que esses agrupamentos variavam de acordo com os encontros.

As informações discutidas nessa investigação foram coletadas por meio de observações da pesquisadora registradas em seu diário de campo, das gravações em vídeo e áudio referentes às discussões de cada grupo durante os encontros e do material produzido (respostas das tarefas) pelos alunos. As gravações em vídeo e áudio foram transcritas em sua totalidade e conjuntamente com o diário de campo e os materiais dos alunos constituíram nossas fontes de levantamento de dados. A organização das informações para analise seguiu as perspectivas de Lüdke e André (1986) e Bogdan e Biklen (1994). As informações foram tratadas usando uma análise de conteúdo (Bardin, 1996) e no decorrer desse processo de análise buscamos, os episódios em que foi possível observar as informações relacionadas com as atitudes desenvolvidas pelos alunos, com os procedimentos produzidos por eles durante a resolução das tarefas e conceitos abordados e construídos por tais alunos durante as tarefas da sequência pedagógica.

5 I ALGUNS RESULTADOS E DISCUSSÕES

Nos primeiros encontros, os alunos mostraram-se com pouca autonomia investigativa e antes mesmo de iniciarem a resolução dos problemas, eles solicitavam à pesquisadora que lhes explicasse os enunciados das atividades e, posteriormente, realizasse a confirmação de suas respostas. No entanto, o modo de agir e reagir de forma apenas receptiva foi sendo modificada conforme os encontros foram ocorrendo. Ao longo deles, foi possível observar que os alunos se sentiam mais confortáveis com o ambiente proposto pela pesquisadora e aos poucos eles foram desenvolvendo atitudes de autoestima e autonomia, além de demonstrarem comprometimentos com as tarefas durante suas resoluções (MAURI, 2009).

Tarefas de caráter criptográficos possibilitam uma flexibilidade em relação a seus distintos métodos e procedimentos de solução. Esse tipo de tarefa favorece aos alunos uma situação livre para que eles desenvolvessem suas próprias estratégias de resolução. Essa característica se tornou evidente durante os encontros, à medida que as diferentes estratégias de resolução desenvolvidas pelos alunos para decifrarem as mensagens e resolver as atividades propostas eram discutidas, exploradas e exteriorizadas, por eles, por meio de diferentes representações (ECHEVERRÍA; POZO, 1998; PONTE; SERRAZINA, 2000).

Com o movimento exploratório das tarefas e fazendo uso de seus conhecimentos prévios, os alunos foram se tomando proativos, assumindo atitudes mais investigativas. Essa nova postura contribuía fortemente para a criação e elaboração de diferentes etapas e estratégias de resolução (ECHEVERRÍA; POZO, 1998; PONTE; BROCADO; OLIVEIRA, 2009). A cada tarefa, os alunos discutiam entre si as mensagens cifradas, desenvolviam suas estratégias e as utilizavam conforme eles mesmos achavam interessante para a resolução daquela tarefa. Esse fato se tornou interessante à medida em que os alunos trocavam entre si suas ideias de resolução e a aperfeiçoavam conforme o problema era apresentado. Abaixo apresentamos três episódios que evidenciam os momentos de criação, transição e desenvolvimentos das estratégias criadas pelos alunos.

Fernando começou a decifrar a carta colocando a letra *o* em todos os números dezenove que ele encontrava. Depois, ele fez a mesma coisa com a letra *a* e com a letra*s*, e seguiu essa mesma estratégia de resolução até a decifração de toda a carta. Já as meninas, embora tivessem colocado, de início, todas as letras *o* que apareciam na carta, não seguiram esse mesmo raciocínio para preenchê-la. Elas olhavam qual seria o próximo número da palavra e a preenchiam com sua letra correspondente. Utilizando-se desse processo, Jaciara sugeriu que tentassem formar as palavras antes mesmo de acabar de preenchê-las. Janaína acatou a sugestão e ambas foram decifrando a carta, transitando entre essas duas estratégias de resolução desenvolvidas por elas.

Episódio 1 – Estratégia de Fernando para a tarefa "*Um caso de sequestro*"

Fonte: Litoldo (2016)

Enquanto Igor terminava de escrever o alfabeto cifrado, Gustavo chamou a pesquisadora para dizer que eles desenvolveram vários jeitos de encontrar o alfabeto cifrado. Foi pedido, então, que eles escrevessem quais seriam esses três métodos de encontrar o alfabeto cifrado. Seguem, abaixo, os três exemplos citados por Gustavo.

1) Você pega a letra do alfabeto e soma a ela o mesmo valor da letra, depois você soma mais um no final. O nº cifrado será o nº negativo dessa soma.

Ex.: A=1
$(1+1)+1=3$ => -3 A
B = 2
$(2+2)+2=5$ => -5 B
C = 3
$(3+3)+3=7$ => -7 C

2) Você pensa em uma expressão que utilize o nº do alfabeto normal para se chegar ao alfabeto criptografado.Para a 3ª pista, a expressão é $(-2)\times x-1$ e se faz a conta para todas as letras do alfabeto.

3) Você encontra a expressão utilizada para cifrar as letras, que, neste caso, é $(-2)\times x-$. Realiza os cálculos para as primeiras e observa o padrão que ocorre no resultado das contas. Depois é só completar o alfabeto apenas somando o padrão.

Para a expressão observou-se que os números aumentavam -2. Assim, a partir de x = 8, era só ir somando (-2) aos resultados.

Ex.: $7\times(-2)-1=-15$
$8\times(-2)-1=-17$ e $(-15)+(-2)=-17$
$9\times(-2)-1=-19$ e $(-17)+(-2)=-19$
$10\times(-2)-1=-21$ e $(-19)+(-2)=-21$

Episódio 2 – Estratégias de Gustavo para a tarefa "*O detetive Watson*"

Fonte: Litoldo (2016).

Essa dupla, após observar o criptograma, começou a responder a todas as dicas que eles sabiam. Quando eles não souberam mais responder, Gustavo começou a escrever em seu rascunho todas as informações que sabia sobre as letras cifradas (Figura 1).

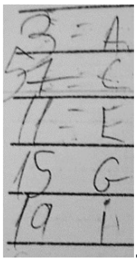


Figura 1 - Informações que Gustavo retirou das dicas respondidas no criptograma

Depois de observar o que Gustavo estava anotando, a pesquisadora o questionou sobre o que ele estava pensando em fazer. Segundo Gustavo, ele apenas estava colocando na folha de rascunho as informações já conhecidas. Com isso, foi perguntado a eles se, com aqueles dados e conhecendo o jeito da função utilizada, seria possível determinar os coeficientes *a* e *b* da função afim. Os meninos pensaram sobre o argumento dado pela pesquisadora, mas Gustavo afirmou que ele conseguiria achar o resto do alfabeto sem ter que encontrar esses coeficientes.

Desse modo, Gustavo observou que os números já conhecidos eram todos números ímpares, começando pelo número 3. De acordo com ele, esse pensamento estava dando certo e, assim, ele escreveu em sua folha de rascunho todo o alfabeto, seguindo a lógica de que os próximos números seriam ímpares. [...] Com todo o alfabeto escrito, Gustavo e Fernando completaram as dicas que faltavam e terminaram rapidamente a atividade.

Episódio 3 – Estratégias de Gustavo para a tarefa "*Criptograma*"

Fonte: Litoldo (2016).

Nos três episódios apresentados, é possível observar que as investigações desenvolvidas pelos alunos envolveram ações de formular conjecturas sobre as possíveis estratégias de resolução e, a partir do emprego delas, foi possível verificar suas validações ou refutações, o que também contribuiu para a organização na exposição das ideias, sendo elas realizadas oralmente ou na forma escrita, para o professor e seus colegas (ECHEVERRÍA; POZO, 1998; PONTE; BROCADO; OLIVEIRA, 2009; BRASIL, 2018).

No momento das elaborações das conjecturas, é importante que os alunos compreendam por inteiro o problema proposto (BRASIL, 2002). Esse entendimento leva-o a conjecturar hipóteses e a tomar decisões sobre suas possíveis estratégias de resolução. As decisões tomadas pelos alunos estavam sempre permeadas por seus conhecimentos prévios. Tais conhecimentos proporcionaram a eles utilizar intuições e estratégias de resolução durante as tarefas, bem como resgatar e explorar outros conceitos da matemática, direcionando algumas etapas para o processo de resolução. No episódio 3, por exemplo, é possível observar que Gustavo utiliza seu conhecimento prévio sobre os números primos, para levantar hipóteses da estrutura do problema e, a partir dela, resolver a tarefa e chegar na decifração da mensagem.

Relativamente ao conceito matemático resgatado pelos alunos, conjuntamente com seus conhecimentos prévios sobre as decifrações das mensagens, apresentamos abaixo três episódios que destacam a maneira como tais conhecimentos foram retomados (e quais) e de que forma eles fizeram parte no processo de resoluções dos alunos.

Para a 2ª pista, Kall chamou a pesquisadora para apresentar sua ideia.

Kall: Agora, aqui, vai ser um esquema diferente. Aqui eu acho que vai ser números...

Jaciara: Nossa! Igual ao 4...

Kall: Números primos.

Pesquisadora: Números primos?... Hum..., mas 12 é um número primo?

Kall: Não!

Pesquisadora: Então uma pista já descartada fora. Uma ideia. Qual a outra ideia?

Jaciara: Aqui não é a cifra de César?

Episódio 4 – Discussão envolvendo a ideia de números primos

Fonte: Litoldo (2016)

Para ajudar os meninos, a pesquisadora questionou sobre o que eles percebiam ao olhar a 4ª pista. Gustavo argumentou que naquela pista havia nº pares e ímpares e Fernando complementou dizendo que aqueles nº eram múltiplos de 3. Nesse momento, a pesquisadora chamou a atenção perguntando se, na pista, havia nº positivos. Gustavo respondeu dizendo que não, e daí Fernando argumentou que, então, eles eram múltiplos de -3.

Episódio 5 – Discussão envolvendo a ideia de números múltiplos de -3

Fonte: Litoldo (2016)

Quando eles chegaram à questão que solicitava a representação do esquema criptográfico por meio do plano cartesiano, Igor se pronunciou dizendo que lembrava o que era um plano cartesiano e, para mostrar isso, ele desenhou com o dedo, no espaço, as retas do plano. Ao ser questionado sobre qual era o eixo das abcissas e qual era o das ordenadas, Igor soube responder corretamente. A pesquisadora também perguntou à dupla se eles saberiam dizer qual alfabeto seria representado pelo eixo *x* e qual pelo eixo *y*. Jaciara respondeu corretamente e Igor explicou rapidamente com gestos o porquê de a resposta dela estar certa.

Episódio 6 – Discussão envolvendo a ideia do plano cartesiano

Fonte: Litoldo (2016)

Nesses episódios, é possível identificar o resgate dos conceitos de números pares, números ímpares, múltiplos de três (e de menos três) e conceito de plano cartesiano como conexões auxiliares para o processo das resoluções (MAURI, 2009). Tais situações evidenciam, como sugerido pelos PCNEM (BRASIL, 2000), Mauri (2009) e Solé e Coll (2009), a relevância que se faz na relação significativa entre os conhecimentos prévios dos alunos com o processo da construção do novo conhecimento, permeados pelos procedimentos de resolução para as tarefas propostas pela professora.

Essas conexões entre alguns conceitos matemáticos puderam ser vistas durante todas as resoluções das tarefas, pois a partir dos conhecimentos prévios, os alunos tiveram subsídios para desenvolveram suas estratégias de resolução e construírem, gradualmente, suas ideias associadas ao conceito de função afim. Esses subsídios, quando organizados e exteriorizados, são pertinentes e relevantes, pois contribuem para interligar as novas informações durante a construção da aprendizagem (MAURI, 2009; PONTE; SERRAZINA, 2000), além de permitir compreende-los em uma diversidade de situações matemáticas (ECHEVERRÍA; POZO, 1998).

Conjuntamente com os conhecimentos prévios destacados acima, os alunos também fizeram uso da calculadora, como uma ferramenta de auxílio para resolver as tarefas. A utilização desse recurso tecnológico esteve presente em todos os encontros. Os alunos a utilizaram sob duas formas: para resolver algum cálculo ou para a verificação de algum já feito. Com a utilização dessa ferramenta e de seus conhecimentos prévios, os alunos articulavam suas hipóteses de resolução e depois de discuti-las, realizavam os cálculos, colocado em prática, nesse momento, suas hipóteses e verificando se elas os ajudavam ou não a resolver o problema. O trabalho coletivo também se fez presente durante os encontros. Os alunos trabalhavam em grupo, ficando evidente em algumas situações a troca de informações na tentativa de auxiliar o outro na resolução e entendimento do problema, com a preocupação de sempre explicitar as ideias de resolução criadas por eles.

O trabalho em grupo oportunizou evidenciar, muitas vezes, as explicações e discussões que ocorriam entre os alunos, possibilitando compartilhar as ideias, na tentativa de explicitar o sentido dado a elas em suas resoluções. Eles se posicionavam abertos ao diálogo e sempre se mostravam dispostos a negociar os significados. Eles também se auto organizavam com o propósito de dividir as ações de decifração e, assim, otimizar o tempo de resolução das tarefas. Toda essa postura se desenvolveu partindo do próprio comportamento dos alunos respaldado na mediação que a pesquisadora realizava por meios de questionamentos, discussões e reflexões acerca das ideias apresentadas por eles (ECHEVERRÍA; POZO, 1998).

No decorrer dos encontros, foi perceptível alguns indícios de comprometimento e responsabilidade com o trabalhado que estávamos realizando. Esses indícios se tronavam mais frequentes à medida que os alunos se envolviam mais com a proposta. As posturas de compromisso se refletiram no pedido dos próprios alunos para levar as atividades para a casa (situação que pode ser vista no episódio 10), visto que, segundo eles, as atividades eram interessantes e eles gostariam de tentar resolve-las fora dos encontros. Essas atitudes proativas e comprometidas com o trabalho proposto, conjuntamente com o movimento de debates entre os alunos e as discussões sobre as ideias desenvolvidas por eles, contribuíram para que eles explorassem, conscientemente, as ideias associadas à função afim, partindo, em alguns casos, de seus conhecimentos prévios permeados por pensamentos e representações algébricas característica desse tipo de função.

As situações de interação e troca de informações ocorreram tanto entre os alunos entre si quanto entre eles e a pesquisadora, e conforme as trocas se sucediam, se estabelecia uma negociação de significados. A pesquisadora, por interesse da pesquisa, sempre tentava direcionar as ações dos alunos em termos de suas ideias e representações de resolução para o campo do pensamento algébrico da função afim. Abaixo apresentamos quatro episódios que evidenciam situações de discussões entre a pesquisadora e os alunos durante a exploração e construção das ideias associadas a função afim.

Kall começou a esboçar a sua ideia [de que aqueles números da carta eram múltiplos de -3] em uma folha de rascunho. Ao mesmo tempo em que falava, ele escrevia:

Kall: $a(-3) = (-3)$ [nesse momento ele pára, corrige seu raciocínio e continua].

Kall: $a(1) = (-3) \times 1$ e $a(2) = (-3) \times 2$.

Pesquisadora: $a(3)$ dá quanto?

Kall: 9.

Pesquisadora: 9?

Kall: Não, -9.

Ao perceber que esse poderia ser o jeito de decifrar a 4ª pista, Kall escreveu em seu rascunho um esquema e depois reescreveu o alfabeto já cifrado (Figura 2).

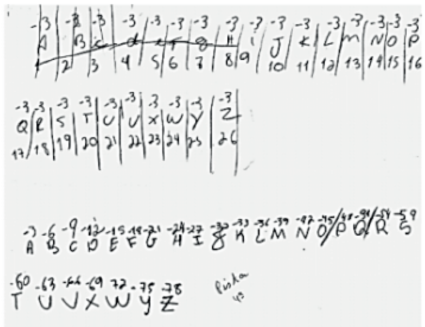


Figura 2 - Esquema de Kall para representar os cálculos do alfabeto (acima) e o alfabeto já cifrado (abaixo).

Episódio 7 – Discussão entre Kall e a pesquisadora a respeito de sua ideia

Fonte: Litoldo (2016)

O episódio 7 ocorreu na terceira atividade (*O detetive Watson*). Embora nos encontros anteriores tenha-se comentado um pouco sobre esse tipo de função e sobre sua notação, sua formalização ainda não havia sido discutida. Nesse episódio é possível observar que Kall retomou algumas discussões realizadas em encontros passados e tentou elaborar uma expressão matemática que fizesse sentido naquela situação. É interessante observar que Kall teve o cuidado em representar o número -3 por meio dos parênteses, discernindo assim, esse valor fixo da expressão das variáveis do alfabeto. Após descobrir a expressão representativa daquela situação, Kall organizou os dados desse alfabeto já designando os valores numéricos as suas respectivas letras.

O episódio 8 apresenta uma situação embasada na discussão sobre a generalização de uma expressão representativa de uma função afim. É possível observar, nesse diálogo, que os alunos Igor e Leandro perceberam que os coeficientes *a* e *b* das expressões encontradas por eles variavam, no entanto, esses coeficientes não representavam a variação do alfabeto. Com a ajuda desses alunos, a expressão geral que representa a função afim foi construída e, posteriormente, várias outras discussões a respeito dela foram desenvolvidas.

Para ajudar os alunos a responderem a essa questão e aproveitando para introduzir alguns termos, como os coeficientes a e b, a pesquisadora iniciou um diálogo com os alunos sobre como seria a representação do modo geral da função que estávamos utilizando.

A pesquisadora, então, foi até à lousa e escreveu algumas expressões das pistas. Ela chamou a atenção dos alunos para os valores que acompanhavam a variável x, mostrando-lhes que esses valores estavam mudando de uma expressão para outra. Então, ela perguntou de que maneira eles poderiam olhar a variável x e os valores que a acompanham de uma forma generalizada. Depois de mais algumas explicações, Leandro se pronunciou dizendo:

Leandro: y ou x... sei lá...

Pesquisadora: y aonde?

Leandro: y no lugar do x, eu acho...

Pesquisadora: No lugar do x?

Igor: No caso, só está mudando a letra.

Leandro: É... pode ser x vezes y mais...

Pesquisadora: x vezes y mais quem?

Leandro: Mais uma letra...

Pesquisadora: Mais... chuta uma letra aí.

Igor: z.

Nesse momento, conforme Leandro foi dizendo, a pesquisadora foi escrevendo na lousa as ideias de Leandro e, no final, chegou-se à seguinte expressão, em que x representava a variável e y e z representavam os coeficientes. Leandro discutiu com Igor sobre esse modo generalizado e ambos demostravam entender o que eles haviam acabado de construir.

Episódio 8 – Discussão sobre a generalização da expressão algébrica de uma função afim

Fonte: Litoldo (2016)

O episódio 9 evidencia a tentativa de Igor em resolver a tarefa fazendo uso da definição de função afim, discutida nos encontros anteriores. Igor e Jaciara iniciaram a tarefa respondendo às dicas que eles já conheciam; depois, Igor recordou a expressão e começou uma busca pelos valores a e b que pudessem resultar na expressão algébrica utilizada na cifração daquela tarefa. É importante destacar que a ideia de buscar uma função afim que representasse a cifração utilizada para facilitar a resolução da tarefa partiu de Igor. Essa atitude evidencia as associações e explorações que Igor realizou sobre as ideias do conceito de função afim que foram discutidas nos encontros anteriores.

Essa dupla observou o criptograma e, de início, começou a responder às dicas. Após responder às duas primeiras, Igor sugeriu a Jaciara que eles fossem completando os quadrinhos em que havia os números correspondentes às letras que elas já conheciam. Jaciara aceitou a sugestão e começou a colocar, em todos os quadrinhos com o número 3, a letra *a*. Ela continuou fazendo isso para as outras letras conhecidas. Enquanto Jaciara fazia esse processo, Igor pegou uma folha de rascunho e escreveu nela a expressão $a \times x + b$ e começou a pensar nos valores de *a* e *b*. Igor tentou primeiro substituir os valores $a = 1$ e $b = 2$ e resolveu os cálculos para $x = 1$. Embora a expressão $1 \times x + 2$, para $x = 1$, tenha dado 3 (a letra *a*), ele verificou que ela não dava certo para a letra *c*, pois $1 \times x + 2$, para $x = 3$, dava 5 e não 7, como teria que ser (Figura 3). Desse modo, Igor pensou em outros valores para os coeficientes *a* e *b*. Com a intenção de que seus cálculos dessem certo para a letra *c*, Igor pensou nos valores $a = 5$ e $b = 2$. Assim, ele resolveu a expressão $5 \times x + 2$, para $x = 1$, e verificou que o resultado dava 7, mas, nesse momento, Jaciara chamou a atenção de Igor, dizendo que ele havia utilizado $x = 1$ e não $x = 3$, como ele queria (Figura 4). Igor demonstrou entender o que Jaciara estava dizendo. Assim, ambos perceberam que aqueles valores para *a* e *b* ainda não estavam bem definidos. Nesse momento, os dois demonstraram desânimo, pois não haviam ainda acertado os valores para *a* e *b*.

Para que os alunos continuassem com o raciocínio de encontrar os valores dos coeficientes *a* e *b*, a pesquisadora interveio, sugerindo que, ao invés de eles utilizarem $a = 1$ e $b = 2$, que tentassem $a = 2$ e $b = 1$. Igor aceitou a sugestão e escreveu em sua folha de rascunho a expressão $2 \times 1 + 1$. Ao resolver a conta, ele verificou que o resultado dava 3, em seguida ele resolveu $2 \times 3 + 1$ e também observou que a resposta era 7. Desse modo, eles perceberam que a expressão $2 \times x + 1$, com *x* variando nas letras do alfabeto ($A = 1, B = 2, \dots, Z = 26$), estava correspondendo às letras cifradas do criptograma.

Figura 3 - Igor pensando sobre os coeficientes *a* e *b* e depois testando os coeficientes *a* = 2 e *b* = 1.

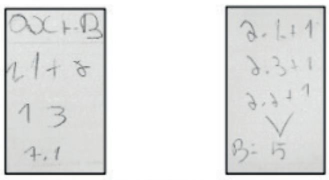
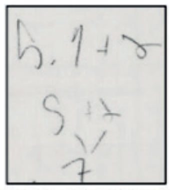
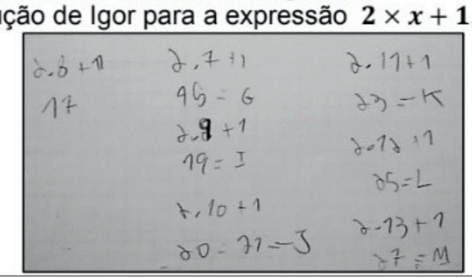


Figura 4 - Igor testando os coeficientes *a* = 5 e *b* = 2.



Com isso, Igor afirmou a Jaciara que, para essa cifra, os valores dos coeficientes eram $a = 2$ e $b = 1$, e que *x* representava a variável da expressão $2 \times x + 1$. Desse modo, Igor continuou variando *x* de acordo com as letras do alfabeto (Figura 5).

Figura 5 - Resolução de Igor para a expressão **$2 \times x + 1$**, para *x* = 1, ..., 26.



Episódio 9 **–** Estratégias e representações de Igor e Jaciara baseados em ideias associadas a função afim

Fonte: Litoldo (2016)

O episódio 10 evidencia uma sistematização das ideias e explorações que Igor realizou acerca da função afim. A tarefa que condicionou a situação descrita nesse episódio era constituída por alguns gráficos de funções afins. Dando continuidade ao seu raciocínio, Igor buscou na expressão algébrica possíveis valores de *a* e *b* que pudessem satisfizer visivelmente o gráfico da tarefa escolhido. Desse modo, primeiramente, Igor descobriu a função que representava o gráfico verde, atribuindo aleatoriamente valores para *a* e *b*. Essa mesma estratégia acabou não sendo eficaz para os outros gráficos da tarefa. Diante desse impasse, como se pôde observar no episódio, a pesquisadora interveio, tentando auxiliar Igor a encontrar a função por meio dos pontos pertencentes aos eixos. A Figura 6 ilustra o raciocínio que Igor realizou para encontrar a função cifradora depois da intervenção da pesquisadora. Munido dessa mesma estratégia, Igor e Jaciara descobriram todas as outras funções afim referentes aos gráficos e decifraram, no final, as mensagens da tarefa.

Ao iniciar esse encontro, a pesquisadora perguntou se eles haviam trazido a atividade e o que eles haviam desenvolvido sobre ela em suas casas. Igor respondeu que havia pensado e chegado à decifração de uma mensagem. Sendo assim, a pesquisadora solicitou que Igor explicasse para as meninas tudo o que ele havia pensado e feito em casa.

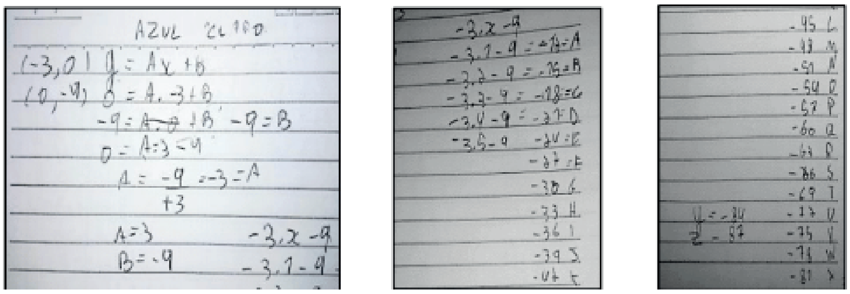
Igor explicou que havia conseguido encontrar a função $f(x) = 2 \times x - 2$ que representava o gráfico verde. Segundo Igor, ele foi "chutando" os valores para os coeficientes *a* e *b* e mudando o sinal de *b* até dar certo. Fazendo isso, com a função $f(x) = 2 \times x - 2$, ele havia conseguido decifrar a frase que correspondia a essa função [...].

Após essa explicação, todos deram continuidade às resoluções. Igor estava muito preso à ideia de ficar "chutando" os valores para os coeficientes *a* e *b* da função. As meninas demonstraram estar um pouco confusas sobre os cálculos de Igor.

Percebendo que o rendimento das discussões e das resoluções havia baixado, a pesquisadora decidiu interferir, fazendo uma explicação sobre como eles poderiam encontrar as funções sem ter que ficar "chutando" os valores, como Igor estava fazendo. Assim, a pesquisadora retomou a explicação sobre os pontos e suas coordenadas e como, através deles, se poderia encontrar a função do gráfico passando por esses dois pontos.

Conforme a pesquisadora explicava, os alunos começaram a se lembrar um pouco das discussões feitas no encontro anterior. Igor, rapidamente, iniciou seus cálculos em seu rascunho, mas as meninas ainda tiveram algumas dúvidas e dificuldades em iniciar suas resoluções.Igor escolheu um gráfico e procurou nele os pontos sobre os eixos x e y. Os pontos encontrados por ele foram (-3,0) e (0,-9). Igor desenvolveu os cálculos com esses pontos sem mostrar dificuldades, embora, às vezes, ele cometesse alguns erros na hora de resolver a equações, por exemplo, $-3 \times a - 9 = 0$ => $a = 3 + 9$=> $a = 12$. Ao perceber que Igor estava cometendo esse erro, a pesquisadora chamou a atenção dele sobre a maneira como ele estava resolvendo a equação. Após observar o erro, Igor refez os cálculos e conseguiu chegar à função $f(x) = 3 \times x - 9$ e, com isso, descobriu os valores das letras cifradas por essa função (Figura 6).

Figura 6 - À esquerda, a resolução de Igor para os pontos (-3,0) e (0,-9) e, à direita, os cálculos que designam o alfabeto cifrado.



Episódio 10 – Estratégias de Igor baseados em ideias associadas a função afim para descobrir o alfabeto cifrado
Fonte: Litoldo (2016)

Nos quatro episódios apresentados acima, é possível observar que os alunos mobilizaram seus conhecimentos prévios e procedimentais para resolver os problemas da tarefa (MAURI, 2009), e por meio da investigação, exploração, organização, e compreensão exteriorizaram as etapas de resolução realizadas, em muitas vezes, pelo trabalho do grupo (ECHEVERRÍA; POZO, 1998; PONTE; BROCADO; OLIVEIRA, 2009; PONTE; SERRAZINA, 2000).

6 I CONSIDERAÇÕES FINAIS

Essa investigação buscou apresentar alguns resultados que se destacaram na pesquisa de mestrado desenvolvida acerca de tarefas criptografas para desenvolver o o conceito de função afim. Ao tratar as informações, pode-se concluir que a sequência pedagógica de tarefas envolvendo problemas criptográficos permitiu que os alunos explorassem e resgatassem diferentes conceitos matemáticos advindos de seus conhecimentos prévios, os quais deram subsídios para que investigassem as tarefas propostas. Para a resolução dos problemas, era necessário que os alunos se atentassem à estrutura dos problemas. Tais situações promoveram o desenvolvimento do Pensamento Algébrico, conjuntamente com suas etapas de resolução e suas representações. O trabalho de discutir essas representações juntamente com as estratégias de resolução advindas de seus conhecimentos prévios contribuiu para que os alunos explorassem as ideias associadas à função afim.

Como um resultado, observa-se que tarefas envolvendo o tema Criptografia, em um ambiente investigativo, podem contribuir para o desenvolvimento da autonomia dos alunos, proporcionando um ambiente de sala de aula com posturas mais ativas e investigativas. Essas atividades também podem influenciar a criatividade dos alunos e a liberdade dos mesmos em buscar, tanto em recursos tecnológicos, neste caso a calculadora, como em seus conhecimentos prévios, os suportes para o desenvolvimento de estratégias que os auxiliem no levantamento de conjecturas e planos de execução da resolução de problemas, ao mesmo tempo em que constroem novos conhecimentos matemáticos.

Assim, ao observar o conjunto das informações coletadas, levando em consideração o trabalho em grupo realizado pelos alunos, as atitudes investigativas assumidas por eles, o envolvimento com as tarefas propostas e a atenção dada a elas durante os encontros se pode inferir que uma sequência pedagógica de tarefas aliadas ao tema Criptografia pode contribuir para desenvolver em sala de aula um ambiente diferenciado baseado nos processos de resolução de problemas e exploração do conceito matemático escolhido para ser trabalhado, o qual, nesse caso, foi função afim. Como apontamentos para pesquisas futuras, elenca-se alguns questionamentos: Qual o conhecimento especializado do professor sobre o tema Criptografia? De que forma esse tema poderia ser abordado em uma formação inicial e continuada? Qual seria o conhecimento especializado do formador de professor sobre esse tema?

REFERÊNCIAS

Bardin, L. (1996). *El análisis de contenido*. Madrid: Akal Ediciones.

BOGDAN, R.; BIKLEN, S. *Investigação Qualitativa em Educação: uma introdução à teoria e aos métodos*. Porto, Portugal: Porto Editora, 1994.

BRASIL. *Base Nacional Comum Curricular*. Brasília-DF: Ministério da Educação, 2018.

BRASIL. *Parâmetros Curriculares Nacionais: Terceiro e Quarto Ciclos de Ensino Médio - Matemática. Brasil*. Brasília-DF: Ministério da Educação / Secretaria de Educação Média e Tecnológica, 2000.

FIARRESGA, V. M. C. *Criptografia e Matemática*. 2010. 144 f. Mestrado em Matemática para Professores – Universidade de Lisboa, Portugal, 2010.

FINCATTI, C. A. *Criptografia como agente motivador na aprendizagem da matemática em sala de aula.* 2010. 82 f. Trabalho de conclusão de curso – Universidade Presbiteriana Mackenzie, São Paulo, 2010.

GROENWALD, C. L. O.; FRANKE, R. F.; OLGIN, C. DE A. Códigos e Senhas no Ensino Básico. *Educação Matemática em Revista*, v. 2, p. 41–50, 2009.

GROENWALD, C. L. O.; OLGIN, C. DE A. Criptografia e o Currículo de Matemática no Ensino Médio. *Revista de Educação Matemática*, v. 13, p. 71–78, 2011.

LITOLDO, B. F. *As potencialidades de atividades pedagógicas envolvendo problemas criptograficos na exploração das ideias associadas à função afim*. 2016. 198 f. Dissertação (Mestrado em Educação Matemática) – Universidade Estadual Paulista "Júlio de Mesquita Filho", Rio Claro (SP), 2016.

LÜDKE, M.; ANDRÉ, M. E. D. A. *Pesquisa em Educação: Abordagens Qualitativas*. São Paulo: E.P.U., 1986.

OLGIN, C. DE A.; GROENWALD, C. L. O. Temas de Interesse no Currículo de Matemática do Ensino Médio. *Clame: Comité Latinoamericano de Matemática Educativa*, 2011.

PONTE, J. P.; SERRAZINA, M. DE L. *Didática da Matemática do 1º Ciclo*. 1. ed. Lisboa/Portugal: Artes Gráficas, 2000.

SINGH, S. *O livro dos códigos: A ciência do sigilo - do antigo Egito à criptografia quântica*. 7º ed. Rio de Janeiro: Record, 2008.

SOLÉ, I.; COLL, C. Os professores e a concepção construtivista. In: COLL, C. *et al. O Construtivismo na Sala de Aula*. Tradução Cláudia Schilling. 6º ed. São Paulo - SP: Ática, 2009. p. 09–28.

TAMAROZZI, A. C. Codificando e Decifrando mensagens. *Revista do Professor de Matemática*, v. 45, p. 41–43, 2001.