



Universidade do Estado do Rio de Janeiro

Centro de Tecnologia e Ciências

Instituto de Matemática e Estatística

Bruno Laranjeira Nunes

Aplicações de Criptografia no Ensino Básico

Rio de Janeiro

2017

Bruno Laranjeira Nunes

Aplicações de criptografia no Ensino Básico



Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, da Universidade do Estado do Rio de Janeiro.

Orientadora: Prof.^a Dra. Jeanne Denise Bezerra de Barros

Rio de Janeiro

2017

CATALOGAÇÃO NA FONTE
UERJ / REDE SIRIUS / BIBLIOTECA CTC-A

N972 Nunes, Bruno Laranjeira.
Aplicações da Criptografia no Ensino Básico / Bruno
Laranjeira Nunes. - 2017.
80 f. : il.

Orientadora: Jeanne Denise Bezerra de Barros.
Dissertação (Mestrado Profissional em Matemática em Rede
Nacional - PROFMAT) - Universidade do Estado do Rio de
Janeiro, Instituto de Matemática e Estatística.

1. Criptografia - Teses. 2. Matrizes (Matemática) – Teses. 3.
Língua brasileira de sinais – Teses.. I. Barros, Jeanne Denise
Bezerra de. II. Universidade do Estado do Rio de Janeiro. Nome
do Instituto. III. Título.

CDU 003.26

Autorizo, para fins acadêmicos e científicos, a reprodução total ou parcial desta
dissertação, desde que citada a fonte.

Assinatura

Data

Bruno Laranjeira Nunes

Aplicações de Criptografia no Ensino Básico

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, da Universidade do Estado do Rio de Janeiro.

Aprovada em 18 de agosto de 2017.

Banca Examinadora:

Prof.^a Dra. Jeanne Denise Bezerra de Barros (Orientadora)
Instituto de Matemática e Estatística- UERJ

Prof. Dr. Rubens André Sucupira
Instituto de Matemática e Estatística - UERJ

Prof.^a Dra. Ângela Cássia Biazutti
Instituto de Matemática - UFRJ

Prof. Dr. Fernando Antônio de Araújo Carneiro
Instituto de Matemática e Estatística – UERJ

Rio de Janeiro

2017

DEDICATÓRIA

Dedico este trabalho primeiramente a Deus, pois sem ele eu não teria forças para esta longa jornada, ao meu pai Valmer de Freitas Nunes e à minha mãe Valdinete Francisca Laranjeira Nunes.

AGRADECIMENTOS

Primeiramente à Deus, que permitiu e me deu força para chegar até aqui.

À Universidade Estadual do Rio de Janeiro, pela oportunidade de fazer o curso em um ambiente criativo e amigável.

À Professora Jeanne, por seu empenho total à elaboração desse trabalho, sempre orientando, apoiando e me passando confiança nos momentos que senti fraqueza.

Aos professores do PROFMAT, não somente por terem me ensinado, mas por terem me feito aprender.

Aos meus pais, por todo amor, carinho, incentivo e apoio incondicional.

Ao meu amigo e professor Adriano Araújo do Nascimento, pela cumplicidade durante minha graduação e pelo apoio profissional depois de graduado.

Meus agradecimentos aos meus familiares, amigos e aos colegas de trabalho, que fizeram parte da minha formação e que continuarão presentes em minha vida.

À CAPES, que concedeu bolsa de estudos, me proporcionando tranquilidade durante o curso.

Aos companheiros de turma do mestrado, pela união e companheirismo.

A todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

A Matemática, quando a compreendemos bem, possui não somente a verdade, mas também a suprema beleza.

Bertrand Russel

RESUMO

NUNES, Bruno Laranjeiras. **Aplicações de Criptografia no Ensino Básico**. 2017. 86 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - Profmat) – Instituto de Matemática e Estatística, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2017.

Este trabalho tem como objetivo apresentar uma sequência de atividades utilizando a Criptografia como instrumento de desenvolvimento no ensino dos conceitos e propriedades das funções e das matrizes, além de desenvolver uma sequência de atividades com libras, inserindo o aluno no mundo dos deficientes auditivos, que poucos conhecem. A criptografia foi escolhida como tema, por ser atual e para também desconstruir essa imagem de algo impossível de ser compreendida. As atividades propostas com libras foram aplicadas em quatro turmas de oitavo ano do Ensino Fundamental da Escola Municipal Ginásio Francisco Caldeira de Alvarenga. Em um primeiro instante, foi dada uma aula de história da criptografia, falando sobre a origem e os grandes feitos até a atualidade, o que já deixou de ser uma aula tradicional. A segunda etapa, foi composta por atividades onde os alunos escreviam palavras com os sinais do alfabeto de libras e também traduziam as que já se encontravam escritas por esses símbolos. Após esta prática, os alunos enviavam mensagens a algum colega fazendo os gestos com suas mãos, enquanto eles descobriam o que estava sendo gesticulado. A terceira etapa consiste na aplicação destas atividades anteriores, usando números e operações, fazendo o aluno entender o conceito básico de função de forma lúdica. Nas etapas 2 e 3 foram aplicadas pequenos questionários para serem feitas análises sobre as melhorias causadas no ensino e na aprendizagem do tema. Tais metodologias deram suporte aos resultados obtidos de que as atividades desenvolvidas melhoram o interesse, o desempenho e a compreensão dos alunos, motivando-os na disciplina através de uma aula mais lúdica. Já as atividades com funções e com matrizes não foram aplicadas nesse trabalho, mas serão trabalhadas em outra oportunidade. Ambas precisam de conhecimento prévio de seus conceitos e propriedades para serem aplicadas e fixadas de forma lúdica. As atividades com funções, serão divididas em três partes: Função Afim, Função Quadrática e Funções Exponencial e Logarítmica. Todas serão aplicadas em turmas do primeiro ano do Ensino Médio, sempre após à aprendizagem de cada uma. Com as atividades de matrizes, terá uma aula pra relembrar conceitos, para na aula seguinte aplicar as atividades. Cada uma das atividades possui um questionário subjetivo ao final para os alunos poderem avaliar com seu ponto de vista.

Palavras-chave: Criptografia. Libras. Funções Afim. Quadrática. Exponencial e Logarítmica. Matrizes.

ABSTRACT

NUNES, B. **Applications of Cryptography in Basic Education**. 2017. 86 f.
Dissertação (Mestrado Profissional em Matemática em Rede Nacional - Profmat) – Instituto de Matemática e Estatística, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2017.

This work aims to present a sequence of activities using Cryptography as an instrument of development in teaching the concepts and properties of functions and matrices, as well as developing a sequence of activities with pounds, inserting the student in the world of the hearing impaired, which few know. Encryption was chosen as a theme, because it is current and also to deconstruct this image from something impossible to understand. The activities proposed with pounds were applied in four classes of eighth grade of Elementary School of the Municipal School Gymnasium Francisco Caldeira de Alvarenga. At first, a history of cryptography was given, talking about the origin and the great achievements to date, which is no longer a traditional classroom. The second stage was composed of activities where the students wrote words with the signs of the alphabet of pounds and also translated those already written by these symbols. After this practice, the students sent messages to a classmate doing the gestures with their hands while they discovered what was being gesticulated. The third step is to apply these previous activities, using numbers and operations, making the student understand the basic concept of function in a playful way. In steps 2 and 3, small questionnaires were used to analyze the improvements made in teaching and learning the subject. Such methodologies have supported the results obtained that the activities developed improve students' interest, performance and understanding, motivating them in the discipline through a more playful class. However, activities with functions and matrices have not been applied in this work, but will be worked on at another time. Both need prior knowledge of their concepts and properties to be applied and fixed in a playful way. The activities with functions will be divided into three parts: Related Function, Quadratic Function and Exponential and Logarithmic Functions. All will be applied in classes of the first year of High School, always after learning each one. With the activities of matrices, you will have a class to remember concepts, in order to apply the activities in the next class. Each of the activities has a subjective questionnaire at the end so that the student can evaluate with their point of view.

Keywords: Cryptography. Pounds. Afim. Quadratic. Exponential and Logarithmic Functions. Matrices.

LISTA DE FIGURAS

Figura 1 –	Relação professor - aluno - saber na Metodologia Sequência Fedathi.....	23
Figura 2 –	Hieróglifo em parede de templo egípcio.....	25
Figura 3 –	Imagem de uma cítala.....	26
Figura 4 –	Cifra de César.....	27
Figura 5 –	Cifra de Vigenère.....	27
Figura 6 –	Palavra chave sendo usada para cifrar.....	28
Figura 7 –	Ilustração da máquina do enigma.....	29
Figura 8 –	Criptografia Assimétrica.....	30

LISTA DE ABREVIATURAS E SIGLAS

LDB	Leis e Diretrizes e Bases da Educação
PCNs	Parâmetros Curriculares Nacionais
PROFMAT	Mestrado Profissional em Matemática em Rede Nacional
SEEDUC/RJ	Secretaria Estadual de Educação do Rio de Janeiro
SME/RJ	Secretaria Municipal de Educação do Rio de Janeiro
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
UFC	Universidade Federal do Ceará

SUMÁRIO

	INTRODUÇÃO	13
1	JUSTIFICATIVA	15
1.1	Objetivos	15
1.1.1	Objetivo Geral	15
1.1.2	Objetivos específicos	16
2	PRESSUPOSTOS TEÓRICOS	17
2.1	Fundamentos Teóricos da Pesquisa em Educação	17
2.1.1	<u>Metodologia Sequência Fedathi</u>	17
2.1.2	<u>Definição Metodologia Sequência Fedathi</u>	18
2.2	Fundamentação Matemática da Criptografia	20
2.2.1	<u>Um Pouco de História</u>	20
2.2.2	<u>Criptografia Clássica</u>	21
2.2.3	<u>Criptografia Moderna</u>	24
2.2.4	<u>Aplicação da Metodologia Sequência Fedathi com Criptografia e Libras, Funções e Matrizes</u>	26
3	METODOLOGIA	29
3.1	Libras	29
3.2	Funções	30
3.3	Matrizes	32
4	ALICAÇÃO E ANÁLISE DAS ATIVIDADES DE LIBRAS EM SALA DE AULA	34
4.1	Questionário Subjetivo da Atividade I	34
4.2	Questionário Subjetivo da Atividade II	50
	CONSIDERAÇÕES FINAIS	59
	REFERÊNCIAS	62
	ANEXO A - Atividade explicativa da aplicação de criptografia em libras.....	64
	ANEXO B -Atividade de fixação da aplicação de criptografia em libras.....	65
	ANEXO C - Continuação da primeira atividade com libras	66
	ANEXO D -Atividade explicativa da aplicação de criptografia em	

Função afim.....	68
ANEXO E -Atividade de fixação da aplicação de criptografia em Função Afim	70
ANEXO F -Atividade explicativa da aplicação de criptografia em Função Quadrática.....	71
ANEXO G -Atividade de fixação da aplicação de criptografia em Função Quadrática.....	73
ANEXO H -Atividade explicativa da aplicação de criptografia em Função Exponencial.....	74
ANEXO I -Atividade de fixação da aplicação de criptografia em Função Exponencial.....	76
ANEXO J -Atividade explicativa da aplicação de criptografia em Matrizes	77
ANEXO K -Atividade de fixação da aplicação de criptografia em Matrizes	79
ANEXO L –Termo de Consentimento Informado.....	80

INTRODUÇÃO

Este estudo foi motivado pelo convívio em sala de aula, onde o estudante demonstra dificuldades e desinteresse por matemática. Muitos desses alunos as vezes fazem perguntas do tipo "pra que serve matriz?", "pra que serve funções?" ou "o que é libras?", o que nos mostra que parte disso também é culpa de quem ensina, que apenas usa o quadro para dar uma aula tradicional.

A partir desses problemas demonstrados, é necessário um olhar mais atento para a forma que esses conteúdos são transmitidos. O professor tem que deixar de olhar para sua profissão como apenas um ganha pão e tratar com amor o que faz, pois nós "professores de matemática" devemos planejar aulas, buscar assuntos interessantes e recorrentes, para usá-los em nossas aulas de forma lúdica e assim despertar interesse nos alunos.

A escolha da criptografia, além de uma boa aplicação que desenvolve o raciocínio lógico, também trata-se de um tema bem atual onde desperta curiosidade nos adolescentes.

A presente dissertação é requisito parcial para obtenção do título de Mestre, pelo programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, da Universidade do Estado do Rio de Janeiro e foi desenvolvido ao longo do ano de 2016, a partir de uma pesquisa de campo realizada com alunos dooitavo ano do Ensino Fundamental da Escola Municipal Ginásio Francisco Caldeira de Alvarenga, escola a qual o autor é professor efetivo de Matemática, desde 2011.

E este trabalho de conclusão está dividido em 5 (cinco) capítulos organizados da seguinte forma: o capítulo 1 (um) traz a justificativa do tema abordado, além abordar os objetivos gerais e os objetivos específicos.

No capítulo 2 (dois), vem a apresentação dos pressupostos teóricos, mostrando o modelo desenvolvido, apresentando a Sequência Fedathi, onde e quando surgiu, como se define e qual a sua proposta. Ainda neste capítulo, falaremos um pouco da parte histórica da criptografia, retratando de forma resumida criptografia clássica e criptografia moderna. Após, falaremos sobre a relação entre a Sequência Fedathi, a criptografia e libras, funções ou matrizes.

No terceiro capítulo, será mostrado a metodologia usada nas aplicações das atividades envolvendo libras, funções afim, quadrática e exponencial, e também, matrizes.

No capítulo 4, estão todos os passos da narrativa envolvendo a aplicação do trabalho de campo. Sendo mostrado também os gráficos envolvendo as respostas dos questionários subjetivos para analisar a opinião dos alunos em relação ao trabalho.

O quinto capítulo, conclui o trabalho através das considerações finais.

1 JUSTIFICATIVA

O tema "Criptografia" foi escolhido por além de ser bem atual, também por estabelecer dentro da prática educativa uma relação entre aprender conhecimentos sistematizados e as questões da vida real e de sua transformação. Desta forma, aplicando a transversalidade, que é uma orientação dos PCNs, que foram definidos a partir da elaboração da LDB. Colocar em prática essas recomendações tem um papel fundamental, pois por ser professor das redes estadual (SEEDUC/RJ) e municipal (SME/RJ), o que sempre vejo são alunos desmotivados com a disciplina matemática, chegando ao Ensino Fundamental sem base e sem vontade de aprendê-la. A utilização desse tema nos permite sair da rotina, e não ensinar de forma tão clássica como a matemática vem sendo apresentada ainda nos dias de hoje. Groenwald e Franke (2008) afirmam que

E como a criptografia possibilita interligar os conteúdos matemáticos à situações do mundo real, e ajuda a desenvolver habilidades e competências na resolução de problemas, a criar estratégias de resolução, a ter autonomia durante o processo de aprendizagem.

Segundo Perrenoud (2009), "A escola não pode ignorar o que passa pelo mundo. As novas tecnologias da informação e da comunicação transformam espetacularmente não só nossas maneiras de comunicar, mas também de trabalhar, de decidir, de pensar". Assim, esta pesquisa tem por objetivo motivar os alunos, fazendo com que eles deixem de ver a matemática de forma negativa, usar a tecnologia como recurso para a aplicação dos conteúdos citados e buscar a melhora na eficiência da abordagem desses conteúdos.

1.1 Objetivos

1.1.1 Objetivo Geral

Este trabalho tem como objetivo promover uma aprendizagem significativa aplicando a criptografia no Ensino da Matemática das escolas públicas e tornando-a mais lúdica para que assim possamos ensinar conceitos e propriedades de funções

e matrizes, além de aplicar libras e inserir os alunos no mundo dos deficientes auditivos.

Atualmente o estudo de matrizes é dado no segundo ano do Ensino Médio, enquanto o ensino de funções é introduzido no nono ano do Ensino Fundamental e ensinado plenamente no primeiro ano do Ensino Médio. Já as atividades de libras, podem ser aplicada em turmas de oitavo e nono anos do Ensino Fundamental. Dessa forma, espera-se que o aluno desenvolva as habilidades e competências em seu respectivo ano.

1.1.2 Objetivos Específicos

- Apresentar aos alunos uma aula mais interessante através da relação existente entre Criptografia e libras e desenvolver atividades aliando o tema aos conteúdos selecionados;
- Usar a Metodologia Sequência Fedathi na aplicação das atividades;
- Conseguir despertar o interesse dos alunos, estimulando-os durante a apresentação das atividades, mostrando que a matemática pode ser ensinada de uma forma lúdica;
- Criar interação entre alunos e professor , desenvolvendo neles a autonomia para que possam atuar em sala de aula com um papel mais ativo.

2 PRESSUPOSTOS TEÓRICOS

2.1 Fundamentos Teóricos da Pesquisa em Educação

2.1.1 Metodologia Sequência Fedathi

A Metodologia Sequência Fedathi constitui-se de uma proposta que fora desenvolvida por professores, pesquisadores e alunos de pós-graduação da Faculdade de Educação da UFC (Universidade Federal do Ceará). Segundo Borges Neto (1995), essas pessoas que compõem o grupo que fora formado no início dos anos 90, para tratar de questões relativas a didática da matemática.

Esta metodologia tem por objetivo apresentar um ensino que se preocupa com antes, durante e depois do momento de aula. A prática didática do docente deve começar bem antes de entrar em uma sala de aula, pois o mesmo deve planejar uma aula através de reflexões baseadas em significados e preocupações diagnósticas, pois o processo não é apenas ensinar, mas também motivar, mover e refletir sobre. Essas questões tratam-se de métodos direcionados para a melhoria da prática pedagógica que visa a postura do professor de maneira mais adequada em sala de aula, fazendo com que o aluno supere os obstáculos epistemológicos e didáticos na abordagem dos conceitos matemáticos. Desta forma, a metodologia se baseia em quatro fases: tomada de posição, maturação, solução e prova. Portanto, o educador ensina cada vez menos enquanto o educando aprende cada vez mais, sendo movidos pelas situações a-didáticas. Segundo Silva (2008):

As situações a-didáticas constituem o momento de grande potencialidade onde o aluno poderá vir a romper as velhas práticas da repetição e do modelo, entretanto é importante lembrar que a intenção pedagógica caracteriza todas as etapas do processo didático uma vez que todo o trabalho do professor é previamente determinado por objetivos, métodos e noções conceituais.

De acordo com Brousseau, citado por Silva (2008), o planejamento de uma situação didática precisa ter momentos onde o aluno se encontra sozinho diante do problema a resolver e sem a intervenção do professor. Então, entende-se que o método visa uma nova relação de aprender a aprender considerando o tripé: professor-conhecimento-aluno.

Este trabalho tem o objetivo de apresentar esta metodologia como uma forma facilitadora para o ensino aprendizagem da matemática.

2.1.2 Definição da Metodologia Sequência Fedathi

Neste tópico, veremos a definição desta metodologia e suas etapas como uma alternativa no processo de ensino aprendizagem.

O aprendizado em matemática não pode ficar restrito apenas a um momento em sala de aula, como se a disciplina fosse somente uma fase que está de passagem na vida do aluno. Para Borges Neto & Dias (1995):

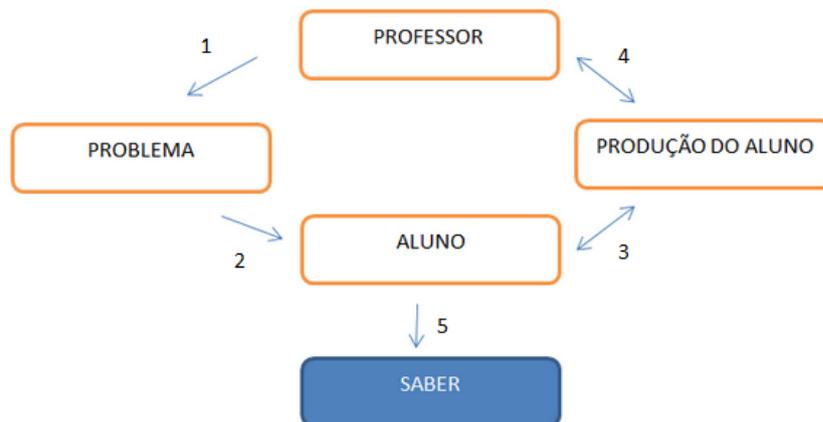
O aluno reproduz ativamente os estágios que a humanidade percorreu para compreender os ensinamentos matemáticos, sem que, para isso, necessite dos mesmos milênios que a história consumiu para chegar ao momento atual.

Entendemos o quanto é importante reproduzir esse ambiente na sala de aula, para possibilitar ao aluno a constuição de conceitos com significados, através da resolução de problemas, onde suas produções são observadas e tomadas como objeto de partida para conduzir o processo de mediação a fim de construir o conhecimento em jogo. Nesse processo, o docente deverá aproveitar todos os experimentos que o aluno obteve e todo o histórico acerca das atividades desenvolvidas.

De acordo com o grupo que desenvolveu este método (1996), reproduzir o trabalho do matemático significa abordar uma situação de ensino, levando em consideração as fases de trabalho vivenciadas por esse profissional no desenvolvimento de suas experimentações e produções técnicas.

A figura abaixo sintetiza as relações entre o professor e o aluno no processo de construção do saber.

Figura 1 - Relação professor - aluno - saber na Metodologia Sequência Fedathi



Fonte: Borges Neto (2001)

De acordo com o esquema esboçado na figura 8, o processo de ensino ocorre da seguinte forma:

1. O professor seleciona um problema relacionado ao assunto que pretende ensinar;
2. em seguida, deverá abordar o problema em uma linguagem adequada aos alunos;
3. com o problema apresentado, os alunos irão investigá-los até que ache uma solução.
4. a solução encontrada será analisada pelo professor junto aos alunos.
5. Os passos 3 e 4 acontecerão alternadamente até o aluno construa o conhecimento.

Este método tem como princípios quatro estágios básicos para realizar o modelo acima. Estes são:

1. **Tomada de Posição:** A apresentação do problema feita pelo professor.
2. **Maturação:** Compreensão e identificação das variáveis envolvidas no problema através de discussão entre o professor e os alunos, em busca de possíveis caminhos que possam levar a solução.

3. **Solução:** Representação e organização de esquemas ou modelos que visem a solução do problema.
4. **Prova:** Apresentação e formalização do modelo matemático a ser ensinado.

Na matemática é o momento em que são apresentadas as demonstrações rigorosas de um problema resolvido.

2.2 Fundamentação Matemática da Criptografia

2.2.1 Um Pouco de História

Segundo Tkotz(2005), a criptografia vem do grego, onde, Kryptós significa escondido e gráphein significa grafia, é o conjunto de técnicas para ocultar informações de assuntos privados. O seu objetivo é transformar uma mensagem legível em algo impossível de ser compreendido(Dizemos cifrar uma mensagem), onde só quem possui a chave necessária pode interpretá-la(dizemos decifrar a mensagem).

A história da criptografia começou há milhares. Até poucas décadas, era chamada de criptografia clássica, ou seja, métodos que usam caneta e papel ou auxílios mecânicos simples. No início do século XX, com a invenção de máquinas mais complexas, que são mecânicas ou eletro-mecânicas, implicou em meios mais sofisticados e eficientes pra cifrar uma mensagem. E com o avanço tecnológico, a criptografia evoluiu também introduzindo a eletrônica e a computação aumentando a complexidade.

Junto ao desenvolvimento da criptografia, tivemos também o desenvolvimento da criptoanálise, que significa a quebra de códigos e cifras. A descoberta desde cedo foi preponderante para o curso da história, que teve como exemplos a motivação da entrada dos Estados Unidos na Primeira Guerra Mundial e o encurtamento da Segunda Guerra Mundial.

2.2.2 Criptografia Clássica(Medieval ao fim da 2ª Guerra Mundial)

Os primeiros indícios sobre criptografia nos leva aos egípcios, a cerca de 4500 a.C., quando encontraram hieróglifos irregulares esculpidos para cifrar seus documentos. Apesar de não ser considerados tentativas sérias de mensagens secretas, mas eram escritas que pertenciam apenas a um grupo seleta (sacerdotes, membros da realeza, altos cargos e escribas). Tivemos outros exemplos de criptografia, como na Mesopotâmia, que usavam tabuletas de argila para proteger informações e receitas de valor comercial. Posteriormente, por volta de 500 e 600 a.C., foi descoberto o uso da criptografia por estudiosos hebreus, como exemplo a cifra de Atbash.

Figura 2 - Hieróglifos em parede de templo egípcio



Fonte:Fedor Selivanov / Shutterstock.com

O exército espartano também se comunicava através de mensagens codificadas. Esse método consistia de forma que o emissor e o receptor possuíam

bastões cilíndricos de mesmo diâmetro ou em forma de prismas regulares com o lado da base de mesma medida, para que assim, fosse enrolada uma faixa de pergaminho em torno desse bastão, que era chamado de cítala, de forma que fosse espiralada. Após isso, a mensagem era escrita em cima da cítala ao longo de seu comprimento e depois desenrolava e entregava ao receptor que repetiria esse processo para a leitura do recado.

Figura 3 - Imagem de uma cítala de formato de prisma de um prisma hexagonal com tira de couro

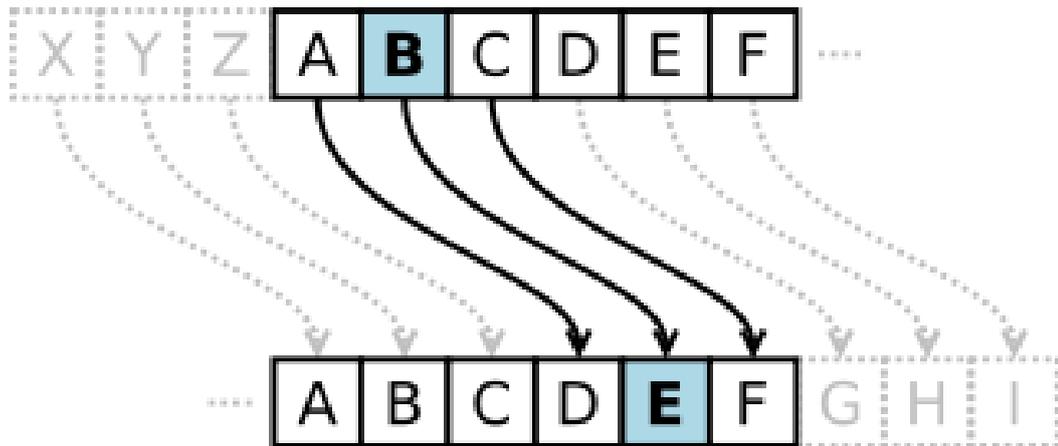


Fonte: <https://upload.wikimedia.org/wikipedia/commons/5/51/Skytale.png>

No primeiro século antes de Cristo, o governante Júlio César, considerado um dos maiores gênios militares da história, criou uma forma de codificar mensagens para manter seus segredos militares. Esse método consisti em substituir cada letra do alfabeto pela terceira seguinte e as três últimas pelas três primeiras, por exemplo, substitui o "A" por "D", o "J" por "M", o "Z" por "C" e assim sucessivamente.

Qualquer substituição de uma letra por outra letra ou símbolo é chamada de cifra, por isso esse método se chama Cifra de César.

Figura 4 - Cifra de César



Fonte: https://pt.wikipedia.org/wiki/Cifra_de_C%C3%A9sar

Desta forma, se quiser mandar a mensagem "GUERRAS DA GÁLIA" usando essa cifra, ficaria "JXHUUAV GD JDOLD".

Passado um tempo, essa cifra se tornou insegura, já que a regularidade das letras começava a ser percebida e desta forma a necessidade por cifras mais elaboradas e seguras surgia. A solução veio no século XVI com o diplomata e criptógrafo francês Blaise de Vigenère, que inventou um sistema polialfabético que leva seu nome, Cifra de Vigenère.

Figura 5 - Cifra de Vigenère

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

Fonte: https://pt.wikipedia.org/wiki/Cifra_de_Vigen%C3%A8re

Para decifrar uma mensagem o receptor precisa saber o alfabeto utilizado e a palavra-chave. Se cifrar a mensagem "Blaise de Vigenère" com a palavra-chave "cifra", associaremos as letras da palavra-chave, repetindo se necessário, com as da mensagem na mesma ordem.

Figura 6 - Palavra chave sendo repetida acima da mensagem letra por letra até a própria acabar

C	I	F	R	A	C	I	F	R	A	C	I	F	R	A	C
B	L	A	I	S	E	D	E	V	I	G	E	N	E	R	E

Fonte: Própria

Dessa forma, usaremos as letras que substituem "B" na chave "C", "L" na chave "I", "A" na chave "F" e assim sucessivamente, formando a mensagem "DTFZSG LJ MIIMSVRG". Assim, fica difícil de analisar qualquer frequência e por isso ficou conhecida por cerca de dois séculos com indecifrável.

Em 1929, o matemático norte americano Lester S. Hill inventou um tipo de cifra de substituição, que levou seu nome chamando-se Cifra de Hill, se baseando em conhecimentos em álgebra linear para codificar as mensagens. Em seu procedimento, primeiro converte-se as letras em números usando uma chave de substituição polialfabética, depois agrupe-os em uma matriz quadrada e multiplique por outra de mesma ordem que seja invertível. Os números resultantes são passados para letras novamente e temos a mensagem codificada. O receptor decifrará a mensagem usando a matriz inversa.

2.2.3 Criptografia Moderna

Com o avanço tecnológico e o envio de textos de modo seguro, surgiu a necessidade de cifrar mensagens através do uso da internet. Com isso, veio o surgimento da criptografia de chave simétrica, assimétrica e híbrida.

A **criptografia simétrica** usa somente uma chave para cifrar e decifrar a mensagem, que tem que conhecer o emissor e o receptor antecipadamente. Este que se torna o ponto frágil desse sistema, já que é mais fácil de interceptar uma chave que é transmitida sem segurança.

Teoricamente deveria ser mais fácil conhecer a chave interceptando-a em vez de provando-a uma por uma por força bruta, tendo em conta que a segurança de uma mensagem cifrada deve recair sobre a chave e nunca sobre o algoritmo.

Um exemplo de método simétrico que dependia de uma chave é a máquina enigma, que era uma máquina eletromecânica que cifrava as mensagens gerando letras segundo as posições de uns rolos que poderiam ser usados em diversas ordens e posições.

Figura 7 - Ilustração da máquina do enigma



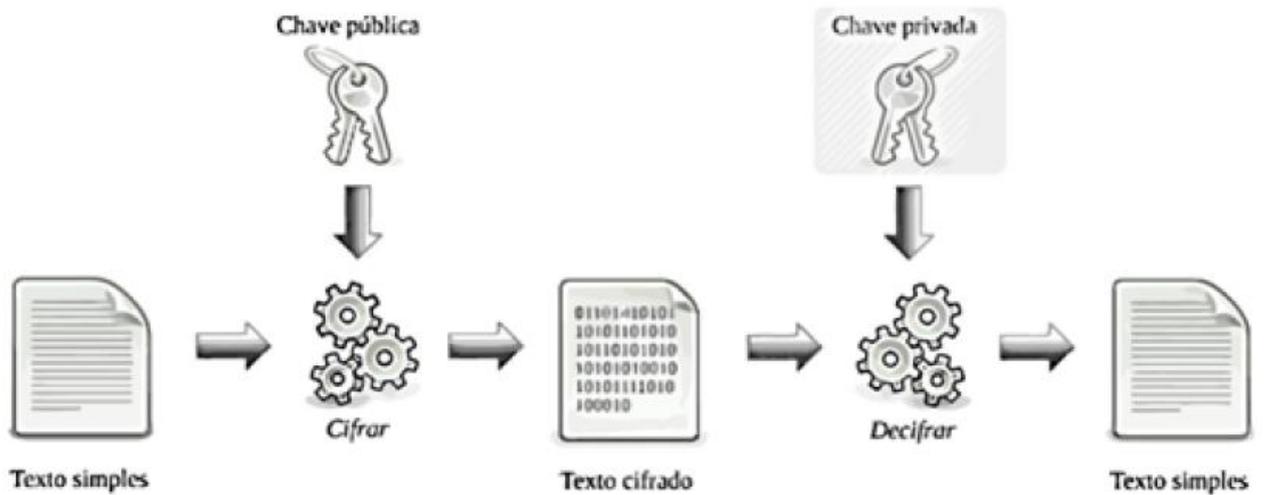
Fonte: Malagutti et. al. (2012)

Para cifrar a mensagem da máquina enigma era necessário possuir o livro de chaves que continha a chave do dia. Mas não era uma chave segura o suficiente para que não pudesse descobrir, tanto que os ingleses, com a ajuda dos poloneses, conseguiram o algoritmo, e por este motivo conseguiram as chaves da maioria dos dias.

A **criptografia assimétrica** se baseia no uso de uma chave pública, que pode ser contada as pessoas q entregaram a mensagem cifradas, e uma privada, que jamais deve ser revelada.

Outro propósito deste sistema é também o de poder firmar documentos, certificando que o emissor é quem disse ser, firmando com a chave privada e verificando a identidade com a chave pública.

Figura 8 - Criptografia Assimétrica



Fonte: Pigatto (2012)

As diferenças entre criptografia simétrica e assimétrica são que a primeira é mais insegura, já que o fato de passar uma única chave a torna muito vulnerável, porém, se pode cifrar e decifrar em menor tempo do que a assimétrica, que é o principal inconveniente e por esta razão que criou-se a **criptografia híbrida**.

A criptografia híbrida é um sistema criado com as vantagens das duas anteriores, resolvendo os problemas de que a simétrica é insegura e a assimétrica é lenta.

O processo de envio de um arquivo por esse sistema consiste em: gerar uma chave pública e uma privada; cifrar um arquivo de forma síncrona; o receptor envia uma chave pública; ciframos a chave que temos para enviar o arquivo com a chave pública do receptor; enviamos o arquivo cifrado, de forma síncrona, e a chave do arquivo cifrada, de forma assíncrona e somente o receptor pode ver.

Esses são os métodos criptográficos modernos que são usados até os dias de hoje. Por isso podemos realizar compras, pagamentos de faturas, transferências de dinheiro para outras contas, conversar com privacidade através de aplicativos, entre outras vantagens, com toda modernidade, segurança e eficácia.

2.2.4 Aplicação da Metodologia Sequência Fedathi com Criptografia e Libras, Funções e Matrizes

Mostraremos abaixo, situações de ensino de acordo com o modelo, voltadas para o ensino de libras com os alunos do Ensino Fundamental e para o ensino de

funções e matrizes com os alunos do Ensino Médio, tendo como foco o trabalho com criptografia como um facilitador no aprendizado.

1. Tomada de posição

De começo, indica-se ao professor que explique o que é criptografia, aborde seus conceitos, faça um resumo de sua história, conte sua evolução ao longo do tempo e sua importância nos dias de hoje para a sociedade.

Em seguida, recomenda-se que o professor aborde os conhecimentos prévios dos alunos através de algumas perguntas.

Feito isso, poderá propor uma situação problema, indicando uma palavra e despertando a curiosidade dos alunos de como poderia cifrá-la através de libras, função ou matriz (dependendo do caso). E depois como faria para decifrar.

Para direcionar o raciocínio dos alunos o professor poderá fazer uma atividade explicativa mostrando como cifrar e decifrar uma mensagem, e também formar grupos para que divida as tarefas e ocorra uma interação entre eles.

2. Maturação

Após apresentar a criptografia e a relação com a matéria desejada, e estimular os alunos, o professor deverá observar as estratégias para a solução e as dificuldades encontradas. Deverá mediar e estimular a interação entre eles para resolver os problema com tempo suficiente para discussões e experimentações.

Caso eles tomem um caminho errado, o professor intervém fazendo perguntas investigativas para que eles retomem o caminho da solução correta. Nesta fase, os alunos irão testar suas hipóteses, discutir com os colegas e considerar a opinião de todos. O professor deverá continuar passivo para observar as estratégias dos alunos.

3. Solução

Serão realizadas nesta etapa, duas ações: exposição das resoluções e e discuti-las com os outros alunos e o professor. Nesta fase teremos interação entre os alunos e o professor, e mesmo que o docente seja responsável pela mediação,

sugere-se que permita os alunos com um papel ativo, revendo seus resultados com os colegas.

O professor observará todas as estratégias usadas, analisar suas conjecturas e suas observações. Todas as resoluções deveram ser consideradas, até as que contiveram erros. Nesta etapa, deve ser dada ênfase ao raciocínio e estratégias dos alunos.

4. Prova

Neste momento o professor formaliza os conceitos, pois tais conteúdos são essenciais para o entendimento da situação problema. Neste último estágio, os alunos deverão ter adquiridos subsídios teóricos para entenderem e estabelecerem relações entre os resultados achados por eles e o modelo científico do conhecimento a ser aprendido.

3 METODOLOGIA

A proposta apresentada foi desenvolvida através das aplicações de atividades envolvendo libras, conceitos das funções afim, quadrática, exponencial e logarítmica, e também, conceitos e propriedades de matrizes, afim de relaciona-las com criptografia.

3.1 Libras

As atividades com libras foram aplicadas em quatro turmas do oitavo ano do Ensino Fundamental, nas quais o autor leciona no ano letivo de 2017. Foi usado um roteiro de aula e um trabalho de campo com duas atividades com questionários subjetivos repondidos ao fim de cada atividade. Com isso, obtivemos importantes informações sobre a eficiência do que foi aplicado.

A tabela 1 mostra o planejamento que define a quantidade de aulas necessárias para a execução das atividades propostas. Todas as etapas foram aplicadas ns quatro turmas de oitavo ano.

Tabela 1 - Roteiro de atividades propostas de libras

ETAPAS	TURMAS	DESCRIÇÃO	DURAÇÃO	DATA
Etapa 1	1, 2, 3 e 4.	Exposição do alfabeto de libras, mostrando a importância que ele possui.	2 tempos de aula (50 min cada)	09/05
Etapa 2	1, 2, 3 e 4.	Atividade explicativa (Anexo A).	1 tempo de aula (50 min)	10/05
Etapa 3	1, 2, 3 e 4.	Atividade de fixação em duplas e depois responder o questionário subjetivo (Anexo B).	1 tempos de aula (50 min cada)	10/05
Etapa 4		Aplicação de atividades	2 tempo de	22/05

	1, 2, 3 e 4.	associando o aprendizado a par ordenado/funções e ao final, responder questionário subjetivo. (Anexo C)	aula (50 min)	
--	-----------------	--	---------------	--

Fonte: o autor, 2017.

A seguir, com mais detalhes, é possível entender melhor o roteiro com as atividades que foram implementadas ao longo das etapas do trabalho, de acordo com a sequência mencionada na tabela 1:

1. Explicação teórica sobre o mundo dos deficientes auditivos e apresentação do alfabeto de libras; Apresentação de um breve resumo da história da criptografia.
2. Atividade explicativa de transformar palavras em sinais do alfabeto de libras, e logo em seguida fazer o inverso, transformando uma sequência de sinais em uma palavra. Depois, realização de uma dinâmica em que os alunos se comunicam usando apenas as mãos.
3. Divisão da turma em duplas para realização da atividade que os dois alunos, escolhem cada um, uma palavra, tendo que cifrá-la com o alfabeto de libras. Após os dois fazerem esse procedimento, um entregará ao outro a palavra cifrada, cada um tendo que decifrar. No final, os alunos respondem algumas perguntas para avaliar o que foi apresentado.
4. Aplicação de outra atividade usando os conhecimentos adquiridos na atividade anterior para aprender o conteúdo de maneira lúdica. Após isso, os alunos respondem outro questionário subjetivo.

3.2 Funções

As atividades com funções devem ser aplicadas em turmas de primeiro ano do Ensino Médio, onde os alunos devem assimilar conceitos e propriedades

aprendidos sobre as funções afim, quadrática, exponencial e logarítmica com a criptografia.

A tabela 2 mostra o roteiro com a sequência das atividades propostas.

Tabela 2 - Roteiro de atividades propostas de funções

ETAPAS	DESCRIÇÃO	DURAÇÃO
Etapa 1	Atividade explicativa sobre aplicação de criptografia no ensino de função afim (Anexo D).	1 tempo de aula (50 min cada)
Etapa 2	Atividade de fixação da etapa 1 e um questionário subjetivo (Anexo E).	2 tempos de aula (50 min)
Etapa 3	Atividade explicativa sobre aplicação de criptografia no ensino de função quadrática (Anexo F).	1 tempo de aula (50 min cada)
Etapa 4	Atividade de fixação da etapa 3 e um questionário subjetivo (Anexo G).	2 tempos de aula (50 min)
Etapa 5	Atividade explicativa sobre aplicação de criptografia no ensino de função exponencial (Anexo H).	1 tempo de aula (50 min)
Etapa 6	Atividade de fixação da etapa 5 e um questionário subjetivo (Anexo I).	2 tempos de aula (50 min)

Fonte: o autor, 2017.

Em seguida, as atividades do roteiro serão detalhadas de acordo com as etapas implementadas seguindo a sequência acima na tabela 2:

1. Atividade demonstrativa para o aluno aprenda sobre domínio e imagem da função afim, além de trabalhar os conceitos de função inversa.
2. Cada aluno escolherá um(a) parceiro(a) para trocarem palavras cifradas afim de repetirem todo o processo da etapa anterior.

3. Atividade que mostrará ao aluno sobre domínio e imagem da função quadrática, mostrando a função inversa da mesma.
4. Cada aluno formará dupla para trocarem palavras cifradas para aplicarem o processo da etapa 3.
5. Atividade que mostra ao aluno o domínio e a imagem da função exponencial, mostrando a relação de sua função inversa com a função logarítmica.
6. Cada aluno escolherá um(a) colega para refazer o procedimento da atividade explicativa.

3.3 Matrizes

As atividades com matrizes devem ser desenvolvidas em turmas de segundo ano do Ensino Médio, onde os alunos normalmente aprendem seus conceitos sem muitas aplicações. Usar criptografia para este ensino, ajudará a familiarizar o tema com os alunos, já que não é tão explorado nos livros de matemática da educação básica.

A tabela 3 mostra uma sequência que demonstra uma forma lúdica de desenvolver o aprendizado de matrizes.

Tabela 3 - Roteiro de atividades propostas de matrizes

ETAPAS	DESCRIÇÃO	DURAÇÃO
Etapa 1	Atividade explicativa sobre aplicação de criptografia no ensino de matrizes (Anexo J).	1 tempo de aula (50 min cada)
Etapa 2	Atividade de fixação colocando em prática a atividade explicativa e um questionário subjetivo (Anexo K).	2 tempos de aula (50 min)

Fonte: o autor, 2017.

Abaixo teremos detalhes das atividades implementadas nas etapas da tabela

3.

1. Atividade demonstrativa que através de seu passo a passo trabalha propriedades de matrizes.
2. Atividade em cada aluno escolhe uma palavra cifrada e entrega ao seu parceiro, e recebe a palavra que foi cifrada por ele, assim, refazendo todo o procedimento anterior.

4 APLICAÇÃO E ANÁLISE DAS ATIVIDADES DE LIBRAS EM SALA DE AULA

Neste capítulo exibiremos a aplicação das atividades de libras em quatro turmas de oitavo ano do Ensino Fundamental de turno integral da Escola Municipal Ginásio Francisco Caldeira de Alvarenga. A escola está localizada em uma comunidade chamada Urucânia perto da divisa com a comunidade Antares. Ela oferece ensino para turmas de sétimo, oitavo e nono anos. Parte do público local sente atração por esportes, pois já tivemos alunos de destaque em diversos esportes, principalmente no atletismo e no futebol, um grande exemplo, é o jogador de futebol Thiago Silva, ex aluno da escola. Uma outra parte tende à vida do crime.

A idéia de trabalhar esse tipo de atividade diferenciada, foi para sair do ensino tradicional, acabando com a idéia de que cumprir conteúdos programados é o suficiente. Através de um ensino diferenciado, devemos mostrar para os alunos que eles têm condições de mudar de vida. Segundo SADOVSKY (2007):

A Matemática, não só no Brasil, é apresentada sem vínculos com os problemas que fazem sentido na vida das crianças e dos adolescentes. Os aspectos mais interessantes da disciplina, como resolver problemas, discutir ideias, checar informações e ser desafiado, são pouco explorados na escola. O ensino se resume a regras mecânicas que ninguém sabe, nem o professor, para que servem.

Vivemos uma educação sucateada e desvalorizada, e se não tomarmos uma atitude nas práticas de ensino, o ambiente de aula torna-se desgastante para os alunos e para os professores.

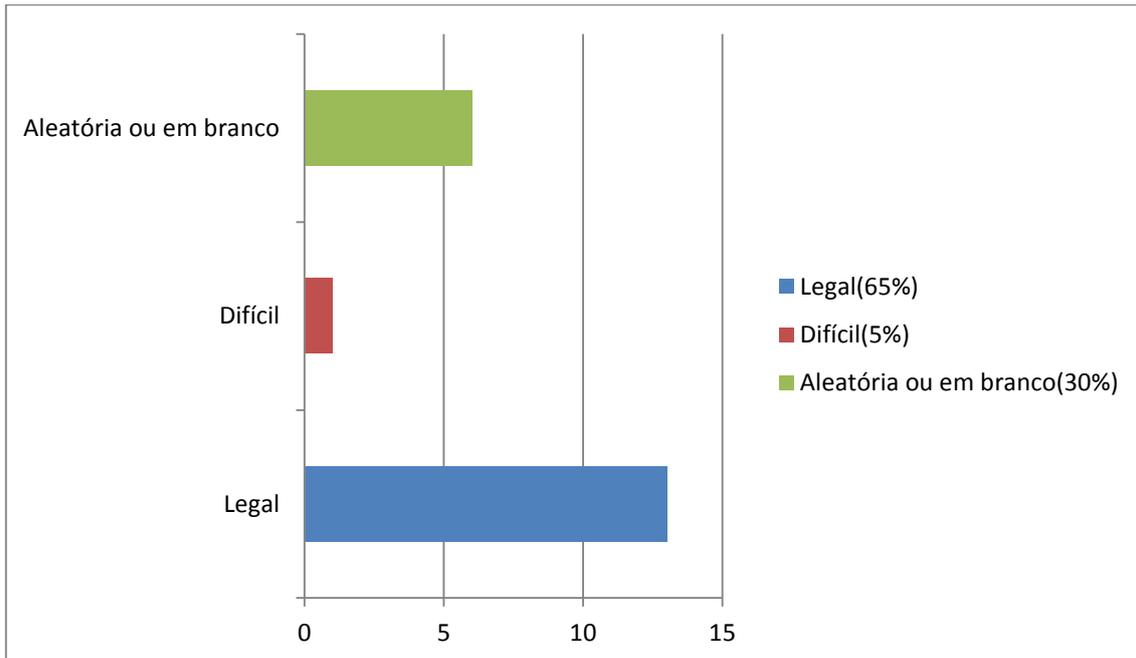
4.1 Questionário Subjetivo da Atividade I

Ao final da primeira atividade, foi realizado um questionário subjetivo (Anexo B) individual com 5 perguntas a fim de receber uma avaliação sobre a aula do ponto de vista dos alunos. As aplicações foram feitas em 4 turmas nos dias 08/05/2017 (nas turmas 1 e 2) e 09/05/2017 (nas turmas 3 e 4). Para esta etapa da pesquisa participaram 20 alunos da turma 1, 21 alunos da turma 2, 29 da turma 3 e 29 da turma 4.

Pergunta 1 - O que você acha de fazer isso (símbolos de libras) apenas usando as mãos?

- Turma 1 - Na pergunta 1, 6 alunos deram respostas aleatórias ou deixaram em branco, 1 achou difícil e 13 acharam legal.

Gráfico 1 - Resultado da pergunta 1 -Atividade I - Turma 1

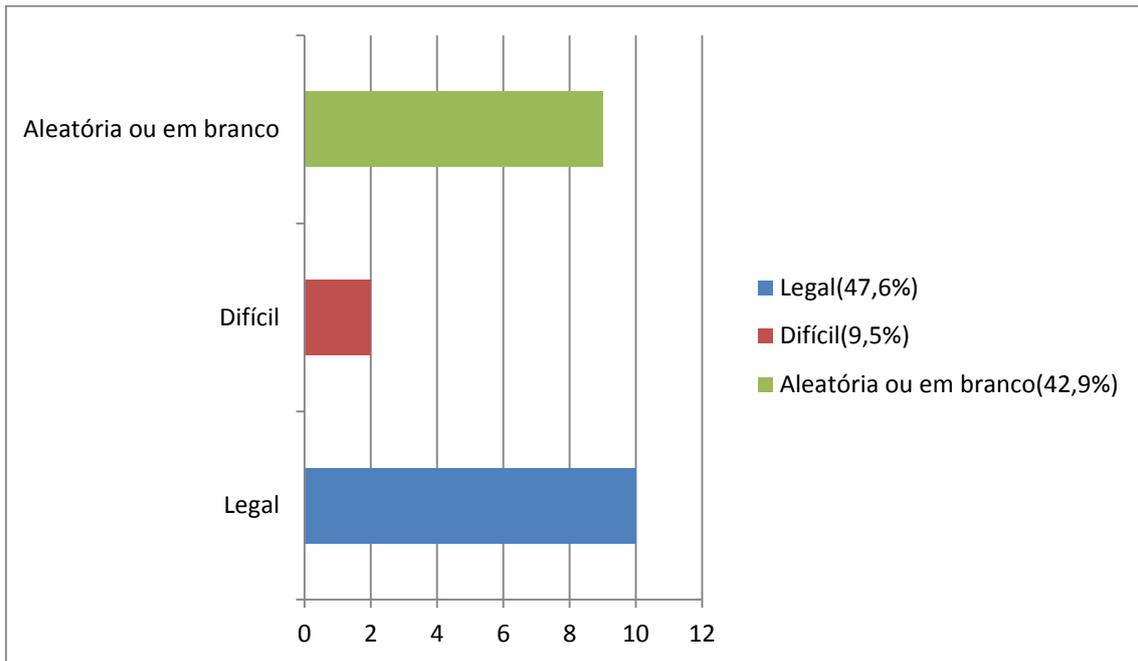


Fonte: O autor, 2017.

Na turma 1, vemos que 65% gostaram da atividade, tendo em vista que 30% não responderam a pergunta.

- Turma 2 - Na pergunta 1, 9 alunos deram respostas aleatórias ou deixaram em branco, 2 acharam difícil e 10 acharam legal.

Gráfico 2 - Resultado da pergunta 1 - Atividade I - Turma 2

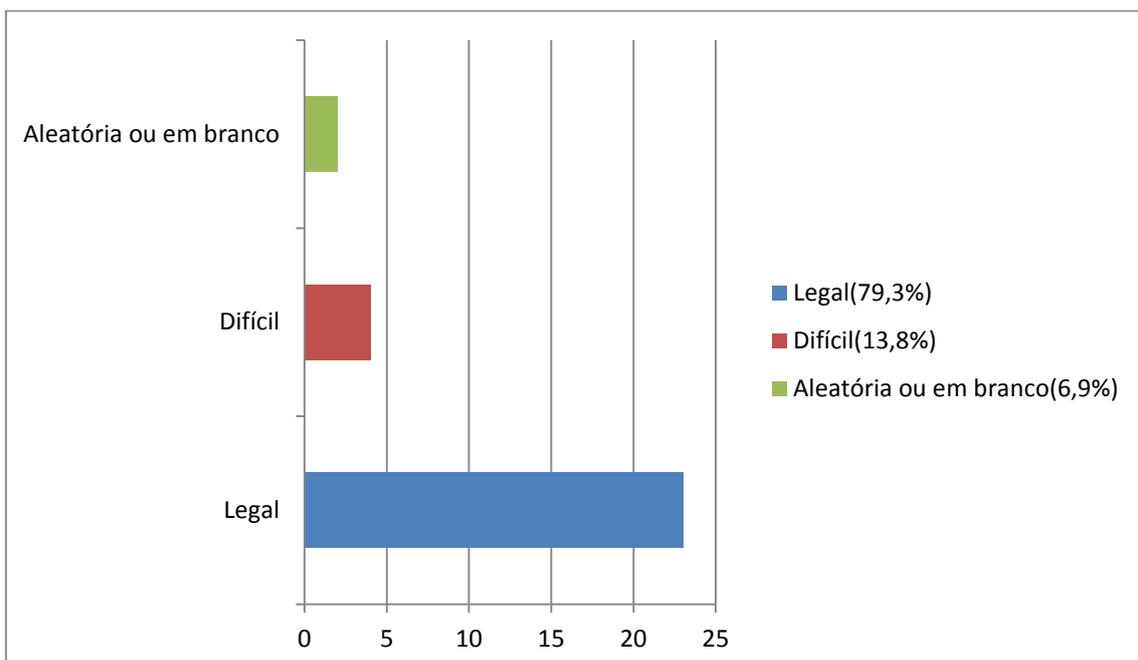


Fonte: O autor, 2017.

Na turma 2, tivemos bom aproveitamento de 47,6%, tendo em vista que nessa turma boa parte dos alunos não quiseram responder.

- Turma 3 - Na pergunta 1, 2 alunos deram respostas aleatórias ou deixaram em branco, 4 acharam difícil e 23 acharam legal.

Gráfico 3 - Resultado da pergunta 1 - Atividade I - Turma 3

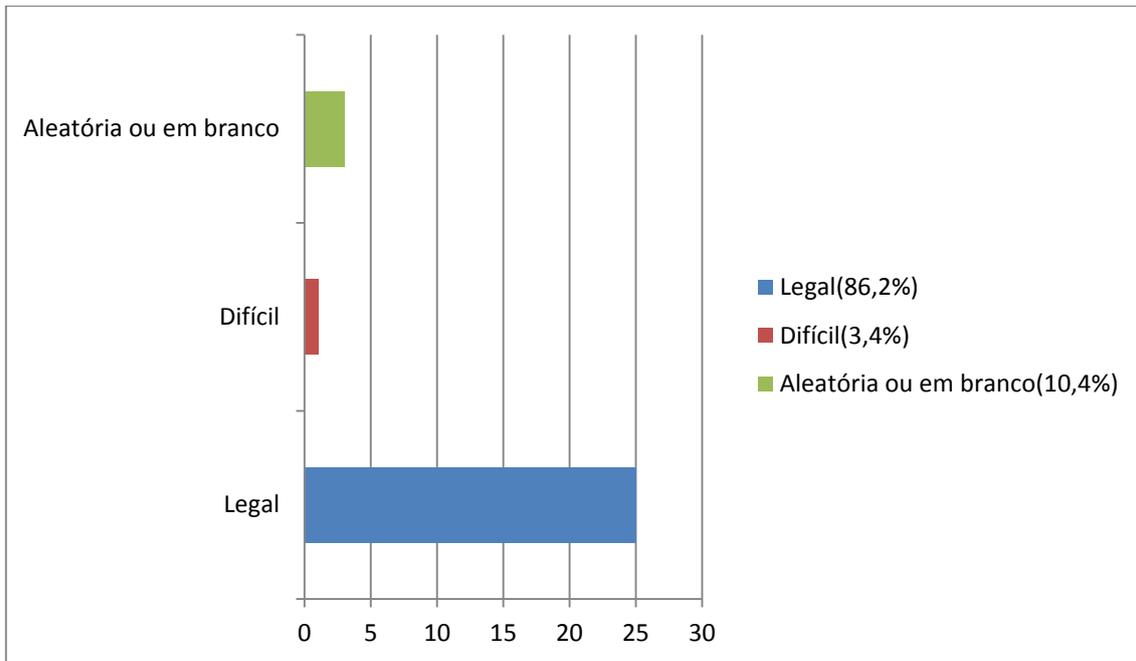


Fonte: O autor, 2017.

Na turma 3, quase todos que opnaram gostaram da atividade.

- Turma 4 - Na pergunta 1, 3 alunos deram respostas aleatórias ou deixaram em branco, 1 achou difícil e 25 acharam legal.

Gráfico 4 - Resultado da pergunta 1 - Atividade I - Turma 4



Fonte: O autor, 2017.

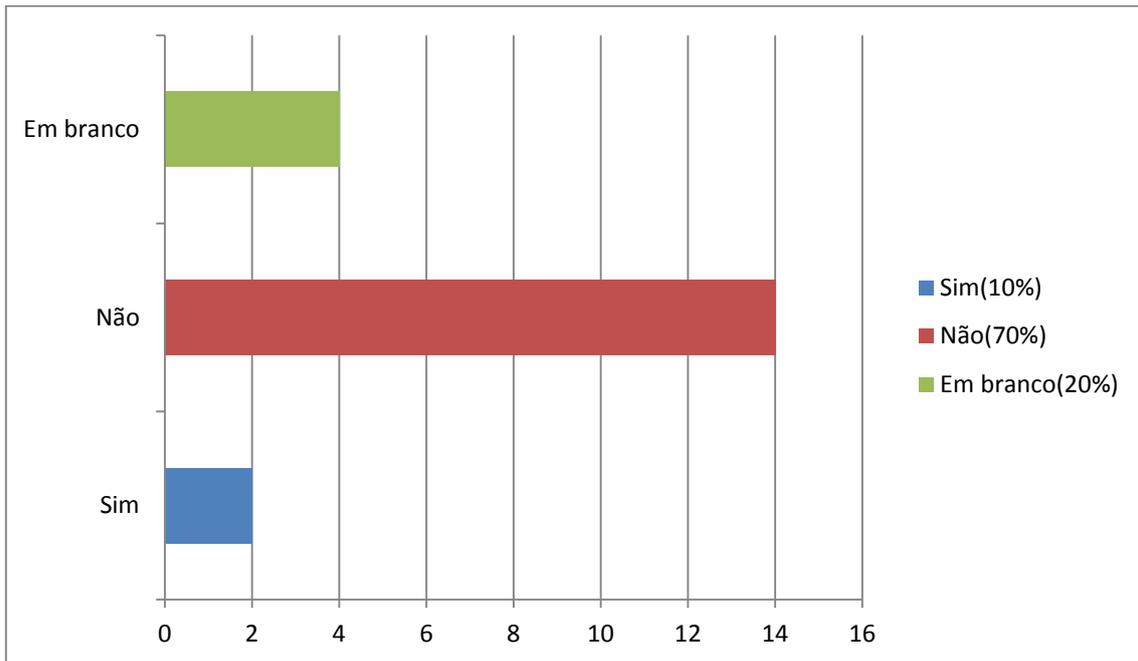
Na turma 4, também a grande maioria da turma achou a atividade legal.

Pergunta 2 - Você acha que as pessoas teriam dificuldades para te entender?

Observação: Depois conversei com as turmas para compreender as respostas dos gráficos e vi que esta pergunta gerou duplo sentido de interpretação em boa parte dos alunos, fazendo com que eles entendessem que as pessoas teriam dificuldades para entender porque não teriam aprendido libras.

- Turma 1 - Na pergunta 2, 4 alunos deixaram em branco, 14 acharam que não e 2 acharam que sim.

Gráfico 5 - Resultado da pergunta 2 - Atividade I - Turma 1

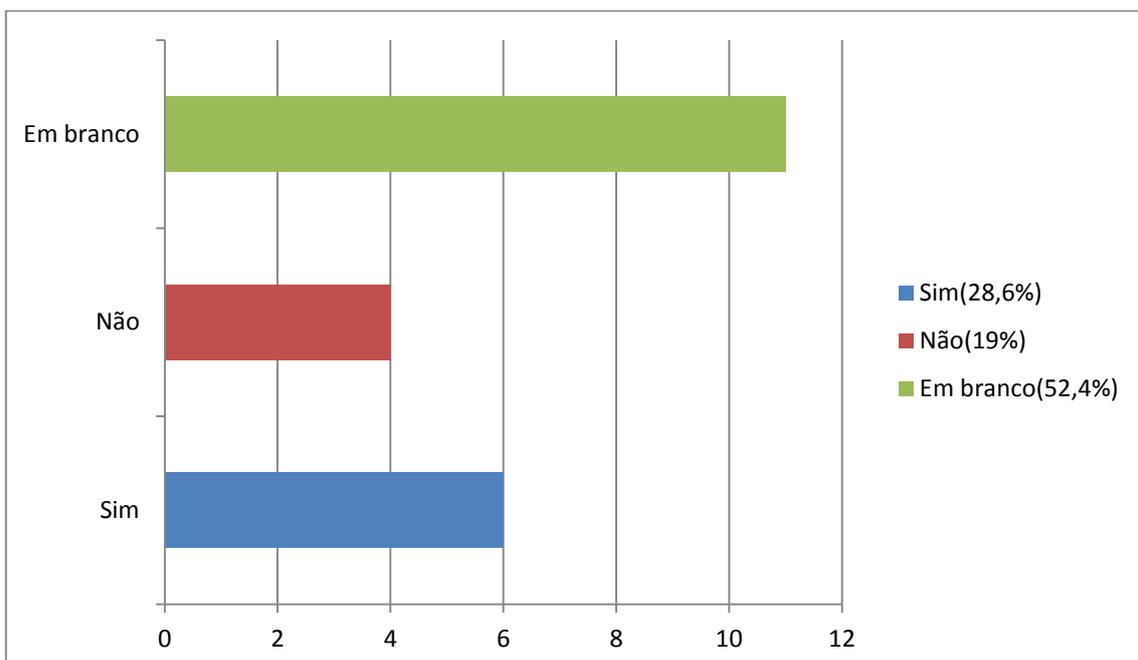


Fonte: O autor, 2017.

Na turma 1, 70% acho que não e 10% que sim, achei um bom aproveitamento.

- Turma 2 - Na pergunta 2, 11 alunos deixaram em branco, 4 acharam que não e 6 acharam que sim.

Gráfico 6 - Resultado da pergunta 2 - Atividade I - Turma 2

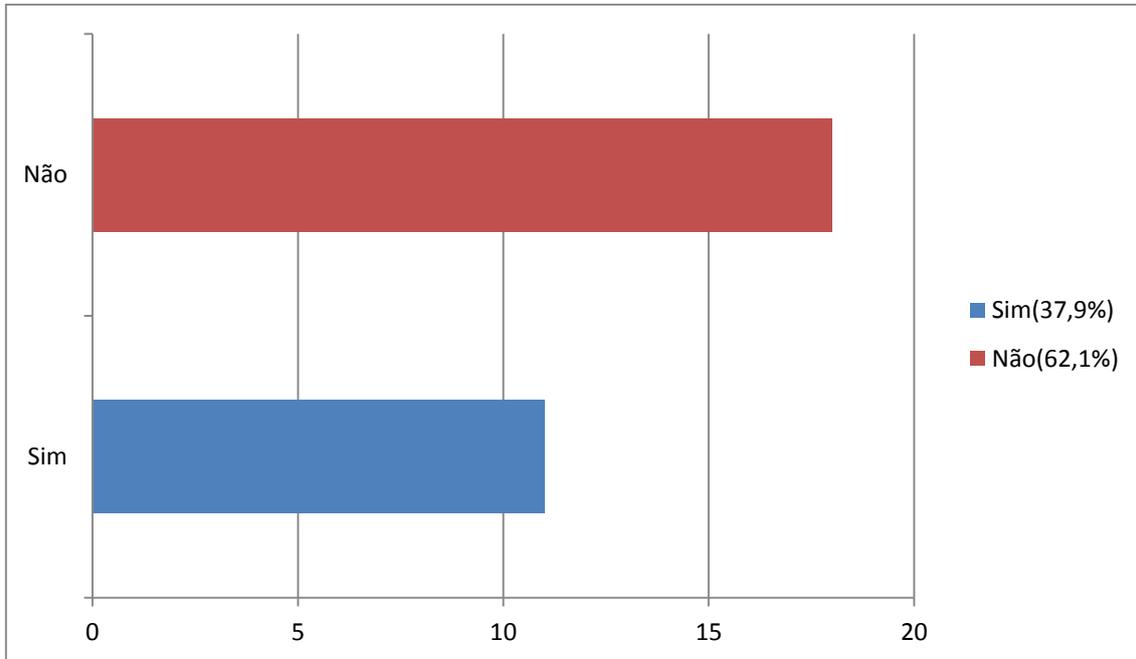


Fonte: O autor, 2017.

Por desinteresse, grande parte da turma deixou em branco essa pergunta.

- Turma 3 - Na pergunta 2, 17 acharam que não e 12 acharam que sim.

Gráfico 7 - Resultado da pergunta 2 - Atividade I - Turma 3

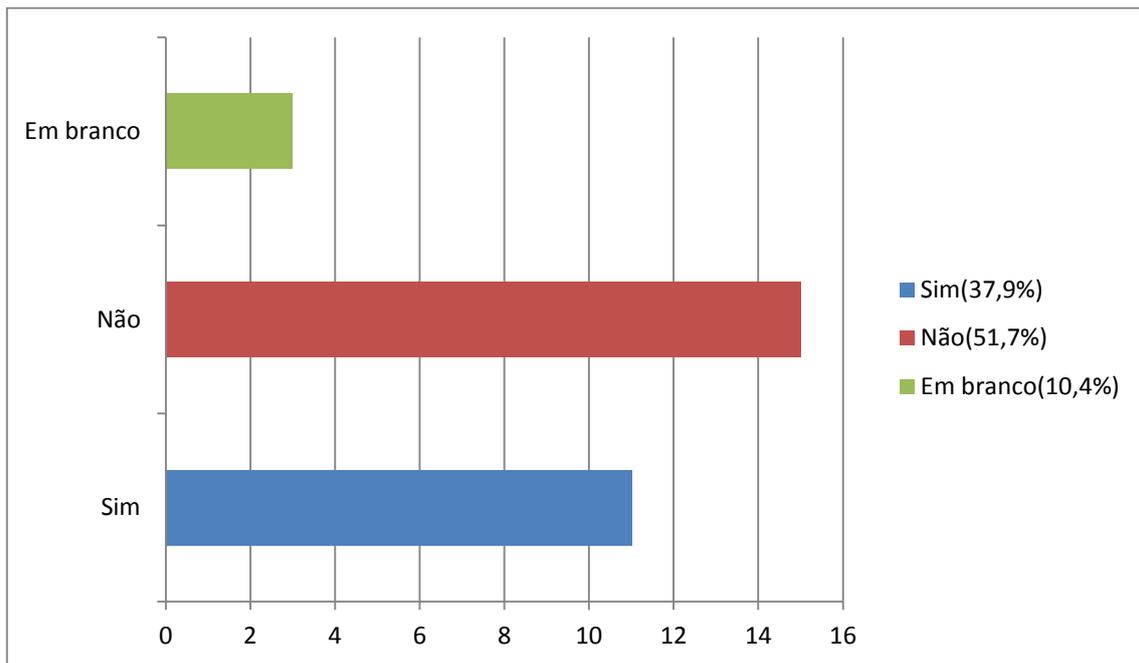


Fonte: O autor, 2017.

Na turma 3, a maioria achou que seria tranquilo, mas o sim teve um percentual considerável devido ao motivo observado acima.

- Turma 4 - Na pergunta 2, 3 alunos deixaram em branco, 15 acharam que não e 11 acharam que sim.

Gráfico 8 - Resultado da pergunta 2 - Atividade I - Turma 4



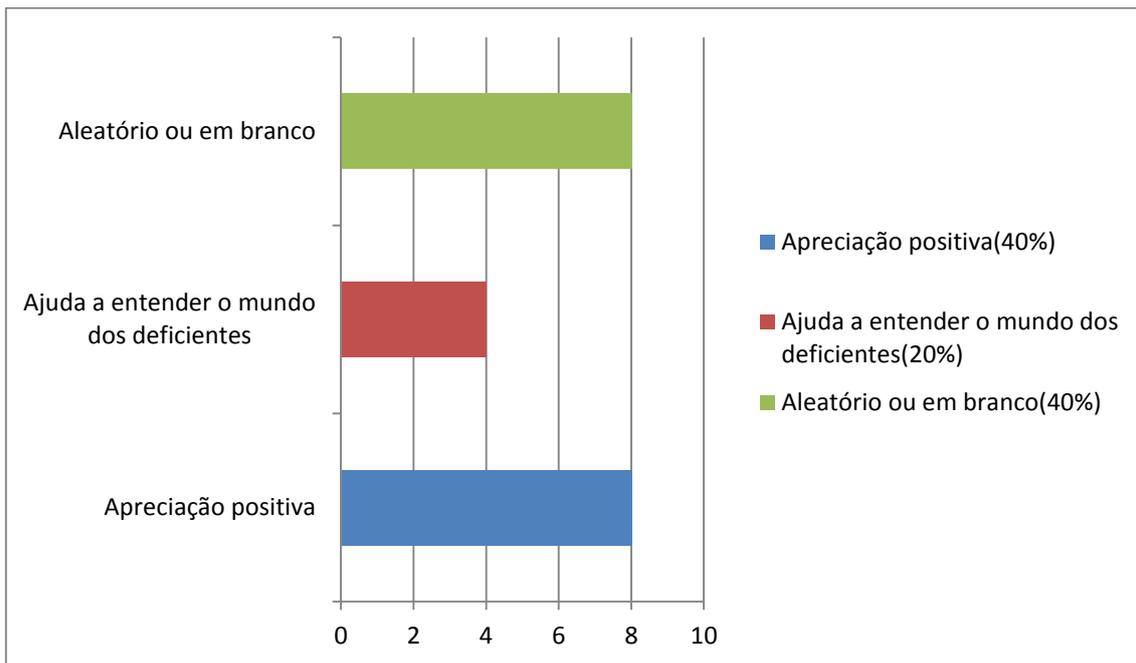
Fonte: O autor, 2017.

Nesta turma houve o mesmo problema citado na observação acima, pois o percentual de sim se encontra alto.

Pergunta 3 - Que conclusão você tira com isso?

- Turma 1 - Na pergunta 3, 8 alunos deram respostas aleatórias ou deixaram em branco, 4 acharam que ajuda a entender o mundo dos deficientes e 8 tiveram apreciação positiva.

Gráfico 9 - Resultado da pergunta 3 - Atividade I - Turma 1

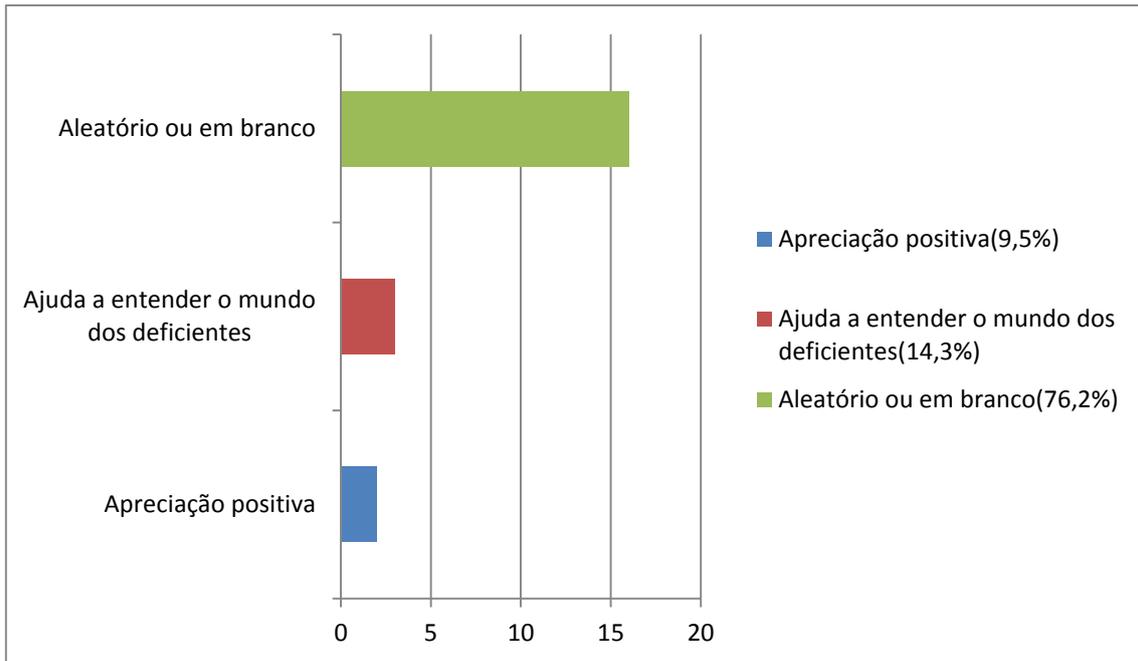


Fonte: O autor, 2017.

Dentre os que avaliaram, houve uma boa porcentagem com apreciação positiva.

- Turma 2 - Na pergunta 3, 16 alunos deram respostas aleatórias ou deixaram em branco, 3 acharam que ajuda a entender o mundo dos deficientes e 2 tiveram apreciação positiva.

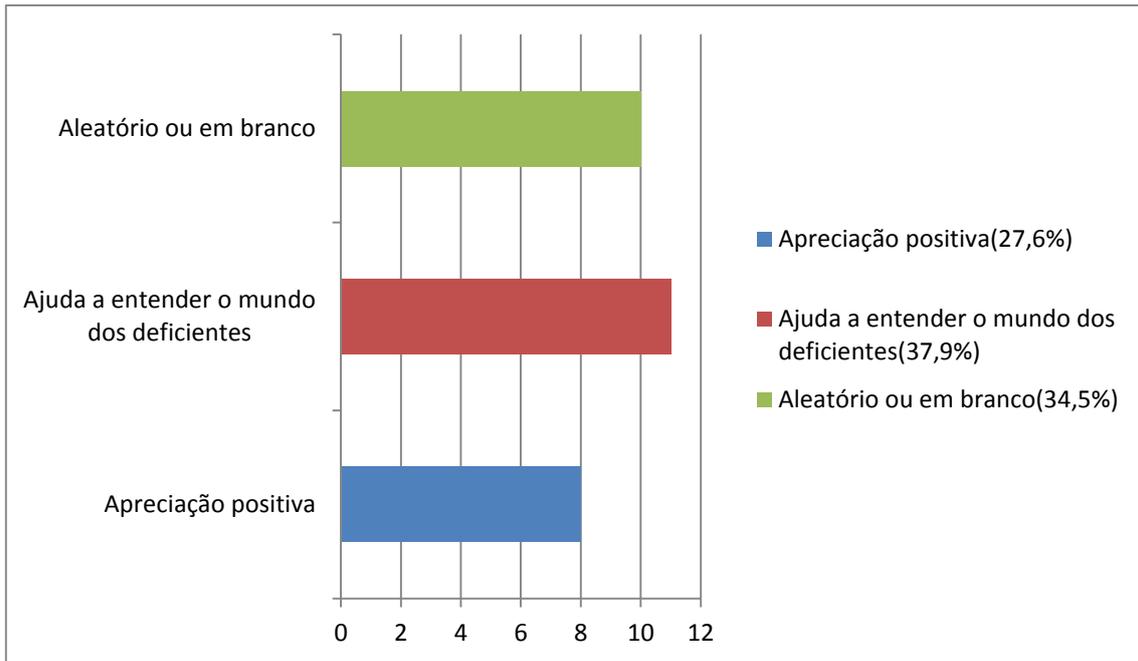
Gráfico 10 - Resultado da pergunta 3 - Atividade I - Turma 2



Fonte: O autor, 2017.

Ficou difícil de avaliar nesta turma devido ao fato de muitos não responderem.

- Turma 3 - Na pergunta 3, 10 alunos deram respostas aleatórias ou deixaram em branco, 11 acharam que ajuda a entender o mundo dos deficientes e 8 tiveram apreciação positiva.

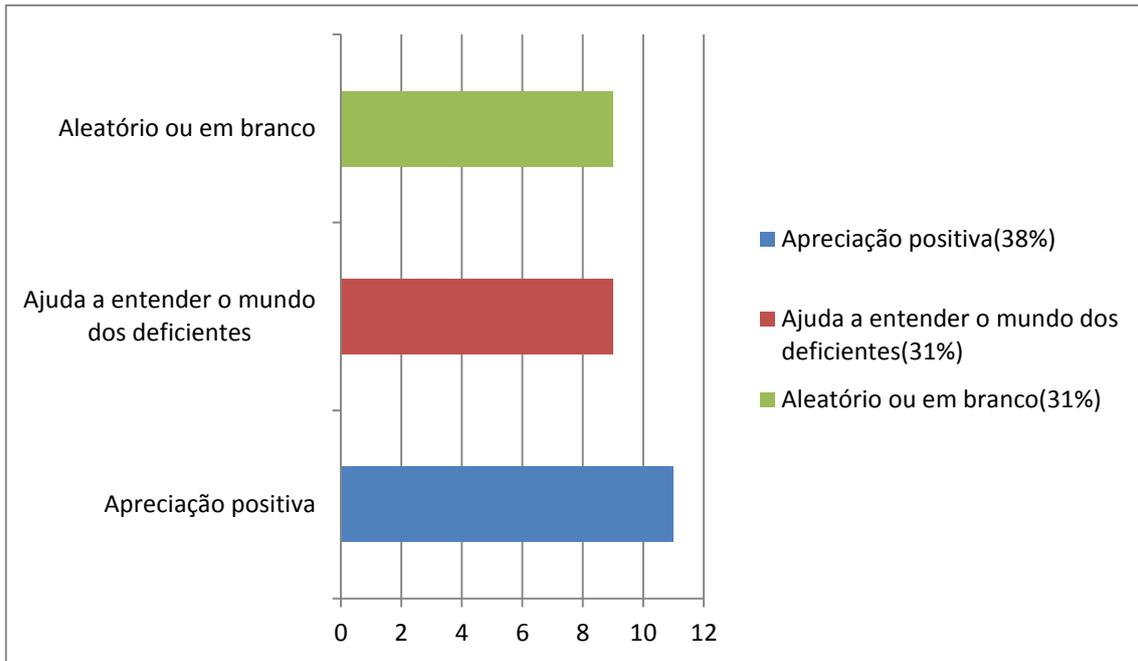


Avaliação positiva, tendo em vista que mais de 65% da turma viram pontos positivos.

Fonte: O autor, 2017.

- Turma 4 - Na pergunta 3, 9 alunos deram respostas aleatórias ou deixaram em branco, 9 acharam que ajuda a entender o mundo dos deficientes e 11 tiveram apreciação positiva.

Gráfico 12 - Resultado da pergunta 3 - Atividade I - Turma 4



Fonte: O autor, 2017.

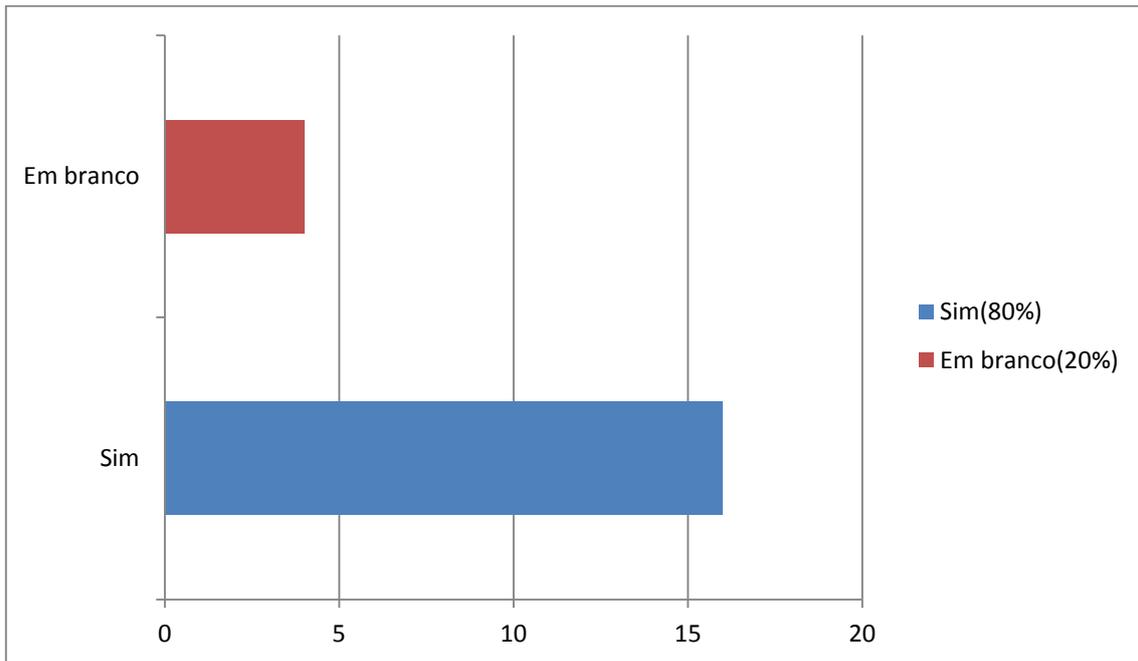
Nesta turma, a pergunta 3 foi bem respondida por 69%.

Pergunta 4 - Você acha que esta atividade ajudou a entender um pouco de criptografia e também sobre o mundo dos deficientes auditivos?

- Turma 1 - Na pergunta 4, 4 alunos deixaram em branco e 16 acharam sim.

]

Gráfico 13 - Resultado da pergunta 4 - Atividade I - Turma 1

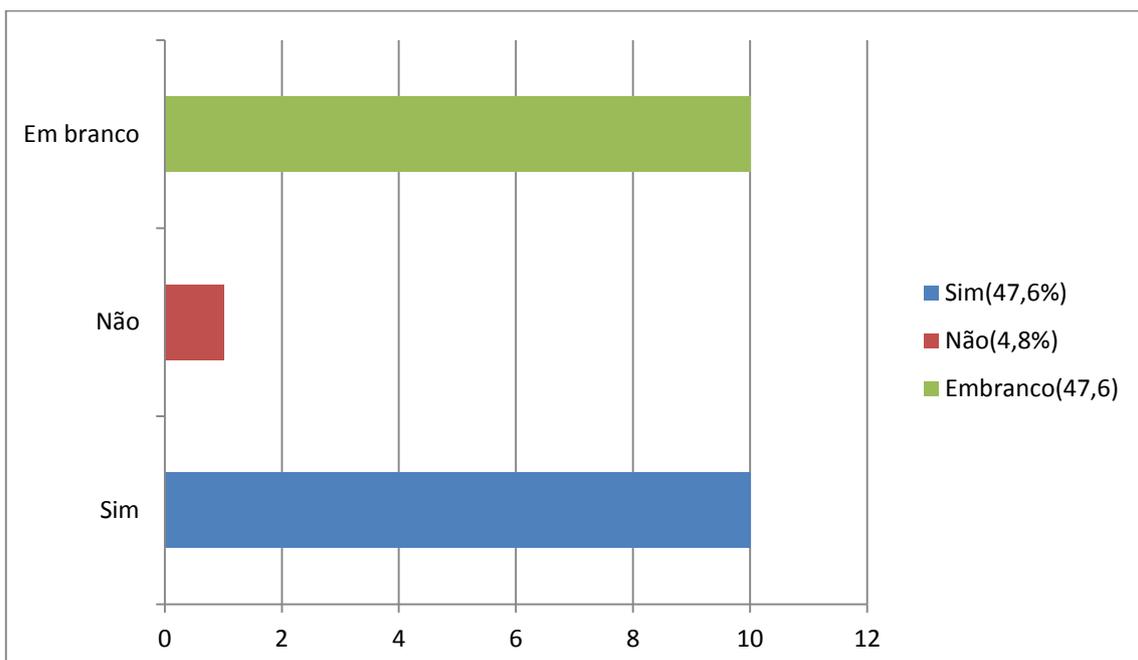


Fonte: O autor, 2017.

Como visto, 80% da turma aprovaram a atividade.

- Turma 2 - Na pergunta 4, 10 alunos deixaram em branco, 1 achou não e 10 acharam sim.

Gráfico 14 - Resultado da pergunta 4 - Atividade I - Turma 2

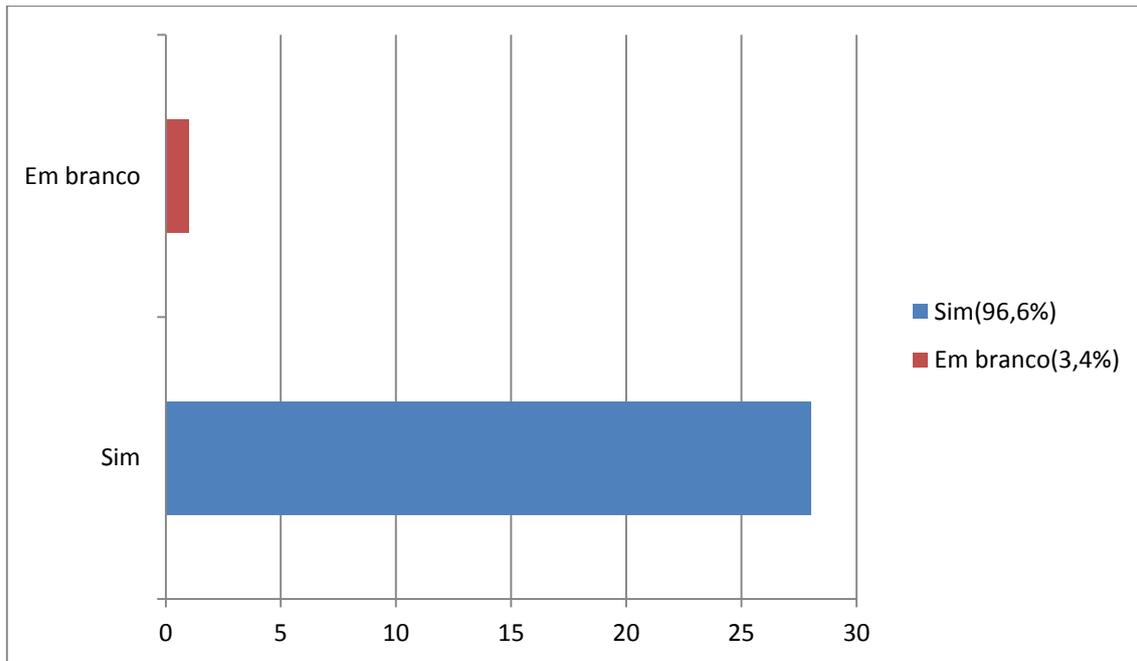


Fonte: O autor, 2017.

Apesar de muitos deixarem em branco, dos que avaliaram a grande maioria gostou.

- Turma 3 - Na pergunta 4, 1 aluno deixou em branco e 28 acharam sim.

Gráfico 15 - Resultado da pergunta 4 - Atividade I - Turma 3

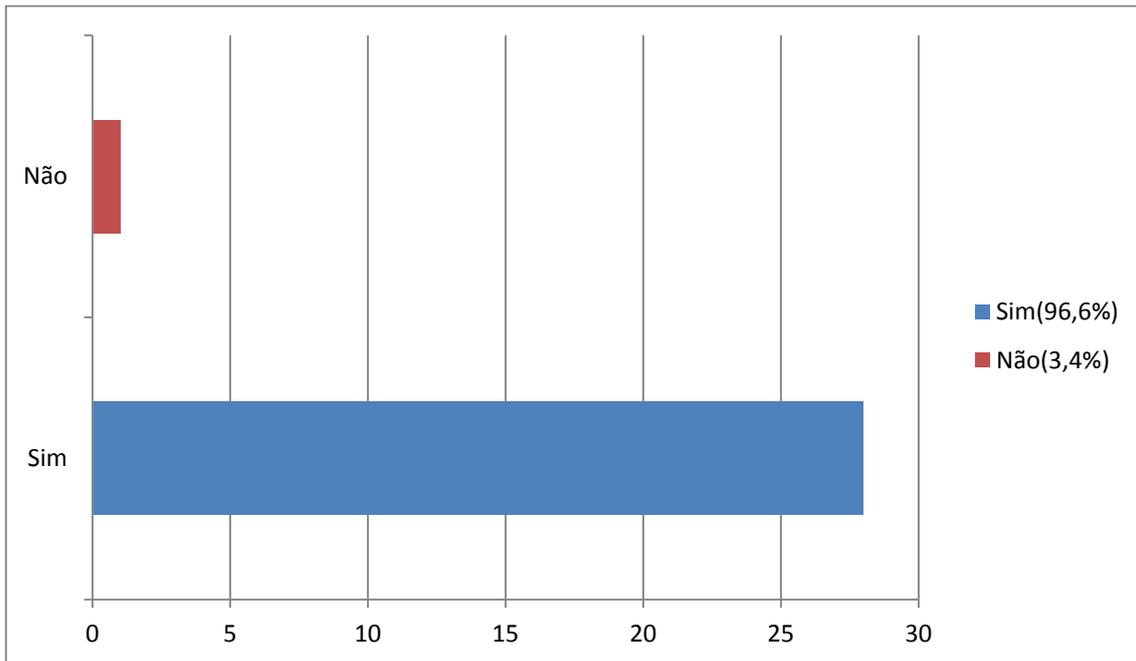


Fonte: O autor, 2017.

Aplicação da atividade foi um sucesso nessa turma.

- Turma 4 - Na pergunta 4, 1 aluno achou não e 28 acharam sim.

Gráfico 16 - Resultado da pergunta 4 - Atividade I - Turma 4



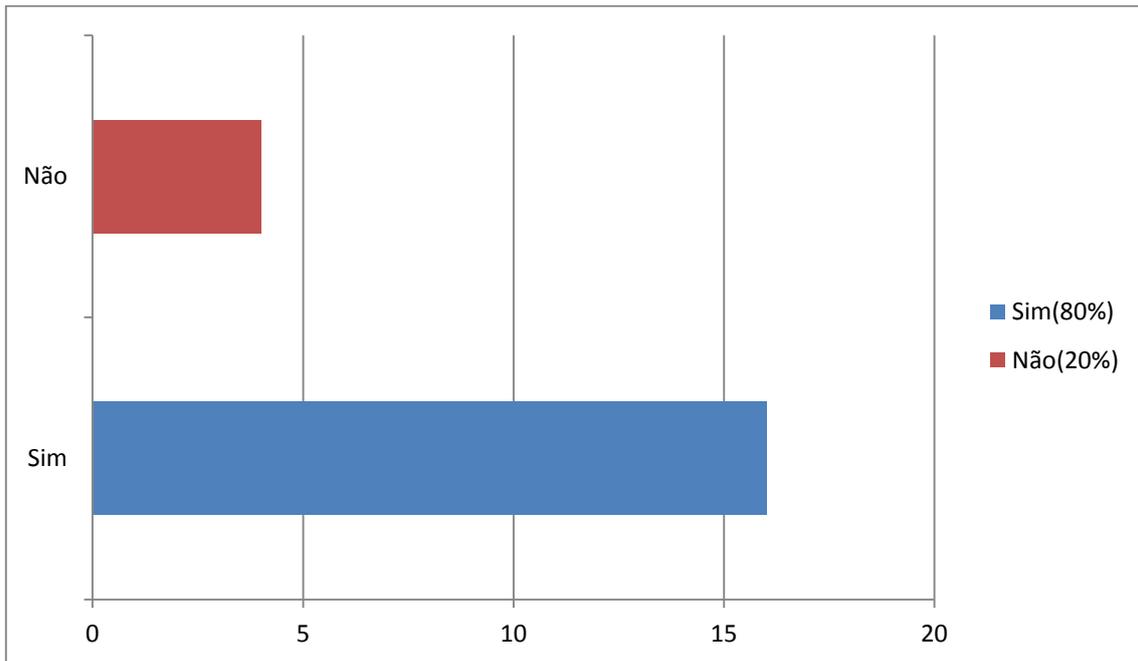
Fonte: O autor, 2017.

A aplicação da atividade também foi um sucesso nessa turma.

Pergunta 5 -Recomendaria que outras turmas tivessem uma aula dessa?

- Turma 1 - Na pergunta 5, 4 alunos acharam que não e 16 acharam que sim.

Gráfico 17 - Resultado da pergunta 5 - Atividade I - Turma 1

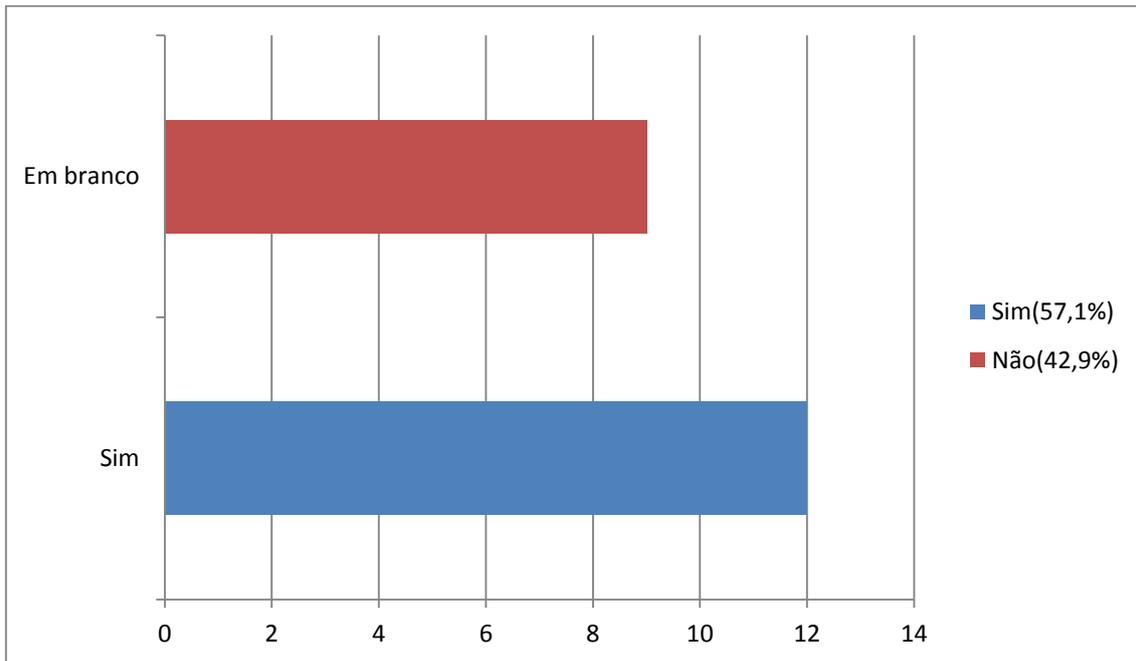


Fonte: O autor, 2017.

Como podemos ver, a cada 5 alunos 4 recomendam essa atividade para outra turma.

- Turma 2 - Na pergunta 5, 9 alunos deixaram em branco e 12 acharam que sim.

Gráfico 18 - Resultado da pergunta 1 - Atividade I - Turma 2

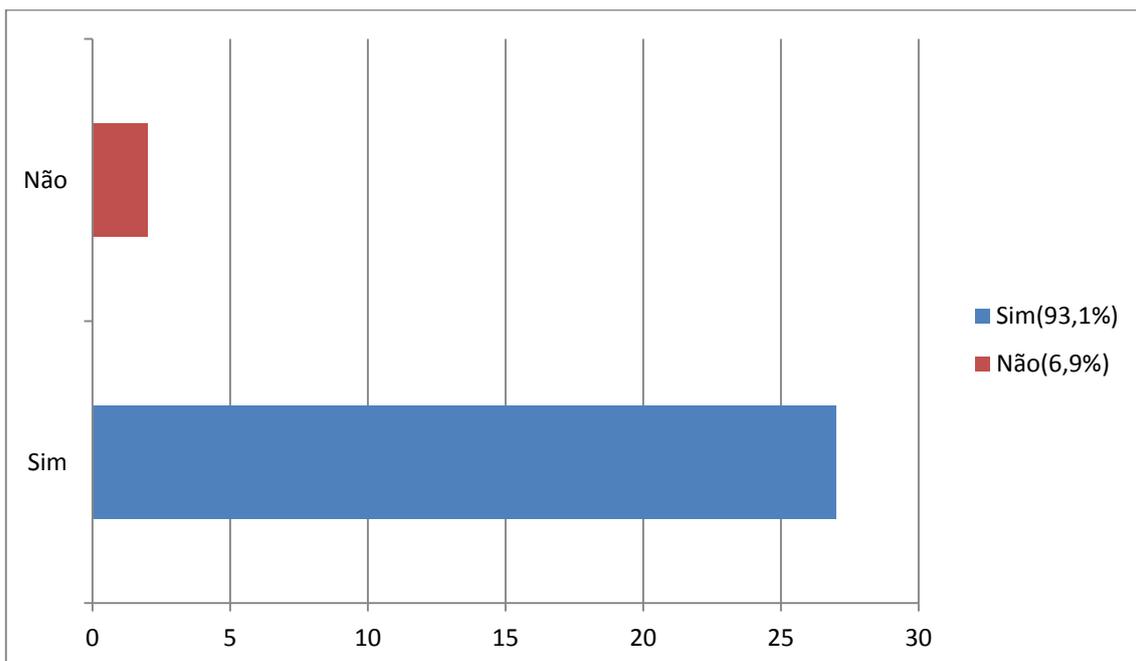


Fonte: O autor, 2017.

Nesta turma muitos deixaram em branco.

- Turma 3 - Na pergunta 5, 2 alunos acharam que não e 27 acharam que sim.

Gráfico 19 - Resultado da pergunta 5 - Atividade I - Turma 3

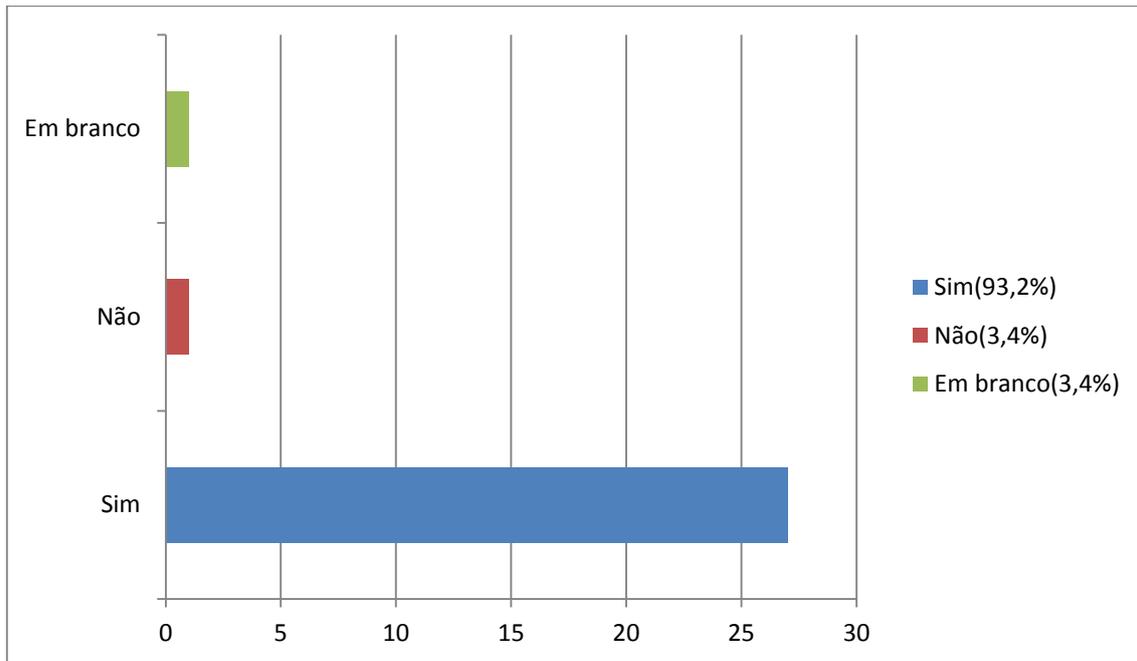


Fonte: O autor, 2017.

Nesta turma, quase todos os alunos recomendaram esta atividade.

- Turma 4 - Na pergunta 5, 1 aluno deixou em branco, 1 aluno achou que não e 27 acharam que sim.

Gráfico 20 - Resultado da pergunta 5 - Atividade I - Turma 4



Fonte: O autor, 2017.

Nesta turma também quase todos os alunos recomendam a atividade.

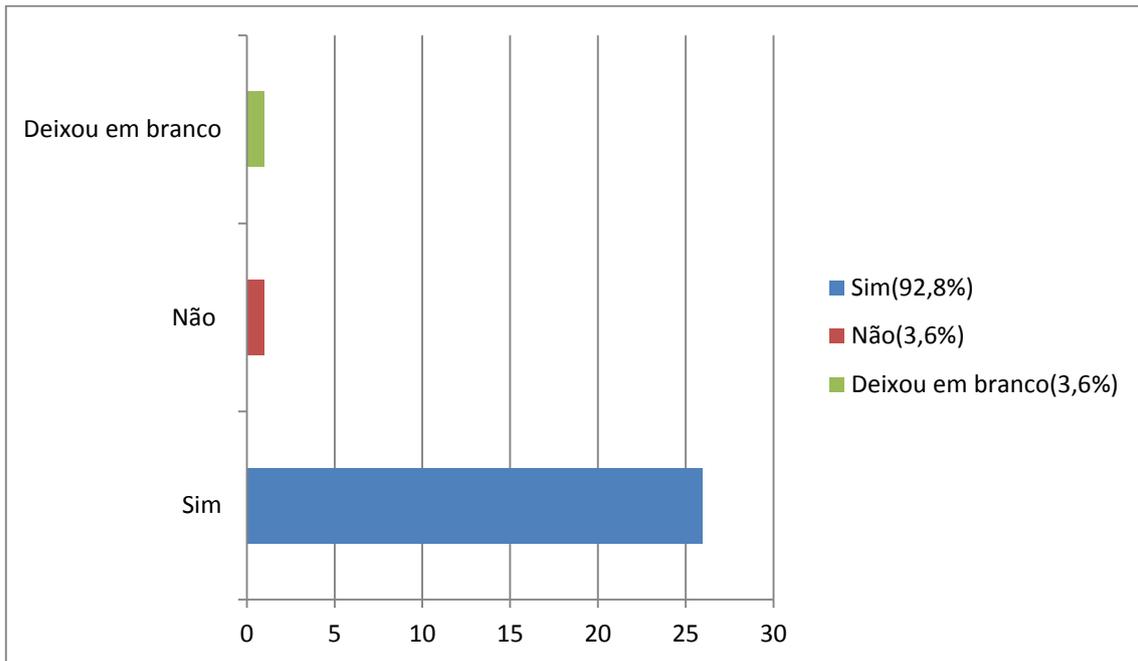
4.2 Questionário Subjetivo da Atividade II

Ao final da segunda atividade, foi realizado outro questionário subjetivo (Anexo C) individual com 3 perguntas a fim de receber uma avaliação sobre a aula do ponto de vista dos alunos. As aplicações foram feitas em 4 turmas no dia 22/05/2017. Para esta etapa da pesquisa participaram 28 alunos da turma 1, 26 alunos da turma 2, 28 da turma 3 e 33 da turma 4.

Pergunta 4 - Você achou essa atividade legal?

- Turma 1 - Na pergunta 4, 1 aluno deixou em branco, 1 aluno achou que não e 26 acharam que sim.

Gráfico 21 - Resultado da pergunta 4 - Atividade II - Turma 1

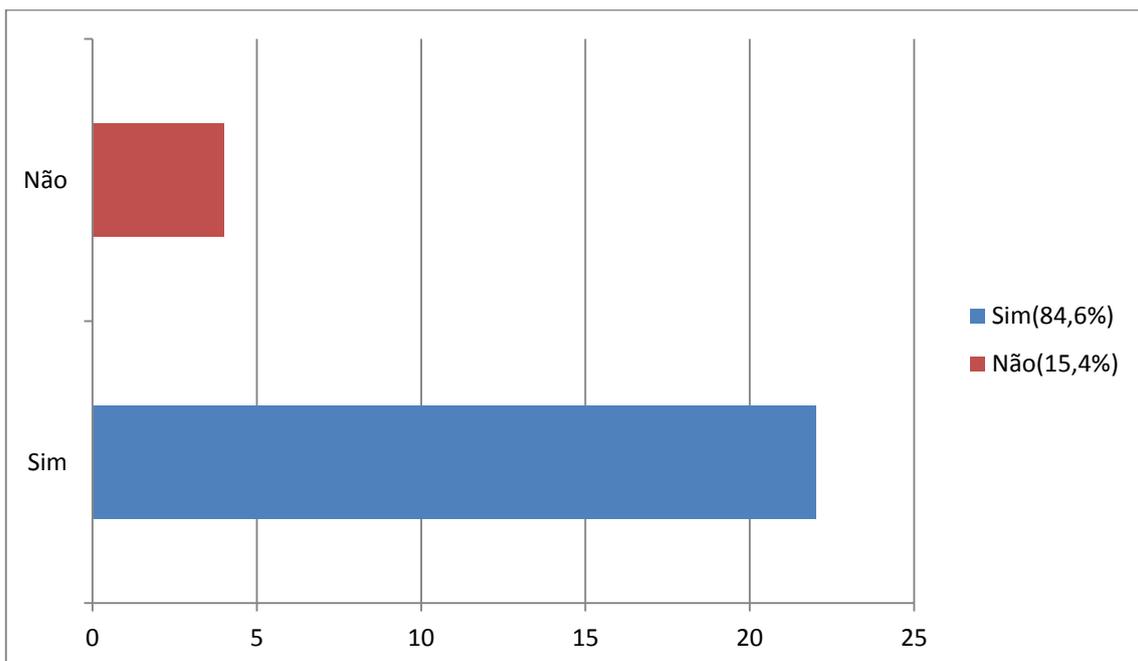


Fonte: O autor, 2017.

Atividade foi bem apreciada pela turma.

- Turma 2 - Na pergunta 4, 4 alunos acharam que não e 22 acharam que sim.

Gráfico 22 - Resultado da pergunta 4 - Atividade II - Turma 2

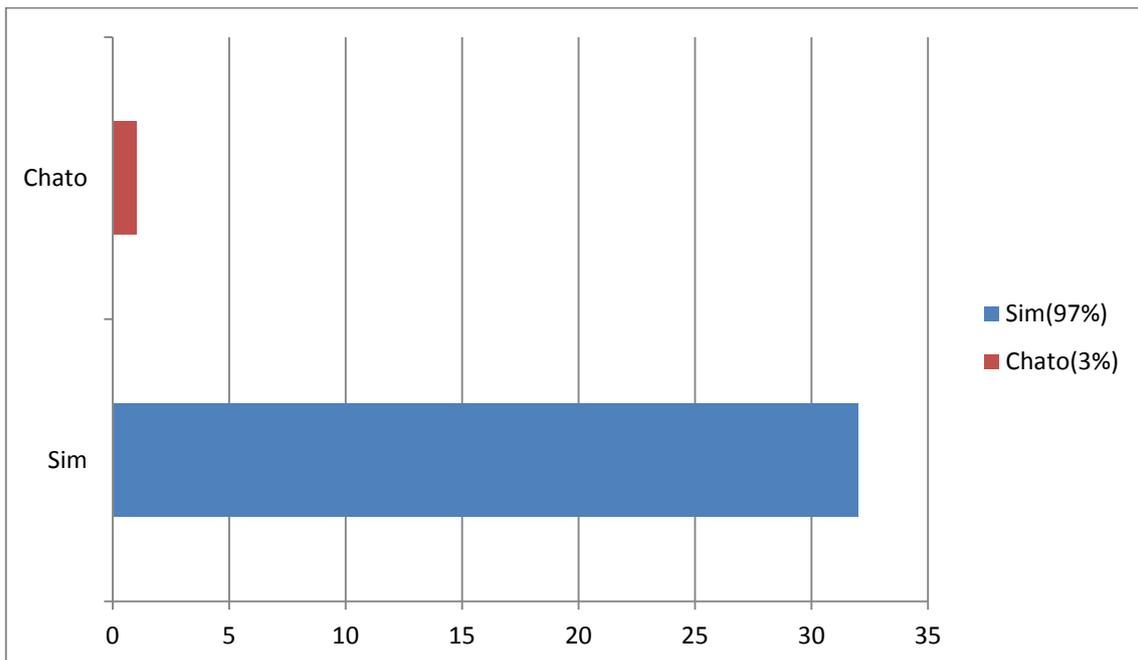


Fonte: O autor, 2017.

Atividade foi bem recebida também por esta turma.

- Turma 3 - Todos marcaram sim. O que nos mostra uma excelente recepção da atividade
- Turma 4 - Na pergunta 4, 1 aluno achou chato e 32 acharam que sim.

Gráfico 23 - Resultado da pergunta 4 - Atividade II - Turma 4



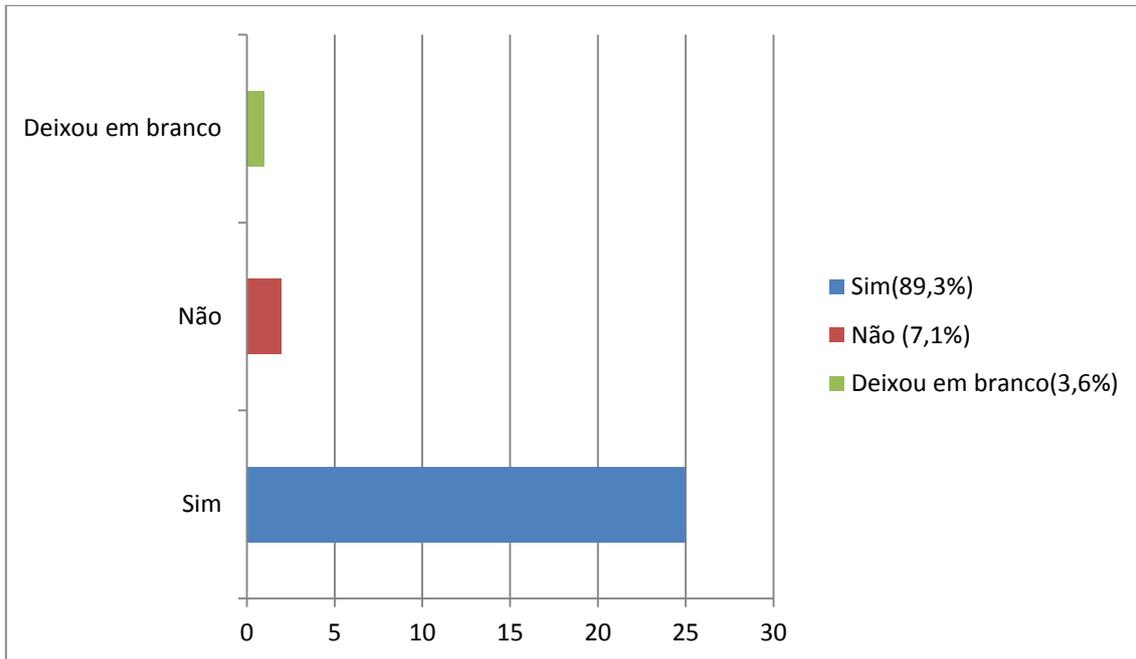
Fonte: O autor, 2017.

Atividade muito bem aceita pela turma também.

Pergunta 5 - Gostaria de ter mais aulas assim?

- Turma 1 - Na pergunta 5, 1 aluno deixou em branco, 2 alunos acharam que não e 25 acharam que sim.

Gráfico 24 - Resultado da pergunta 5 - Atividade II - Turma 1

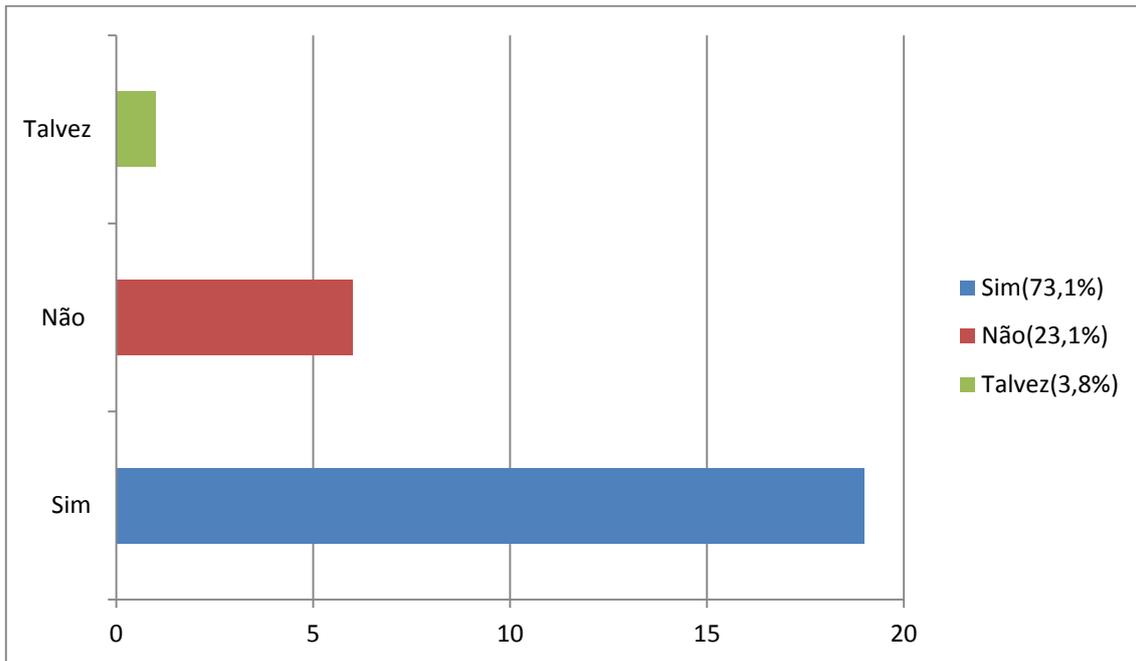


Fonte: O autor, 2017.

O gráfico nos mostra que quase 90% da turma deseja por mais aulas diferenciadas

- Turma 2 - Na pergunta 5, 1 aluno achou talvez, 6 alunos acharam que não e 19 acharam que sim.

Gráfico 25 - Resultado da pergunta 5 - Atividade II - Turma 2

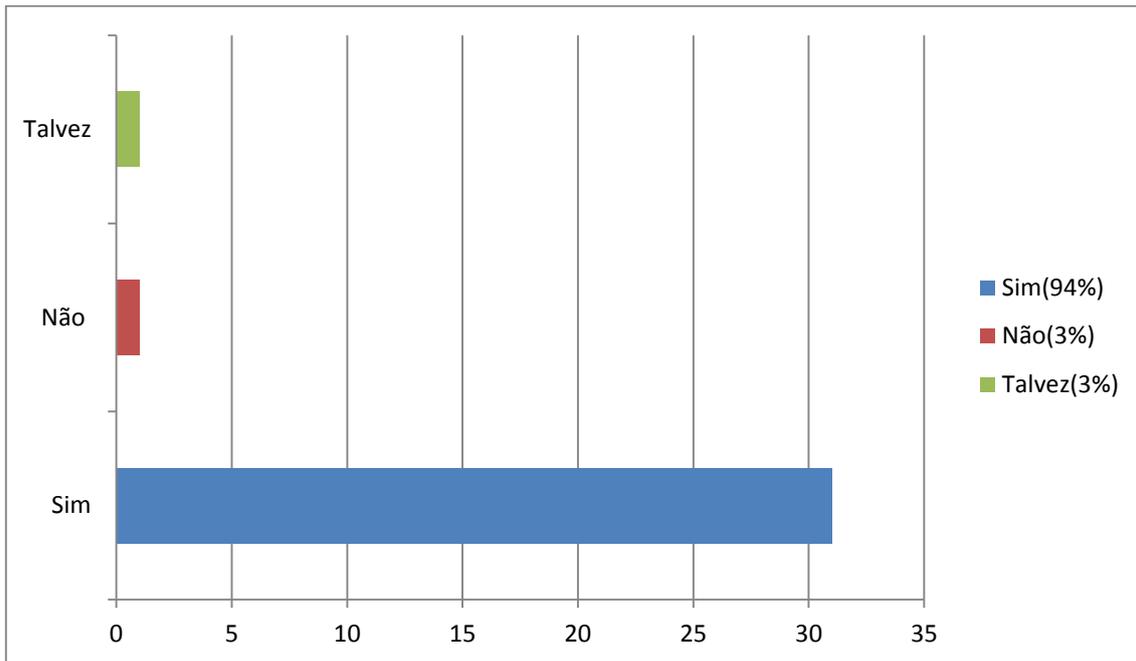


Fonte: O autor, 2017.

Esta turma também deseja por mais atividades como esta.

- Turma 3 - Todos marcaram sim.
- Turma 4 - Na pergunta 5, 1 aluno marcou talvez, 1 aluno achou que não e 31 acharam que sim.

Gráfico 26 - Resultado da pergunta 5 - Atividade II - Turma 4



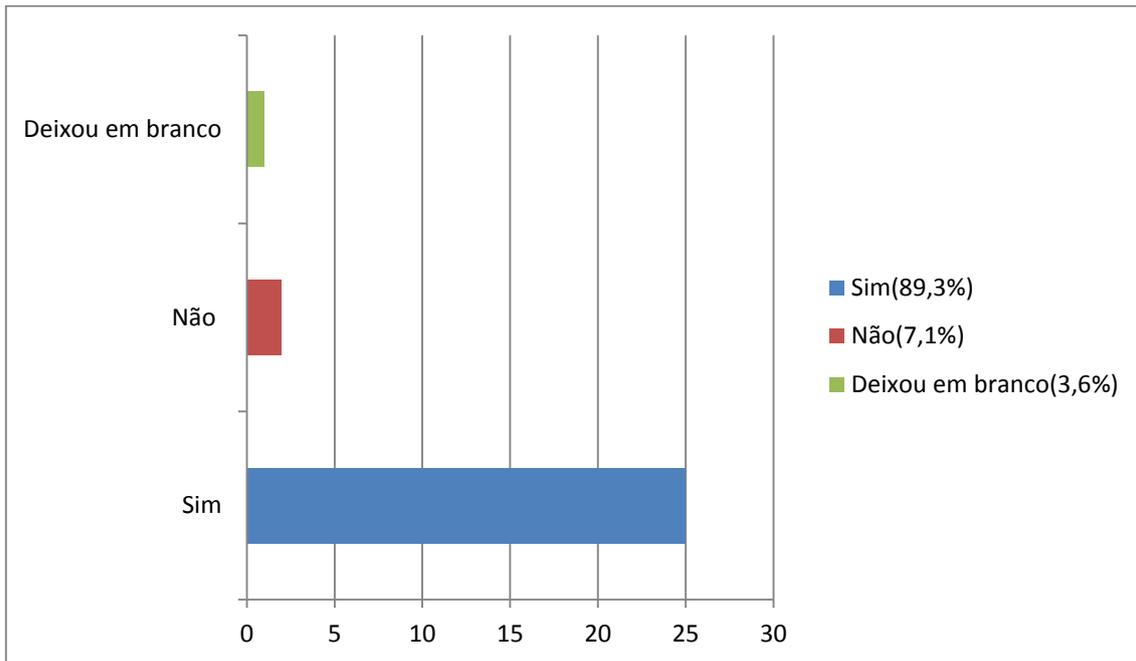
Fonte: O autor, 2017.

Esta turma também recebeu muito bem esta atividade.

Pergunta 6 - Indicaria para outras turmas?

- Turma 1 - Na pergunta 6, 1 aluno deixou em branco, 2 alunos acharam que não e 25 acharam que sim.

Gráfico 27 - Resultado da pergunta 6 - Atividade II - Turma 1

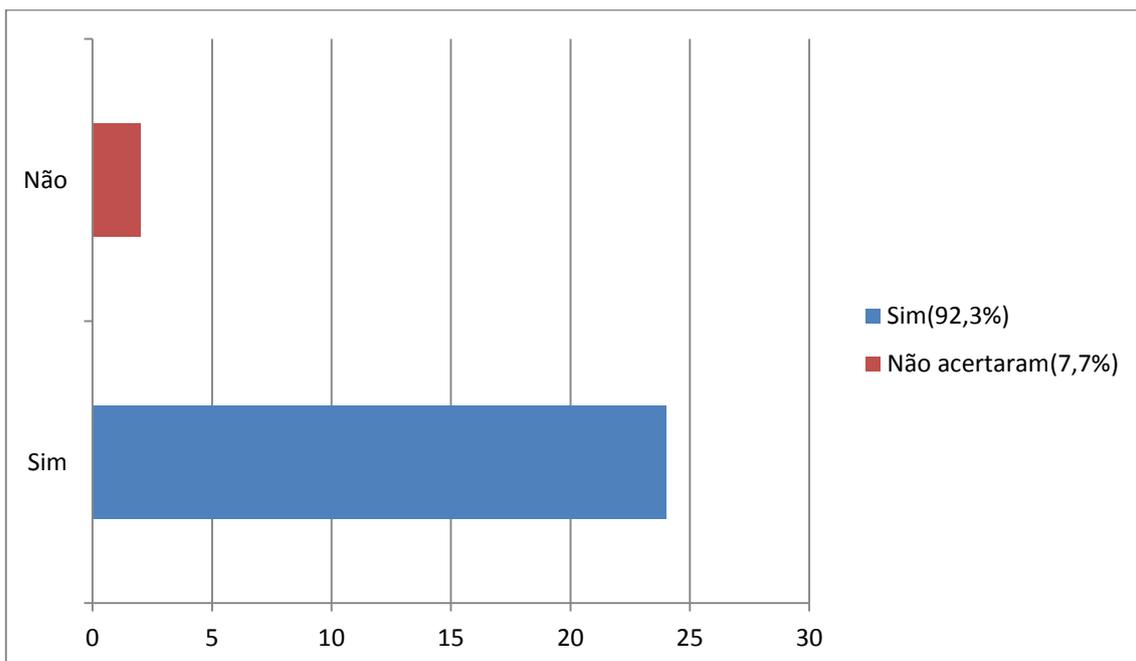


Fonte: O autor, 2017.

Como vimos, quase 90% da turma recomenda essa atividade.

- Turma 2 - Na pergunta 6, 2 aluno acharam que não e 24 acharam que sim.

Gráfico 28 - Resultado da pergunta 6 - Atividade II - Turma 2

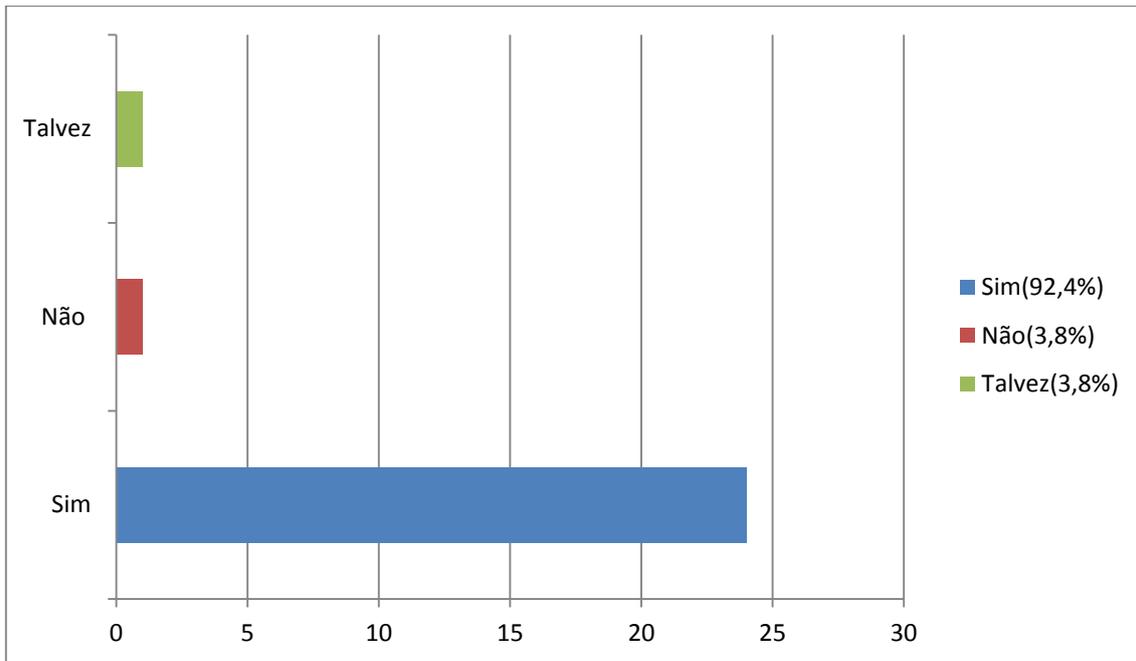


Fonte: O autor, 2017.

Mais de 90% da turma recomendam essa atividade.

- Turma 3 - Na pergunta 6, 1 aluno achou talvez, 1 aluno achou que não e 24 acharam que sim.

Gráfico 29 - Resultado da pergunta 6 - Atividade II - Turma 3

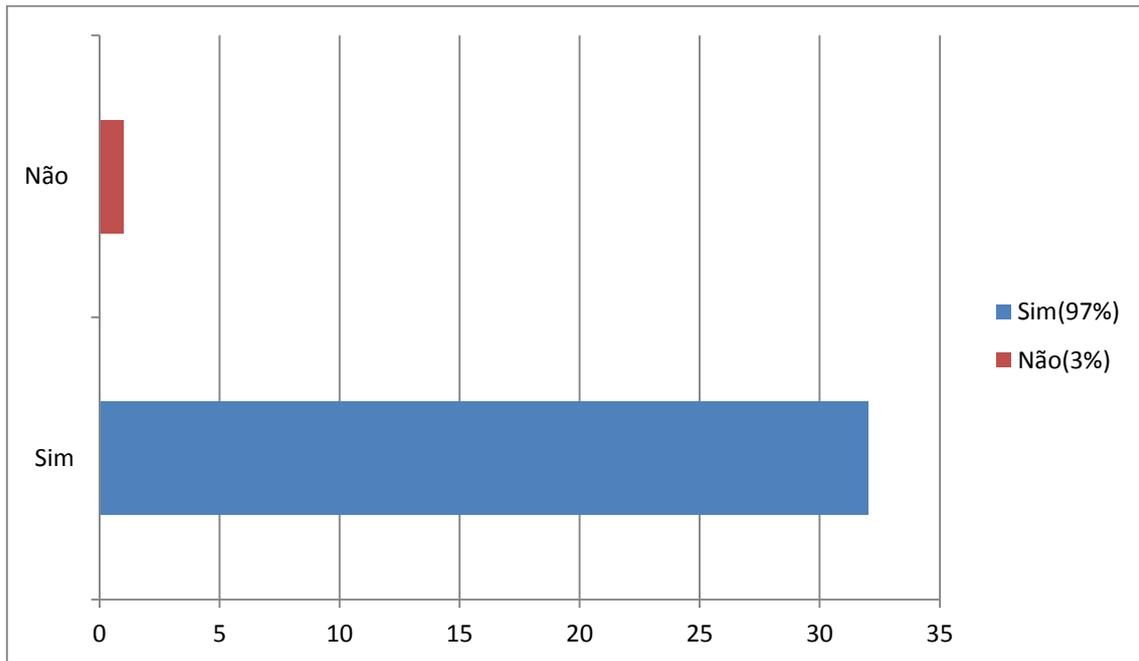


Fonte: O autor, 2017.

Nesta turma também mais de 90% indicam essa atividade por que gostaram.

- Turma 4 - Na pergunta 6, 1 aluno achou que não e 32 acharam que sim.

Gráfico 30 - Resultado da pergunta 6 - Atividade II - Turma 4



Fonte: O autor, 2017.

Nessa turma foi um sucesso, pois quase todos recomendam essa atividade.

CONSIDERAÇÕES FINAIS

A Matemática não pode ser tratada como uma disciplina sem importância no cotidiano do aluno, e muito menos como se fosse um livro de fórmulas, que o aluno tem que decorar ao longo de sua vida escolar, não fazendo sentido algum com a vida que leva, ou seja, ensinamentos que ele não pode colocar em prática. Precisamos mostrar que a matemática é aplicada o tempo inteiro em nossas vidas, através de um gráfico no jornal, de uma tabela para fazer compras em um supermercado, de um troco recebido, de cálculos de área para colocar piso em sua própria casa, entre outros. Além de tudo isso, a matemática é uma disciplina que sempre está presente nas outras, por exemplo, questões de geografia possui bastante tratamento da informação, em história, o cálculo de idades através de datas, em química usa muita porcentagem e produtos com números racionais, etc.

No contexto que nos encontramos, ainda vemos a matemática sendo tratada de forma isolada por muitas escolas, fazendo o aluno não perceber a sua devida importância.

De acordo com os PCNs, temos que fazer uso de diferentes fontes de informação, assim como devemos utilizar recursos tecnológicos a fim de construir o conhecimento (PCN, 1997, p. 6). Foi a partir desse contexto que tomei como base a minha pesquisa, inserindo a criptografia como algo atual e tecnológico. Além de também inserir libras, para proporcionar uma aula diferenciada e mais atraente. O trabalho aplicado usava a cifragem e decifragem de mensagens através dos sinais do alfabeto de libras.

De início, alguns alunos tiveram certa resistência a participar, como é comum de acontecer nas outras aulas. Mas na medida que estes alunos perceberam a motivação dos demais, eu percebi a mudança de comportamento de uma parte desses que apresentavam certa apatia. Mas na parte das atividades aplicadas no dia 22/05/2017 (Anexo C), os alunos de todas as 4 turmas estavam bem mais empenhados. O primeiro objetivo específico (apresentar aos alunos uma aula mais interessante através da relação existente entre Criptografia e libras e desenvolver atividades aliando o tema aos conteúdos selecionados) foi contemplado de forma absoluta.

Nessas atividades foram empregadas a Metodologia Sequência Fedathi (contemplando o segundo objetivo específico), onde em um primeiro momento foi abordado um resumo da história da criptografia, falando de que forma ela é aplicada e para que serve. Em seguida, foi apresentado o alfabeto de libras para eles, para depois passar uma atividade explicativa para o aluno se ambientar com os temas. Depois, pude propor situações desafiadoras em duplas, em que uma dupla poderia ajudar a outra. A partir daí, eles fizeram as atividades pedidas e quando estiveram com dúvidas, consultavam o colega de outra dupla. Após todo esse processo, os alunos trouxeram as atividades prontas e discutimos as formas que eles usaram para fazerem, a palavra escolhida, a forma que cifrou e enviou para o colega, a palavra recebida e a forma que decifrou. Então, no final podemos aproveitar o que eles fizeram e mostrá-lo um modelo de resolução.

A aplicação dessas atividades foram grandes surpresas positivas, pois as turmas em que os trabalhos foram aplicados, eram turmas extremamente inquietas e com alguns grupos que demonstram certa indiferença. Foi aí que o terceiro objetivo específico foi alcançado, quando os trabalhos despertaram o interesse desses alunos, estimulando-os durante a apresentação das atividades, mostrando que a matemática pode ser ensinada de forma lúdica, e eles passaram a tirar dúvidas, a pesquisarem e a discutirem entre eles, além de se autoavaliarem. Depois da realização da primeira lista de atividades, eles passaram a pedir para repetir aulas como aquela (aulas lúdicas) e até hoje os alunos fazem gestos com as mãos pedindo que eu diga o significado para eles. E quando eu dei a outra atividade no dia 22/05/2017, até aqueles que se negavam a responder na primeira atividade, participaram e interagiram para saberem se estavam certos. E as atividades foram tão apreciadas que a coordenação pedagógica pediu que eu desse uma cópia de cada atividade. Por serem lúdicos, os trabalhos foram ensinados sem esforços para os alunos, sem a necessidade de decorar fórmulas.

A partir desse momento, o quarto objetivo foi contemplado, pois no momento da maturação, eles interagem entre eles, cheios de autonomia para resolverem os exercícios em conjunto, e quando não resolviam, passavam a interagir com o autor que os encaminhavam para o caminho da solução. Dessa forma, o professor deixou de ser o centro da aula para termos alunos mais atuantes e interessados. Com isso, houve uma melhora significativa no comportamento deles, e conseqüentemente, no aprendizado.

Os educadores da matemática deveriam sair do comodismo e aplicar aulas diferenciadas, pois assim a matemática ganhará significado. Em alguns momentos podem ter havido falhas, mas nada que nos impeça de melhorar e aplicar novamente em outras turmas.

REFERÊNCIAS

BRASIL. Secretaria de Educação Média e Tecnológica. Parâmetros Curriculares Nacionais do Ensino Médio: Matemática v.3. Brasília: MEC/SEF, 1998.

BRASIL. Ministério da Educação. Base Nacional Comum Curricular (BNC). Brasília: MEC, 2016.

BRASIL. Ministério de Educação e Cultura. LDB - Lei no 9394/96, de 20 de dezembro de 1996. Estabelece as diretrizes e bases da Educação Nacional. Brasília: MEC, 1996.

FALEIROS, Antonio Cândido. Criptografia. São Carlos: SBMAC, 2011, 138 P, (Notas em Matemática Aplicada; v. 52). Disponível em:

http://www.sbmac.org.br/arquivos/notas/livro_52.pdf. Acesso em: 17 jul. 2017.

MALAGUTTI, Pedro Luiz; BEZERRA, Débora de Jesus; RODRIGUES, Vânia Cristina da Silva. Aprendendo criptologia de forma divertida. Paraíba, 2010. Disponível em:

http://www.mat.ufpb.br/bienalsbm/arquivos/O_cinasCompletos=O1Completo.pdf:

Acesso em : 8 jul. 2017.

Orientações Curriculares 1º ao 9º ano. Secretaria Municipal de Educação. Rio de Janeiro, 2013. Disponível em:

<http://www.rio.rj.gov.br/dlstatic/10112/4246635/4104937/MAT_Orientacoes_2013.pdf>. Acesso em:6 jul. 2017.

MORENO, Edward David; PEREIRA, Fábio Dacêncio; CHIARAMONTE, Rodolfo Barros. Criptografia em software e hardware. São Paulo: Novatec, 2005.

AZEREDO, José Carlos de. Escrevendo pela nova ortografia: como usar as regras do novo acordo ortográfico da Língua Portuguesa. Rio de Janeiro: Instituto Antônio Houaiss. 1a edição, Publifolha, 2008.

CARMINATI, NL. Modelagem Matemática: Uma Proposta de Ensino Possível na Escola Pública, 2007.

OLIVEIRA, RJ. O Bom Professor de Matemática segundo a Percepção de Alunos do Ensino Médio. Universidade Católica de Brasília 2007.

GROENWALD, Claudia Lisete Oliveira; FRANKE, Rosvita Fuelber. Currículo de Matemática e o tema Criptografia no Ensino Médio. Educação Matemática em Revista, Rio Grande do Sul, p. 51-57, 2008.

SHOKRANIAN, Salahoddin. Criptografia para Iniciantes. 2a Edição. Rio de Janeiro: Editora Ciência Moderna Ltda., 2012.

BORGES NETO, Hermínio e outros. A Sequência Fedathi como proposta metodológica no ensino de Matemática e sua aplicação no ensino de retas paralelas. XV EPENN Encontro de Pesquisa Educacional do Norte e Nordeste. São Luiz/MA: UFMA, 2001.

BORGES NETO, Hermínio e SANTANA, J. Rogério. Sequência Fedathi: uma proposta de mediação pedagógica na relação ensino/aprendizagem.

VASCONCELOS, José Gerardo. Filosofia, Educação e realidade. Fortaleza: EUFC, 2003

BARBOSA, MP. Recursos Tecnológicos Como Ferramentas Didáticas no Processo Ensino-Aprendizagem de Função Quadrática (Dissertação), Rio de Janeiro. UERJ – 2016.

Jesus , André Luís Neris de. Criptografia na educação básica: utilização da criptografia como elemento motivador para o ensino aprendizagem de matrizes (Dissertação), Juazeiro - BA. UNIVASF - 2013

ANEXO A - Atividade explicativa da aplicação de criptografia em libras.

ESCOLA:

TURMA:

DATA:

HORÁRIO DE APLICAÇÃO:

ALUNO(A):

- Vamos cifrar uma mensagem seguindo os passos abaixo:

1) Escolha uma frase.

A frase escolhida foi "Criptografia com libras".

2) Substitua cada letra pelo gesto correspondente na tabela 1.

tabela 1

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

Nesse caso obtemos "criptografia com libras".

3) Envie essa mensagem para a pessoa que forma a dupla com você.

- Agora para decifrar a mensagem, siga as orientações:

1) Receba a mensagem cifrada de sua dupla.

2) Substitua cada símbolo pela letra correspondente na tabela 1.

Logo, a mensagem recebida é "CRIFTOGRAFIA COM LIBRAS".

Anexo B – Atividades de Fixação e questionário subjetivo**ESCOLA:****TURMA:****DATA:****HORÁRIO DE APLICAÇÃO:****ALUNO(A):****ATIVIDADE DE FIXAÇÃO**

- Cifre uma palavra para enviar à sua dupla.
- 1) Escolha uma palavra.
 - 2) Utilize a tabela 1 para cifrar a palavra escolhida.
 - 3) Como ficou a mensagem cifrada?
 - 4) Envie-a para seu parceiro.
- Para decifrar a mensagem:
- 1) Use a tabela 1 para decifrar a frase, substituindo cada gesto pela letra correspondente.
 - 2) Qual a palavra enviada pelo seu amigo?
- Agora repita todo esse procedimento usando apenas as mãos, ou seja, tente se comunicar com seus colegas usando a linguagem de libras.
- 1) O que acha de fazer isso apenas usando as mãos?
 - 2) Você acha que as pessoas teriam dificuldades para te entender?
 - 3) Que conclusão você tira com isso?
 - 4) Você acha que esta atividade ajudou a entender um pouco de criptografia e também sobre o mundo dos deficientes auditivos?
 - 5) Recomendaria que outras turmas tivessem uma aula dessa?

ANEXO C – Continuação da primeira atividade com libras.

ESCOLA:

TURMA:

DATA:

HORÁRIO DE APLICAÇÃO:

ALUNO(A):

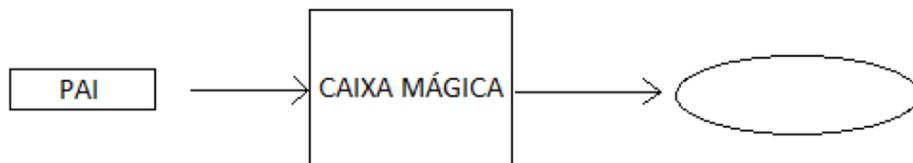
1) Suponha que exista uma caixa mágica em que você coloca uma palavra em português e ela sai transformada em libras. De acordo com a tabela 1, descubra a palavra que sai da caixa e marque a única resposta correta.

tabela 1

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



- TIO MIA TIA



- PIA PAI PIO

2) Se você chegasse depois da palavra ter passado pela caixa mágica, ela já estaria transformada na linguagem de libras. Tente descobrir que palavra tinha entrado nessa caixa utilizando a tabela 1.

ANEXO D - Atividade explicativa de aplicação de criptografia no ensino de função afim.

ESCOLA:

TURMA:

DATA:

HORÁRIO DE APLICAÇÃO:

ALUNO(A):

- Para cifrar uma mensagem usando os conceitos de função afim:

1) Será considerada a função afim $f(x) = x - 10$.

2) Selecione uma palavra para ser usada como mensagem, por exemplo "MATEMÁTICA".

3) Substitua cada letra pelo número utilizando a tabela 1 abaixo:

tabela 1

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Ao substituir a palavra "MATEMÁTICA" obtemos a sequência "13 1 20 5 13 1 20 9 3 1"

4) Usando a função dada $f(x) = x - 10$ para cifrar a mensagem, é determinada a imagem de cada número: $f(13)$, $f(1)$, $f(20)$, $f(5)$, $f(9)$ e $f(3)$.

tabela 2

Letra	M	A	T	E	M	A	T	I	C	A
x	13	1	20	5	13	1	20	9	3	1
f(x)	3	-9	10	-5	3	-9	10	-1	-7	-9

5) Assim a mensagem é cifrada conforme é apresentada na tabela 2.

- Para decifrar a mensagem entregue ao receptor:

1) O receptor deve encontrar a função inversa de $f(x)$, que corresponde a $f^{-1}(x) = x + 10$.

2) Usando a função $f^{-1}(x)$, é completada a tabela 3:

tabela 3

Mensagem Recebida	3	-9	10	-5	3	-9	10	-1	-7	-9
-------------------	---	----	----	----	---	----	----	----	----	----

$f^{-1}(x)$	13	1	20	5	13	1	20	9	3	1
Mensagem Decifrada	M	A	T	E	M	A	T	I	C	A

CONCLUSÃO:Portanto, a mensagem decifrada é a palavra "MATEMÁTICA".

ANEXO E– Atividade de fixação de aplicação de criptografia no ensino de função afim.

ESCOLA:

TURMA: DATA: HORÁRIO DE APLICAÇÃO:

ALUNO(A):

- Use os conceitos de função afim para cifrar uma mensagem:

1) Escolha uma palavra relacionada ao tema função afim para ser a mensagem que será enviada.

2) Escolha uma função afim: $g(x) = \underline{\hspace{2cm}}$

3) Utilizando a tabela 1 substitua as letras.

4) Qual a sequência obtida ao substituir a mensagem escolhida?

5) Preencha a tabela abaixo usando a função $g(x)$ para cifrar a mensagem.

Letra										
x										
g(x)										

6) Qual foi a mensagem cifrada?

- Entregue a mensagem à pessoa que forma dupla com você, para que possa decifrá-la seguindo os seguintes passos:

1) Encontre a função inversa $g^{-1}(x)$.

2) Complete a tabela abaixo.

Mensagem Recebida										
$g^{-1}(x)$										
Mensagem Decifrada										

3) Qual a mensagem descoberta?

4) O que você achou dessa atividade?

5) Posso usar função quadrática? Justifique.

6) Você acha que atividades desse tipo ajudam no processo de ensino aprendizagem?

7) Dê idéias, sugestões e críticas sobre a atividade.

ANEXO F – Atividade explicativa de aplicação de criptografia no ensino de função quadrática.

ESCOLA:

TURMA:

DATA: **HORÁRIO DE APLICAÇÃO:**

ALUNO(A):

- Para cifrar uma mensagem usando os conceitos de função quadrática:

1) Seja $f: \mathbb{R}_+ \rightarrow \mathbb{R}_+$ a função $f(x) = x^2$.

2) Selecione uma mensagem, nesse caso usaremos "QUADRÁTICA".

3) Substitua cada letra da mensagem escolhida pelo número correspondente utilizando a tabela 1.

tabela 1

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Após fazer a substituição da palavra "QUADRÁTICA" obtemos a sequência "16 20 0 3 17 0 19 8 2 0".

4) Usando a função $f(x)$ dada, cifre a mensagem determinando as imagens de $f(16)$, $f(20)$, $f(0)$, $f(3)$, $f(17)$, $f(19)$, $f(8)$ e $f(2)$. Depois preencha a tabela 2.

Letra	Q	U	A	D	R	A	T	I	C	A
x	16	20	0	3	17	0	19	8	2	0
f(x)	256	400	0	9	289	0	361	64	4	0

5) A mensagem cifrada é a sequência "256 400 0 9 289 0 361 64 4 0".

- Para decifrar a mensagem entregue ao receptor:

1) O receptor deve encontrar a função inversa $f^{-1}(x)$.

$$x = f^{-1}(x)^2$$

$$f^{-1}(x) = \sqrt{x}$$

2) Complete a tabela 3 usando a função $f^{-1}(x)$.

tabela 3

Mensagem	256	400	0	9	289	0	361	64	4	0
----------	-----	-----	---	---	-----	---	-----	----	---	---

Recebida										
$f^{-1}(x)$	16	20	0	3	17	0	19	8	2	0
Mensagem Decifrada	Q	U	A	D	R	A	T	I	C	A

CONCLUSÃO: Logo, a mensagem decifrada é "QUADRÁTICA".

ANEXO G – Atividade de fixação de aplicação de criptografia no ensino de função quadrática.

ESCOLA:

TURMA: **DATA:** **HORÁRIO DE APLICAÇÃO:**

ALUNO(A):

- Siga as orientações abaixo para cifrar a mensagem para seu amigo escolhido para formar a dupla.

- 1) Escolha uma função quadrática $g(x) = \underline{\hspace{2cm}}$.
- 2) Escolha uma mensagem.
- 3) Substitua cada letra da mensagem escolhida pela letra correspondente na tabela 1.
- 4) Use a função dada $g(x)$ para cifrar a mensagem determinando as imagens de cada número e determine a sequência obtida.
- 5) Preencha a tabela abaixo usando a função $g(x)$ para cifrar a mensagem.

Letra										
x										
g(x)										

- 6) Qual mensagem você enviará?

- Entregue a mensagem à pessoa que forma dupla com você, para que possa decifrá-la seguindo os seguintes passos:

- 1) Determine a função inversa $g^{-1}(x)$ e complete a tabela abaixo.

Mensagem Recebida										
$g^{-1}(x)$										
Mensagem Decifrada										

- 2) Após decifrar, qual a mensagem achada?
- 3) O que você achou dessa atividade?
- 4) Posso usar função exponencial e logarítmica? Justifique.

ANEXO H – Atividade explicativa de aplicação de criptografia no Ensino de função exponencial.

ESCOLA:

TURMA:

DATA:

HORÁRIO DE APLICAÇÃO:

ALUNO(A):

- Vamos cifrar uma mensagem usando os conceitos de função.

1) Considere a função $f(x) = 2^x$.

2) Use a palavra "POTÊNCIA" como exemplo nesta atividade.

3) Substitua cada letra pelo número correspondente na tabela 1.

tabela 1

A	B	C	D	E	F	G	H	I	J	K	L	M
-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	0
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13

Ao fazer a substituição obtemos a sequência "3 2 7 -8 1 -10 -4 -12".

4) Use a função dada $f(x)$ para cifrar a mensagem determinando a imagem de cada número da sequência: $f(3)$, $f(2)$, $f(7)$, $f(-8)$, $f(1)$, $f(-10)$, $f(-4)$ e $f(-12)$.

5) Preencha a tabela 2 abaixo.

tabela 2

Letra	P	O	T	E	N	C	I	A		
x	3	2	7	-8	1	-10	-4	-12		
f(x)	8	4	128	1/256	2	1/1024	1/14	1/4096		

Logo, a mensagem cifrada é "8 4 128 1/256 2 1/1024 1/16 1/4096".

- Para decifrar a mensagem entregue ao receptor:

1) O receptor deve encontrar a função inversa $f^{-1}(x)$.

$$x = 2^{f^{-1}(x)}$$

$$\log_2 2^{f^{-1}(x)} = \log_2 x$$

$$f^{-1}(x) = \log_2 x$$

2) Usando a função $f^{-1}(x)$, é completada a tabela 3:

tabela 3

Mensagem Recebida	8	4	128	1/256	2	1/1024	1/16	1/4096		
$f^{-1}(x)$	3	2	7	-8	1	-10	-4	-12		
Mensagem Decifrada	P	O	T	E	N	C	I	A		

CONCLUSÃO:Então, a mensagem decifrada é a palavra "POTÊNCIA".

ANEXO I – Atividade de fixação de aplicação de criptografia no Ensino de função exponencial.

ESCOLA:

TURMA:

DATA:

HORÁRIO DE APLICAÇÃO:

ALUNO(A):

- Cifre a mensagem para depois enviar ao seu colega.

1) Use a função $g(x) = \left(\frac{1}{2}\right)^x$ e selecione uma mensagem.

2) Utilize a tabela 1 para fazer a substituição de cada letra pelo número correspondente.

3) Usando a função $g(x)$, determine as imagens de cada número da sequência e preencha a tabela abaixo.

Letra										
x										
g(x)										

4) Qual foi a mensagem cifrada?

- Envie a mensagem cifrada a um colega para que ele possa decifrar seguindo os seguintes passos:

1) Encontre a função inversa de $g(x)$, que corresponde a $g^{-1}(x)$.

2) Use $g^{-1}(x)$ para completar abaixo.

Mensagem Recebida										
$g^{-1}(x)$										
Mensagem Decifrada										

3) Qual a mensagem encontrada?

4) Se a função escolhida fosse a logarítmica, qual seria sua inversa?

5) Essa atividade ajudou a melhorar a compreensão em relação as funções exponenciais e logarítmicas?

ANEXO J – Atividade explicativa de aplicação de criptografia no Ensino de matrizes.**ESCOLA:****TURMA:****DATA:****HORÁRIO DE APLICAÇÃO:****ALUNO(A):**

- Para cifrar uma mensagem utilizando os conceitos de matrizes:

1) Escolha uma matriz A de forma que seu determinante seja -1 ou 1 , afim de garantir que todos os elementos de A^{-1} sejam inteiros.

Neste caso escolhi $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$.

2) Determine A^{-1} .

$$A^{-1} = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}$$

3) Agora selecione uma palavra para ser cifrada.

Vamos usar a palavra "MATRIZES".

4) Substitua cada letra pelo número correspondente na tabela 1.

tabela 1

A	B	C	D	E	F	G	H	I	J	K	L	M
-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	0
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13

Ao substituir a palavra "MATRIZES" obtemos a sequência "0 -12 7 5 -4 13 -8 6"

5) Use esses números como elementos de uma matriz 2×4 que chamaremos de Y .

$$Y = \begin{bmatrix} 0 & 7 & -4 & -8 \\ -12 & 5 & 13 & 6 \end{bmatrix}$$

6) Para cifrar a mensagem, basta fazer o produto $A \cdot Y$:

$$\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 7 & -4 & -8 \\ -12 & 5 & 13 & 6 \end{bmatrix} = \begin{bmatrix} -12 & 19 & 5 & -10 \\ -12 & 12 & 9 & -2 \end{bmatrix}$$

- A matriz $A \cdot Y$ obtida será enviada para o receptor decifrar seguindo os seguintes passos:

1) O receptor deverá usar A^{-1} como chave para decifrar a mensagem recebida, fazendo o produto $A^{-1} \cdot (A \cdot Y)$.

$$\begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} \cdot \begin{bmatrix} -12 & 19 & 5 & -10 \\ -12 & 12 & 9 & -2 \end{bmatrix} = \begin{bmatrix} 0 & 7 & -4 & -8 \\ -12 & 5 & 13 & 6 \end{bmatrix}$$

2) O receptor deverá obter a sequência numérica respeitando a ordem sequencial das colunas da matriz resultante: "0 -12 7 5 -4 13 -8 6".

3) Por último, substitua a sequência numérica pelas letras correspondentes na tabela 1.

Logo, a mensagem recebida é "MATRIZES".

ANEXO K – Atividade de fixação de aplicação de criptografia no Ensino de matrizes.**ESCOLA:****TURMA:****DATA:****HORÁRIO DE APLICAÇÃO:****ALUNO(A):**

- Cifre uma mensagem para enviar à sua dupla.
- 1) Escolha outra palavra.
 - 2) Ache outra matriz B cujo determinante seja -1 ou 1.
 - 3) Determine o valor de B^{-1} .
 - 4) Use a tabela 1 para cifrar a mensagem e depois use a sequência numérica achada como elementos de uma matriz que será chamada de Z.
 - 5) Envie ao receptor a matriz obtida a partir do produto $B \cdot Z$.
 - Após enviar a sua mensagem cifrada, você também receberá outra mensagem cifrada onde terá que seguir os passos a seguir:
- 1) Após receber as matrizes B^{-1} e $B \cdot Z$, faça o produto delas.
 - 2) Use a sequência numérica e decifre-a utilizando a tabela 1.
 - 3) Qual a palavra obtida?
-
- Você acha que esta atividade ajudou a fixar os conceitos de matrizes?

 - Recomendaria que outras turmas tivessem uma aula dessa?

ANEXO L –Termo de Consentimento Informado

Obs.: Todos os participantes mencionados nesta pesquisa assinaram este termo.

TERMO DE CONSENTIMENTO INFORMADO

Eu, _____, por meio deste termo, declaro que concordo com minha participação na pesquisa de dissertação de Mestrado do Professor Bruno Laranjeira Nunes, com temática sobre Aplicações de Criptografia no Ensino Básico, para o Programa de Mestrado Profissional em Rede Nacional –PROFMAT, da Universidade do Estado do Rio de Janeiro, sob a orientação da Professora Dra. Jeanne Denise Bezerrade Barros. Estou ciente de que esta pesquisa tem finalidade acadêmica e suas conclusões poderão contribuir para o aperfeiçoamento de estudos sobre o ensino de criptografia aplicado ao ensino da matemática. O uso das informações concedidas é apenas para fins de pesquisa (seminários, artigos, palestras etc.), identificado-me apenas pelo primeiro nome e idade.

Rio de Janeiro, 15 de agosto de 2017

Assinatura do Informante

Assinatura do Pesquisador

Assinatura do Orientador