XI JORNADA DE INICIAÇÃO CIENTÍFICA E TECNOLÓGICA
EVENTO ON-LINE
23 A 26 DE NOVEMBRO
UNIVERSIDADE FEDERAL DA FRONTEIRA SUL

GRUPO DIEDRAl E MÚSICA

JACOB DANIEL DAROS[1], GRAZIELI SOLANGE SIVA[2], EVERTON ARTUSO[3]

1 INTRODUÇÃO

Em [3], os autores desenvolvem a teoria musical das tríades através da teoria de grupos, em especial a teoria de grupos diedrais. Os grupos diedrais encontram um lugar privilegiado nesse contexto, pois são grupos de simetrias. Nesse caso, especificamente, a sequência das tríades forma um grupo diedral de ordem 24 e é gerado por duas ações de grupo definidas no século XIX por Hugo Riemann.

Paralelamente, em [2] o autor aborda mensagens cifradas nos acordes da obra de Robert Alexander Schumann (1810-1856), um pianista, compositor e crítico musical alemão. Já em [1], o autor apresenta uma série de criptogramas inseridos pelo músico Edward Elgar em sua obra e uma possível solução para tal enigma.

A cifragem musical consiste simplesmente na codificação de uma sequência de acordes cada qual associado com um símbolo (ou significado) específico. Por outro lado, *softwares* como o Shazam, por exemplo, são capazes de decodificar sinais sonoros e identificar qual é a música que está tocando. Tal processo é realizado utilizando-se um grande banco de dados de modo que, para cada música, haja um "espectograma" (uma espécie de gráfico 3D) associado, o qual é obtido através da decomposição de frequências por meio de transformadas de Fourier.

Tendo em vista esse cenário como motivação, será apresentada brevemente uma ideia sobre a criptografia e alguns conceitos e resultados de teoria dos grupos que a fundamenta.

2 OBJETIVOS

- Introduzir alguns conceitos e resultados de teoria dos grupos com o propósito de fundamentar suas aplicações;
- Apresentar uma forma de codificação/decodificação de informações consolidada.

3 METODOLOGIA

[1] Acadêmico do curso de Física – Licenciatura, Universidade Federal Fronteira Sul, *campus* Realeza, contato: jacobdanieldaros@gmail.com
[2] Acadêmica do curso de Física – Licenciatura, Universidade Federal Fronteira Sul, *campus* Realeza, contato: grazielisolsiva@hotmail.com
[3] Docente, Universidade Federal Fronteira Sul, *campus* Realeza, **orientador.**

No contexto da cifragem/decodificação musical, apresenta-se uma forma de codificação de informações consolidada, a criptografia RSA. Para fundamentá-la, será desenvolvido conceitos e resultados de teoria dos grupos, como o Teorema de Lagrange e o pequeno Teorema de Fermat, este último podendo ser usado para testar se números realmente grandes são primos. Grandes números primos são essenciais para a codificação de mensagens na criptografia RSA.

4 RESULTADOS E DISCUSSÃO

Para a proposta da resolução da criptografia RSA através do Pequeno Teorema de Fermat é necessário uma abordagem do Teorema de Lagrange.

4.1 Classes laterais e o Teorema de Lagrange

Seja G um grupo e H um subgrupo de G, pode-se definir a relação de equivalência à esquerda "$\sim_E$"dada por $y \sim_E x$ se, e somente se, existir $h \in H$ tal que $y = xh$.

Por definição, o conjunto $\{ y \in G \mid y \sim_E x \} = \{ xh \mid h \in H \}$ é a classe de equivalência que contém x, e o indicaremos como xH, que é a classe lateral à esquerda de H em G que contém x. Analogamente, pode-se obter as classes laterais à direita de H em G, como sendo $Hx = \{ hx \mid h \in H \}$.

Definição 4.2. H sendo um subgrupo de G, com G sendo um grupo finito, tem-se que o número de classes laterais distintas módulo H em G é o índice de H em G e é denotado por $(G : H)$

Teorema 4.3 (Teorema de Lagrange)**.** *Se G for um grupo finito e H um subgrupo de G, então a ordem de H divide a ordem de G e* $|G| = |H|\,(G : H)$.

Demonstração. A quantidade de elementos presentes em uma classe lateral Hxé a mesma quantidade de elementos em H. Assim, sendo $\psi: H \to Hx$, como sendo $\psi(h) = hx$.

Assim, se $\psi(h_1) = \psi(h_2)$, então $h_1x = h_2x$ implica que $h_1xx^{-1} = h_2xx^{-1}$e daí $h_1 = h_2$, logo ψ é injetora. Por outro lado, se $y \in Hx$, então existe $h_1 \in H$ tal que $y = h_1x$, logo $\psi(h_1) = h_1x = y$ e portanto, ψ é sobrejetora. Sendo assim, ψ uma bijeção de H em Hx, de onde vem $|H| = |Hx|$. Sabendo que $G = x_1H \cup x_2H \cup \cdots \cup x_nH$, obtem-se $|G| = |x_1H| + |x_2H| + \cdots + |x_nH|$, logo $|G| = |H| + |H| + \cdots + |H| = n|H|$ e, portanto, $|G| = (G : H) \cdot |H|$.

Uma das aplicações do Teorema de Lagrange é o pequeno Teorema de Fermat, que é um caso especial do teorema de Euler, tendo importância nas aplicações das teorias dos números elementares, com testes de primalidade e criptografia de chave pública. Em outros termos, o pequeno Teorema de Fermat oferece um teste simples e eficiente para ignorar

números não-primos. Dessa maneira, aqui o será utilizado como forma de testar se números grandes são primos.

Teorema 4.4 (Pequeno Teorema de Fermat)**.** *Sendo p um primo e mdc*$(p,a) = 1$*, tem-seque* $a^{p-1} \equiv 1 \bmod p$*, para todo a* $\in \mathbb{Z}$*. Além disso, vale* $a^p \equiv a \bmod p$.

Demonstração via Teorema de Lagrange. Se $a = 0$, tem-se o resultado. Caso $a \neq 0$,tem-se que $a \bmod p \in \mathbb{Z}_p^{\times} = ({}_p\backslash\{0\}, \cdot) = (\{1, \ldots, p-1\}, \cdot)$. Seja H o subgrupo de $\mathbb{Z}_p^{\times}$ gerado por a mod$p$, então a ordem do subgrupo Hé a ordem do elemento a mod$p$. Pelo Teorema de Lagrange, $|H| \mid |\mathbb{Z}_p^{\times}|$, e como $|\mathbb{Z}_p^{\times}| = p - 1$, pode-se escrever $p-1=|H|m$para algum $m \in \mathbb{N}$. Daí, vem $a^{p-1} \bmod p = a^{|H|m} \bmod p = 1^m \bmod p = 1 \bmod p$, logo $a^{p-1} \equiv 1 \bmod p$, e multiplicando ambos lados por a, tem-se$a^p \equiv a \bmod p$, o que prova o resultado.

4.2 Criptografia RSA

A criptografia RSA é uma criptografia de chave pública e privada, ou seja, possui uma chave para codificação e outra para decodificação. Baseando-se na teoria dos números, a chave pública é de livre acesso, enquanto que a privada tem acesso restrito ao responsável por decodificar a mensagem.

Para o funcionamento da criptografia RSA, é necessário o produto de dois números primos $n = pq$. Também é importanteo valor de $\varphi(n) = (p-1)(q-1)$ e outros dois números inteiros e e d, sendo $e < \varphi(n)$, de modo que o máximo divisor comum (mdc) de $(e,\varphi(n))$ seja 1, então $d < \varphi(n)$ de forma que $1 = k\varphi(n)+de$. Dessa maneira, os termos (e,n) e (d,n) formam, respectivamente, as chaves de codificação e decodificação.

Em vista disso, antes de realizar a codificação é necessário transformar as letras em números, definindo o espaço entre duas palavras como 99. Nesse sentido, a Tabela 1 apresenta o alfabeto transformado em números, utilizada para iniciar a pré-codificação.

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

Tabela 1: Alfabeto pré-codificado

Com isso, torna-se possível separar os números pré-codificados em blocos, que devem ter valores numéricos inferiores a n^2, e pode-se prosseguir com a codificação da mensagem.

Como exemplo,será codificada a mensagem ”Resumo da JIC”. Considerando $p = 17$ e $q = 29$, então $n = 493$. Desse modo, com base na Tabela 1, a mensagem pré-codificada torna-se:

$$271428302224991310991918 12$$

Separando a mensagem em blocos obtém-se:

$$271 - 428 - 302 - 224 - 99 - 13 - 10 - 99 - 191 - 81 - 2$$

Para a codificação é necessário que $C(b)$ = resto da divisão de b^3 por n, ou seja, $C(b) = b^3 mod\, n$. Deste modo, os blocos tornam-se:

$$C(271) = (271^3) mod 493 = 19902511 mod\ 493 = 101$$

Seguindo-se com o mesmo processo, obtém-se todos os códigos dos blocos, formando a mensagem codificada:

$$101 - 469 - 191 - 10 - 75 - 225 - 14 - 75 - 302 - 480 - 8.$$

Posteriormente, é possível realizar a decodificação da mensagem através da chave privada, ou seja, pelo valor de d, que neste caso é obtido através da equação $3d = 1[mod(p - 1)(q - 1)] = 1 mod(448)$. Dessa maneira, utiliza-se o par (n,d) para decodificar a mensagem por blocos, com $D(c)$ sendo a decodificação do bloco c, de modo que $D(c) = c^d mod\ n$.

Sendo $p = 5 mod\ 6$ e $q = 5 mod\ 6$, tem-se $p - 1 = 4 mod 6$ e $q - 1 = 4 mod\ 6$. Então,

$$(p - 1)(q - 1) mod 6 = 16 mod 6 = 4 mod 6 = -2 mod 6.$$

Como $(p-1)(q-1) = 6k - 2$, com k sendo um inteiro positivo, e $6k - 2 = n$, tem-se,

$$n = 6k - 2 \Rightarrow n - 1 = 6k - 3 \Rightarrow n - 1 = 3(2k - 1) \Rightarrow n = 3(2k - 1) + 1,$$

e portanto,

$$[3(2k - 1) + 1] \equiv n mod\ n \Rightarrow 3(2k - 1) + 1 \equiv 0 mod\ n \Rightarrow 3(1 - 2k) \equiv 1 mod\ n,$$

de modo que $d = 1 - 2k$, com k pertencendo aos inteiros positivos. Como d é negativo, deve-se utilizar o resíduo para obter-se $d = 4k - 1$. Sabendo que $p = 17$ e $q = 29$ obtém-se,

$$(p - 1)(q - 1) = 16 \cdot 28 = 448 = 6 \cdot 75 - 2.$$

Dessa forma, como $k = 75$ e $d = 4k - 1$, tem-se que $d = 299$. Então, tendo em vista que $D(a) = a^d mod\ n$, incia-se a decodificação da mensagem:

$$101 - 469 - 191 - 10 - 75 - 225 - 14 - 75 - 302 - 480 - 8$$

$$D(101) = 101^{299} mod\ 493 = 271$$

Prosseguindo-se com este processo para os demais códigos, é possível retornar aos blocos pré-codificados, são eles: $271-428-302-224-99-13-10-99-191-81-2$. Em seguida, ao abrir os blocos, obtém-se a mensagem pré-codificada:

271428302224991310991918l2. Finalmente, aplicando os valores da Tabela 1, obtém-se a mensagem: ”RESUMO DA JIC”.

5 Conclusão

O funcionamento da criptografia RSA é dado através do sistema de chave pública e privada, respectivamente (e,n) e (d,n), onde n é formado pelo produto entre p e q. Na exemplificação abordada, os valores de p e q foram escolhidos de modo que a decodificação fosse realizada de maneira simples, para fins de demonstração.

Contudo, a segurança da criptografia baseia-se na dificuldade de encontrar os valores de p e q, uma vez que, esses valores são de conhecimento apenas do portador da chave privada e devem ser descobertos por quem deseja quebrar a criptografia. Desse modo, usualmente, os valores criados para p e q são da ordem de 60 algarismos. É neste processo que encontra-se o pequeno Teorema de Fermat, o qual é utilizado para filtrar os números primos e excluir os demais, simplificando assim a fatoração de n e, portanto, a decodificação. Nesse sentido, o pequeno Teorema de Fermat auxilia na decodificação da criptografia, que ainda assim é muito complexo.

Referências

AUGUSTO, Paulo Roberto Peloso. **Elgar: the enigma of the variation.** *Per Musi*, [S.L], n. 35, p. 147-178, dezembro, 2016.

SAMS. Eric. **The Schumann Ciphers.** *The musical Times,*[S.L], p. 392-400, maio, 1966.

CRANS, Alissa S.; FIORE, Thomas M.; SATYENDRA, Ramon. **Musical Actions of Dihedral Groups**. *The American Mathematical Monthly*, [S.L.], v. 116, n. 6, p. 479-495, junho 2009.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA**. Rio de Janeiro. 2ªed. Rio de Janeiro:IMPA, 2005. 226 p.

GARCIA, Arnaldo; LEQUAIN, Yves. **Elementos de Álgebra**. 4ªed. Rio de Janeiro:IMPA, 2006.

Palavras-chave: Criptografia, Pequeno Teorema de Fermat, Teoria de grupos.

Nº de Registro no sistema Prisma: PES-2020-0073

Financiamento: Fundação Araucária