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

Beatriz Fernanda Litoldo
Universidade Estadual Paulista
Beatrizfernanda_rc@hotmail.com

Arlete de Jesus Brito
Universidade Estadual Paulista
arlete@rc.unesp.br

Resumo:
O intuito deste artigo é apresentar alguns resultados de uma pesquisa qualitativa que buscou evidenciar as potencialidades que uma sequência pedagógica de atividades envolvendo problemas de criptografia pode oferecer durante seu desenvolvimento. O objetivo da pesquisa foi de tentar compreender em que uma sequência pedagógica de atividades de caráter criptográfico auxilia os alunos na exploração das ideias associadas à função afim. Como resultados observou-se que eles desenvolveram autonomias em seus próprios processos de aprendizagem tomando posturas investigativas, o que propiciou na criação de diferentes estratégias de resolução e refletiu nas explorações e investigações realizadas por eles acerca das ideias associadas ao conceito de função afim. Assim, conclui-se que esse tipo de atividade contribuiu para que os alunos adquirissem atitudes ativas e indagativas em seus procedimentos de resolução, incidindo na exploração do conceito abordado.
Palavras-chave: Educação Matemática; Ensino Médio; Cifras; Sequência Pedagógica; Criptoanálise.

1. Introdução

Os Parâmetros Curriculares Nacionais para o Ensino Médio (PCNEM) (BRASIL, 2000) e a Base Nacional Comum Curricular (BNCC) (BRASIL, 2015) argumentam que sobre a necessidade de alternativas metodológicas variadas para o ensino e aprendizagem da Matemática. As orientações dadas aos professores, nesses documentos, remetem às estratégias de ensino respaldadas na resolução de problemas e sugerem que deve-se partir dos conhecimentos prévios dos alunos e ajudá-los a ampliar e dar sentido matemático a tais conhecimentos. De acordo com os PCNEM (BRASIL, 2000),

> Os alunos, confrontados com situações-problema, novas mas compatíveis com os instrumentos que já possuem ou que possam adquirir no processo, aprendem a desenvolver estratégia de enfrentamento, planejando etapas, estabelecendo relações, verificando regularidades, fazendo uso dos próprios erros cometidos para buscar novas alternativas; adquirem espírito de pesquisa, aprendendo a consultar, a experimentar, a organizar dados, a

> s
> istematizar resultados, a validar soluções; desenvolvem sua capacidade de raciocínio, adquirem auto-confiança e sentido de responsabilidade; e, finalmente, ampliam sua autonomia e capacidade de comunicação e de argumentação (BRASIL, 2000).

Ao observar tais orientações percebe-se a importância da postura do professor quanto ao planejamento das atividades. Situações que proporcionam problemas como descritos acima podem partir de atividades estimulantes e desafiadoras. Tais atividades podem promover situações atraentes que os alunos se sintam motivados 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, 2015).

É no sentido de pensar em tais atividades, que se enquadra o tema Criptografia. Com a característica de não haver um método pronto para se decifrar uma mensagem, atividades envolvendo problemas criptográficos abrem um leque de possibilidades de resolução, além de despertar a curiosidade e as atitudes investigativas dos alunos. De acordo com Groenwald, Franke e Olgin (2009, p. 42) utilizando os recursos de cifração e decifração, o tema Criptografia se configura como sendo um agente "motivador e gerador de situações didáticas que permitam o aprofundamento da compreensão dos conceitos matemáticos, possibilitando ao aluno perceber a utilização do conhecimento matemático em situações práticas". Fiarresga (2010) argumenta sobre as possibilidades que esse tema tem ao desenvolver e facetar 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 atividades.

As autoras Fincatti (2010) e Groenwald e Olgin (2011) também refletem sobre a possibilidade de contextualização desse tema em sala de aula, visto que a Criptografia se encontra presente no cotidiano da sociedade. Atividades *on-line*, como, compras e vendas, transações bancárias, auditorias eletrônicas, senhas de e-*mail*, de *facebook*, dentre outras, são exemplos de situações da vida moderna que necessitam o uso da Criptografia. Com as ideias de cifração e decifração[1] o professor tem, então, a oportunidade de criar materiais didáticos que combinem alguns conteúdos matemáticos com a Criptografia, a fim de dispor desse

[1] Cifração é uma transformação, que pode ser de origem matemática ou não, utilizada para se criptografar uma mensagem, ou seja, transformar uma mensagem original em um texto cifrado. Decifração é a ação contraria a cifração, ou seja, a descoberta do texto cifrado.

ISSN 2178-034X

material para trabalhar a matemática em sala de aula (TAMAROZZI, 2001). Nessa direção Olgin e Groenwald (2011), inferem que:

> A Criptografia é um exemplo de tema que pode ser abordado no Currículo do Ensino Médio, pois permite: desenvolver atividades didáticas utilizando padrões e regras de codificação e decodificação; trabalhar os conteúdos matemáticos, já desenvolvidos em sala de aula pelos professores, dentro de um contexto que envolve segurança de dados; possibilita recontextualizar um conteúdo dentro de outro tema, produzindo novos significados e relações enriquecedoras (OLGIN; GROENWALD, 2011, p. 75).

Em nosso mestrado buscamos refletir sobre as possibilidades de utilização desse tema aliado ao conceito de função afim, é que a proposta de tentar desenvolver um material didático na forma de uma sequência pedagógica de atividades envolvendo problemas criptográficos foi realizada. Tivemos o intuito de olhar para suas potencialidades a fim de explorar as ideias associadas ao conceito de função afim. Este artigo tem como objetivo apresentar alguns resultados dessa pesquisa.

2. Público e Metodologia da Investigação

Para tentar alcançar o objetivo da pesquisa, optou-se por desenvolver uma intervenção de caráter qualitativo, visto que para tentar encontrar respostas ao objetivo da pesquisa seria preciso compreender e analisar o processo discutido e vivenciado pelos alunos acerca das investigações desenvolvidas por eles durante a resolução das atividades propostas. Nesse sentido, propusemos a sete alunos do primeiro ano do Ensino Médio de uma escola pública da cidade de Rio Claro/ SP, uma sequência pedagógica composta por oito atividades[2] que abordam a definição de função afim, bem como outros conceitos, tais como, função linear, função identidade e função constante, além de trabalhar com a parte gráfica e as respectivas funções inversas.

Assim, os sete alunos foram convidados a participar de encontros, na própria escola (em sala de vídeo ou em sala de aula), com o propósito de desenvolver a sequência pedagógica de atividades envolvendo problemas criptográficos desenvolvidos pela pesquisadora. A partir do aceite dos mesmos, os encontros aconteceram entre os meses de

[2] As atividades, a saber, Si-lá-box, Um caso de sequestro, O detetive Watson, Cifrando um poema, Criptograma, O jogo, O poeta assassino e Cifrando sua história, foram estruturadas na forma de enigmas envolvendo contos baseados no personagem Sherlock Holmes, de Sir Arthur Conan Doyle. Para mais informações sobre as atividades ver em Litoldo (2016, no prelo).

maio e setembro de 2014, ocorrendo um ou dois encontros por semana e tendo como duração duas horas cada encontro[3]. No total foram realizados dezoito (18) encontros.

Os alunos eram agrupados entre si para desenvolver as atividades e os grupos variavam de acordo com os encontros. Os procedimentos metodológicos para registrar os dados foram: as observações da pesquisadora registradas em seu diário de campo, as gravações em vídeo e áudio referentes às discussões de cada grupo durante os encontros, o material produzido (respostas das atividades) pelos alunos e entrevistas semiestruturadas. A partir dos dados coletados, organizamos as categorias observadas em: atitudes desenvolvidas, procedimentos utilizados e conceitos construídos.

3. 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 cada vez

[3] Vale salientar que o período de coleta dos dados ultrapassou o tempo estimado pela pesquisadora visto que o ano de 2014 teve um calendário atípico em virtude da Copa do Mundo no Brasil.

ISSN 2178-034X

mais cifras seguras e 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 são encontrados nos documentos que narram a *Guerra de Gália*. Júlio César, imperador romano, utilizava muito uma escrita de substituição a qual ficou conhecida como sendo a *Cifra de César*. Tal cifra pode ser definida com sendo um deslocamento do alfabeto, três casas a esquerda, ou seja, a letra A de uma mensagem seria cifrada pela letra D, B por E, e, assim por diante. A cifra de Vigenère pode ser considerada uma evolução da *Cifra de César*. Desenvolvida em sua forma final por Blaise de Vigenère, por volta de 1562, ela é composta por 26 alfabetos cifrados distintamente e uma palavra chave.

A partir dessas duas cifras, muitas outras se originaram (cifra *ADFGVX*, cifra do *Chiqueiro,* cifra *Lucifer* entre outras[4]). Com o surgimento dos aparelhos eletrônicos, tais como o telégrafo (1842) e o rádio (1935), as comunicações começaram a fluir de maneira mais rápida, no entanto, esses meios também apresentavam ineficiência quanto a sua segurança de intercepção, visto que, não era difícil invadir tais meios e adquirir as mensagens transmitidas. Essa vulnerabilidade impulsionou o primeiro grande salto no desenvolvimento de cifras seguras. Esse primeiro salto 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. De acordo com Singh (2008, p. 146) a *Enigma* "se tornaria [naquele período] o mais terrível sistema de cifragem da história" 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 grande salto 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 na matemática um método de

[4] Para mais informações a respeito dessas cifras ver SINGH, S. *O livro dos códigos: A ciência do sigilo - do antigo Egito à criptografia quântica*. 7. ed. Rio de Janeiro: Record, 2008.

cifragem que garantisse, mesmo com intercepções, 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. Resultados e discussões

Nos primeiros encontros, os alunos mostraram-se com pouca autonomia investigativa e solicitavam à pesquisadora que lhes explicasse os enunciados das atividades e confirmasse as respostas. No entanto, conforme os encontros foram ocorrendo, observou - se que os alunos se sentiam mais confortáveis com o ambiente proposto pela pesquisadora e aos poucos foram desenvolvendo atitudes de autoestima e autonomia. A flexibilidade que as atividades apresentavam sobre seus métodos de solução concedia aos alunos uma situação livre para que eles desenvolvessem suas próprias estratégias de resolução. Isso ficou evidente quando se observou as diferentes estratégias desenvolvidas pelos alunos para decifrarem as mensagens e resolver as atividades propostas. Os conhecimentos prévios dos alunos proporcionaram aos mesmos utilizar intuições e estratégias de resolução durante as atividades, bem como resgatar e explorar outros conceitos da matemática. Discussões sobre os conceitos de números primos, números pares, números ímpares, múltiplos de três, conceito de plano cartesiano e paralelismo entre retas foram abordados pelos alunos e resgatados para fazerem parte de suas resoluções.

Com o movimento exploratório das atividades, fazendo uso de seus conhecimentos heurísticos, os alunos foram tomando atitudes investigativas, o que contribuía para a criação e elaboração de diferentes estratégias de resolução. A cada atividade, os alunos desenvolviam suas estratégias e as utilizavam conforme eles mesmos achavam interessantes para aquela

[5] Utilização de chaves diferentes para cifração e decifração. Para mais informações ver em:
RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. *A method for obtaining digital signatures and public-key cryptosystems*. CACM, l21, p. 120–126, 1978. Disponível em: < http://people.csail.mit.edu/rivest/Rsapaper.pdf >.

ISSN 2178-034X

atividade proposta.

Esse fato se tornou interessante na medida em que os alunos trocavam entre si suas ideias de resolução e a aperfeiçoavam conforme o problema apresentado. Os três episódios abaixo apresentam momentos de criação, transição e desenvolvimentos das estratégias criadas pelos alunos[6].

Episódio 1
Fernando começou a decifrar a carta[7] 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.

Fonte: Gravações de vídeo e áudio e diário de campo (2015).

Episódio 2
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 $(-2) \times x - 1$.
   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 $(-2) \times x - 1$, 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 $(-15) + (-2) = -17$

[6] Os nomes dados aos alunos aqui apresentados são fictícios.
[7] A carta é uma mensagem cifrada que faz parte da atividade chamada "*Um caso de sequestro*".

$$9 \times (-2) - 1 = -19 \text{ e } (-17) + (-2) = -19$$
$$10 \times (-2) - 1 = -21 \text{ e } (-19) + (-2) = -21$$

Fonte: Gravações de vídeo e áudio, ficha de perguntas e diário de campo (2015).

Episódio 3

Essa dupla, após observar o criptograma[8], 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).

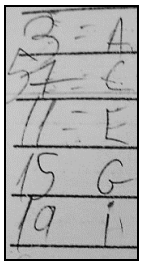

Figura 1 - Informações que Gustavo retirou das dicas respondidas no criptograma.

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.

Fonte: Gravações de vídeo e áudio, ficha de perguntas e diário de campo (2015).

Junto com os conhecimentos prévios abordados, os alunos também utilizaram a calculadora como uma ferramenta de auxilio para resolver as atividades (Figura 2). A utilização desse recurso tecnológico esteve presente em todos os encontros. Os alunos souberam utilizá-la das seguintes 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 se articulavam acerca de algumas hipóteses de resolução e depois de discuti-las, colocavam-nas em prática e verificavam se essas hipóteses os ajudavam ou não a resolver o problema.

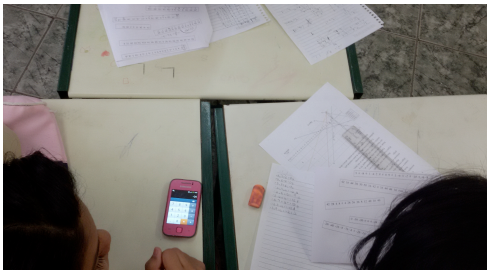

Figura 2 - Utilização da calculadora.
Fonte: Litoldo (2016, no prelo).

[8] Criptograma é uma atividade que envolve dicas onde suas respostas são mensagens cifradas.

ISSN 2178-034X

Assim, observou-se que durante os encontros, o movimento de debates entre os alunos e as discussões sobre as ideias desenvolvidas por eles contribuíram para as explorações dos procedimentos de estratégias, para uma afirmação das atitudes investigativas, para as organizações dos pensamentos e das resoluções e, por fim, para as explorações do conceito de função afim.

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. Após as primeiras atividades que abordou a definição de função afim e suas particularidades, os alunos sempre que sentiam a necessidade traziam para a resolução das atividades seguintes as representações e os pensamentos algébricos relacionados a esta função. A figura 3 faz parte de uma das resoluções da atividade "*O jogo*". Essa atividade era composta por gráficos de funções afim, os quais eram apresentados aos alunos como sendo as pistas para as decifrações das mensagens. É possível observar que nesse caso, os alunos retomaram a expressão algébrica da função afim utilizando os pontos encontrados nos gráficos. Realizando esses cálculos, os alunos conseguiram encontrar a função cifradora das mensagens e com isso construir o alfabeto cifrado. Desenvolvendo essa estratégia de resolução, os alunos decifraram as mensagens e concluíram a atividade proposta.

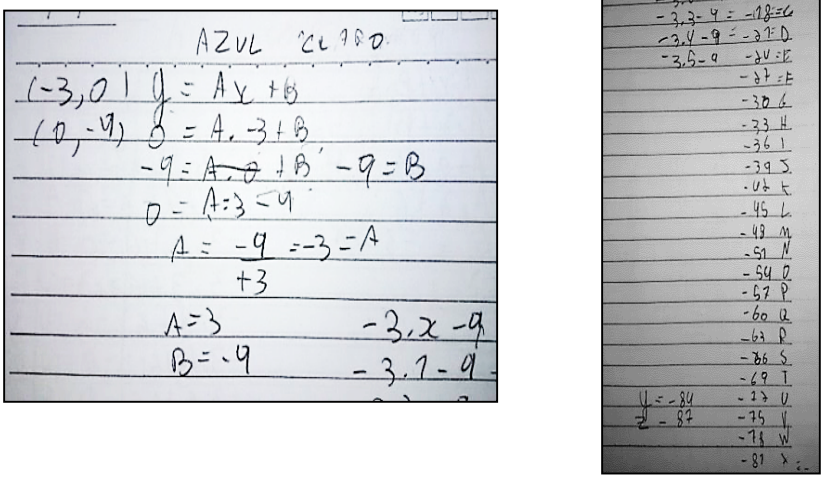

Figura 3 - Estratégia de resolução realizada por um dos grupos por meio do pensamento algébrico.
Fonte: Litoldo (2016, no prelo).

Durante os encontros também ficou evidente o trabalho coletivo que os alunos desenvolveram entre si (Figura 4). Os alunos trabalharam em grupo, ficando evidente em algumas situações a troca de informações na tentativa de auxiliar o outro na resolução do problema. Havia a preocupação dos mesmos em explicitar as ideias de resolução criadas por eles. Os alunos explicavam e discutiam com os seus colegas suas ideias, tentando explicitar o sentido dado a elas em suas resoluções. Eles se posicionavam abertos ao dialogo e sempre se mostravam dispostos a negociar os significados. Essas atitudes contribuíram para que eles explorassem as ideias associadas à função afim, partindo, em alguns casos, dos pensamentos e representações algébricas dessa função.

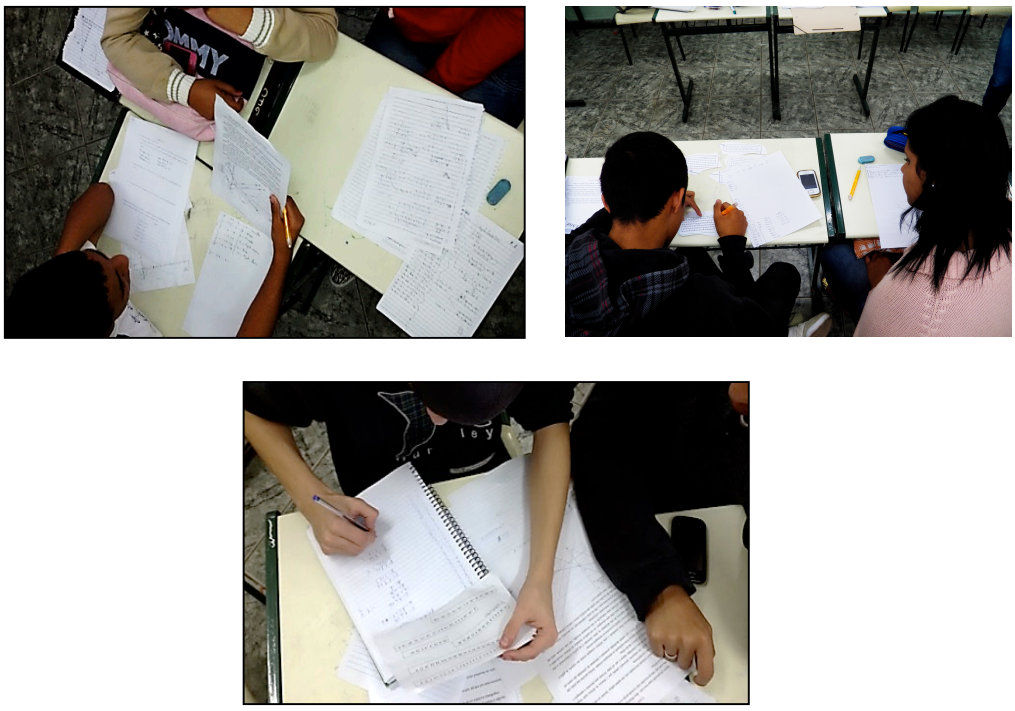

Figura 4 - Alunos desenvolvendo a atividade em grupo.
Fonte: Litoldo (2016, no prelo).

Os alunos também se organizavam entre os grupos a fim de dividir as tarefas de decifração e otimizar o tempo de resolução das atividades. 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.

Conforme os alunos resolviam as atividades, apareciam alguns indícios de comprometimento e responsabilidade com o trabalhado ali realizado. Esses indícios se tronavam mais frequentes à medida em que os alunos se envolviam mais com a proposta. As

ISSN 2178-034X

indicações dessa postura de compromisso refletiram no pedido dos próprios alunos em levar as atividades para a casa, visto que, segundo eles, as atividades eram interessantes e eles gostariam de tentar resolve-las fora dos encontros.

5. Considerações Finais

Na seção acima foram apresentados alguns resultados que se destacaram na pesquisa de mestrado desenvolvida acerca da proposta apresentada. Ao analisar esses dados pode-se concluir que a sequência pedagógica de atividades envolvendo problemas criptográficos permitiu que os alunos explorassem e resgatassem diferentes conceitos matemáticos advindos de seus conhecimentos prévios, os quais deram subsídios para que eles investigassem as atividades propostas. O pensamento algébrico e suas representações foram aos poucos sendo desenvolvidos e resgatados pelos alunos como estratégias de resolução. O trabalho de discutir essas representações juntamente com as ideias de resoluções advindas de seus conhecimentos prévios contribuiu para que os alunos explorassem as ideias associadas à função afim.

Como um resultado, observa-se que atividades envolvendo o tema Criptografia 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 procedimentos heurísticos 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 dos dados, levando em consideração o trabalho em grupo realizado, as atitudes investigativas assumidas pelos alunos, o envolvimento com as atividades propostas e a atenção dada a elas durante todo o trabalho de campo é que se pode inferir que uma sequência pedagogia de atividades 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.

6. Referências

BRASIL. *Base Nacional Comum Curricular*. Brasília-DF: Ministério da Educação, 2015. Disponível em: <http://basenacionalcomum.mec.gov.br/#/site/inicio>. Acesso em: 7 jan. 2016.

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. Disponível em: <http://portal.mec.gov.br/seb/arquivos/pdf/ciencian.pdf>. Acesso em: 20 fev. 2016.

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, n. 10, 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 uma sequência pedagógica de atividades envolvendo problemas criptográficos na exploração das ideias associadas à função afim*. 2016. 200 f. Dissertação – Universidade Estadual Paulista "Júlio de Mesquita Filho", Rio Claro - SP, 2016, no prelo.

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.

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

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