Moroni Menessés Bruch Bora

Divulgação Científica Online em Teoria de Códigos e Criptografia

Brasil

9 de Abril de 2021

Moroni Menessés Bruch Bora

Divulgação Científica Online em Teoria de Códigos e Criptografia

Modelo canônico de Relatório Técnico e/ou Científico em conformidade com as normas ABNT apresentado à comunidade de usuários LaTeX.

Universidade Federal do Paraná

Setor de Ciências Exatas

Matemática

Brasil

9 de Abril de 2021

Agradecimentos

Primeiramente agradeço a Deus, que nunca me abandonou e nunca me deixou. Agradeço a minha família, minha mãe, Vanderleia Aparecida Bruch que lutou muito para que eu pudesse estudar, ao meu pai Lucas Bora, e as minhas irmãs Manuela Helena Bruch Bora e Lorena Leoni Bruch Bora. Eles me apoiaram e sempre estiveram ali por mim. Agradeço a minha orientadora, professora Ximena, que me ajudou principalmente com os códigos em latex que tornaram esta escrita possível. Agradeço também a toda a equipe do Matematicativa de 2020, cujo trabalho tornou tudo isso possível. Agradeço também aos meus amigos e colegas em geral, que tiveram paciência para me explicar que o mundo pode ser realmente um lugar melhor.

Resumo

Este Trabalho de Conclusão de Curso é um estudo sobre a divulgação online das atividades da Cifra Espartana e Cifra de César, assim como a Matemática aprendida através dessas divulgações. É feita uma revisão teórica sobre a divulgação científica para pautar a discussão e os resultados.

Palavras-chave: Códigos, Criptografia, Divulgação Científica, Ensino

Lista de ilustrações

Sumário

1 Introdução

A divulgação científica é um desafio em tempos de pandemia. Visto isso, esse TCC apresenta o aprendizado das atividades de divulgação científica pela equipe do MatematicATIVA de 2020.

O MatematicAtiva é um projeto de extensão da Universidade Federal do Paraná que, através de jogos e brincadeiras lúdicas, tenta mostrar uma Matemática diferente daquela que é apresentada nas Escolas.

Em 2020, em vista da pandemia do Coronavírus, essa equipe se viu desafiada a divulgar as brincadeiras de forma remota.

O que esse TCC relata é o aprendizado dos alunos do MatematicAtiva em relação a 2 atividades relacionadas com Criptografia: Cifra de César e Cifra Espartana.

O primeiro capítulo é uma formalização de conceitos de Criptografia e Teoria de Códigos, além de falar como isso se aplica a Cifra de César e Cifra Espartana.

O segundo capítulo trata da metodologia de divulgação e coleta de resultados.

2 O MatematicATIVA

O MatematicAtiva é um projeto de extensão da Universidade Federal do Paraná coordenado pelas professoras doutoras Ximena Mujica e Paula Rogéria Lima Couto. Antes da pandemia, o projeto visitava escolas com o objetivo de apresentar um lado mais lúdico da Matemática através de jogos e brincadeiras. Alguns dos jogos são Xadrez Africano, Figuras Replicantes, Jogo das Cordas, Pesca de Peixes, Cifra de César e Cifra Espartana (os dois últimos são tema central deste trabalho). Com o advento da pandemia, o projeto de extensão projetou-se para o ambiente online, aonde publica posts e vídeos sobre as diversas brincadeiras, explicando como é a Matemática delas e como reproduzir essas brincadeiras em casa. A cada ano, há uma nova equipe de alunos trabalhando no projeto, tanto bolsistas como voluntários.

Eu comecei minha trajetória com o MatematicATIVA em 2019, entrando como voluntário para o projeto. Lá, eu e a Professora Doutora Ximena Mujica pensamos nas atividades da Cifra de César e Cifra Espartana, e como adaptá-las para mandar ás escolas. Essas atividades foram apresentadas nas escolas em 2019, e intrigou a maioria dos alunos que a fizeram.

No início de 2020, dei uma aula na Escola Estadual Dom Orione sobre a Cifra Esparana, como parte do projeto de TCC de Educação Não-Formal, porém na sala de aula. Com o advento da pandemia, não houveram mais aulas possíveis, pois não houve mais aulas presenciais.

Assim como a escola que eu apresentei a aula, todas as outras escolas haviam fechado, e isso foi o que fez o MatematicATIVA projetar suas atividades para o ambiente online.

3 Premilinares em Teoria de Códigos e Criptografia

3.1 Preliminares

Operações elementares:

Dada uma matriz M, definimos as seguintes operações, chamadas de *operações elementares*:
Troca de linhas, Multiplicação de uma linha por um escalar, Substituição de uma linha por ela mesma subtraída de outra linha.

Dizemos que duas matrizes A e B são *equivalentes* quando é possivel obter B a partir de A através de operações elementares.

Um dos resultados a serem usados é que dado um espaço vetorial X e um subespaço Y, quando a dimensão é finita temos que $Y^{\perp\perp} = Y$ (A definição para esta notação se encontra na pagina 12).

Outro resultado muito importante é sobre teoria de números, o Teorema Fundental da Aritmética. Esse teorema diz que todo número maior do que 2 ou é primo ou é o produto de potências de primos.

Mais um resultado importante, é que é possivel definir, para os números inteiros, conjuntos quocientes dos inteiros, os $\mathbb{Z}_n$.

Tais conjuntos são definidos da seguinte forma: Para um número n dado e um número k, definimos

$$\bar{k} = \{x; x = nq + k\}$$

sendo $0 \leq k < n$.

Este conjunto, em geral, é um anel abeliano. Ou seja, a soma e produto sãõ bem definidos. A soma é definida como:

$$\bar{k_1} + \bar{k_2} = \overline{k_1 + k_2}$$

E o produto é definido por:

$$\bar{k_1}\bar{k_2} = \overline{k_1 k_2}$$

Quando n é coprimo de k, $\bar{n}$ é inversível em $\mathbb{Z}_n$.

3.2 Definições Básicas Sobre Teoria de Códigos

O texto a seguir pode ser aprofundado na referência (6).
Primeiramente, definamos as coisas básicas sobre um código:
Alfabeto: É um conjunto finito de elementos pelos quais poderá se definir um código.
Dado um alfabeto, que será denotado por A, um subconjunto de A^n pode ser denominado um *código*.
Dizemos então que um código é o subconjunto de uma n-upla de um alfabeto. Alguns exemplos de códigos:

3. A lingua portuguesa. Seu alfabeto é o conjunto das letras com os acentos e o código é um subconjunto de A^{27} pois a maior palavra da língua portuguesa tem 27 letras.

- Os computadores usam códigos baseados em zeros e ums. Neste caso o alfabeto seria o conjunto $A = \{0, 1\}$.

- O código Morse é baseado em sons para formar letras. Aqui o alfabeto é o conjunto de sons do código Morse, e se esse alfabeto pode ser rdenotado por M, o código é um subconjunto de M^5.

Uma das coisas mais importantes sobre códigos é a *Métrica de Hamming.*
Basicamente, trata-se de uma função cujo dominio é C^2 (em que C representa um código), com contradomínio no conjunto dos naturais positivos, que é definida da seguinte maneira:

$$h(u, v) = |\{i; u_i \neq v_i\}|,$$

sendo $u = (u_1, u_2, ..., u_n)$ e $v = (v_1, v_2, ..., v_n)$ elementos do código $C \subset A$.
Algumas propriedades fazem da métrica de Hamming importante para o estudo dos códigos. Essas propriedades tornam uma função com um domínio da forma, C^2 ou uma métrica. Uma *métrica* tem as 4 seguintes propriedades:

- A primeira é o fato de que essa função nunca é negativa.

- A segunda é que ela é simétrica. Ou seja, dados dois elementos a e b em C, $d(a, b) = d(b, a)$.

- A terceira é que para todo $u \in C$, $d(u, u) = 0$ e se existem a e b em C tais que $d(a, b) = 0$, então, necessariamente esses a e b são o mesmo elemento.

- A quarta propriedade é que dados a, b, e c em C, $d(a, b) \leq d(a, c) + d(b, c)$.

Para provar que a métrica de Hamming satisfaz da primeira à terceira propriedade é bem fácil, e fica a cargo do leitor. O mais difícil é provar a quarta propriedade, o que faremos a seguir.

Uma maneira muito fácil de provar é por indução no número n pois o código C é subconjunto de A^n.

Primeiramente, suponha $n = 1$. Neste caso, dados $a, b, c \in C$, temos as seguintes possibilidades:

1. $a = b = c$ e neste caso:

$$d(a, b) = 0 \leq 0 + 0 = d(a, c) + d(b, c);$$

2. $a \neq b = c$. Neste caso $a \neq c$ e

$$d(a, b) = 1 < 1 + 0 = d(a, c) + d(b, c);$$

3. $a = b \neq c$. Neste caso $a \neq c$ e temos:

$$d(a, b) = 0 < 2 = d(a, c) + d(b, c).$$

Assim, o caso $n = 1$ está provado.

Agora, supondo que vale do caso 1 até o caso n, provemos que vale para o caso $n+1$. Sejam $a, b, c \in C \subset A^{n+1}$. Denotemos $a = (a_1, a_2, ..., a_n, a_{n+1})$, $b = (b_1, b_2, ..., b_n, b_{n+1})$ e $c = (c_1, c_2, ..., c_n, c_{n+1})$
Seja $f \in A$ fixo. Considere $a' = (a_1, a_2, ..., a_n, f)$, $b' = (b_1, b_2, ..., b_n, f)$, $c' = (c_1, c_2, ..., c_n, f)$, $a'' = (f, f, ..., a_{n+1})$, $b'' = (f, f, ..., b_{n+1})$, $c'' = (f, f, ..., c_{n+1})$.Como $\{1, ..., n\}$ e $\{n + 1\}$ são conjuntos disjuntos, temos que:

$$d(a, b) = d(a', b') + d(a'', b'')$$
$$d(a, c) = d(a', c') + d(a'', c'')$$
$$d(b, c) = d(b', c') + d(b'', c'')$$

.
Considere $C' \subset A^n$ e $C'' \subset A$ códigos que são projeções de C sobre A e A^n, respectivamente. Considere também $a'_0 = (a_1, ..., a_n) \in C'$, $b'_0 = (b_1, ..., b_n) \in C'$, $c'_0 = (c_1, ..., c_n) \in C'$, $a''_0 = (a_{n+1}) \in C''$, $b''_0 = (b_{n+1}) \in C''$ e $c''_0 = (c_{n+1}) \in C''$ e sejam d' e d'' as métricas de Hamming em A^n e A respectivamente.
É fácil ver que:

$$d(a', b') = d'(a'_0, b'_0)$$

$$d(a', c') = d'(a'_0, c'_0)$$
$$d(b', c') = d'(b'_0, c'_0)$$
$$d(a'', b'') = d''(a''_0, b''_0)$$
$$d(a'', c'') = d''(a''_0, c''_0)$$
$$d(b'', c'') = d''(b''_0, c''_0)$$

Logo, pela hipótese de indução, temos que:

$$d(a', b') \leq d(a', c') + d(b', c')$$
$$d(a'', b'') \leq (a'', c'') + d(b'', c'').$$

Somando as duas inequações teremos:

$$d(a, b) \leq d(a, c) + d(b, c)$$

assim como queríamos demonstrar.

Essas propriedades tornam a métrica de Hamming muito boa para estudar códigos, porque dão ao código uma noção de distância entre as palavras.
Se duas palavras forem muito próximas, ou seja, se a distância de Hamming for muito pequena, então o código poderá ser confuso ou corrompível. Isso nos leva a querer definir parâmetros de eficiência de códigos.
Primeiro, definamos a *distância mínima* de um código:
A distância mínima de um código C é definido como o mínimo da distância entre dois elementos distintos do código, ou seja:

$$d = min\{d(x, y)|x, y \in C, x \neq y\}$$

Denotando para um número positivo qualquer x a sua parte inteira como $|||x|||$ denotamos: $\kappa = |||\frac{d-1}{2}|||$.

Sendo $B(x, k)$, chamada de *bola aberta* de centro x e raio k, o conjunto dos elementos de A^n que distam menos de k do elemento x. Dizemos que um código C é *perfeito* quando:

$$A^n \subset \cup_{x \in C} B(x, \kappa)$$

É importante notar que em qualquer caso, nenhuma das bolas de raio κ centrada em elementos do código se intersectam, porque κ é sempre menor que a distância entre quaisquer dois elementos de um código. Quando um código é perfeito, é sempre possivel entender alguma mensagem mesmo que o código venha corrompido. Assim, a tendência é que códigos perfeitos sejam melhores para a comunicação.

Por esses motivos, torna-se interessante que nosso código ofereça facilidades de cálculo de sua distância mínima. Uma maneira interessante de fazer isso, é pedir que nosso código tenha uma certa estrutura que nos permita calcular a distância mínima usando apenas um elemento do código e comparando com outros ao invés de comparar todos entre si, como acontece com os códigos lineares, que já vamos definir. A partir daqui, é necessário entender conceitos de espaço vetorial, produto interno e transformações lineares, pois esses conceitos são intrinsicamente ligados ao conceito de linearidade.

Primeiramente, seja K um corpo finito. Podemos pedir que nosso corpo K seja um alfabeto e que nosso código C seja um subespaço vetorial de K^n espaço vetorial sobre o corpo K. Se isso ocorrer, dizemos que C é um código linear. Podemos definir como *norma* de um $c \in C$, a distância de Hamming dessa palavra até o elemento nulo.
Uma coisa interessante de se provar, é que $d(x-y,0) = d(x,y)$, e é isso que faremos agora. Primeiramente, denotemos $x = (x_1, x_2, ..., x_n)$, $y = (y_1, y_2, ..., y_n)$. Escrevendo: $0 = (0, 0, .., 0)$ e sabendo que $d(x-y,0) = \|\{i|x_i - y_i \neq 0\}|$. Das propriedades de corpos, $x_i - y_i \neq 0$ implica $x_i \neq y_i$ e vice-versa. Logo, o conjunto $\{i|x_i - y_i \neq 0\}$ e o conjunto $\{i|x_i \neq y_i\}$ têm a mesma cardinalidade. A cardinalidade do segundo conjunto citado é a definição de $d(x,y)$, enquanto o primeiro é a definição de $d(x-y,0)$. Logo,

$$d(x-y,0) = d(x,y)$$

como queríamos provar.

Isso significa basicamente que não precisamos calcular todas as distâncias de Hamming para conseguir a distância mínima. Basta calcular a distância das palavras até o 0 para conseguir isso. A distância mínima de um código linear C é dito *peso* do código C.
Para codificar mensagens em um código linear, usar transformações lineares é uma boa opção. Considere uma matriz com entradas em K cujas linhas são uma base de C e tem o número de colunas igual à dimensão de C. Essa matriz é definida como *Matriz Geradora* de C.
Considere as operações elementares em matrizes equivalentes. Dizemos que dois códigos são *equivalentes* se possuirem matrizes geradoras equivalentes.
Outra coisa interessante a se definir antes de continuarmos é o produto interno entre dois elementos de K^n. Dados $a = \{a_1, a_2, a_3, ..., a_n\}$ e $b = \{b_1, b_2, b_3, ..., b_n\}$ elementos de K^n definimos o *produto interno* de a e b por:

$$< a, b >= a_1b_1 + a_2b_2 + a_3b_3 + ... + a_nb_n$$

.
A menos da propriedade de produto interno $< a, a > \geq 0$, que vale quando o corpo sobre o qual o espaço vetorial se encontra é o corpo ou dos reais ou dos complexos, todas as outras são válidas. Isso porque não podemos falar de maior ou menor em um corpo finito

como K. Mas observe o seguinte:

$$< a, b >= a_1b_1 + ... + a_nb_n = b_1a_1 + ...b_na_n =< b, a >$$

Além disso, se $\lambda \in K$, temos:

$$< \lambda a, b >= \lambda a_1b_1 + \lambda a_2b_2 + \lambda a_3b_3 + ...\lambda a_nb_n = \lambda(a_1b_1 + a_2b_2 + a_3b_3 + ...a_nb_n) = \lambda < a, b >$$

A propriedade $< a, a >= 0 \implies a = 0$, é em geral falsa. Isso porque, em Z_2, tem-se 1+1=0, e para $(1, 1, 0) \in \mathbb{Z}^3{}_2$, teremos $< (1, 1, 0), (1, 1, 0) >= 1 + 1 + 0 = 0 + 0 = 0$ sendo esse vetor diferente de (0,0,0).
Agora podemos continuar. Definimos primeiramente para o código C, código dual de C como sendo:

$$C^{\perp} = \{x \in K_n; < x, y >= 0 \forall y \in C\}$$

Observe que esse é de fato um *código linear*. Isso porque para qualquer vetor x de C temos $< 0, x >= 0$ e portanto o vetor nulo está contido em $C^{\perp}$. Considerando $y, z \in C^{\perp}$ e um $\lambda \in K$ temos que se $x \in C$:

$$< y + \lambda z, x >=< y, x > + < \lambda z, x >=< y, x > +\lambda < z, x >= 0 + \lambda 0 = 0 + 0 = 0,$$

e portanto, $y + \lambda z \in C^{\perp}$. Logo, $C^{\perp}$ é um subespaço vetorial de K^n e portanto é um código linear.
Considere a matriz geradora de $C^{\perp}$. Definimos, para cada C sua *matriz de paridade* como sendo a matriz geradora de $C^{\perp}$. Denotemos a matriz de paridade de C como H.
Dado um vetor j em K^n, definimos como *síndrome* de j em relação ao código C, o vetor resultante do cálculo de Hj^t.

Esses conceitos são muito importantes, pois darão uma ideia de decodificação, isto é, de correção de erros.

Definimos o *erro* como sendo a diferença entre a palavra recebida e a palavra transmitida, ou seja, se a palavra recebida é r e a transmitida é c o erro é:

$$e = r - c$$

Se aplicarmos a matriz de paridade no erro, veremos que:

$$H\bar{e}^t = H(r^t - c^t) = Hr^t - H^t = 0$$

pois $c \in C$, obtemos:

$$H\bar{e}^t = Hr^t.$$

E portanto o erro e a palavra recebida têm a mesma síndrome.
Isto é interessante, porque mostra que, um código C ter capacidade de correção κ, implica que se uma palavra r dista menos de κ de uma palavra $c \in C$, existe um único erro e tal que $c = r - e$.

Sabemos que $e = r - c$ já satistaz o que queremos, já que seu peso tem que ser a distância entre r e c que já é menor que κ.
Se existe outro erro que satistaz isso, então:

$$He^t = He'^t$$

e portanto, se h^i representa a i-ésima coluna de H, temos:

$$\sum_{i=1}^{n} a_i h^i = \sum_{i=1}^{n} \bar{a}_i h^i$$

O que tornaria as colunas de H linearmente dependentes, e isso seria um absurdo, a não ser que tivéssemos que $\bar{e} = e$.
Isso nos leva a poder decodificar caso apenas um erro tenha sido cometido. Se supormos $d \geq 3$, calculamos para a palavra recebida, Hr^t. Se $Hr^t = 0$ deixa como está. Se estiver diferente, podemos procurar i e a números inteiros tais que $s^t = ah^i$ e então e seria a n-upla com a na posição i e 0 nas outras. Se isso não ocorrer, então houve mais de um erro.
Podemos falar de decodificações mais complexas mas antes precisamos falar de outras coisas.
Primeiramente, definamos, para um vetor $v \in K^n$ o conjunto:

$$v + C = \{v + c; c \in C\}$$

Isso é basicamente um elemento do espaço quociente K^n/C, e portanto, pelo que sabemos de Álgebra Linear, há uma relação de equivalência envolvida.

Podemos dizer que dois elementos de uma mesma classe de equivalência tem síndromes iguais, e se têm sindromes iguais, estão na mesma classe de equivalência.
De fato, tome dois elementos u e v com a mesma síndrome. Então teremos $Hu^t = Hv^t$. Se isso acontece então a síndrome da diferença é nula. Ou seja $H(u - v)^t = 0$. Como a matriz de paridade é constituida pelos elementos da base de $C^\perp$, teremos que $u - v$ será perpendicular a $C^\perp$, e portanto, $u - v \in C$ pela propriedadede que ser perpendicular ao perpendicular de um subespaço é ser pertencente a esse espaço. A volta também é válida. Logo, como $u = v + (u - v)$ e $u - v \in C$ teremos que $u \in v + C$ e vice versa.

Outra coisa que precisamos definir é o líder de uma classe. Definimos um *líder* de uma classe de equivalência como sendo um vetor não nulo que assume o peso mínimo da classe de equivalência.
Uma coisa interessante de se observar é que se o líder tem o peso menor que a capacidade de correção κ, esse líder é único. De fato, se considerarmos u e v como dois líderes e $\omega(x)$ a notação para peso de x teremos:

$$\omega(u-v) \leq \omega(u) + \omega(v) \leq \frac{d-1}{2} + \frac{d-1}{2} \leq d-1$$

e portanto, como d é a distância mínima, e $u-v \in C$ pelo que sabemos de Álgebra Linear, temos que $u - v = 0$ e portanto $u = v$.

Disso podemos inferir que todos os elementos de K^n com peso menor que a capacidade de correção são os líderes de suas respectivas classes.
Logo podemos falar em um algorítmo de Decodificação mais complexo. O algorítmo é o seguinte:
Dada uma palavra recebida, seja $s^t = Hr^t$. Se s estiver dentro do conjunto dos códigos possíveis, considera o elemento líder da classe de s, o elemento ℓ. Se o lider tiver peso menor que a capacidade de correção, corrige como $r - \ell$, caso contrário, foram cometidos mais de κ erros.
Tudo isso pode ser encontrado na referência (6)

3.2.1 Noções Básicas de Criptografia RSA

O que segue pode ser aprofundado na referência (4) .A criptografia RSA funciona da seguinte forma: Para cada letra do alfabeto escolhemos um conjunto ordenado de dois números, que pode ser: A=11,B=12,C=13,D=14,... sem acentuação. A barra de espaço é o 99. Essa é a pré-codificação Dito isso ciframos a mensagem.

Para decifrar, escolhemos dois primos p e q e fazemos $pq = n$, sendo n o primeiro elemento da chave de codificação, que definiremos logo. Esses primos serão os parâmetros da codificação. Em seguida, definamos $\Phi(n) = (p-1)(q-1)$, que é um elemento que será importante. Tomemos um número e tal que $mdc(e, \Phi(n)) = 1$. Esse número é inversível módulo $\Phi(n)$. Definimos a chave de codificação como sendo a dupla (n, e).

Então para cada bloco feito na pré-codificação, cujo número chamaremos de b, calculamos o resto da divisão de b^e por n. Esse número calculado vai ser substituído na hora de cifrar.
Para decifrar, basicamente tomamos o inverso de e na congruência por $\Phi(n)$, que chamaremos de a. A dupla (n, a) será a chave de decodificação da mensagem. Tomamos cada bloco codificado da mensagem, que chamaremos de c e calculamos o resto da divisão por n de c^a. Teremos então a mensagem em números decifrada.

4 Discussões Teóricas Sobre Divulgação Científica

4.1 Introdução à Discussão

A discussão sobre divulgação científica ainda é recente no Brasil, ainda está em seus primeiros passos, mas já há material sobre o assunto. Em (9) Marandino et al discutem a questão por dois vieses: Um teórico e outro prático.

4.2 Discussão Teórica

O que faremos neste tópico é falar sobre qual é a concepção na qual fizemos a divulgação científica.

Primeiramente, observo que (1) nos fala que o divulgador não deve ensinar. Por isto, estamos dizendo que não estamos apenas divulgando, mas também ensinando.

Porém, entre outras concepções, podemos dizer que estamos apenas divulgando. Por exemplo, em (7) consta que para José Reis, a divulgação científica tem dois papéis principais: ensinar e fomentar o ensino. Roqueplo, em (10), também nos fala de divulgação científica como toda atividade de divulgação de conhecimentos fora do ambiente formal escolar e sem a intenção de formar especialistas, e neste sentido, nossa oficina se encaixa neste aspecto, se considerarmos o ambiente formal como sendo a sala de aula e no horário formal de funcionamento.

Depois, pesquisamos mais sobre a divulgação científica, a fim de situá-la no contexto da pandemia em que o trabalho foi feito.

Em (9), Caldas nos alerta para o problema da divulgação científica descontextualizada, que não expõe a metodologia científica nas discussões. Nosso trabalho tenta avaliar também o quanto contornamos esse problema. Como estamos fazendo divulgação científica de uma área da Matemática, os métodos matemáticos devem ser levados em conta. Por isso, os quizzes tentam avaliar se aqueles que respondem os questionários entenderam o conceito matemático por trás dessas atividades. Então, quando perguntamos no quiz o que acontece se rodarmos duas vezes a chave B, estamos tentando mensurar o conceito de composição de transformações lineares no código que foi construido. Ao compor a chave B com a mesma, estamos compondo duas vezes uma transformação linear. Entender que isso dá uma chave D é importante.

Também é importante compreender sobre as redes sociais em que estamos inseri-

dos. O Facebook, por exemplo, é uma rede social centrada no outro. Por isso, é importante lembrar que a divulgação científica no facebook é feita em meio a muitos posts. Os resultados são influenciados por isso. O instagram segue a mesma perspectiva através de fotos.

5 Objetivos e Metodologia

5.1 Objetivos

O objetivo desse trabalho é tentar mensurar o quanto foi aprendido e qual o efeito da divulgação científica do MatematicATIVA no Facebook e Instagram.

5.2 Metodologia

5.2.1 Introdução à Metodologia

Serão analisadas as respostas de 3 perguntas feitas nos stories do MatematicATIVA no facebook e Instagram. As respostas serão relativas a duas atividades, Cifra de César e Cifra Espartana, como veremos a seguir:

5.2.2 Cifra de Cesar

A Cifra de Cesar era um método muito utilizado pelos romanos para enviar e receber mensagens. Para realizar a cifragem, é necessario ter uma folha de papel, um lápis, dois alfabetos e uma lata, como mostra a seguinte imagem:

Figura 1 – Cifra de Cesar

Para cifrar, primeiro seleciona-se um caractere (letra ou número), e gira-se o cifrador de forma que a caractere escolhido esteja aparecendo no buraco. Esse caractere é o que aparece na parte de baixo do tubo, ou no caso da imagem, da latinha. Desta forma, haverá uma correspondência entre os caracteres superiores e inferiores. Há, por exemplo, uma correspondência entre A e o 2. Então, para escrevermos uma frase, é necessário primeiramente que busquemos, para cada caractere da frase um caractere codificado correspondente.

Digamos que queiramos dizer "oi" e a letra selecionada é a letra "c". Então, nossa codificação mandará cada letra da palavra para duas letras à frente na ordem. Logo, o "o" será substituido pelo "q", e o "i" será substituido pelo "k" e a pessoa escreverá "qk" para dizer "oi".

5.2.3 Cifra Espartana

Para cifrar neste método, é necessário, primeiramente, de uma fita de papel, um lápis ou caneta, e um tubo, e este tubo será tanto a chave de cifragem quanto a chave de decifragem.

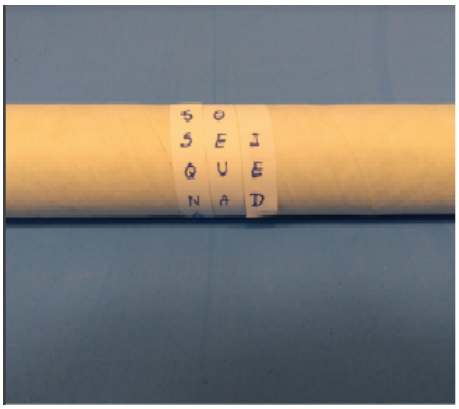

Figura 2 – Cifra Espartana

A cifragem consiste, basicamente, em enrolar a fita de papel no tubo, e, em cima do tubo, escrever a mensagem. Quando for desenrolada a fita de papel, a mensagem estará irreconhecível, pois a mensagem foi escrita em cima do tubo. Assim, a mensagem estará cifrada.

É preciso achar o tubo certo, pois, a princípio, os tubos terão diâmetros distintos.

A pessoa receberá várias tiras e tentará achar a chave certa para cada tira tentando achar o tubo certo. A seguir os posts feitos pelo MatematicATIVA para o Facebook e o Instagram: Este primeiro post é início do trabalho. Foi feito para despertar a curiosidade.

Figura 3 – Storie

5.3 Cronograma

Com o advento da pandemia, o cronograma mudou. Na segunda semana de Novembro, foram feitas perguntas no Instagram e no Facebook do MatemáticAtiva e, a partir dessas perguntas, usamos para mensurar e discutir a divulgação científica.

5.4 Jornada

A equipe do projeto MatematicATIVA postou uma série de vídeos sobre as atividades da Cifra de César e da Cifra Espartana. Os primeiros vídeos ensinavam, entre outras coisas, como construir chaves de César e Tubos hexagonais a partir de materiais que as pessoas tivessem em casa, que posteriormente serviriam para a atividade da Cifra Espartana. Depois, a mesma equipe postou nas mesmas redes as formas de interagir com esses materiais. Em seguida, a equipe postou coisas relacionadas à relação matemática existente entre essas duas atividades. No Facebook e Instagram, o primeiro post relacionado a Criptografia ocorreu no dia 18 de Setembro de 2020. O post possui 4 imagens, que estão a seguir, e este post teve 8 reações até Fevereiro de 2021:

Figura 4 – Postagem 1

O segundo post, que ocorreu no dia 21 de Setembro de 2020, explica como funciona a Cifra Espartana

Figura 5 – Postagem 2

No dia 25, a equipe do MatematicATIVA postou um vídeo mostrando como construir uma chave de Cifra Espartana usando um cilindro e uma tira de papel. Esse vídeo pode ser acessado nos links abaixo:

- instagram: https://www.instagram.com/p/CFkzhKchreb/
- facebook: https://www.facebook.com/MatematicAtiva.UFPR/videos/665412597447033

Figura 6 – Postagem 3

No dia 28 de Setembro de 2020, a equipe do MatematicATIVA postou imagens explicando a relação entre Cifra Espartana e Cifra por Transposição, como podemos ver

na última figura acima.

No dia 2 de Outubro de 2020, a equipe do MatematicATIVA postou 3 imagens sobre a Cifra de Cesar, como podemos ver abaixo.

Figura 7 – Postagem 4

No dia 5 de Outubro de 2020, a equipe do MatematicATIVA postou um vídeo explicando como montar uma chave de Cesar com papelão.
Esse vídeo pode ser acessado nos links abaixo:
• instagram: https://www.instagram.com/p/CF-h7KTBx0x/
• facebook: https://www.facebook.com/MatematicAtiva.UFPR/videos/340541307372883

As publicações foram simultâneas.

5.5 Reflexões sobre a Jornada

Enquanto eu lia em diversos textos a teoria sobre a divulgação científica em diversas redes sociais, me deparei com algumas perguntas. A primeira é saber se estávamos fazendo, de fato, uma divulgação científica. Definir a divulgação científica é uma grande questão das discussões acadêmicas nos dias de hoje. Outra pergunta que nos fizemos é se nós teríamos resultados significativos para esse processo. Felizmente temos resultados possíveis de serem analisados.

É interessante frisar que o MatematicATIVA teve um aumento muito grande de seguidores recentemente em razão do evento "Meninas nas Exatas". Então, acreditamos que os resultados talvez fossem mais promissores se fossem feitos agora.

5.6 O Processo de Aprendizagem

O MatematicAtiva fazia toda semana uma reunião sobre quais posts colocar. Uma pessoa ficava encarregada de fazer o post, outra de postar, outra de colocar o resultado. Cada pessoa fazia alguns posts. Os quizzes, em geral, foram uma coisa constante durante todo o trabalho do MatemarticAtiva. Porém, eu ajudei a pensar nos quizzes relacionados a parte de Criptografia. Eu e Isac Messias Michelon pensamos nos quizzes. Fizemos uma reunião a parte para isso. Nosso objetivo era realmente avaliar o aprendizado daqueles que tinham acesso aos posts e tiveram contato com eles.
Foi um trabalho árduo para todos os envolvidos.

5.7 Resultados

Os rssultados estão como descritos a seguir.
Houve duas enquetes no Instagram porque queríamos testar as diferenças de respostas da primeira para a segunda. Basicamente, houve uma queda de respostas e interações da segunda enquete em relação à primeira.

Além disto, a maioria das pessoas acertou os desafios, o que nos faz crer que, em pelo meno algum sentido, conseguimos educar através de nossa divulgação científica.

Como o MatematicATIVA começou as atividades online em meados de 2020, achamos natural que houvesse poucas interações.
Das interações, a maioria foi de alunos do próprio curso de Matemática, mas também houve interações de fora do círculo matemático.
A seguir, imagens do resultado:

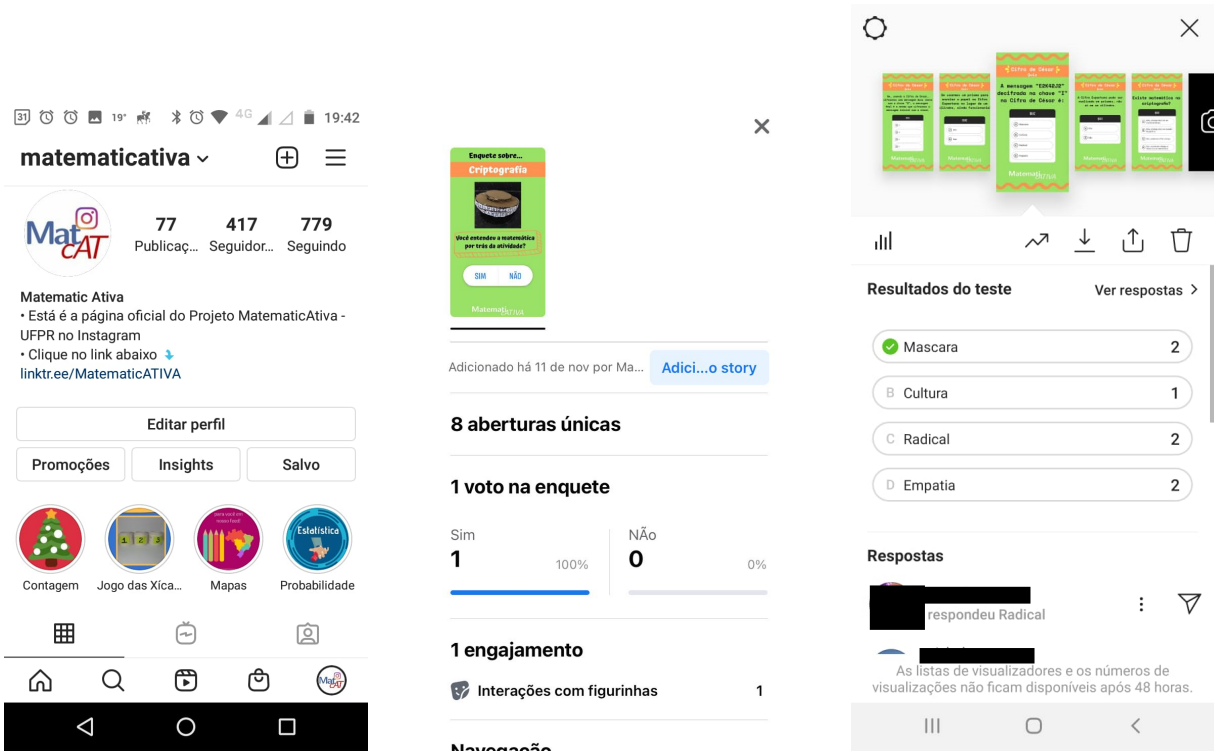

Figura 8 – Imagens 1, 2 e 3

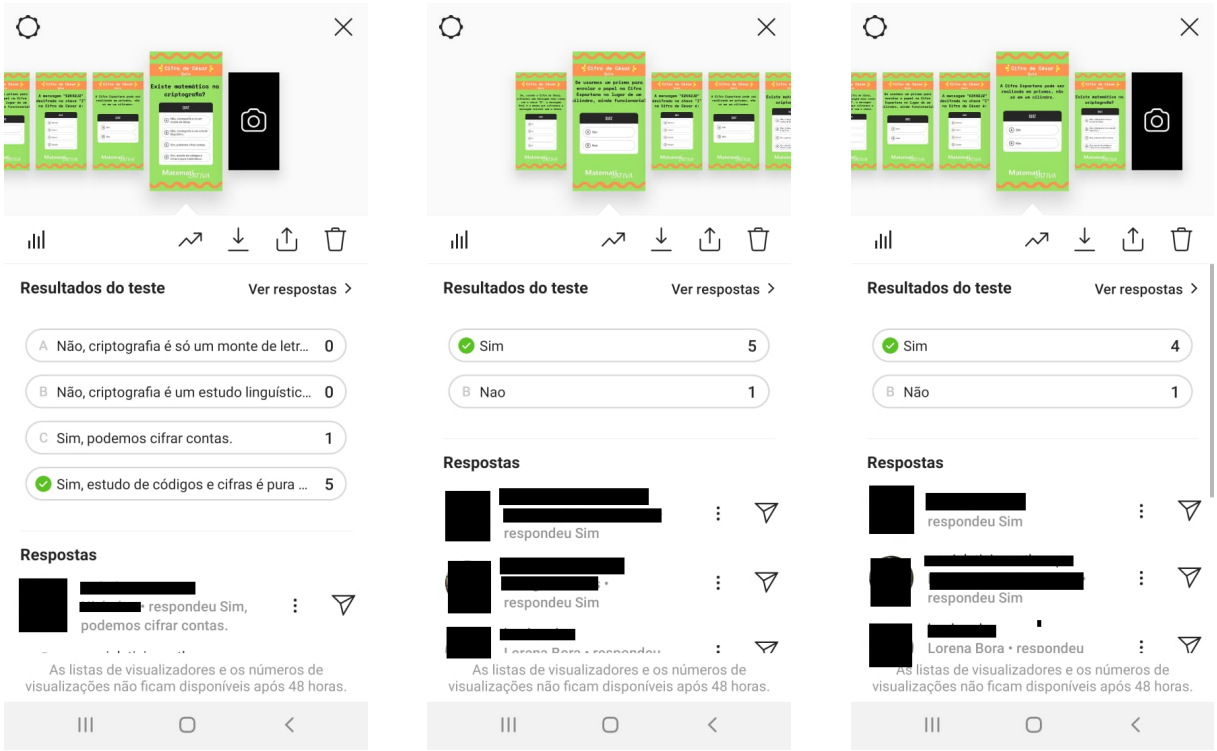

Figura 9 – Imagens 4,5 e 6

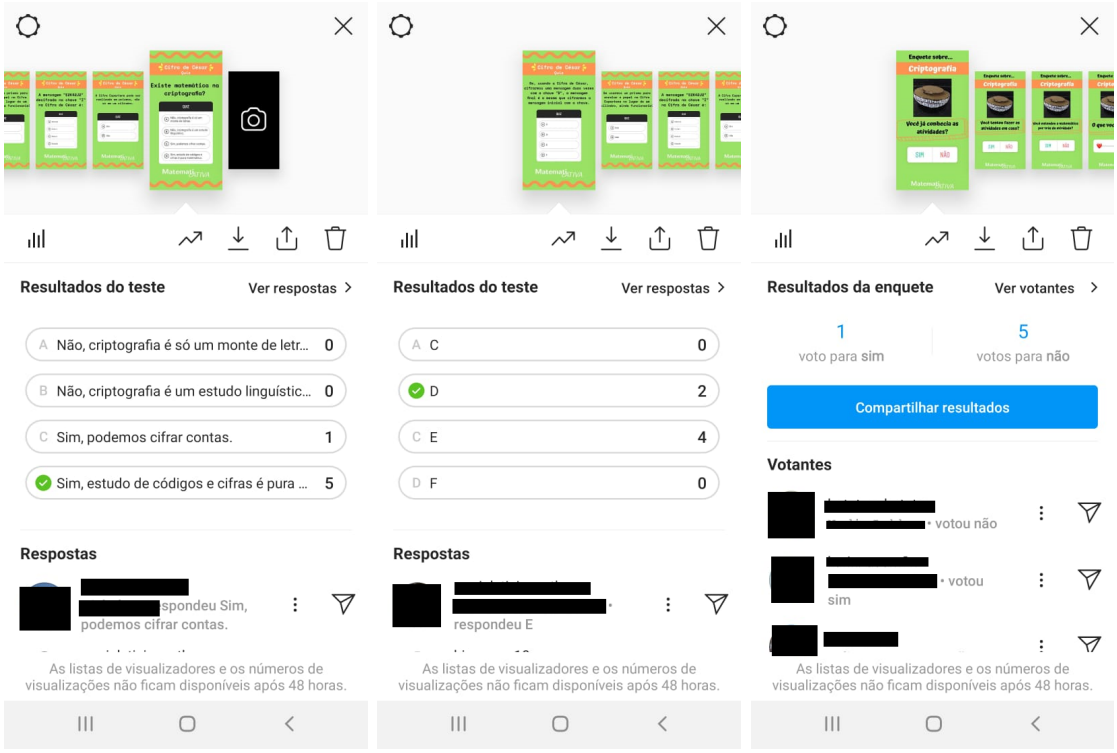

Figura 10 – Imagens 7, 8 e 9

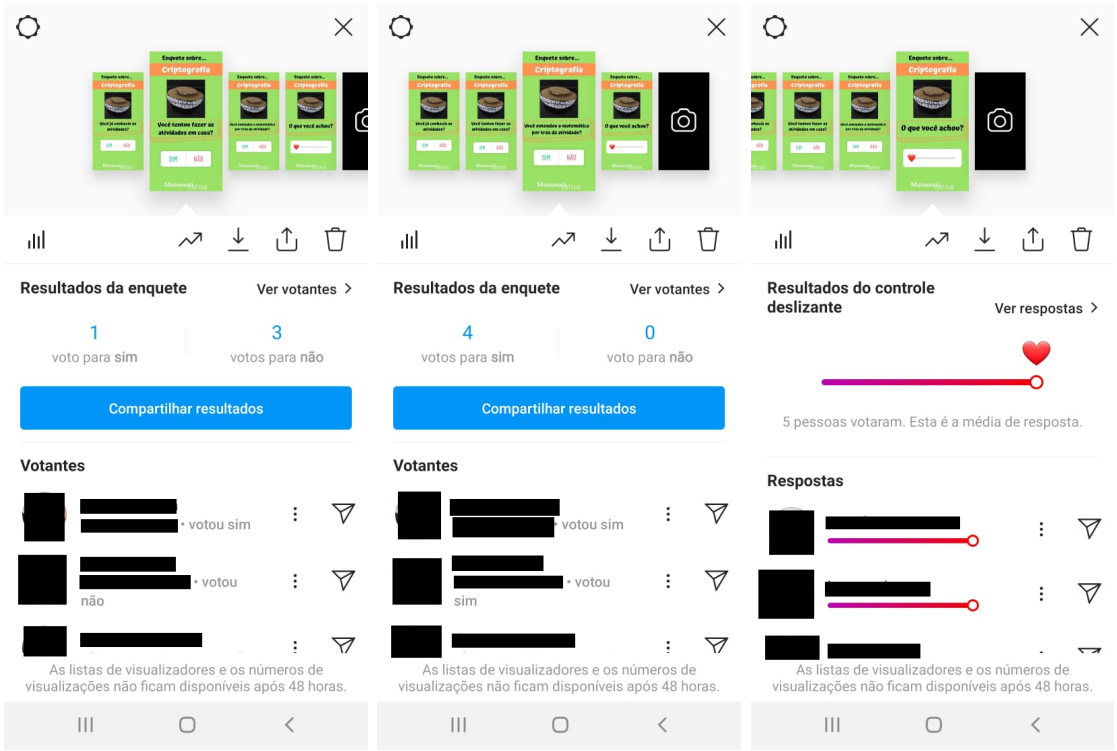

Figura 11 – Imagens 10,11 e 12

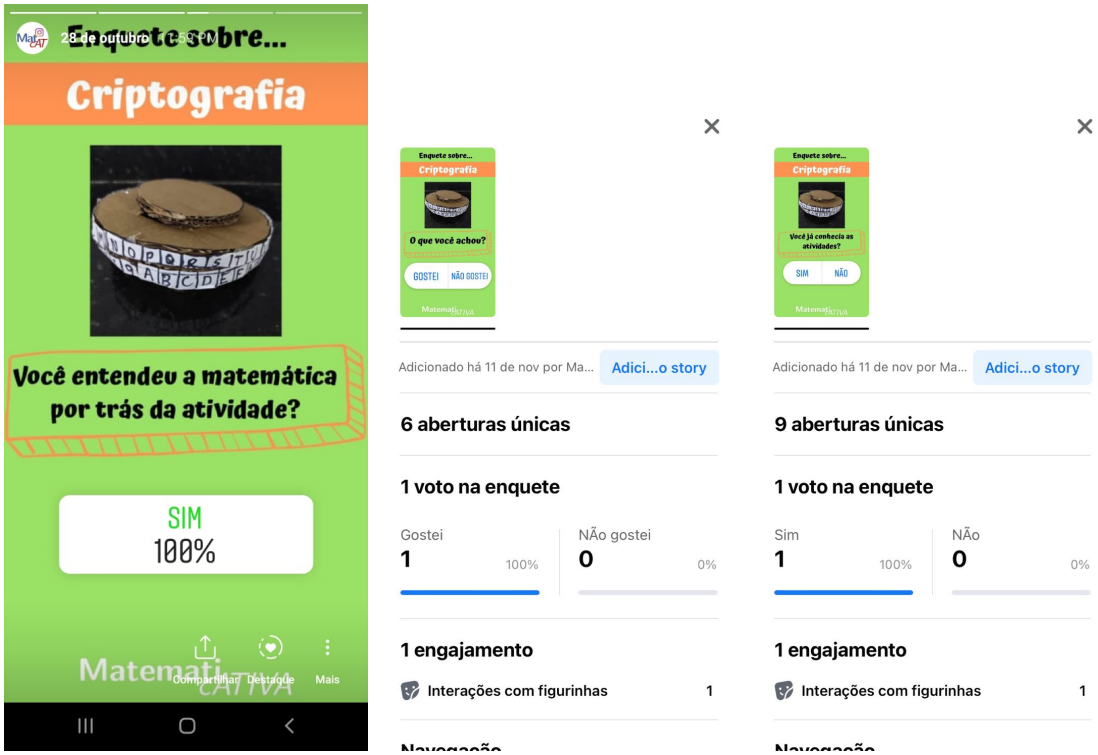

Figura 12 – Imagens 13,14 e 15

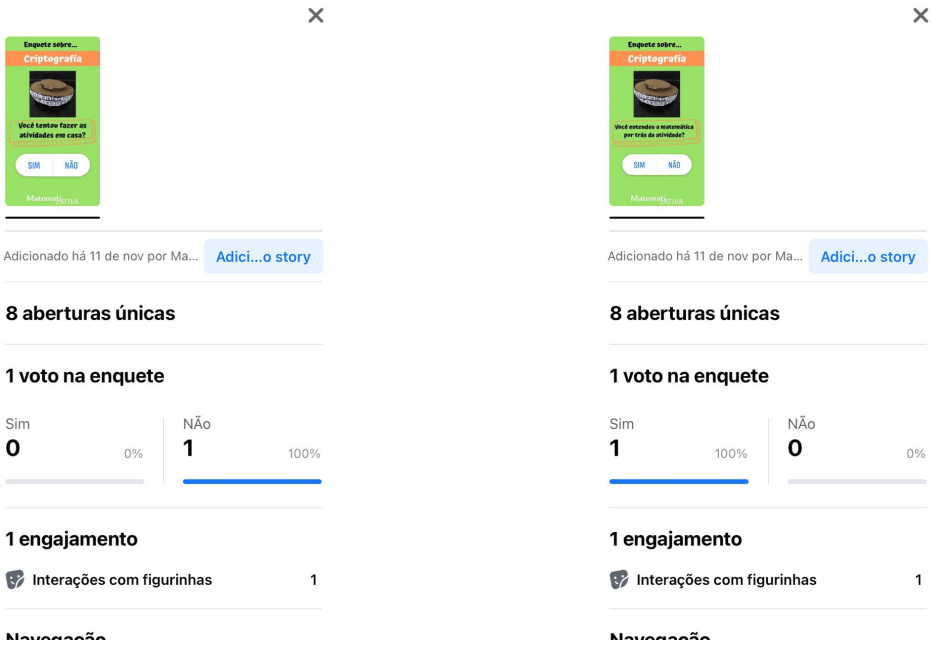

Figura 13 – Imagens 16 e 17

Figura 14 – Imagens 18 e 19

5.8 Interpretação dos Resultados via Discussão Teórica

De maneira geral, 75% das interações com as enquetes do Instagram, tanto na primeira quanto na segunda vez, são de pessoas de dentro da comunidade do curso de matemática. Uma pessoa em especial, externa à comunidade, se interessou pelo trabalho e respondeu as enquetes, mas como não pedimos permissão, não colocaremos seu nome. A maioria dos feedbacks foram positivos.

Citando Couto (5), "No entanto, não há como escapar da re-significação da concepção de ensino-aprendizagem com as mídias sociais, portanto, não há como escapar às formas de divulgação em (dis)cursos que produzem sentidos a partir dessa re-significação. É preciso compreender, portanto, as mudanças e suas implicações para a forma-sujeito contemporânea, para as relações de poder (econômicas, sociais) que significam a divisão dos sentidos na produção de conhecimento."
Sendo assim, é normal que os efeitos dessa re-significação não sejam os mesmos. Nas sala de aula, tínhamos um controle muito maior da situação de aprendizagem. Já nas redes sociais, toda a relação é re-significada, configurando um modo inédito de produção de conhecimento se comparado ao plano original.

Citando Meness (8), a Web 2.0, na qual os usúarios produzem tanto conteúdo quanto eles consomem (que é o caso do Facebook e Instagram) "não é uma Web de

publicação textual, mas uma Web de comunicação multisensitiva.". Não são apenas textos que interagem com as pessoas, mas todo o conjunto de sensações deve ser levado em conta. Sendo assim, é comum que haja poucas interações.

6 Relação entre a Divulgação Científica Realizada e os Conceitos Matemáticos Envolvidos

A Cifra de Cesar é basicamente uma forma de decodificação baseada no código $\mathbb{Z}_{33}$. Não é diretamente possivel relaciona-lo com o conceito de código linear se incluidos os números no alfabeto.Mesmo se incluídas somente letras, teremos $\mathbb{Z}_{26}$, e assim não podemos falar diretamente em linearidade de código. Cada letra pode ser vista como uma função, e se a letra é n, então a função correspondente é $n(a) = a + n$, que a principio não é uma função linear, porém é possivel estabelecer uma função linear entre $\mathbb{Z}_{26}$ e o conjunto das funções. O que temos é que podemos usar alguns dos teoremas da Teoria de Códigos, que não usam todo o conceito de corpo finito
Com os números, podemos falar de ortogonalidade com produto interno, e com isso podemos falar de erros, paridade etc, mesmo sem a inversibilidade.
Já a Cifra Espartana, podemos ver na figura 6 (na página 22) uma relação explícita entre a Cifra Espartana e a Matemática. Nesse caso, se considerarmos apenas as letras, teremos de fato a cifragem da Cifra Espartana como um código linear de $\mathbb{Z}_{26}^n$ onde n é o número de letras que cabem na linha da Cifra Espartana. Nesse sentido, não temos um código linear,mas temos algo parecido, que é basicamente uma permutação de coordenadas de $\mathbb{Z}_{26}^n$ para $\mathbb{Z}_{26}^n$

7 Conclusão

Acreditamos, em vista dos resultados, que houve de fato uma aprendizagem do público fora da comunidade matemática, acerca dos conceitos que quisemos trabalhar. Concluímos também que é possível o ensino assíncrono através das redes sociais. De certa forma, sentimos ter feito uma descoberta de possibilidades de Educação Não-Formal e Divulgação Científica.

Não subestimamos de forma alguma as limitações inerentes à diferença entre o ensino síncrono presencial e o assíncrono não presencial. Esperamos, através deste trabalho, contribuir para a discussão acerca da Educação Não-Formal no contexto da pandemia e também após a mesma.

Através de conceitos da Criptografia e da Teoria dos Códigos, nosso objetivo sempre foi contribuir para a discussão acerca de possibilidades de ensino. Quando começamos o planejamento, pensamos as atividades, a metodologia e toda a epistemologia do processo no sentido de trabalhar intuições relacionadas à codificação de mensagens, o que envolve conceitos variados da Matemática, principalmente relacionados à Teoria de Grupos e Álgebra Linear.

Porém, com o advento da pandemia de 2020, nós pensamos em maneiras de contribuir para a discussão, de preferência usando os mesmos conceitos ou semelhantes, porém adaptado para as formas remotas de divulgação. Não havia como garantir que um certo grupo de pessoas fosse ensinada de forma institucionalizada. Por isso, aceitamos essa limitação e pensamos possibilidades dentro destas limitações. Dito isso, não nos surpreendeu que, enquanto na situação pré-pandemia tivéssemos mais de 30 alunos contribuindo para os dados, nos vimos então com 4 ou 5 pessoas dando a mesma contribuição. Mesmo assim, nós conseguimos estes dados.

Em geral, boa parte dos respondentes interagiram positivamente, demonstrando, nos resultados dos stories, uma aquisição cognitiva significativa no que se refere aos conceitos matemáticos que havíamos pensado antes do COVID-19.

Com isso, acreditamos que nossas atividades e os resultados e experiências advindas delas podem contribuir para pensar possibilidades de ensino dos mais diversos conceitos matemáticos durante e após o contexto da pandemia.

Referências

(1) BRAGANÇA, G e LOURENÇO - *Que Cultura para o Século XXI? O Papel Essencial dos Museus de Ciência e Técnica*. In VI Reunião da Red-Pop, Museu de Astronomia e Ciências Afins/UNESCO, Rio de Janeiro, junho, 1999.

(2) CIMINO, A. - *A História da Quebra dos Códigos Secretos*. Ed. M. Books do Brasil Editora Ltda., 2018.

(3) COELHO, F. U. e LOURENÇO, M. L. - *Um curso de Álgebra Linear*. Editora da Universidade de São Paulo, 2^a edição revista e ampliada, 3^a reimpressão, 2013.

(4) COUTINHO, S. C. - *Números Inteiros e Criptografia RSA*. Coutinho, S.C. IMPA, 2014.

(5) COUTO, O. F. e DIAS, C. - *As Redes Sociais na Divulgação e Formação do Sujeito do Conhecimento: Compartilhando a Produção Através da Circulação de Ideias*. Linguagem em (dis)curso. Vol. n. 3. Tubarão, 2011. Disponível em https://www.scielo.br/scielo.php?script=sci_arttext&pid=S1518-76322011000300009&lng=pt&tlng=pt

(6) HEFEZ, A., VILELA, M. L. T. - *Códigos Corretores de Erros*. IMPA. 2^a ed., 2017.

(7) KREINZ, G. - *Teoria e Prática da Divulgação Científica*. In KREINZ, G. e PAVAN, C. - Os Donos da Paisagem - Estudos sobre Divulgação Científica. NJR/ECA/USP, P. 71-110, 2000.

(8) MANESS, J. M. - *Teoria da Biblioteca 2.0: Web 2.0 e suas Implicações para as Bibliotecas*. Disponível em: https://brapci.inf.br/_repositorio/2010/11/pdf_d1b75c96ad_0012775.pdf

(9) MARANDINO, M. , DA SILVEIRA, R.V.M ,CHELINI, M.J , FERNANDES, A.B., RACHID, V., MARTINS, L.C., LOURENÇO, M.F., FERNANDES, J.A.,

FLORENTINO, H. A. - *A Educação Não Formal e A Divulgação Científica: O que pensa quem faz?* Faculdade de Educação da Universidade de São Paulo. Disponível em http://abrapecnet.org.br/enpec/iv-enpec/orais/ORAL009.pdf

(10) ROQUEPLO, P. *La partage du savoir*. Paris: éditions du Sueli. 1974.