Universidade Federal de São Paulo

Instituto de Ciência e Tecnologia

Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

Explorando Códigos Corretores de Erros e Criptografia como Ferramentas Didáticas no Ensino Básico

Gilvania Carla Busatta

Orientadora: Profª. Drª. Grasiele Cristiane Jorge

São José dos Campos
19 de junho de 2024

PROFMAT

Título: *Explorando Códigos Corretores de Erros e Criptografia como Ferramentas Didáticas no Ensino Básico*

Dissertação apresentada ao Instituto de Ciência e Tecnologia da UNIFESP, campus São José dos Campos/SP, como parte dos requisitos exigidos para a obtenção do título de Mestre pelo Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT.

São José dos Campos
19 de junho de 2024

Busatta, Gilvania Carla

Explorando Códigos Corretores de Erros e Criptografia como Ferramentas Didáticas no Ensino Básico, Gilvania Carla Busatta – São José dos Campos, 2024.

ix, 109f.

Dissertação (Mestrado) – Universidade Federal de São Paulo. Instituto de Ciência e Tecnologia. Programa de Pós-Graduação em Matemática em Rede Nacional (PROFMAT).

Exploring Error-Correcting Codes and Cryptography as Didactic Tools in Elementary Education

1. Códigos. 2. Criptografia. 3. Dígitos Verificadores. 4. Códigos Corretores de Erros. 5. Código de Hamming.

UNIVERSIDADE FEDERAL DE SÃO PAULO

INSTITUTO DE CIÊNCIA E TECNOLOGIA

Mestrado Profissional em Matemática em Rede Nacional
PROFMAT

Chefe de departamento:

Prof. Dr. Marcelo Cristino Gama

Coordenadora do Programa de Pós-Graduação:

Profª. Drª. Grasiele Cristiane Jorge

Gilvania Carla Busatta

Explorando Códigos Corretores de Erros e Criptografia como Ferramentas Didáticas no Ensino Básico

Presidente da banca: Prof[a]. Dr[a]. Grasiele Cristiane Jorge

Banca examinadora:

Prof[a]. Dr[a]. Fernanda de Andrade Pereira

Prof[a]. Dr[a]. Mirela Vanina de Mello

Prof[a]. Dr[a]. Sara Díaz Cardell

Data da Defesa: 19 de Junho de 2024

"Não é apenas a questão, mas a maneira como você tenta resolvê-la."
Maryam Mirzakhani

AGRADECIMENTOS

Começo agradecendo a Deus, que sempre me deu força e saúde para realizar o PROFMAT. Sou profundamente grata ao meu marido, Jacyr, pelo apoio ao longo dos dois anos, incentivando-me, acompanhando-me até São José dos Campos, compreendendo minhas ausências durante este período de estudos e por nunca ter me deixado desistir. Sou muito grata à minha orientadora, Profª. Drª. Grasiele Cristiane Jorge, por sua paciência, apoio, incentivo e ensinamentos. Agradeço também aos professores do PROFMAT pelos seus ensinamentos e aos meus colegas de curso. Por fim, expresso minha gratidão a todos que, de alguma maneira, direta ou indiretamente, me incentivaram e apoiaram durante essa jornada.

RESUMO

A sociedade moderna está cada vez mais dependente da comunicação segura de dados. Nesta dissertação de mestrado, investigamos alguns tipos de códigos detectores e corretores de erros e alguns sistemas criptográficos. Inicialmente, exploramos a Cifra de César, depois passamos para cifras de substituição simples e para o criptossistema RSA. Em seguida, estudamos dígitos verificadores, cuja finalidade não é corrigir erros mas verificar se os dados inseridos ou transmitidos estão corretos. Para finalizar a parte teórica, estudamos códigos corretores de erros, que são sistemas projetados para identificar e corrigir uma determinada quantidade de erros que possam ocorrer na transmissão ou na leitura de informações. Nosso foco foi no estudo de códigos lineares em geral, e, em particular, nos códigos de Hamming. Após uma abordagem teórica para ampliar o conhecimento e fornecer uma base sólida sobre a temática, construímos um *e-book* para alunos do Ensino Fundamental II envolvendo alguns dos conceitos abordados. Utilizar criptografia e códigos no ensino de Matemática como temas geradores pode estimular o interesse dos estudantes, promover o desenvolvimento de habilidades cognitivas e práticas, e estabelecer uma conexão mais significativa entre a disciplina, a interdisciplinaridade e a realidade. Para fechar o trabalho é feito um relato de experiência de duas atividades do *e-book* que foram trabalhadas em sala de aula.

Palavras-chave: 1. Códigos. 2. Criptografia. 3. Dígitos Verificadores. 4. Códigos Corretores de Erros. 5. Código de Hamming.

A B S T R A C T

Modern society is increasingly dependent on secure data communication. In this master's dissertation, we investigate some types of error-detecting and error-correcting codes, as well as some cryptographic systems. Initially, we explore the Caesar cipher, then move on to simple substitution ciphers and the RSA cryptosystem. Next, we study check digits, whose purpose is not to correct errors but to verify whether the inputted or transmitted data is correct. To conclude the theoretical part, we study error-correcting codes, which are systems designed to identify and correct a certain amount of errors that may occur in the transmission or reading of information. Our focus was on the study of linear codes in general, and particularly on Hamming codes. After a theoretical approach to broaden understanding and provide a solid foundation on the topic, we developed an e-book for middle school students incorporating some of the concepts discussed. Using cryptography and codes in teaching Mathematics as generative themes can stimulate students' interest, promote the development of cognitive and practical skills, and establish a more meaningful connection between the subject, interdisciplinary aspects, and reality. To conclude the work, we provide an account of the experience of two activities from the e-book that were conducted in the classroom.

Keywords: 1. Codes. 2. Cryptography. 3. Check Digits. 4. Error Correcting Codes. 5. Hamming Code.

S U M Á R I O

INTRODUÇÃO

Os códigos corretores de erros foram desenvolvidos com o propósito de identificar e corrigir erros que podem ocorrer durante a transmissão ou o armazenamento de informações. A teoria dos códigos corretores de erros propriamente dita teve início na década de 1940 com os trabalhos de Richard W. Hamming [9], Marcel J. E. Golay [8] e Claude E. Shannon [24]. Seus trabalhos pioneiros estabeleceram as bases matemáticas para o desenvolvimento de códigos capazes de detectar e, em alguns casos, corrigir erros, proporcionando uma comunicação mais eficaz em meios sujeitos a interferências. Ao longo das décadas seguintes, os códigos corretores de erros evoluíram significativamente, impulsionados pelos avanços da computação, e hoje desempenham um papel essencial em uma ampla gama de aplicações.

A criptografia, por sua vez, tem uma história fascinante que remonta a milênios atrás, quando civilizações antigas buscavam maneiras de proteger suas comunicações. Os primeiros registros de técnicas criptográficas datam de civilizações como o Egito Antigo e o Império Romano. Ao longo dos séculos, a criptografia evoluiu significativamente, passando por diversas transformações, desde métodos simples de substituição de letras até algoritmos complexos baseados em matemática avançada. Como Simon Sigh destacou no seu livro,"O Livro dos Códigos" [25, p.12]:

> "A batalha contínua entre os criadores e os decifradores de códigos inspirou uma série de notáveis descobertas científicas. Os codificadores têm buscado sempre criar códigos mais fortes, para defender as comunicações, enquanto os decifradores inventam sempre métodos mais poderosos para atacá-los."

Durante guerras e períodos de conflito, a criptografia desempenhou um papel vital na comunicação militar e no compartilhamento seguro de informações entre aliados. Hoje, a criptografia é uma parte fundamental da infraestrutura da internet e está presente em diversas atividades cotidianas, desde o envio de mensagens pelo *WhatsApp*, transações bancárias e compras *online*.

Nesta dissertação, serão explorados alguns métodos criptográficos e alguns tipos de códigos corretores de erros com o objetivo de oferecer uma base sólida para o desenvolvimento de atividades em sala de aula com alunos de Ensino Básico, promovendo uma aprendizagem mais engajadora e prática. Como proposta didática, será apresentado um *e-book* visando tornar alguns dos conceitos abordados acessíveis e interessantes para os alunos do Ensino Fundamental II, estimulando assim o interesse e a compreensão desses assuntos essenciais no contexto tecnológico atual.

A dissertação está dividida em 8 capítulos e dois apêndices, descritos a seguir.

No Capítulo 1, revisamos alguns conceitos básicos de aritmética dos restos, classes residuais, Teorema de Euler e Teorema de Fermat, que serão utilizados nos demais capítulos.

No Capítulo 2, abordamos alguns sistemas criptográficos. Iniciamos o capítulo explorando a Cifra de César, depois estudamos as Cifras de Substituição Simples, que são vulneráveis à análise da frequência das letras no idioma, e terminamos com o RSA, que é um dos sistemas criptográficos mais utilizados atualmente, porém conta com uma estrutura matemática mais avançada.

No Capítulo 3, apresentamos alguns exemplos de códigos detectores de erros, a saber, o código de barras, o ISBN e o registro geral (RG). Esses códigos possuem a finalidade de verificar se os dados digitados estão corretos.

Nos Capítulos 4, 5 e 6, estudamos códigos corretores de erro. Em particular, no Capítulo 4, introduzimos a teoria de códigos corretores de erros e apresentamos a métrica de Hamming, que é a métrica mais utilizada neste contexto. Depois, no Capítulo 5, restringimos nosso estudo aos códigos lineares, que possuem uma estrutura algébrica associada. Para apresentar um exemplo de uma família de códigos lineares com um algoritmo eficaz de decodificação, no Capítulo 6, focamos em códigos de Hamming binários.

O Capítulo 7 é dedicado à apresentação da proposta didática, onde foi desenvolvido um *e-book* em quadrinhos para o Ensino Fundamental II. Neste *e-book*, trabalhamos com conceitos de criptografia e códigos no ensino de Matemática como temas geradores para estimular o interesse dos estudantes. Ao longo da narrativa, são propostas atividades e desafios. A escolha dos nomes das personagens principais é uma homenagem a mulheres importantes para a Matemática e permite que os alunos entrem em contato desde cedo com uma ciência mais diversa. O *e-book* foi desenvolvido na plataforma Canva, com imagens geradas por uma plataforma de inteligência artificial. Para finalizar a dissertação, no Capítulo 8, é apresentado o relato da aplicação de duas atividades do *e-book* em sala de aula.

O *e-book* é apresentado por completo no Apêndice A. No Apêndice B, inserimos algumas imagens para auxiliar na aplicação de uma das atividades propostas.

1

ARITMÉTICA MODULAR

A aritmética modular não é só fascinante do ponto de vista teórico, mas também é uma ferramenta poderosa para aplicações, como em criptografia e em códigos corretores de erros. Neste capítulo, exploraremos os conceitos fundamentais de congruência modular e os teoremas de Euler e Fermat. O matemático suíço Euler é frequentemente considerado como pioneiro nesse assunto, explorando a ideia de congruência módulo um número natural n em torno de 1750. No entanto, foi Carl Friedrich Gauss quem desenvolveu uma abordagem mais moderna da aritmética modular em seu livro "Disquisitiones Arithmeticae", publicado em 1801.

Assumimos que o leitor esteja familiarizado com o conceito de divisibilidade nos inteiros, números primos e máximo divisor comum. Para um estudo sobre estes tópicos, sugerimos [10, 11].

1.1 CONGRUÊNCIAS

Nesta seção apresentaremos algumas propriedades elementares de congruências.

Definição 1.1. *[10, p.192] Seja m um número natural. Dois números inteiros a e b são ditos congruentes módulo m se os restos da divisão euclidiana de a e b por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se:*

$$a \equiv b \,(mod\, m).$$

Caso contrário, diz-se que a e b são incongruentes módulo m e escreve-se:

$$a \not\equiv b \,(mod\, m).$$

Exemplo 1.2. *Temos que $26 \equiv 17 \,(mod\, 3)$, pois ambos têm resto 2 quando divididos por 3. Já $17 \not\equiv 35 \,(mod\, 4)$, pois 17 tem resto 1 quando dividido por 4 e 35 tem resto 3 quando dividido por 4.*

Observação 1.3. *[10, p.192] O resto da divisão de um número inteiro m por 1 será sempre zero. Logo, todos os inteiros são congruentes módulo 1. Como este caso não é interessante para o restante do trabalho, consideraremos sempre $m > 1$.*

No que segue, dados $a, b \in \mathbb{Z}$, usaremos a notação $a|b$ para indicar que a divide b nos inteiros, ou seja, existe $k \in \mathbb{Z}$ tal que $b = ak$.

Proposição 1.4. *[10, p.193] Se $a, b, m \in \mathbb{Z}$, com $m > 1$, temos que $a \equiv b \,(mod\, m)$ se, e somente se, $m|(b-a)$.*

Demonstração. ($\Rightarrow$) Pelo algoritmo da divisão euclidiana, existem inteiros q_1, q_2, r_1, r_2 tais que $a = mq_1 + r_1$, com $0 \leq r_1 < m$ e $b = mq_2 + r_2$, com $0 \leq r_2 < m$. Agora

$$b - a = mq_2 + r_2 - (mq_1 + r_1) = (q_2 - q_1)m + (r_2 - r_1).$$

Se $a \equiv b \,(mod\, m)$, então a e b têm restos iguais quando divididos por m, isto é, $r_1 = r_2$. Então, $b - a = (q_2 - q_1)m$, ou seja, $m|(b-a)$.
($\Leftarrow$) Se $m|(b-a)$, então existe $k \in \mathbb{Z}$ tal que $b - a = km$. Dividindo b por m, existem q, r inteiros tais que $b = qm + r$ com $0 \leq r < m$. Desta forma, $b - a = (qm + r) - a = km$. Logo, $a = qm + r - km$, ou seja, $a = (q-k)m + r$, com $0 \leq r < m$. Portanto, a tem resto r quando dividido por m. Logo, a e b têm restos iguais na divisão por m, o que implica $a \equiv b \,(mod\, m)$. □

Proposição 1.5. *[10, p.192] Seja $m \in \mathbb{Z}$ com $m > 1$. Para todos $a, b, c \in \mathbb{Z}$, tem-se que:*

(i) $a \equiv a \,(mod\, m)$.

(ii) Se $a \equiv b \,(mod\, m)$, *então* $b \equiv a \,(mod\, m)$.

(iii) Se $a \equiv b \,(mod\, m)$ *e* $b \equiv c \,(mod\, m)$, *então* $a \equiv c \,(mod\, m)$.

Demonstração. Vamos demonstrar cada item.

(i) Como $m|0$, então $m|(a-a)$. Portanto, $a \equiv a \,(mod\, m)$.

(ii) Temos que $a \equiv b \,(mod\, m)$, então $m|(a-b)$, assim $m|-(a-b)$, ou seja, $m|(b-a)$ também. Portanto, $b \equiv a \,(mod\, m)$.

(iii) Se $a \equiv b \,(mod\, m)$ e $b \equiv c \,(mod\, m)$, temos, respectivamente, que $a - b = mq_1$ e $b - c = mq_2$ para algum q_1 e algum q_2 inteiros. Fazendo a soma dessas igualdades obtemos, $a - c = mq_1 + mq_2 = (q_1 + q_2)m$, ou seja, $m|(a-c)$. Portanto, $a \equiv c \,(mod\, m)$.

□

Proposição 1.6. *[10, p.194] Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$.*

(i) Se $a \equiv b \,(mod\, m)$ *e* $c \equiv d \,(mod\, m)$, *então:*

$$a + c \equiv b + d \,(mod\, m).$$

(ii) Se $a \equiv b\,(mod\,m)$ *e* $c \equiv d\,(mod\,m)$*, então:*

$$ac \equiv bd\,(mod\,m).$$

Demonstração. Vamos demonstrar cada item.

(i) Se $a \equiv b\,(mod\,m)$ e $c \equiv d\,(mod\,m)$, temos, respectivamente, que $a - b = mq_1$ e $c - d = mq_2$ para algum q_1 e algum q_2 inteiros. Fazendo a soma dessas igualdades membro a membro, obtemos $(a-b)+(c-d) = mq_1 + mq_2 = (q_1+q_2)m$, ou seja, $m|((a+c)-(b+d))$. Portanto, $a + c \equiv b + d\,(mod\,m)$.

(ii) Como $a = b + mq_1$ e $c = d + mq_2$, fazendo a multiplicação dessas igualdades membro a membro, obtemos $ac = (b+mq_1)(d+mq_2)$. Aplicando a propriedade distributiva no segundo membro, obtemos $ac = bd + bmq_2 + dmq_1 + m^2q_1q_2$, ou seja, $ac - bd = (bq_2 + dq_1 + mq_1q_2)m$, assim $m|(ac-bd)$. Portanto, $ac \equiv bd\,(mod\,m)$.

□

Proposição 1.7. *[10, p.196] Sejam* $a, b, c, d, m \in \mathbb{Z}$*, com* $m > 1$*. Tem-se que:*

$$a + c \equiv b + c\,(mod\,m) \iff a \equiv b\,(mod\,m).$$

Demonstração. Se $a \equiv b\,(mod\,m)$, segue imediatamente da Proposição 1.5 (i) que $a + c \equiv b + c\,(mod\,m)$, pois $c \equiv c\,(mod\,m)$. Reciprocamente, se $a + c \equiv b + c\,(mod\,m)$, então m divide $(b+c)-(a+c)$, o que implica que m divide $b + c - a - c$, isto é, $m|b-a$ e, consequentemente, $a \equiv b\,(mod\,m)$. □

Proposição 1.8. *[10, p.194] Para todos* $n \in \mathbb{N}$ *e* $a, b \in \mathbb{Z}$*, se* $a \equiv b\,(mod\,m)$*, então* $a^n \equiv b^n\,(mod\,m)$*.*

Demonstração. Vamos demonstrar por indução sobre n.
Caso base: Para $n = 1$, temos que $a^1 = a$ e $b^1 = b$. Logo, $a^1 \equiv b^1\,(mod\,m)$. Portanto, o resultado é verdadeiro para $n = 1$.
Passo indutivo: Vamos supor que a congruência é verdadeira para algum $n \in \mathbb{N}$, isto é, $a^n \equiv b^n\,(mod\,m)$ e vamos provar que ela também é verdadeira para $n + 1$, ou seja, $a^{n+1} \equiv b^{n+1}\,(mod\,m)$.

Temos que $a^n \equiv b^n\,(mod\,m)$ e $a \equiv b\,(mod\,m)$. Aplicando o item (ii) da Proposição 1.6, obtemos: $a^{n+1} \equiv b^{n+1}\,(mod\,m)$.

Portanto, a congruência $a^n \equiv b^n\,(mod\,m)$ é verdadeira para todo $n \in \mathbb{N}$. □

Exemplo 1.9. *Vamos encontrar o resto da divisão de* 5^{30} *por* 127.

Temos que $5^3 = 125$, *logo* $5^3 \equiv -2\,(mod\,127)$. *Pela Proposição 1.8, segue que* $(5^3)^{10} \equiv (-2)^{10}\,(mod\,127)$. *Agora,* $(-2)^{10} = 1024$. *Assim,* $5^{30} \equiv 8\,(mod\,127)$.

Portanto, o resto da divisão de 5^{30} *por* 127 *é* 8.

Definição 1.10. *[10, p.96] Dois números inteiros a e b serão ditos primos entre si, ou coprimos, se* $mdc(a,b) = 1$, *ou seja, se o único divisor positivo comum a ambos é* 1.

A seguir, é apresentado um resultado associado ao cancelamento multiplicativo.

Proposição 1.11. *[10, p.196] Sejam* $a, b, c, m \in \mathbb{Z}$, *com* $m > 1$. *Se* $ac \equiv bc\,(mod\,m)$, *então* $a \equiv b\,\left(mod\,\frac{m}{mdc(c,m)}\right)$.

Demonstração. Como $ac \equiv bc\,(mod\,m)$, então existe $k \in \mathbb{Z}$, tal que $ac - bc = km$.

Dessa igualdade, segue que

$$(a-b)\frac{c}{\text{mdc}(c,m)} = k\frac{m}{\text{mdc}(c,m)}.$$

Vale notar que $\frac{c}{\text{mdc}(c,m)} \in \mathbb{Z}$ e $\frac{m}{\text{mdc}(c,m)} \in \mathbb{Z}$. Desta forma,

$$\frac{m}{mdc(c,m)} | (a-b)\frac{c}{mdc(c,m)}.$$

Como $\frac{c}{mdc(c,m)}$ e $\frac{m}{mdc(c,m)}$ são coprimos, ou seja, $mdc\left(\frac{c}{mdc(c,m)}, \frac{m}{mdc(c,m)}\right) = 1$, então $\frac{m}{mdc(c,m)} | (a-b)$, o que é equivalente a $a \equiv b\,\left(mod\,\frac{m}{\text{mdc}(c,m)}\right)$. □

Corolário 1.12. *[10, p.197] Sejam* $a, b, c, m \in \mathbb{Z}$, *com* $m > 1$ *e* $mdc(c,m) = 1$. *Temos que* $ac \equiv bc\,(mod\,m)$ *se, e somente se,* $a \equiv b\,(mod\,m)$.

Demonstração. Segue direto da Proposição 1.11, pois $\text{mdc}(c,m) = 1$. □

1.2 CLASSES RESIDUAIS

As congruências módulo um inteiro $m > 1$ permitem definir novas aritméticas, encontrando aplicações em áreas como códigos corretores de erros e criptografia, conforme veremos ao longo da dissertação.

Definição 1.13. *[10, p.263] Seja a um número inteiro. Representaremos por* $\overline{a}$ *o conjunto*

$$\overline{a} = \{x \in \mathbb{Z}; x \equiv a\,(mod\,m)\}.$$

Este conjunto é chamado de classe residual módulo m do elemento a.

Proposição 1.14. *[10, p.264] Dados $a, b \in \mathbb{Z}$, temos que $\overline{a} = \overline{b}$ se, e somente se, $a \equiv b \,(mod\, m)$.*

Demonstração. Se $\overline{a} = \overline{b}$, então $b \in \overline{a}$, pois $b \in \overline{b}$. Com isso, $b \equiv a \,(mod\, m)$. Agora, se $b \equiv a \,(mod\, m)$, então $b \in \overline{a}$. Logo, todo elemento congruente a b também pertence a $\overline{a}$. De forma similar, todo elemento congruente a a pertence a $\overline{b}$. Portanto, $\overline{a} = \overline{b}$. □

Proposição 1.15. *[10, p.264] Sejam a e b inteiros. Se $\overline{a} \neq \overline{b}$, então $\overline{a} \cap \overline{b} = \emptyset$.*

Demonstração. Suponha que existe um inteiro c tal que $c \in \overline{a}$ e $c \in \overline{b}$. Então, $c \equiv a \,(mod\, m)$ e $c \equiv b \,(mod\, m)$. Portanto, temos que $a \equiv b \,(mod\, m)$, o que contradiz a hipótese de que $\overline{a} \neq \overline{b}$. □

Definição 1.16. *O conjunto de todas as classes residuais modulo m será representado por $\mathbb{Z}_m$, ou seja,*

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}.$$

Exemplo 1.17. *Seja $m = 5$. Então:*

$$\overline{0} = \{5k; k \in \mathbb{Z}\},$$

$$\overline{1} = \{5k + 1; k \in \mathbb{Z}\},$$

$$\overline{2} = \{5k + 2; k \in \mathbb{Z}\},$$

$$\overline{3} = \{5k + 3; k \in \mathbb{Z}\} \text{ e}$$

$$\overline{4} = \{5k + 4; k \in \mathbb{Z}\}.$$

Temos que:

$$a \in \begin{cases} \overline{0}, & \text{se } a \text{ é múltiplo de } 5. \\ \overline{1}, & \text{se } a \text{ tem resto } 1 \text{ quando dividido por } 5. \\ \overline{2}, & \text{se } a \text{ tem resto } 2 \text{ quando dividido por } 5. \\ \overline{3}, & \text{se } a \text{ tem resto } 3 \text{ quando dividido por } 5. \\ \overline{4}, & \text{se } a \text{ tem resto } 4 \text{ quando dividido por } 5. \end{cases}$$

Portanto, $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

No que segue, vamos definir as operações da soma e do produto em $\mathbb{Z}_{\mathrm{m}}$.

Definição 1.18. *[10, p.265] Dados $\overline{a}$ e $\overline{b} \in \mathbb{Z}_m$, definimos as seguintes operações:*

$$\overline{a} + \overline{b} = \overline{a + b}$$

$$\overline{a} \cdot \overline{b} = \overline{ab}.$$

Exemplo 1.19. *Vamos fazer as operações de adição e multiplicação em $\mathbb{Z}_5$, onde temos as classes residuais $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}$.*

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Tabela 1: Tabela da adição em $\mathbb{Z}_5$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Tabela 2: Tabela da multiplicação em $\mathbb{Z}_5$

Proposição 1.20. *[10, p.206] Para todo $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$, valem as seguintes propriedades:*

A_1. Associatividade: $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$.

A_2. Comutatividade: $\overline{a} + \overline{b} = \overline{b} + \overline{a}$.

A_3. Existência de zero: $\overline{a} + \overline{0} = \overline{a}$, para todo $a \in \mathbb{Z}_m$.

A_4. Existência de simétrico: $\overline{a} + (\overline{-a}) = \overline{0}$.

M_1. Associatividade: $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$.

M_2. Comutatividade: $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$.

M_3. Existência de unidade: $\overline{a} \cdot \overline{1} = \overline{a}$.

AM. Distributividade: $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$.

Demonstração. Dados $\overline{a}, \overline{b}, \overline{c}, \in \mathbb{Z}_m$, temos:

A$_1$. $(\overline{a} + \overline{b}) + \overline{c} = \overline{a+b} + \overline{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a} + \overline{b+c} = \overline{a} + (\overline{b} + \overline{c})$.

A$_2$. $\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}$.

A$_3$. $\overline{a} + \overline{0} = \overline{a+0} = \overline{a}$.

A$_4$. $\overline{a} + (\overline{-a}) = \overline{a+(-a)} = \overline{0}$.

M$_1$. $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot (\overline{bc}) = \overline{a(bc)} = \overline{(ab)c} = (\overline{ab}) \cdot \overline{c} = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$.

M$_2$. $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \cdot \overline{a}$.

M$_3$. $\overline{1} \cdot \overline{a} = \overline{1a} = \overline{a}$, $\forall\, \overline{a} \in \mathbb{Z}_m$.

AM. $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b+c} = \overline{a(b+c)} = \overline{ab+ac} = \overline{ab} + \overline{ac} = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$.

□

Definição 1.21. *[10, p.206] O conjunto $\mathbb{Z}_m$ com as operações de adição e multiplicação e as propriedades descritas na Proposição 1.20 é chamado de anel das classes residuais módulo m, ou anel dos inteiros módulo m.*

Definição 1.22. *[10, p.207] Um elemento $\overline{a} \in \mathbb{Z}_m$ será dito inversível quando existir $\overline{b} \in \mathbb{Z}_m$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$. Nesse caso, diremos que $\overline{b}$ é o inverso $\overline{a}$.*

Exemplo 1.23. *A Tabela 3 contém a multiplicação de $\mathbb{Z}_2$. Neste caso, temos que apenas o $\overline{1}$ é inversível.*

Tabela 3: Tabela da multiplicação em $\mathbb{Z}_2$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Exemplo 1.24. *A Tabela 4 contém a multiplicação de $\mathbb{Z}_3$. Neste caso, temos que os elementos $\overline{1}$ e $\overline{2}$ são inversíveis.*

Tabela 4: Tabela da multiplicação em $\mathbb{Z}_3$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

As Proposições 1.25 e 1.26 a seguir serão utilizadas na demonstração da Proposição 1.27, que lista quem são os elementos inversíveis de $\mathbb{Z}_m$.

Proposição 1.25. *[23, 5]* **(Identidade de Bézout)** *Dados dois números inteiros a e b, quaisquer, não ambos nulos, existem dois inteiros n e m, tais que:*

$$mdc(a,b) = an + bm.$$

Demonstração. Consideremos o conjunto $A = \{na + mb;\ m, n \in \mathbb{Z}\}$. Este conjunto inclui números positivos, negativos e o zero. Suponhamos que n_0 e m_0 são inteiros tais que $c = n_0a + m_0b$ é o menor inteiro positivo no conjunto. Vamos demonstrar que c é o máximo divisor comum de a e b. Primeiro iremos mostrar que c divide a e b. Suponha que c não divide a. Pelo algoritmo da divisão euclidiana, existem inteiros q e r tais que: $a = qc + r$ com

$0 < r < c$. Então, $r = a - qc$. Como $c = n_0a + m_0b$, então $r = a - qc = a - q(n_0a + m_0b) = a - qn_0a - qm_0b = (1 - qn_0)a + (-qm_0)b$. Isso mostra que $r \in A$, pois $(1 - qn_0)$ e $(-qm_0)$ são inteiros. Portanto, temos uma contradição, pois $0 < r < c$ e c é o menor elemento positivo de A. Isso implica que c divide a. De maneira similar, mostramos que c divide b. Seja agora d o máximo divisor comum de a e b. Então, existem $k_1, k_2 \in \mathbb{Z}$ tais que: $a = k_1d$ e $b = k_2d$. Portanto, $c = n_0a + m_0b = n_0(k_1d) + m_0(k_2d) = (n_0k_1 + m_0k_2)d$, o que implica que d divide c. Como d divide c e ambos d e c são positivos, temos que $d \leq c$. Sabendo que d é o maior divisor comum de a e b, segue que $c \leq d$. Assim, concluímos $d = c$, ou seja, $d = c = n_0a + m_0b$. □

Proposição 1.26. *[10, p.96] Dados dois números inteiros a e b são primos entre si se, e somente se, existem números inteiros m e n tais que $na + mb = 1$.*

Demonstração. Suponha que a e b são números primos entre si. Então, $mdc(a, b) = 1$. Pela Proposição 1.25, sabemos que existem dois números inteiros m e n tais que $na + mb = mdc(a, b) = 1$. Reciprocamente, suponha que existam dois números inteiros m e n tais que $na + mb = 1$. Se d é o máximo divisor comum de a e b, temos que d divide $na + mb$. Logo, d divide 1 e, portanto, $d = 1$. □

Proposição 1.27. *[10, p.269] Um elemento $\overline{a} \in \mathbb{Z}_m$ é inversível se, e somente se, $mdc(a, m) = 1$.*

Demonstração. Suponha que $\overline{a} \in \mathbb{Z}_m$ seja inversível. Desta forma, existe $\overline{b} \in \mathbb{Z}_m$ de forma que $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{1}$. Mas, isto implica ab é congruente a 1 módulo m, ou seja, existe $t \in \mathbb{Z}$ tal que $ab - 1 = tm$. Mas, isso é equivalente a $ab - tm = 1$. Com isso, concluímos que $\text{mdc}(a, m) = 1$. Supondo agora que $\text{mdc}(a, m) = 1$, pela Proposição 1.25 e pela Proposição 1.26, existem $r, s \in \mathbb{Z}$ tais que $ar + ms = 1$. Logo, $ar - 1 = -sm$, o que implica que $ar \equiv 1 \,(mod\, m)$, ou seja, $\overline{ar} = \overline{1}$, isto é, $\overline{a} \cdot \overline{r} = \overline{1}$. Portanto, $\overline{a}$ é inversível módulo m. □

Exemplo 1.28. *Vamos construir a tabela da multiplicação do $\mathbb{Z}_7$.*

Tabela 5: Tabela da multiplicação em $\mathbb{Z}_7$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Em $\mathbb{Z}_7$, temos que apenas $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, $\overline{6}$ são inversíveis.

Definição 1.29. *[10, p.206] Um anel comutativo com unidade onde todo o elemento não nulo possui um inverso multiplicativo é chamado de corpo.*

Observação 1.30. *Pelas tabelas construídas, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$ e $\mathbb{Z}_7$ são corpos.*

Exemplo 1.31. *A Tabela 6 contém a multiplicação de $\mathbb{Z}_6$. Neste caso, os únicos elementos inversíveis são $\overline{1}$ e $\overline{5}$. Logo, $\mathbb{Z}_6$ não é um corpo.*

Tabela 6: Tabela da Multiplicação $\mathbb{Z}_6$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Proposição 1.32. *[10, p.269] Se m é primo, então $\mathbb{Z}_m$ é um corpo.*

Demonstração. Para provar isso, basta notar que, se $\overline{a} \in \mathbb{Z}_m$ com $\overline{a} \neq \overline{0}$, então $\text{mdc}(a, m) = 1$. Logo, $\overline{a}$ é inversível. □

1.3 TEOREMA DE EULER

Antes de provarmos o Teorema de Euler, vamos definir a função φ de Euler, um sistema completo de resíduos módulo m e um sistema reduzido de resíduos módulo m.

Definição 1.33. *[10, p.227] Um sistema completo de resíduos módulo m é um conjunto com m números inteiros, dois a dois incongruentes módulo m.*

Definição 1.34. *[10, p.227] A função φ, conhecida como a função Fi de Euler, é definida para cada $m \geq 1$ natural como*

$$\varphi(m) = \#\{i; 1 \leq i \leq m \text{ e } mdc(i, m) = 1\}.$$

Em outras palavras, $\varphi(m)$ representa a quantidade de números inteiros coprimos com m no intervalo de 1 a m.

Exemplo 1.35. *Vamos calcular $\varphi(m)$ para alguns valores de m.*

- $\varphi(1) = 1$, *pois* $mdc(1,1) = 1$.
- $\varphi(2) = 1$, *visto que* 2 *é coprimo somente com o* 1 *em* $\{1,2\}$.
- $\varphi(3) = 2$, *visto que* 3 *é coprimo somente com* 1 *e* 2 *em* $\{1,2,3\}$.
- $\varphi(4) = 2$, *visto que* 4 *é coprimo somente com* 1 *e* 3 *em* $\{1,2,3,4\}$.
- $\varphi(5) = 4$, *visto que* 5 *é coprimo somente com* $1,2,3,4$ *em* $\{1,2,3,4,5\}$.
- $\varphi(6) = 2$, *visto que* 6 *é coprimo somente com* 1 *e* 5 *em* $\{1,2,3,4,5,6\}$.
- $\varphi(7) = 6$, *visto que* 7 *é coprimo com* $1,2,3,4,5,6$ *em* $\{1,2,3,4,5,6,7\}$.
- $\varphi(8) = 4$, *visto que* 8 *é coprimo com* $1,3,5,7$ *em* $\{1,2,3,4,5,6,7,8\}$.

Proposição 1.36. *[4, p.32] Se* p *e* q *são números primos distintos então,* $\varphi(pq) = (p-1)(q-1)$.

Demonstração. Observamos que $\varphi(pq)$ representa a quantidade de inteiros positivos menores ou iguais a pq que são coprimos com pq. Para que um inteiro não seja coprimo com pq, ele deve ser múltiplo de p ou múltiplo de q, pois os únicos divisores primos de pq maiores do que 1 são p e q. A quantidade de múltiplos de p menores ou iguais a p é $\frac{pq}{p} = q$, e a quantidade de múltiplos de q menores ou iguais a q é $\frac{pq}{q} = p$. Entre os múltiplos de p e os múltiplos de q menores ou iguais a pq, o único elemento que se repete é pq.

Portanto, temos que $\varphi(pq)$ é igual ao total de inteiros positivos menores que pq menos a quantidade de múltiplos de p somados aos múltiplos de q, mais a quantidade da interseção dos múltiplos de p e q. Em termos matemáticos, isso é expresso como, $\varphi(pq) = pq - (p+q) + 1 = pq - p - q + 1 = (p-1)(q-1)$.

□

Exemplo 1.37. *Vamos calcular* $\varphi(34)$.

Observamos que $34 = 2 \cdot 17$. *Logo, pela Proposição 1.36, temos que:*

$$\varphi(34) = \varphi(2 \cdot 17) = (2-1)(17-1) = 16.$$

Portanto, $\varphi(34) = 16$.

Definição 1.38. *Um sistema reduzido de resíduos módulo* m *é um conjunto com* $\varphi(m)$ *elementos* $\{s_1, s_2, \ldots, s_{\varphi(m)}\}$ *satisfazendo* $s_i \not\equiv s_j \pmod m$, *se* $i \neq j$ *e* $mdc(s_i, m) = 1$.

Proposição 1.39. *[10, p.229] Seja* $\{s_1, s_2, \ldots, s_{\varphi(m)}\}$ *um sistema reduzido de resíduos módulo* m *e seja* $a \in \mathbb{Z}$ *coprimo com* m. *Então* $\{as_1, as_2, \ldots, as_{\varphi(m)}\}$ *também é um sistema reduzido de resíduos módulo* m.

Demonstração. Temos que, $\{as_1, as_2, \ldots, as_{\varphi(m)}\}$ tem $\varphi(m)$ elementos dois a dois incongruentes. De fato, se $as_i \equiv as_j \,(mod\, m)$, então $s_i \equiv s_j \,\left(mod \frac{m}{mdc(a,m)}\right)$. Mas, $mdc(a,m) = 1$, então $s_i \equiv s_j \,(mod\, m)$, ou seja, $i = j$, pois $\{s_1, s_2, \ldots, s_{\varphi(m)}\}$ só tem elementos dois a dois incongruentes. Agora, $\text{mdc}(as_i, m) = 1$, pois $\text{mdc}(a,m) = 1$ e $\text{mdc}(s_i, m) = 1$. Portanto, $\{as_1, as_2, \ldots, as_{\varphi(m)}\}$ é um sistema reduzido de resíduos módulo m. □

Teorema 1.40. *[10, p.229]* **(Teorema de Euler)**

Sejam $a, m \in \mathbb{Z}$ com $m > 1$ e $mdc(a,m) = 1$. Então,

$$a^{\varphi(m)} \equiv 1 \,(mod\, m).$$

Demonstração. Seja $\{s_1, s_2, \ldots, s_{\varphi(m)}\}$ um sistema reduzido de resíduos módulo m. Como o $\text{mdc}(a,m) = 1$, então $\{as_1, as_2, \ldots, as_{\varphi(m)}\}$ também é um sistema reduzido módulo m. Portanto,

$$as_1 \cdot as_2 \cdots as_{\varphi(m)} \equiv s_1 \cdot s_2 \cdots s_{\varphi(m)} \,(mod\, m),$$

ou seja,

$$a^{\varphi(m)}(s_1 \cdot s_2 \cdots s_{\varphi(m)}) \equiv s_1 \cdot s_2 \cdots s_{\varphi(m)} \,(mod\, m).$$

Como $\text{mdc}(s_1 \cdot s_2 \cdots s_{\varphi(m)}, m) = 1$, então $a^{\varphi(m)} \equiv 1 \,(mod\, m)$. □

Exemplo 1.41. *Vamos calcular o resto da divisão de 3^{100} por 34.*

Temos que $\varphi(34) = \varphi(2 \cdot 17) = (2-1)(17-1) = 16$. Como $mdc(3, 34) = 1$, pelo Teorema de Euler, $3^{16} \equiv 1 \,(mod\, 34)$. Mais ainda, $3^{100} = (3^{16})^6 \cdot 3^4 \equiv 1^6 \cdot 13 \,(mod\, 34)$, logo $3^{100} \equiv 13 \,(mod\, 34)$. Portanto, o resto é 13.

Teorema 1.42. *[10, p.230]* **(Pequeno Teorema de Fermat)**

Sejam $a \in \mathbb{Z}$ e p um número primo tais que $mdc(a,p) = 1$. Tem-se que

$$a^{p-1} \equiv 1 \,(mod\, p).$$

Demonstração. Como $m = p$ é primo, então $\varphi(p) = p - 1$. Pelo Teorema de Euler, temos que $a^{\varphi(m)} \equiv 1 \,(mod\, m)$. Logo, $a^{p-1} \equiv 1 \,(mod\, p)$. □

Exemplo 1.43. *Vamos encontrar o resto da divisão de 5^{200} por 11.*

Como $mdc(5, 11) = 1$, pelo Pequeno Teorema de Fermat, temos que $5^{10} \equiv 1 \,(mod\, 11)$. Mas $5^{200} = (5^{10})^{20} \equiv 1^{20} \,(mod\, 11)$, isto é, $5^{200} \equiv 1 \,(mod\, 11)$. Portanto, o resto é 1.

Teorema 1.44. *[10, p.230]* **(Teorema de Fermat)**

Dado um número primo p, tem-se que $a^p \equiv a \,(mod\, p)$, para todo $a \in \mathbb{Z}$.

Demonstração. Se $\text{mdc}(a,p) = 1$ o resultado segue do fato que $a^{p-1} \equiv 1\,(mod\,p)$ e multiplicando ambos os membros da congruência por a, isto é, $a^{p-1} \cdot a \equiv 1 \cdot a\,(mod\,p)$, tem-se $a^p \equiv a\,(mod\,p)$.

Agora, no caso em que $mdc(a,p) \neq 1$, segue que $p|a$ e consequentemente $p|a^p - a$, o que garante que, $a^p \equiv a\,(mod\,p)$. □

Exemplo 1.45. *Vamos encontrar o resto da divisão de de* 3^{14} *por* 7.

Temos, pelo Teorema de Fermat, que $3^7 \equiv 3\,(mod\,7)$ *e, então,* $3^{14} = (3^7)^2 \equiv 3^2\,(mod\,7)$, *isto é,* $3^{14} \equiv 2\,(mod\,7)$. *Portanto, o resto é* 2.

Teorema 1.46. *[10, p.232] Se* $n = p \cdot q$ *com* p *e* q *primos distintos, então para todos* $a, k \in \mathbb{Z}$ *temos*

$$a^{1+k\varphi(n)} \equiv a\,(mod\,n).$$

Demonstração. Vamos considerar alguns casos:

- Se $\text{mdc}(a,n) = 1$, então o resultado segue do Teorema de Euler, pois $a^{1+k\varphi(n)} \equiv a \cdot \left(a^{\varphi(n)}\right)^k \equiv a \cdot 1^k \equiv a\,(mod\,n)$.
- Se $\text{mdc}(a,n) = p$, então $\text{mdc}(a,q) = 1$ e $p|a$. Desta forma, pelo Pequeno Teorema de Fermat, $a^{q-1} \equiv 1\,(mod\,q)$. Logo, $a^{1+k\varphi(n)} \equiv a \cdot \left(a^{q-1}\right)^{k(p-1)} \equiv a \cdot 1^{k(p-1)} \equiv a\,(mod\,q)$. Portanto, q divide $a^{1+k\varphi(n)} - a$. Por outro lado, como $p|a$, então p divide $a^{1+k\varphi(n)} - a$. Uma vez que p e q são coprimos, $n = pq$ divide $a^{1+\varphi(n)} - a$. Portanto, $a^{1+k\varphi(n)} \equiv a\,(mod\,n)$.
- Se $\text{mdc}(a,n) = q$, a análise é similar.
- Se $\text{mdc}(a,n) = pq$, então pq divide a. Logo, pq divide $a^{1+k\varphi(n)} - a$.

□

2

CRIPTOGRAFIA

A criptografia é uma forma de transformar mensagens claras em mensagens ilegíveis para pessoas não autorizadas. Um marco importante da sua história é a Cifra de César, uma das técnicas mais antigas e simples de criptografia. Nela, cada letra do alfabeto é substituída por outra deslocada um certo número de posições à frente na sequência alfabética. Apesar de sua aparente simplicidade, essa técnica ilustra como ocultar informações por meio de transformações sistemáticas.

A partir da década de 1950, a criptografia passou por um renascimento impulsionado por avanços na matemática, ciência da computação e engenharia. Hoje, desempenha um papel essencial na segurança de dados em um mundo cada vez mais digitalizado. Segundo Faleiros [6, p.11]:

> "A história da Criptologia se divide em três fases distintas. Na primeira, a dos cifrários que usavam lápis e papel. Na segunda, a do telégrafo, com o Código Morse e as máquinas eletro-mecânicas (o Enigma da Alemanha e a Púrpura do Japão). Na terceira, a dos cifrários da época computacional. Está surgindo uma outra fase, a que envolve técnicas resistentes ao ataque de um computador quântico, tecnologia que se encontra em sua infância."

Neste capítulo, exploraremos a Cifra de César, as cifras de substituição e o RSA, que é um dos sistemas criptográficos mais utilizados atualmente. As principais referências utilizadas foram [10], [3], [4] e [6].

2.1 A CIFRA DE CÉSAR

Um método de criptografia bastante conhecido foi o utilizado por Júlio César na Roma Antiga, por volta de 58 a.C., denominado Cifra de César. De acordo com registros históricos é considerado o primeiro algoritmo criptográfico, por utilizar a substituição de letras. Nesse sistema, cada letra da mensagem original é substituída pela letra que se encontra três posições adiante no alfabeto. Por exemplo, a letra A seria substituída pela letra D, seguindo essa lógica de deslocamento.

É importante mencionar que a cítala espartana é o primeiro artefato criptográfico conhecido. A cítala era formada por um cilindro de madeira em que uma tira de pergaminho era enrolada sem sobreposição (ver Figura 1). O texto a ser cifrado era dividido em blocos de caracteres de

mesmo tamanho, sendo que somente o último bloco poderia ter menos caracteres. Nesse caso, letras nulas poderiam ser inseridas aleatoriamente para completar a mensagem, sem alterar seu sentido. As letras de cada bloco eram escritas ao longo do eixo do cilindro em cima do pergaminho. Ao desenrolar a tira, a mensagem ficava criptografada. A chave desse método era o diâmetro do bastão.

Figura 1: Cítala Espartana

Fonte: Wikipédia. Disponível em https://pt.wikipedia.org/wiki/C%C3%ADtala.

Voltando na Cifra de César, a seguir está a Tabela 7, que mostra como cada letra da mensagem original é substituída pela letra que se encontra três posições adiante no alfabeto.

Tabela 7: Cifra de César

ALFABETO	CRIPTOGRAFADO	ALFABETO	CRIPTOGRAFADO
a	D	n	Q
b	E	o	R
c	F	p	S
d	G	q	T
e	H	r	U
f	I	s	V
g	J	t	W
h	K	u	X
i	L	v	Y
j	M	w	Z
k	N	x	A
l	O	y	B
m	P	z	C

Fonte: Livro de Aritmética - Coleção Profmat [10].

Este método de criptografia, conhecido como cifra de substituição simples monoalfabética, é o utilizado na Cifra de César e em suas 25 variações. Entretanto, é extremamente frágil e

não é utilizado atualmente. Esse método funcionava na época de César porque a maioria das pessoas não sabia ler. Para descriptografar uma mensagem, basta conhecer o método e testar as 25 variações ou encontrar uma letra que já revele o deslocamento necessário.

Exemplo 2.1. *Vamos codificar a mensagem "Eu adoro Aritmética" utilizando a Cifra de César.*

Mensagem original:	Eu	adoro	Aritmética.
Mensagem Criptografada:	HX	DGRUR	DULWPHWLFD.

2.2 CIFRAS DE SUBSTITUIÇÃO SIMPLES

Na Cifra de Substituição Simples, uma letra do alfabeto é substituída por outra sem seguir necessariamente uma regra de deslocamento. Para fazer essa cifra, criamos uma tabela com as 26 letras do alfabeto na primeira linha, organizadas em ordem alfabética. Na segunda linha, distribuímos as letras de forma aleatória.

Na Cifra de Substituição Simples com uso de palavra-chave, a codificação das letras iniciais é realizada de acordo com uma palavra-chave escolhida. Inicialmente, as letras do alfabeto são dispostas em ordem alfabética na primeira linha de uma tabela. Em seguida, utilizando a palavra-chave como ponto de partida, as letras são distribuídas aleatoriamente na segunda linha, sem repetições. Com isso, as letras da palavra-chave são atribuídas às primeiras posições da segunda linha, seguidas pelo preenchimento das letras restantes de forma aleatória.

Exemplo 2.2. *Vamos decodificar a mensagem a seguir usando a palavra-chave* **Enigma***:*

E MJWTKE MCE XKE KEZXWJE MOMLCBKMIEJWIE XVEGE JE ICWFLBTCEFWE, ABW XVEGE FECE IBGWAWIEC M GMIWACEC IBGWTBV GM TXMCCE.

Primeiro vamos construir uma tabela com o alfabeto na primeira linha e na segunda linha iniciaremos com a palavra ***ENIGMA****.*

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
E	N	I	G	M	A																				

Tabela 8: Alfabeto com a palavra-chave

Após decifrarmos as letras da palavra-chave na mensagem, verificamos se é possível formar alguma palavra ou se devemos continuar a decifrar mais letras.

E		M	J	W	T	K	E		M	C	E		X	K	E		K	E	-	
a		e					a		e		a				a			a	-	
Z	X	W	J	E		M	O	M	L	C	B	K	M	I	E	J	W	I	E	
				a		e		e					e	c	a			c	a	
X	V	E	G	E		J	E		I	C	W	F	L	T	C	E	F	W	E	
		a	d	a			a		c							a			a	
A	B	W		X	V	E	G	E		F	E	C	E		I	B	G	W	A	W
f						a	d	a			a		a		c		d		f	
I	E	C		M		G	M	I	W	A	C	E	C		I	B	G	W	-	
c	a			e		d	e	c		f		a			c		d			
T	B	V		G	M		T	X	M	C	C	E								
				d	e				e			a								

Tabela 9: Mensagem decifrada com a palavra-chave

Neste exemplo, percebemos que a palavra ***GMIWACEC*** *poderia ser decifrada como* **decifrar**, *encontrando assim mais letras cifradas. Em seguida, voltamos a fazer a substituição na mensagem e, junto com a análise da frequência das letras, conseguimos decifrar a mensagem com sucesso.*

E		M	J	W	T	K	E		M	C	E		X	K	E		K	E	-	
a		e	n	i	g	m	a		e	r	a		u	m	a		m	a	-	
Z	X	W	J	E		M	O	M	L	C	B	K	M	I	E	J	W	I	E	
q	u	i	n	a		e	l	e	t	r	o	m	e	c	a	n	i	c	a	
X	V	E	G	E		J	E		I	C	W	F	L	B	T	C	E	F	W	E
u	s	a	d	a		n	a		c	r	i	p	t	o	g	r	a	f	i	a
A	B	W		X	V	E	G	E		F	E	C	E		I	B	G	W	A	W
f	o	i		u	s	a	d	a		p	a	r	a		c	o	d	i	f	i
I	E	C		M		G	M	I	W	A	C	E	C		I	B	G	W	-	
c	a	r		e		d	e	c	i	f	r	a	r		c	o	d	i		
T	B	V		G	M		T	X	M	C	C	E								
g	o	s		d	e		g	u	e	r	r	a								

Tabela 10: Mensagem decifrada com a palavra-chave

Portanto, a mensagem decifrada fica: ***A Enigma era uma máquina eletromecânica usada na criptografia, foi usada para codificar e decifrar códigos de guerra.***

As cifras de substituição, embora ofereçam um número razoável de chaves, apresentam fragilidades devido às diferentes frequências de ocorrência das letras em um idioma combina-

das com o conhecimento da estrutura ortográfica da língua, fornecendo pistas valiosas para criptoanalistas, especialistas dedicados à decifração de códigos. Essa divergência de frequência facilita a análise e a decodificação das mensagens criptografadas.

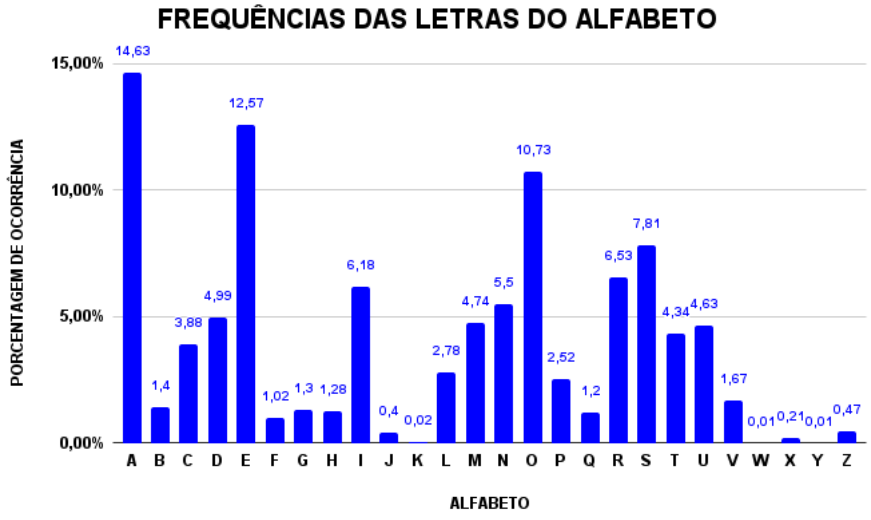
Ao estudarmos a situação da língua portuguesa, as proporções de utilização das letras no alfabeto são evidenciadas pelos dados expostos na Tabela 11, retirados do livro de Aritmética da coleção PROFMAT. Veja também o gráfico na Figura 2.

Tabela 11: Porcentagens de frequência das letras na língua Portuguesa

ALFABETO	PORCENTAGEM (%)	ALFABETO	PORCENTAGEM (%)
A	14,63	N	5,5
B	1,40	O	10,73
C	3,88	P	2,52
D	4,99	Q	1,20
E	12,57	R	6,53
F	1,02	S	7,81
G	1,30	T	4,34
H	1,28	U	4,63
I	6,18	V	1,67
J	0,40	W	0,01
K	0,02	X	0,21
L	2,78	Y	0,01
M	4,74	Z	0,47

Fonte: Livro de Aritmética - Coleção Profmat [10, p.311].

Figura 2



2.3 CIFRA DE VIGENÈRE

Além desses métodos, a Cifra de Vigenère, inventada no século XVI, representa um avanço na criptografia. Conhecida como cifra de autochave de Vigenère, essa técnica utiliza uma palavra-chave para cifrar a mensagem, substituindo uma letra por várias outras de acordo com a posição da letra na palavra-chave. Diferente da Cifra de César, a Cifra de Vigenère é polialfabética, o que significa que cada letra pode ser substituída por várias outras, dependendo o contexto. Essa cifra foi considerada segura por quase 300 anos, até ser quebrada pelo método Kasiski, que explora a repetição de padrões na cifra para descobrir a palavra-chave.

No século XX, as máquinas criptográficas destacaram um avanço significativo na história da criptografia. Além da famosa Enigma desenvolvida pelo inventor alemão Arthur Scherbius em 1918, houve outras inovações como a máquina de Hill, utilizada na Cifra de Hill, inventada pelo matemático americano Lester Hill em 1929. A Cifra de Hill é uma cifra de substituição polialfabético, que utiliza a álgebra linear.

2.4 ENIGMA

A máquina Enigma foi uma das mais complexas e poderosas máquinas criptográficas de seu tempo. Ela era uma máquina com rotores, consistia na integração de sistemas mecânicos e elétrico, composta por três elementos fundamentais: um teclado para a entrada do texto a ser criptografado, um misturador para cifrar a mensagem e um mostrador para exibir o texto cifrado. Embora seu funcionamento não seja complicado, é detalhado e interessante de se entender.

Sua unidade de cifração era formada por três cilindros móveis, que podiam alternar sua posição dentro da máquina, e um cilindro fixo chamado espelho. Cada um desses cilindros continha vinte e seis letras do alfabeto. Entre o teclado e o primeiro cilindro havia um painel de ligação que permitia a troca de seis pares de letras do alfabeto. Essa característica aumentou significativamente o número de chaves possíveis, tornando a Enigma uma máquina poderosa em termos de criptografia.

> Por cada letra cifrada, o primeiro cilindro roda um sexto sempre no sentido direto, quando dá uma volta completa, o segundo cilindro roda também um sexto, após seis voltas do primeiro cilindro, o segundo dá uma volta completa e o terceiro roda um sexto. Ou seja, por cada seis letras cifradas, o segundo cilindro move-se e por cada 36 letras move-se o terceiro, o que permite o uso de 17576 alfabetos de cifra diferentes [7, p.22].

A atividade de decifrar as mensagens cifradas pela Enigma exigiu anos de dedicação, iniciando-se antes mesmo do início da Segunda Guerra Mundial. O que ocasionava a dificuldade na quebra do sistema que era frequentemente a Enigma propiciava uma permutação diferente do alfabeto. O sistema de criptografia foi quebrado pelos britânicos com a participação de Alan Turing, conhecido como um dos precursores da computação. A Enigma representou um desafio significativo para os aliados, mas sua decifração foi fundamental para o desenrolar da guerra e para o desenvolvimento futuro da criptografia e da computação.

Figura 3: Máquina Enigma

Fonte: Wikipédia.
Disponível em https://pt.wikipedia.org/wiki/Enigma. Acessado em 18/05/2024.

2.5 CRIPTOSSISTEMA RSA

A criptografia pode ser dividida de duas maneiras: criptografia simétrica e criptografia assimétrica. Na criptografia simétrica, a mesma chave é usada para cifrar e para decifrar a mensagem, significando que ambas as partes precisam compartilhar a chave de maneira segura antes de iniciar a comunicação. Temos como exemplos o algoritmo DES (*Data Encryption Standard*) e o AES (*Advanced Encryption Standard*). A principal vantagem da criptografia simétrica é sua eficiência; algoritmos simétricos geralmente são mais rápidos e precisam menos recursos computacionais. Mas, a gestão das chaves é um grande desafio, pois a chave deve ser mantida em segredo e trocada de forma segura entre as partes. Por outro lado, a criptografia assimétrica utiliza um par de chaves, uma pública e outra secreta. A chave pública pode ser divulgada livremente, enquanto a chave secreta o proprietário a mantém em segredo. As mensagens cifradas com a chave pública só podem serem decifradas com a chave secreta correspondente, e vice-versa. Um dos primeiros algoritmos de criptografia pública amplamente adotado foi o RSA. A principal vantagem é a segurança na troca das chaves. Mas, algoritmos assimétricos são mais lentos e utilizam mais recursos computacionais que os simétricos.

Antes de aplicar o método RSA é necessário transformar a mensagem que se deseja encriptar em uma sequência de números usando a conversão da Tabela ASCII (que é a sigla inglês para Código Padrão Americano para o Intercâmbio de Informações).

Binário	Decimal	Símbolo	Binário	Decimal	Símbolo	Binário	Decimal	Símbolo
00100000	32		01000000	64	@	01100000	96	‘
00100001	33	!	01000001	65	A	01100001	97	a
00100010	34	“	01000010	66	B	01100010	98	b
00100011	35	#	01000011	67	C	01100011	99	c
00100100	36	$	01000100	68	D	01100100	100	d
00100101	37	%	01000101	69	E	01100101	101	e
00100110	38	&	01000110	70	F	01100110	102	f
00100111	39	´	01000111	71	G	01100111	103	g
00101000	40	(	01001000	72	H	01101000	104	h
00101001	41	)	01001001	73	I	01101001	105	i
00101010	42	*	01001010	74	J	01101010	106	j
00101011	43	+	01001011	75	K	01101011	107	k
00101100	44	,	01001100	76	L	01101100	108	l
00101101	45	-	01001101	77	M	01101101	109	m
00101110	46	.	01001110	78	N	01101110	110	n
00101111	47	/	01001111	79	O	01101111	111	o
00110000	48	0	01010000	80	P	01110000	112	p
00110001	49	1	01010001	81	Q	01110001	113	q
00110010	50	2	01010010	82	R	01110010	114	r
00110011	51	3	01010011	83	S	01110011	115	s
00110100	52	4	01010100	84	T	01110100	116	t
00110101	53	5	01010101	85	U	01110101	117	u
00110110	54	6	01010110	86	V	01110110	118	v
00110111	55	7	01010111	87	W	01110111	119	w
00111000	56	8	01011000	88	X	01111000	120	x
00111001	57	9	01011001	89	Y	01111001	121	y
00111010	58	:	01011010	90	Z	01111010	122	z
00111011	59	;	01011011	91	[	01111011	123	{
00111100	60	<	01011100	92	\	01111100	124	|
00111101	61	=	01011101	93	]	01111101	125	}
00111110	62	>	01011110	94	∧	01111110	126	∼
00111111	63	?	01011111	95	_			

Tabela 12: Tabela ASCII

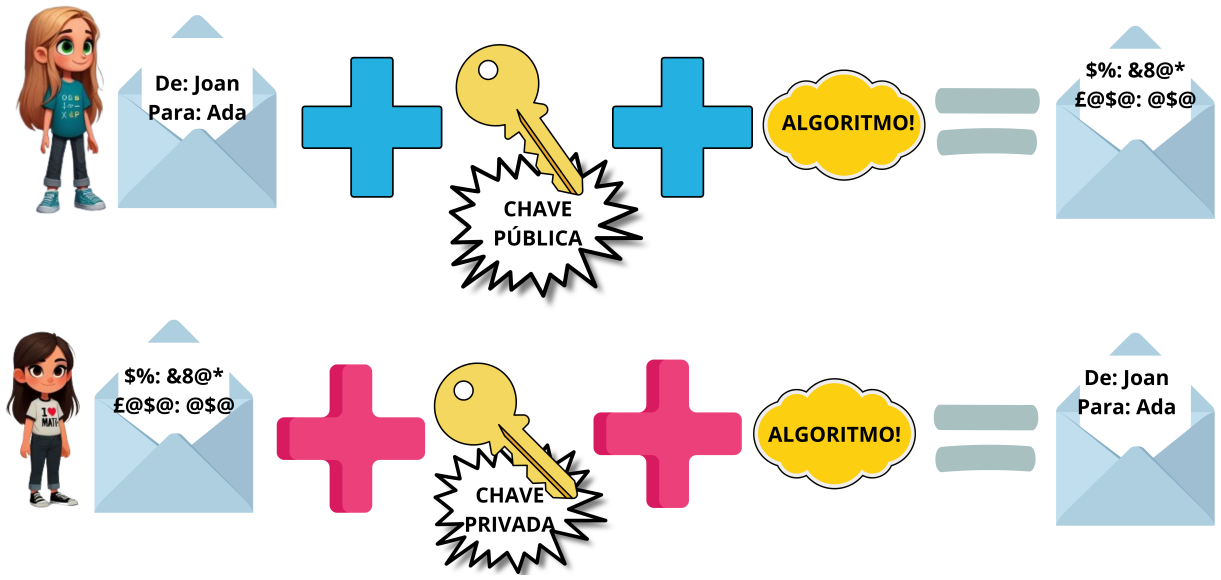
Fonte: Livro de Aritmética Profmat [10, p.324]

No ASCII, cada letra, número ou símbolo é trocado por um valor numérico específico. Esses valores podem ser representados na forma decimal (base 10), hexadecimal (base 16) ou em binário (base 2). Transformar uma mensagem em ASCII envolve converter cada caractere da mensagem em seu valor numérico conforme Tabela 12. Este passo é fundamental, pois os algoritmos de criptografia, como RSA operam com números. Portanto, a mensagem original é convertida em uma sequência numérica, que então é processada pelo algoritmo de criptografia para garantir a segurança da comunicação.

Uma vez que as mensagens já foram transformadas em números, podemos iniciar o processo. Vamos exemplificar todo o processo utilizando duas personagens fictícias: Ada e Joan.

Vamos supor que Ada deseja se comunicar com Joan via RSA. Ada terá que gerar uma chave pública e uma chave privada. A chave pública servirá para Joan cifrar a mensagem e a chave privada para Ada decifrar a mensagem.

Figura 4: Criptografia RSA



Primeiramente, Ada deve escolher dois números primos muito grandes p e q, com $p \neq q$, e calcular o seu produto, isto é, $n = p \cdot q$. É simples calcular n, difícil é fazer a sua fatoração, isto é, o processo inverso.

Em seguida, Ada deve calcular $\varphi(n)$. Como p e q são números primos distintos temos que $\varphi(n) = (p-1)(q-1)$.

O próximo passo de Ada é escolher dois inteiros α e β, de modo que $1 < \alpha, \beta < \varphi(n)$ e

$$\alpha\beta \equiv 1 \,(mod\, \varphi(n)).$$

Para isso, Ada deve escolher primeiro um α de maneira que $\text{mdc}(\alpha, \varphi(n)) = 1$. Em seguida, deve resolver a congruência $\alpha x \equiv 1 \, (mod\, \varphi(n))$ e encontrar o valor de β.

Então, Ada torna públicos os valores de n e β, os quais são chamados de chave pública. A chave secreta, que só Ada tem acesso, é formada pelo número $\varphi(n)$ e por α.

Joan, ou qualquer outra pessoa que conheça a chave pública de Ada, pode enviar uma mensagem cifrada para Ada.

Para Joan enviar a mensagem para Ada, uma vez que ela já transformou a mensagem em sequência numérica usando a Tabela ASCII, ela deve dividir a sequência x em blocos de tamanhos variados de forma que todos sejam menores do que n, isto é, Joan deve particionar x como $x = x_1 x_2 \dots x_m$, onde $x_i < n$ para todo i.

Para cada x_i da sequência, Joan deve calcular x_i^β e depois o resto da divisão de x_i^β por n. Este resto será chamado de $C(x_i)$ e será a codificação da sequência x_i. Em termos de congruência, temos que:

$$x_i^\beta \equiv C(x_i) \, (mod\, n), \; 1 < C(x_i) < n.$$

Após realizar a cifração de todos os blocos, Joan envia cada um deles para Ada, isto é,

$$C(x_1)\_C(x_2)\_ \dots \_C(x_m).$$

Ada recebe os blocos $C(x_i)$ e com a sua chave secreta α irá decifrá-los. Para decifrar cada bloco, ela deverá calcular $C(x_i)^\alpha$ e depois o resto da divisão de $C(x_i)^\alpha$ por n. Chamaremos de $D(C(x_i))$ cada bloco decifrado por Ada. Em termos de congruência:

$$C(x_i)^\alpha \equiv D(C(x_w)) \, (mod\, n), \;\; \text{onde} \;\; 1 < D(C(x_i)) < n.$$

Por fim, depois que Ada resgatar a sequência numérica original enviada por Joan, ela consultará a mesma tabela que Joan utilizou para pré-codificar a mensagem e transformará a sequência numérica em texto novamente.

Com o intuito de ilustrar o método, vamos fazer um exemplo utilizando números primos pequenos e a Tabela 13.

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

Tabela 13: Tabela para Pré Codificação
Fonte: Criptografia - OBMEP. Disponível em [3, p.147].

Exemplo 2.3. *Primeiramente, Ada escolhe os dois números primos distintos* $p = 3$ *e* $q = 11$*, e calcula o valor de* n*, isto é,* $n = 3 \cdot 11 = 33$*.*

Em seguida, Ada calcula $\varphi(n) = (p-1)(q-1)$*, ou seja,* $\varphi(n) = 2 \cdot 10 = 20$*.*

Ada então escolhe $\alpha = 7$*, pois* $mdc(\varphi(n), 7) = 1$*, ou seja,* $mdc(20, 7) = 1$*. Agora ela deve resolver a congruência* $\alpha x \equiv 1 \,(mod\,(\varphi(n))$*, isto é,* $7\beta \equiv 1 \,mod\,(20)$*, isto é, calcular o inverso multiplicativo de* α *módulo* $\varphi(n)$*, que é o equivalente a resolver a equação Diofantina,* $7\beta - 20y = 1$*, para* $\beta, y \in \mathbb{Z}$*. O valor obtido é* $\beta = 3$*.*

A chave pública de Ada é $(n, \beta) = (33, 3)$ *e a sua chave secreta é* $(\varphi(n), \alpha) = (20, 7)$*. Ela divulga a chave pública para Joan.*

Joan irá criptografar a mensagem FELIZ ANIVERSARIO. Transformado essa mensagem em uma sequência numérica através da Tabela 13 e inserindo 99 *no espaço entre as palavras, a sequência numérica fica* $15 - 14 - 21 - 18 - 35 - 99 - 10 - 23 - 18 - 31 - 14 - 27 - 28 - 10 - 27 - 18 - 24$*. Joan, escolhe então como quebrar a sequência em blocos de forma que o número contido em cada bloco não ultrapasse* $n = 33$*. A escolha de Joan é*

$$15 - 14 - 21 - 18 - 3 - 5 - 9 - 9 - 10 - 23 - 18 - 31 - 14 - 27 - 28 - 10 - 27 - 18 - 24,$$

totalizando 19 *blocos.*

Para cada bloco x_i *da sequência, Joan deve encontrar* $1 < C(x_i) < n$ *de modo que:* $x_i^{\beta} \equiv C(x_i) \,(mod\, n)$*. A seguir, detalhamos os cálculos feitos por Joan:*

- *Primeiro bloco:* $x_1 = 15$ *e* $15^3 \equiv 9\,(mod\,33)$. *Logo* $C(x_1) = 9$.
- *Segundo e décimo terceiro blocos:* $x_2 = x_{13} = 14$ *e* $14^3 \equiv 5\,(mod\,33)$. *Logo,* $C(x_2) = C(x_{13}) = 5$.
- *Terceiro bloco:* $x_3 = 21$ *e* $21^3 \equiv 21\,(mod\,33)$. *Logo,* $C(x_3) = 21$.
- *Quarto, décimo primeiro e décimo oitavo blocos:* $x_4 = x_{11} = x_{18} = 18$ *e* $18^3 \equiv 24\,(mod\,33)$. *Logo,* $C(x_4) = C(x_{11}) = C(x_{18}) = 24$.
- *Quinto bloco:* $x_5 = 3$ *e* $3^3 \equiv 27\,(mod\,33)$. *Logo,* $C(x_5) = 27$.
- *Sexto bloco:* $x_6 = 5$ *e* $5^3 \equiv 26\,(mod\,33)$. *Logo,* $C(x_6) = 26$.
- *Sétimo e oitavo blocos:* $x_7 = x_8 = 9$ *e* $9^3 \equiv 3\,(mod\,33)$. *Logo,* $C(x_7) = C(x_8) = 3$.
- *Nono e décimo sexto blocos:* $x_9 = x_{16} = 10$ *e* $10^3 \equiv 10\,(mod\,33)$. *Logo,* $C(x_9) = C(x_{16}) = 10$.
- *Décimo bloco:* $x_{10} = 23$ *e* $23^3 \equiv 23\,(mod\,33)$. *Logo,* $C(x_{10}) = 23$.
- *Décimo segundo bloco:* $x_{12} = 31$, $31^3 \equiv 25\,(mod\,33)$. *Logo,* $C(x_{12}) = 25$.
- *Décimo quarto e décimo sétimo blocos:* $x_{14} = x_{17} = 27$, $27^3 \equiv 15\,(mod\,33)$. *Logo,* $C(x_{14}) = C(x_{17}) = 15$.
- *Décimo quinto bloco:* $x_{15} = 28$, $28^3 \equiv 7\,(mod\,33)$. *Logo,* $C(x_{15}) = 7$.
- *Décimo nono bloco:* $x_{19} = 24$, $24^3 \equiv 30\,(mod\,33)$. *Logo,* $C(x_{19}) = 30$.

Joan envia os blocos criptografados para Ada:

$$9-5-21-24-27-26-3-3-10-23-24-25-5-15-7-10-15-24-30.$$

Para descriptografar a mensagem, Ada usa a sua chave secreta da seguinte maneira:

- *Primeiro bloco:* $C(x_1) = 9$ *e* $9^7 \equiv 15\,(mod\,33)$. *Logo,* $D(x_1) = 15$.
- *Segundo e décimo terceiro blocos:* $C(x_2) = C(x_{13}) = 5$ *e* $5^7 \equiv 14\,(mod\,33)$. *Logo,* $D(x_2) = D(x_{13}) = 14$.
- *Terceiro bloco:* $x_3 = 21$ *e* $21^7 \equiv 21\,(mod\,33)$. *Logo,* $D(x_3) = 21$.
- *Quarto, décimo primeiro e décimo oitavo blocos:* $C(x_4) = C(x_{11}) = C(x_{18}) = 24$ *e* $24^7 \equiv 18\,(mod\,33)$. *Logo,* $D(x_4) = D(x_{11}) = D(x_{18}) = 18$.

- *Quinto bloco:* $C(x_5) = 27$ *e* $27^7 \equiv 3\,(mod\,33)$. *Logo,* $D(x_5) = 3$.
- *Sexto bloco:* $C(x_6) = 26$ *e* $26^7 \equiv 5\,(mod\,33)$. *Logo,* $D(x_6) = 5$.
- *Sétimo e oitavo blocos:* $C(x_7) = C(x_8) = 3$ *e* $3^9 \equiv 3\,(mod\,33)$. *Logo,* $D(x_7) = D(x_8) = 9$.
- *Nono e décimo sexto blocos:* $C(x_9) = C(x_{16}) = 10$ *e* $10^7 \equiv 10\,(mod\,33)$. *Logo,* $D(x_9) = D(x_{16}) = 10$.
- *Décimo bloco:* $C(x_{10}) = 23$ *e* $23^7 \equiv 23\,(mod\,33)$. *Logo,* $D(x_{10}) = 23$.
- *Décimo segundo bloco:* $C(x_{12}) = 25$ *e* $25^7 \equiv 31\,(mod\,33)$. *Logo,* $D(x_{12}) = 31$.
- *Décimo quarto bloco:* $C(x_{14}) = 15$ *e* $15^7 \equiv 27\,(mod\,33)$. *Logo,* $D(x_{14}) = 27$.
- *Décimo quinto bloco:* $C(x_{15}) = 7$ *e* $7^7 \equiv 28\,(mod\,33)$. *Logo,* $D(x_{15}) = 28$.
- *Décimo sétimo bloco:* $x_{17} = 15$ *e* $15^7 \equiv 27\,(mod\,33)$. *Logo,* $D(x_{17}) = 27$.
- *Décimo nono bloco:* $C(x_{19}) = 30$ *e* $30^7 \equiv 24\,(mod\,33)$. *Logo,* $D(x_{19}) = 24$.

Ada obtém então a seguinte sequência numérica:

$$15 - 14 - 21 - 18 - 3 - 5 - 9 - 9 - 10 - 23 - 18 - 31 - 14 - 27 - 28 - 10 - 27 - 18 - 24.$$

Na última etapa, ela consulta a Tabela 13. Assim, a mensagem decifrada revela-se como ***FELIZ ANIVERSARIO****.*

Vamos entender por que o RSA funciona. Suponha que a chave pública de Ada seja n e β e sua chave privada seja $\varphi(n)$ e α. Suponha que Joan enviou a mensagem criptografada

$$C(x) \equiv x^{\beta}\,(mod\,n)$$

para Ada.

Ao receber a mensagem criptografada, Ada faz:

$$D(C(x)) = C(x)^{\alpha} \equiv x^{\alpha\beta}\,(mod\,n).$$

Como $\alpha\beta \equiv 1\,(mod\,\varphi(n))$, então existe $k \in \mathbb{Z}$ tal que $\alpha\beta - 1 = k\varphi(n)$, ou seja,

$$\alpha\beta = 1 + k\varphi(n) = 1 + k(p-1)(q-1),$$

visto que $\varphi(n) = (p-1)(q-1)$.

Portanto, pelo Teorema 1.46,

$$D(C(x)) \equiv x^{1+k(p-1)(q-1)} \equiv x \cdot \left(x^{(p-1)(q-1)}\right)^k \equiv x \cdot 1^k \equiv x \,(mod\, n).$$

Logo, Ada consegue recuperar x.

Vamos supor que Katherine tenha interceptado a mensagem que Joan enviou para Ada. Para Katherine descobrir a chave privada para decifrar a mensagem, ela teria que primeiro fatorar n, o que é computacionalmente inviável para n suficientemente grande, por ser muito dispendioso e demorado. O algoritmo RSA então é fundamentado na dificuldade de fatorar a multiplicação desses dois números primos. Para garantir a segurança do RSA é fundamental que p e q tenham pelo menos 1024 bits em sua representação binária. Além disso, p e q não devem ser muito próximos entre si, pois isso pode comprometer a segurança do sistema.

Outro ponto importante é a escolha do expoente público (chave pública), denotado nesta dissertação por β. Na prática, o valor frequentemente utilizado para β é 65537. Esse número é preferido porque sua representação binária é 10000000000000001, o que facilita o trabalho computacional. Além de ser eficiente computacionalmente, este expoente também oferece um bom equilíbrio entre segurança e desempenho [19].

Além disso, vale a pena mencionar que α e β são inversos multiplicativos e que é possível encontrar esses inversos usando o algoritmo estendido de Euclides. No entanto, esse processo é computacionalmente pesado, o que contribui para a lentidão do algoritmo.

A criptografia pública possui uma alta complexidade matemática envolvida. Por essa razão, ela é frequentemente utilizada apenas para trocar uma chave simétrica antes do início da comunicação segura. Uma vez estabelecida a chave simétrica, a comunicação propriamente dita é conduzida usando algoritmos simétricos mais rápidos, como o AES. Exemplos práticos desse uso incluem plataformas como Amazon e Moodle.

3

DÍGITOS VERIFICADORES

Os dígitos verificadores são utilizados em uma variedade de contextos, como em números de cartões de crédito, códigos de barras e números de identificação (RG e CPF, por exemplo). Esses dígitos são calculados com base nos outros dígitos do conjunto de dados, de acordo com um algoritmo específico. Eles não têm a função de corrigir erros, mas têm como objetivo verificar se os dados inseridos ou enviados estão corretos. Eles ajudam a diminuir os erros e a aumentar a confiança dos sistemas que usam valores numéricos.

A seguir vamos apresentar alguns usos de dígitos verificadores.

3.1 CÓDIGO DE BARRAS

A expressão código de barras tem origem do inglês *barcode*. Os códigos de barras são uma forma eficiente de codificar informações em padrões visuais facilmente legíveis por máquinas. O código de barras tem duas formas de representação: a gráfica e a numérica ou alfanumérica. A representação gráfica se dá pelas barras verticais paralelas e com espessuras e espaçamentos variados, enquanto a representação numérica ou alfanumérica se dá por dígitos do sistema de numeração decimal e letras do alfabeto. Ao escanear um código de barras com um leitor óptico, as informações codificadas são rapidamente capturadas e interpretadas.

A primeira patente de um código de barras foi registrada em 1852 por *Joseph Woodland e Bernard Silver*. O código proposto era um padrão de circunferências concêntricas de várias espessuras (Figura 5) e o leitor do código de barras que eles construíram era do tamanho de uma mesa.

Figura 5: Primeiro Código de Barra com a patente registrada

Fonte: Códigos de Barra Brasil. Disponível em
https://codigosdebarrasbrasil.com.br/a-evolucao-e-historia-do-codigo-de-barras/

Com o passar do tempo, muitas variações dos códigos de barras foram desenvolvida, como exemplificado na Figura 6.

Figura 6: Tipos de Códigos de Barras

Fonte: Códigos de Barras Brasil. Disponível em
https://codigosdebarrasbrasil.com.br/tipos-de-codigos-de-barras/

O código de barras atualmente utilizado em produtos como de alimentação, roupas, calçados, isto é, o utilizado por lojistas, supermercados, é o EAN-13/GTIN-13, com 13 dígitos. Este tipo é o mais usado pela maioria dos países. Os Estados Unidos e o Canadá utilizam o UPC ou Código Universal de Produto que utiliza 12 dígitos.

O código de barras EAN-13 é dividido em partes que, ao serem lidas da esquerda para direita revelam o país de origem, a empresa fabricante e o produto. O último algarismo é o digito verificador, responsável por validar as informações do código, conforme ilustrado na Figura 7.

Figura 7: Descrição do Código de Barras

Fonte: Automaclick.
Disponível em
https://www.automaclick.com.br/blog/saber-de-onde-vem-o-produto-pelo-codigo-de-barras

A seguir, vamos descrever o procedimento para calcular o dígito verificador do código EAN-13, que é utilizado no Brasil.

Consideremos o código de barras

$$b_1b_2b_3b_4b_5b_6b_7b_8b_9b_{10}b_{11}b_{12} - X,$$

onde X representa o dígito verificador. Devemos proceder da seguinte maneira:

- Transformar a representação numérica do código de barras sem o dígito verificador $b_1b_2b_3b_4b_5b_6b_7b_8b_9b_{10}b_{11}b_{12}$ no vetor $v = (b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8, b_9, b_{10}, b_{11}, b_{12})$.
- Considerar o vetor peso $u = (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3)$.
- Calcular o produto escalar entre os vetores v e u, isto é,

$$P = 1 \cdot b_1 + 3 \cdot b_2 + 1 \cdot b_3 + 3 \cdot b_4 + 1 \cdot b_5 + 3 \cdot b_6 + 1 \cdot b_7 + 3 \cdot b_8 + 1 \cdot b_9 + 3 \cdot b_{10} + 1 \cdot b_{11} + 3 \cdot b_{12}.$$

- Calcular o resto R da divisão de P por 10, isto é, $P \equiv R\,(mod\,10)$, com $0 \leq R < 10$.
- Se $R = 0$, então o dígito verificador X é zero, agora se $1 \leq R < 10$, fazemos $X = 10 - R$.

Exemplo 3.1. *Dado o código de barras da Figura 8, vamos calcular o seu dígito verificador.*

Figura 8: Exemplo de Código de Barras

Fonte: Gerador online de Código de Barras.

Disponível em http://barcodept.com/EAN13OnlinePt.asp

- *Primeiro, transformamos a representação numérica* 123456789010 *no vetor*

$$v = (1, 2, 3, 4, 5, 6, 7, 8, 9, 0, 1, 0).$$

- *Agora, calculamos o produto escalar:*

$$P = 1 \cdot 1 + 3 \cdot 2 + 1 \cdot 3 + 3 \cdot 4 + 1 \cdot 5 + 3 \cdot 6 + 1 \cdot 7 + 3 \cdot 8 + 1 \cdot 9 + 3 \cdot 0 + 1 \cdot 1 + 3 \cdot 0 = 86.$$

- *Em seguida, calculamos o resto da divisão de* 86 *por* 10 *e obtemos* $R = 6$.
- *Como* $R = 6$, *segue que* $X = 10 - 6 = 4$. *Portanto o dígito verificador é* 4.

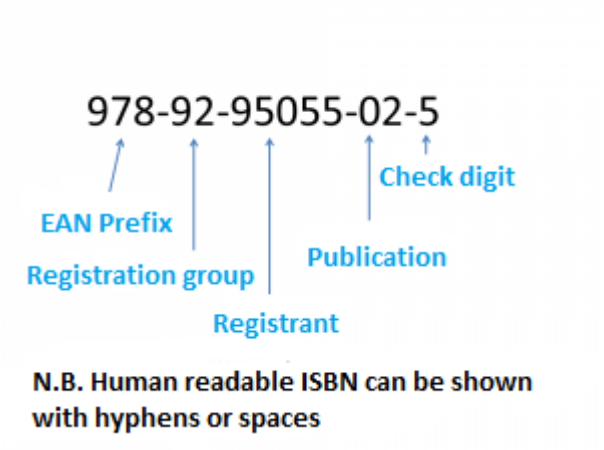
3.2 ISBN *(international standard book number)*

O registro ISBN, criado em 1967, é uma sequencia de dígitos que identifica o livro segundo o título, autor, país, a editora e a edição. Antes de janeiro de 2007 o ISBN era composto por 10 dígitos e depois passou a ser composto por 13 dígitos. Para deixar claro qual padrão é utilizado, coloca-se ISBN-10 e ISBN-13. O ISBN é composto por cinco grupos separados por hífen, descritos na Figura 9.

Da esquerda para a direita, o prefixo *(EAN Prefix)* é composto por três dígitos. O grupo de registro nacional *(Registration group)*, identifica o país, região geográfica ou idioma do material e pode ter de um a cinco dígitos. Depois, o registro editorial *(Registrant)*, identifica o editor ou se é impressão particular e é composto por até sete dígitos. O número de edição *(Publication)*, define a edição e o formato específico de um título e é composto por até 6 dígitos. Por fim, o

dígito verificador *(Check digit)* comprova através de uma fórmula matemática a validação do restante do número.

Figura 9: Padrão ISBN



Fonte: ISBN. Disponível em https://www.isbn-international.org/content/what-isbn/10

Figura 10: Códigos de Barras ISBN

Fonte: ISBN International. Disponível em
https://www.isbn-international.org/content/isbn-bar-coding

Para calcular o dígito verificador do código ISBN-13,

$$b_1b_2b_3b_4b_5b_6b_7b_8b_9b_{10}b_{11}b_{12} - X,$$

onde X é o dígito verificador, devemos proceder de maneira similar ao caso anterior:

- Transformar a representação numérica do código de barras sem o dígito verificador $b_1b_2b_3b_4b_5b_6b_7b_8b_9b_{10}b_{11}b_{12}$ no vetor $v = (b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8, b_9, b_{10}, b_{11}, b_{12})$.
- Considerar o vetor peso $u = (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3)$.
- Calcular o produto escalar entre os vetores v e u, isto é,

$$P = 1 \cdot b_1 + 3 \cdot b_2 + 1 \cdot b_3 + 3 \cdot b_4 + 1 \cdot b_5 + 3 \cdot b_6 + 1 \cdot b_7 + 3 \cdot b_8 + 1 \cdot b_9 + 3 \cdot b_{10} + 1 \cdot b_{11} + 3 \cdot b_{12}.$$

- Calcular o resto R da divisão de P por 10, isto é, $P \equiv R\,(mod\,10)$, com $0 \leq R < 10$.
- Se $R = 0$, então o dígito verificador X é zero, agora se $1 \leq R < 10$, fazemos $X = 10 - R$.

Exemplo 3.2. *O livro de Aritmética da Coleção Profmat tem ISBN-13 978-85-85818-92-0, sendo o último o algarismo o dígito verificador. Vamos fazer a verificação para confirmar o dígito verificador:*

- *Inicialmente, transformamos a representação numérica* $978 - 85 - 85818 - 92$ *no vetor* $v = (9, 7, 8, 8, 5, 8, 5, 8, 1, 8, 9, 2)$.
- *Em seguida, calculamos o produto escalar:*

$$P = (1 \cdot 9 + 3 \cdot 7 + 1 \cdot 8 + 3 \cdot 8 + 1 \cdot 5 + 3 \cdot 8 + 1 \cdot 5 + 3 \cdot 8 + 1 \cdot 1 + 3 \cdot 8 + 1 \cdot 9 + 3 \cdot 2) = 160.$$

- *Dividindo* 160 *por* 10 *obtemos* $R = 0$.
- *Como* $R = 0$, *logo* $X = 0$.

Como obtemos resto zero, o dígito verificador é zero.

3.3 REGISTRO GERAL - RG

O registro geral (RG) de São Paulo segue um formato de nove dígitos, apresentado como $RR.RRR.RRR - D$, onde os dígitos R são valores numéricos e o dígito D é o dígito verificador. Este dígito verificador é calculado a partir dos oito dígitos anteriores usando um algoritmo específico baseado no módulo 11.

Para calcular o dígito verificador do RG, devemos proceder da seguinte maneira:

- Transformar a representação numérica do RG sem o dígito verificador $R_1R_2.R_3R_4R_5.R_6R_7R_8$ no vetor $v = (R_1, R_2, R_3, R_4, R_5, R_6, R_7, R_8)$.
- Considerar o vetor peso $u = (2, 3, 4, 5, 6, 7, 8, 9)$.
- Calcular o produto escalar entre os vetores v e u, isto é,

$$P = 2 \cdot R_1 + 3 \cdot R_2 + 4 \cdot R_3 + 5 \cdot R_4 + 6 \cdot R_5 + 7 \cdot R_6 + 8 \cdot R_7 + 9 \cdot R_8.$$

- Calcular o resto da divisão de P por 11, isto é, $P \equiv R\,(mod\,11)$, com $0 \leq R < 11$.
- Se $R = 0$, o dígito verificador será 0. Caso contrário, fazemos $D = 11 - R$.

- Se $D = 10$, o dígito verificador será X. Se $D \neq 10$, o dígito verificador será D.

Exemplo 3.3. *Dado o RG número* $11.871.896 - 4$*, gerado aleatoriamente em um site gerador com finalidade de aplicarmos o algoritmo descrito acima, vamos fazer a verificação:*

- *Transformamos a representação numérica* $11.871.896$ *no vetor* $v = (1, 1, 8, 7, 1, 8, 9, 6)$.
- *Consideramos o vetor peso* $u = (2, 3, 4, 5, 6, 7, 8, 9)$.
- *Calculamos o produto escalar:*
  $P = 1 \cdot 2 + 1 \cdot 3 + 8 \cdot 4 + 7 \cdot 5 + 1 \cdot 6 + 8 \cdot 7 + 9 \cdot 8 + 6 \cdot 9 = 260$.
- *Calculamos o resto da divisão de* 260 *por* 11 *e obtemos o resto* 7.
- *Como* $r = 7$*, O digito verificador será,* 11 *subtraído do resto encontrado, logo,* $D = 11 - 7 = 4$.

Portanto, o dígito verificador é 4.

4

CÓDIGOS CORRETORES DE ERROS

Os códigos corretores de erros são algoritmos desenvolvidos com a finalidade de identificar e corrigir uma certa quantidade de erros que podem surgir ao longo de uma transmissão de dados. Basicamente, os códigos corretores de erros funcionam adicionando informações redundantes aos dados originais antes deles serem transmitidos ou armazenados. Quando os dados são recebidos ou lidos, esses códigos podem identificar automaticamente se ocorreu algum erro e, em alguns casos, podem corrigir estes erros.

Existem vários tipos de códigos corretores de erros, cada um com sua especificidade e capacidade de correção. A decisão sobre qual código corretor de erros escolher depende das necessidades específicas do sistema e das características do canal de transmissão ou armazenamento.

4.1 ALGUNS FATOS HISTÓRICOS

A Teoria dos Códigos Corretores de Erros surgiu com os trabalhos de Richard W. Hamming, Marcel J. E. Golay e Claude E. Shannon na década de 1940. Inicialmente, os matemáticos foram os principais interessados nesse campo e o melhoraram consideravelmente nas décadas de 1950 e 1960. Na década de 1970, com as pesquisas espaciais, essa teoria também passou a atrair a atenção dos engenheiros.

No que segue, destacamos alguns marcos históricos em que códigos corretores de erros foram utilizados.

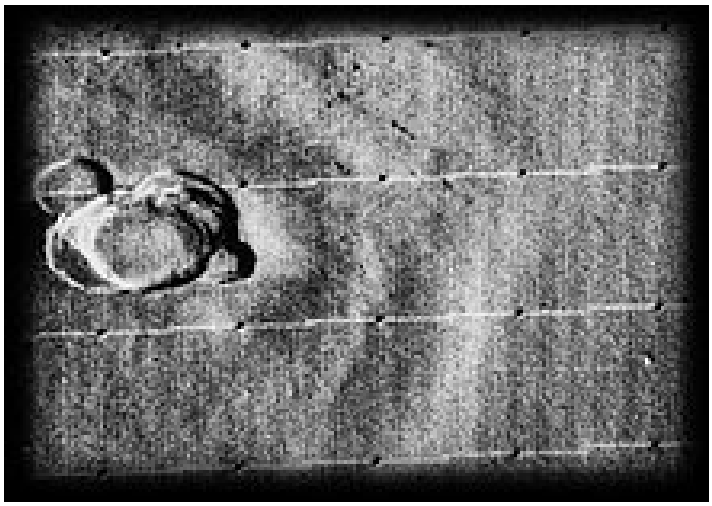
- Em 1965, a sonda *Mariner* 4 enviou 22 fotografias de Marte em escalas de cinza. Cada imagem foi dividida 200×200 elementos de imagem, sendo que a cada um desses elementos foi atribuído um dos 64 tons de cinza predefinidos e codificados. Veja uma das imagens enviadas pela *Mariner* 4 na Figura 11.

Figura 11: Foto de Marte - Mariner 4

Fonte: Nasa Science MARS Exploration. Disponível em
https://mars.nasa.gov/resources/6816/mariner-4-image

- Em 1972, a espaçonave *Mariner* 9 fez progressos significativos, transmitindo novas imagens de Marte. Desta vez, cada imagem foi separada em uma matriz surpreendente de 700×832 elementos, resultando em uma melhora notável na resolução das imagens. Na Figura 12, temos uma imagem de Marte registrada pela espaçonave *Mariner* 9.

Figura 12: Foto de Marte - Mariner 9



Fonte: Wikipedia.

Disponível em https://https://gl.wikipedia.org/wiki/Mariner_9

- Em 1979, a nave espacial *Voyager* abriu novos caminhos ao enviar imagens coloridas de Júpiter. Essas imagens coloridas são na verdade uma sequência de imagens tiradas em

preto e branco através de vários filtros. Cada elemento de imagem foi representado por uma das 4096 tonalidades de cinza previamente selecionadas, elevando consideravelmente a precisão de cada imagem tirada. Na Figura 13 temos a Grande Mancha Vermelha uma tempestade anticiclônica registrada pela *Voyager*.

Figura 13: Foto enviada pela Voyager - A grande Mancha Vermelha

Fonte: Wikipedia.

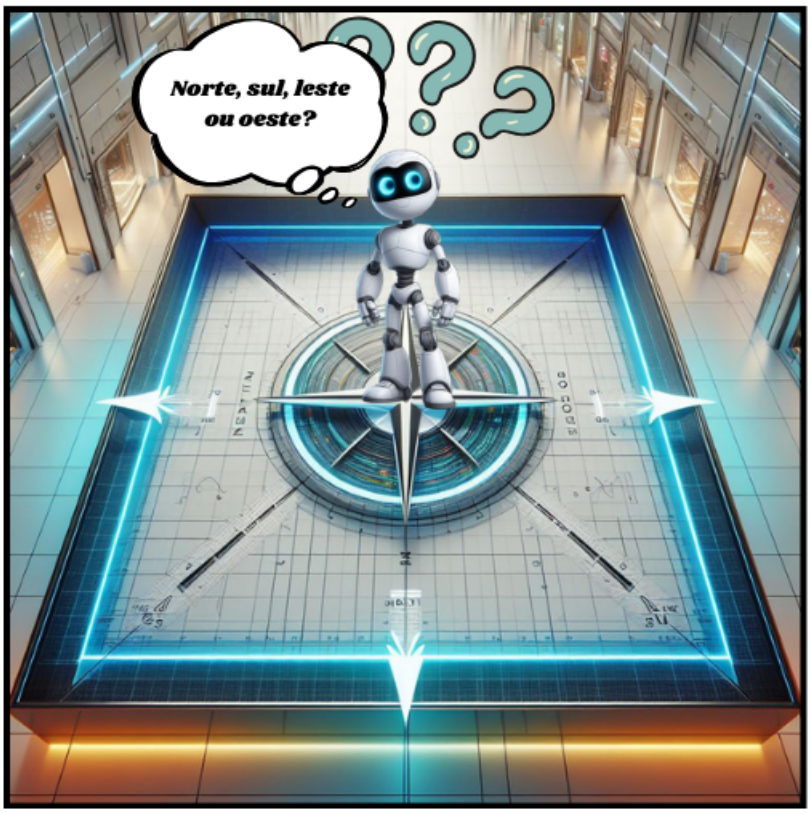
Disponível em https://pt.wikipedia.org/wiki/Voyager

Esses acontecimentos mostram de maneira significativa como a Teoria dos Códigos desempenha um papel importante na transmissão e representação precisa de informações.

4.2 ELEMENTOS ESSENCIAIS E MÉTRICA

Vamos utilizar um exemplo clássico para ilustrar essa teoria. Vamos imaginar um robô que se encontra no centro de um tabuleiro, aguardando o comando para qual lado ele deverá ir. Para controlar o movimento do robô, usamos quatro comandos via rádio: Leste, Oeste, Norte e Sul. Quando emitimos um desses comandos, o robô se move do centro do tabuleiro para a direção apontada, conforme indicado pelo comando.

Figura 14: Ilustração



Esses quatro comandos podem ser representados como elementos de um conjunto binário $\{0,1\} \times \{0,1\}$ da seguinte maneira:

- Oeste $\longmapsto$ 00
- Leste $\longmapsto$ 01
- Sul $\longmapsto$ 10
- Norte $\longmapsto$ 11.

Esta representação pré-codificada é chamada de código da fonte.

Agora, esses comandos são transmitidos via rádio, e ao longo do caminho, o sinal pode sofrer interferências. Considere a situação em que a mensagem “10” seja recebida como “11”, fazendo o robô se mover para o Norte em vez do Sul. Para prevenir erros desse tipo, introduzimos bits (dígitos) de redundâncias na codificação das palavras, possibilitando a detecção e correção de falhas na transmissão. O que fazemos é codificar as palavras pré-codificadas, adicionando redundâncias que permitem identificar e em alguns casos reparar os erros. Uma maneira de fazer isso é redefinir nosso código-fonte da seguinte forma:

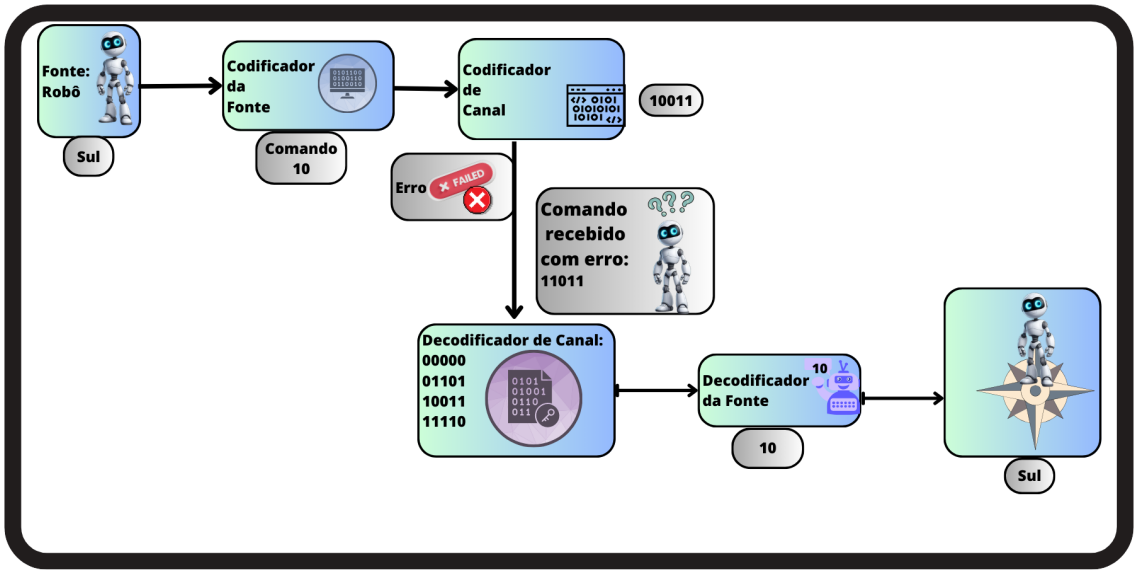
- 00 $\longmapsto$ 00000

- $01 \longmapsto 01101$
- $10 \longmapsto 10011$
- $11 \longmapsto 11110$

Nessa codificação, as duas primeiras posições repetem o código-fonte original, enquanto as três posições restantes representam 3 bits de redundâncias introduzidos. Esse novo código com as redundâncias é chamado de código de canal.

Em seguida, vamos considerar uma situação em que ocorra uma interferência, um ruído durante a transmissão. Por exemplo, a palavra 10011 seja transmitida incorretamente como 11011. Ao comparar a mensagem recebida com as palavras do código, identificamos que houve algum erro. A palavra-código mais próxima da mensagem recebida é 10011, que é exatamente a palavra originalmente transmitida.

Figura 15: Exemplo Esquematizado



Os elementos essenciais para a construção de um código são os seguintes:

- Um conjunto finito, denominado de alfabeto, representado por A.
- Sequências finitas compostas por símbolos pertencentes ao alfabeto, que são chamadas de palavras.
- O comprimento de uma palavra é determinado pelo número de símbolos que a compõem.

Definição 4.1. *Um código de bloco será um subconjunto $\mathcal{C} \subseteq A^n$ de palavras de mesmo comprimento n.*

Definição 4.2. *Um código q-ário é um código em que o alfabeto utilizado tem q elementos. Quando $q = 2$, o código é chamado de binário.*

Exemplo 4.3. *O conjunto $\mathcal{C} = \{(00000), (01101), (10011), (11110)\}$ é um código de bloco binário, de comprimento 5.*

Definição 4.4. *[5, p.14] Dado um conjunto X, uma métrica em X é uma função $d : X \times X \longrightarrow \mathbb{R}$ tal que para todo $x, y, z \in X$:*

1. *$d(x, y) \geq 0$ e $d(x, y) = 0$ se, e somente se, $x = y$;*
2. *$d(x, y) = d(y, x)$;*
3. *$d(x, y) \leq d(x, z) + d(z, y)$ (desigualdade triangular).*

Definição 4.5. *[5, p.19] Dados dois elementos $x, y \in A^n$, com $x = (x_1, x_2, \ldots, x_n)$ e $y = (y_1, y_2, \ldots, y_n)$, a distância de Hamming entre x e y é o número de coordenadas em que eles diferem, isto é:*

$$d_H(x, y) = \#\{i;\, x_i \neq y_i, 1 \leq i \leq n\}.$$

Também podemos escrever

$$d_H(x, y) = \sum_{i=1}^{n} d_H(x_i, y_i),$$

onde $d_H(x_i, y_i) = 0$, se $x_i = y_i$ e $d_H(x_i, y_i) = 1$, caso contrário.

Proposição 4.6. *[5, p.19] A distância de Hamming é de fato uma métrica em A^n.*

Demonstração. As duas primeiras condições decorrem imediatamente da definição. Para a desigualdade triangular, sejam $u = (u_1, u_2, \ldots, u_n)$, $v = (v_1, v_2, \ldots, v_n)$ e $w = (w_1, w_2, \ldots, w_n)$ elementos de A^n. Fixemos a i-ésima coordenada. Se $u_i = v_i = w_i$, para $1 \leq i \leq n$, temos, $d_H(u_i, v_i) = 0$, $d_H(u_i, w_i) = 0$ e $d_H(w_i, v_i) = 0$. Como, $0 \leq 0 + 0$, então $d_H(u_i, v_i) \leq d_H(u_i, w_i) + d_H(w_i, v_i)$. Agora, se $u_i \neq v_i$ e $u_i = w_i$ para algum $1 \leq i \leq n$, temos que $v_i \neq w_i$, $d_H(u_i, v_i) = 1$, $d_H(u_i, w_i) = 0$ e $d_H(w_i, v_i) = 1$. Como $1 \leq 0 + 1$, segue que $d_H(u_i, v_i) \leq d_H(u_i, w_i) + d_H(w_i, v_i)$.

Da mesma forma, se $u_i = v_i$ e $v_i \neq w_i$ para algum $1 \leq i \leq n$, temos que $u_i \neq w_i$, $d_H(u_i, v_i) = 0$, $d_H(u_i, w_i) = 1$ e $d_H(w_i, v_i) = 1$. Como $0 \leq 1 + 1$, então $d_H(u_i, v_i) \leq d_H(u_i, w_i) + d_H(w_i, v_i)$. Por fim, se $u_i \neq v_i$, $u_i \neq w_i$ e $v_i \neq w_i$ para algum $1 \leq i \leq n$, temos que $d_H(u_i, v_i) = 1$, $d_H(u_i, w_i) = 1$ e $d_H(w_i, v_i) = 1$. Como $1 \leq 1 + 1$, então $d_H(u_i, v_i) \leq d_H(u_i, w_i) + d_H(w_i, v_i)$.

Considerando todas as possibilidades descritas acima, temos que em qualquer caso

$$d_H(u_i, v_i) \leq d_H(u_i, w_i) + d_H(w_i, v_i).$$

Segue daí que

$$\begin{aligned} d_H(u,v) &= \sum_{i=1}^{n} d_H(u_i,v_i) \leq \sum_{i=1}^{n} \left(d_H(u_i,w_i) + d_H(w_i,v_i)\right) \\ &\leq \sum_{i=1}^{n} d_H(u_i,w_i) + \sum_{i=1}^{n} d_H(w_i,v_i) = d_H(x,w) + d_H(w,v). \end{aligned}$$

□

Um conceito que está fortemente relacionado à capacidade de correção de erros de um código na métrica de *Hamming* é o de distância mínima do código, que definiremos a seguir.

Definição 4.7. *[12, p.6] Sejam $\mathcal{C} \subseteq A^n$ um código e $d : A^n \times A^n \longrightarrow \mathbb{R}$ uma métrica. Chamamos de distância mínima de $\mathcal{C}$ o número:*

$$d(\mathcal{C}) = \min\{d(x,y);\, x,y \in \mathcal{C}, x \neq y\}.$$

Exemplo 4.8. *Dado o alfabeto $A = \{0,1\}$ e o código do robô $\mathcal{C} = \{00000, 01011, 10110, 11101\}$, temos que as distâncias de Hamming entre as palavras de $\mathcal{C}$ são:*

- $d_H(00000, 01011) = 3$
- $d_H(00000, 10110) = 3$
- $d_H(00000, 11101) = 4$
- $d_H(01011, 10110) = 4$
- $d_H(01011, 11101) = 3$
- $d_H(10110, 11101) = 3$.

Portanto, a distância mínima de $\mathcal{C}$ é $d_H(\mathcal{C}) = 3$.

4.3 RAIO DE EMPACOTAMENTO

Definição 4.9. *[5, p.15] Dados uma métrica d em X, $x \in X$ e um número $r > 0$, chamamos de esfera de raio r centrada em x na métrica d o conjunto*

$$S_d(x,r) = \{y \in X;\, d(x,y) \leq r\}.$$

Proposição 4.10. *[12, p.5] Sejam A um alfabeto q-ário e d_H a métrica de Hamming. Para todo $a \in A^n$ e todo número natural $r > 0$ temos que:*

$$\#S_{d_H}(a,r) = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i$$

Demonstração. Vamos empregar conceitos de combinatória para demonstrar a proposição. Nossa abordagem consistirá em calcular a quantidade de palavras que diferem um, dois, três, até r posições da palavra central a. Temos que:

- Para calcular todas as palavras que distam 1 de a, teremos a combinação de n posições tomadas 1 a 1, multiplicado por $(q-1)$ elementos, ou seja,

$$\binom{n}{1} \cdot (q-1) = n \cdot (q-1).$$

- Agora, para calcular todas as palavras que distam 2 de a, teremos a combinação de n posições tomadas 2 a 2, multiplicado por $(q-1) \cdot (q-1)$, ou seja, em cada uma dessas posições podemos trocar o elemento por $q-1$ outros. O número total de possibilidades é:

$$\binom{n}{2} \cdot (q-1) \cdot (q-1) = \binom{n}{2} \cdot (q-1)^2$$

- Da mesma forma, para calcular todas as palavras que distam 3 de a, teremos a combinação de n posições tomadas 3 a 3, multiplicado por $(q-1) \cdot (q-1) \cdot (q-1)$, ou seja,

$$\binom{n}{3} \cdot (q-1) \cdot (q-1) \cdot (q-1) = \binom{n}{3} \cdot (q-1)^3$$

$$\vdots$$

- Continuaremos a calcular até todas as palavras que estão a uma distância r de a. Teremos então a combinação de n posições tomadas r a r, multiplicado por $(q-1) \cdot (q-1) \cdots (q-1)$, ou seja,

$$\binom{n}{r} \cdot (q-1) \cdot (q-1) \cdot (q-1) \cdots (q-1) = \binom{n}{r} \cdot (q-1)^r$$

Agora, ao somarmos todos os resultados obtidos anteriormente, obtemos a seguinte expressão:

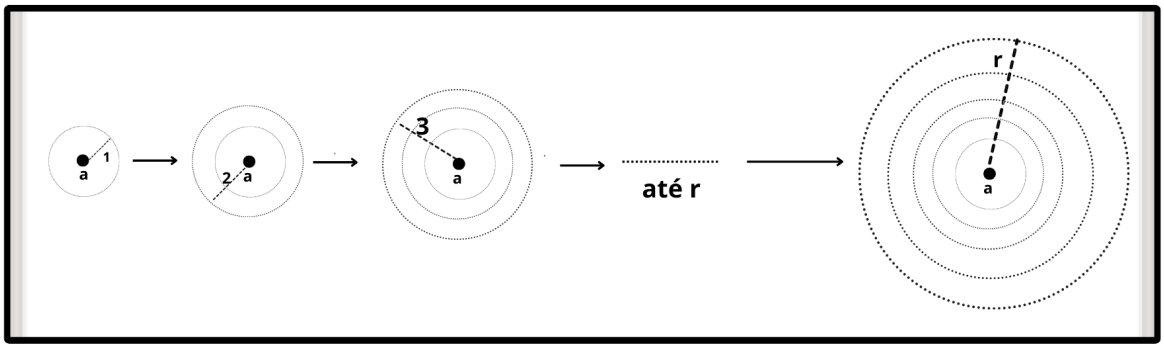
$$\binom{n}{1} \cdot (q-1) + \binom{n}{2} \cdot (q-1)^2 + \binom{n}{3} \cdot (q-1)^3 + \cdots + \binom{n}{r} \cdot (q-1)^r = \sum_{i=0}^{r} \binom{n}{i} \cdot (q-1)^i$$

Portanto,

$$\sum_{i=0}^{r} \binom{n}{i} (q-1)^i = \#S_{d_H}(a, r).$$

□

Figura 16: Ilustração da demonstração da Proposição 4.10



Observe que para calcular a cardinalidade $\#S_{d_H}(a,r)$ precisamos do comprimento do código, da quantidade de elementos do alfabeto e do raio.

Definição 4.11. *[5, p.24] Dado $w \in \mathbb{R}$, usamos $\lfloor w \rfloor$ e $\lceil w \rceil$ para denotar o maior inteiro menor ou igual a w e o menor inteiro maior ou igual a w, respectivamente.*

A próxima proposição irá auxiliar na demonstração da Proposição 4.13.

Proposição 4.12. *Seja d um inteiro. Se $k = \left\lfloor \frac{d-1}{2} \right\rfloor$, então $\left\lfloor \frac{d}{2} \right\rfloor \leq k+1$. Além disso, $d - \left\lfloor \frac{d}{2} \right\rfloor \leq k+1$.*

Demonstração. Temos dois casos para considerar:

- Se d for par, então $d = 2s$. Daí,

$$k = \left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{2s-1}{2} \right\rfloor = \left\lfloor s - \frac{1}{2} \right\rfloor = s-1,$$

  o que implica que

$$\left\lfloor \frac{d}{2} \right\rfloor = \left\lfloor \frac{2s}{2} \right\rfloor = \lfloor s \rfloor = s = k+1.$$

  Mais ainda,

$$d - \left\lfloor \frac{d}{2} \right\rfloor = 2s - s = s = k+1.$$

- Se d for ímpar, então $d = 2s+1$. Daí,

$$k = \left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{2s+1-1}{2} \right\rfloor = \left\lfloor \frac{2s}{2} \right\rfloor = s,$$

  o que implica que

$$\left\lfloor \frac{d}{2} \right\rfloor = \left\lfloor \frac{2s+1}{2} \right\rfloor = \left\lfloor s + \frac{1}{2} \right\rfloor = s = k < k+1.$$

Mais ainda,

$$d - \left\lfloor \frac{d}{2} \right\rfloor = 2s + 1 - s = s + 1 = k + 1.$$

□

Proposição 4.13. *[5, p.6] Sejam $\mathcal{C} \subset A^n$ um código e $d = d_H(\mathcal{C})$ a distância mínima de $\mathcal{C}$ na métrica de Hamming. Se*

$$k = \left\lfloor \frac{d-1}{2} \right\rfloor,$$

então $S_{d_H}(c,k) \cap S_{d_H}(c',k) = \emptyset$ para todo $c, c' \in \mathcal{C}$. Além disso, k é o maior inteiro com esta propriedade.

Demonstração. Se existisse $x \in S_{d_H}(c,k) \cap S_{d_H}(c',k)$, então teríamos pela desigualdade triangular que

$$d_H(c,c') \leq d_H(c,x) + d_H(x,c') \leq 2k.$$

Agora, notemos que

$$k = \left\lfloor \frac{d-1}{2} \right\rfloor \leq \frac{d-1}{2} \iff 2k \leq d-1.$$

Dessa forma,

$$d_H(c,c') \leq 2k \leq d-1 < d,$$

o que é uma contradição, pois d é a distância mínima de $\mathcal{C}$. Vamos mostrar agora que para o raio $k+1$ existem palavras c e c^* em $\mathcal{C}$ tais que $S_{d_H}(c,k+1) \cap S_{d_H}(c^*,k+1) \neq \emptyset$. Sejam $c = (c_1, \ldots, c_n)$ e $c^* = (c_1^*, \ldots, c_n^*)$ palavras de $\mathcal{C}$ tais que $d_H(c,c^*) = d$. Sem perda de generalidade, suponhamos que elas diferem nas d primeiras coordenadas. Seja

$$x = (c_1^*, \ldots, c_{\lfloor d/2 \rfloor}^*, c_{\lfloor d/2 \rfloor + 1}, \ldots, c_d, c_{d+1}, \ldots, c_n) \in A^n.$$

Temos que $d_H(x,c) = \lfloor \frac{d}{2} \rfloor \leq k+1$ e $d_H(x,c^*) = d - \lfloor \frac{d}{2} \rfloor \leq k+1$. Portanto,

$$x \in S_{d_H}(c,k+1) \cap S_{d_H}(c^*,k+1).$$

□

Exemplo 4.14. *O código do robô do Exemplo 4.8, que tem distância mínima $d = 3$, pode corrigir*

$$k = \left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{3-1}{2} \right\rfloor = 1 \text{ erro.}$$

4.4 CÓDIGOS PERFEITOS

Sejam $\mathcal{C} \subseteq A^n$ um código com distância de Hamming mínima $d = d_H(\mathcal{C})$ e

$$k = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Definição 4.15. *Sejam $\mathcal{C}$ um código com distância de Hamming mínima $d = d_H(\mathcal{C})$ e $k = \left\lfloor \frac{d-1}{2} \right\rfloor$. O código $\mathcal{C}$ é dito perfeito se ao traçarmos esferas de raio k com centro nas suas palavras-código, essas esferas são disjuntas e a união delas resulta no espaço todo.*

Exemplo 4.16. *Seja $\mathcal{C} = \{(00000), (01101), (10011), (11110)\}$ o código do robô. Temos que $d = 3$ e $k = [(3-1)/2] = 1$. Vamos verificar se este código é perfeito.*

Para isso, vamos calcular todas as palavras que estão no interior das bolas centradas nas palavras-código de $\mathcal{C}$. Temos o seguinte:

- $B_1[00000, 1] = \{00000, 00001, 00010, 00100, 01000, 10000\}$.
- $B_2[01101, 1] = \{01101, 01100, 01111, 01001, 00101, 11101\}$.
- $B_3[10011, 1] = \{10011, 10010, 10001, 10111, 11011, 00011\}$.
- $B_4[11110, 1] = \{11110, 11111, 11100, 11010, 10110, 01110\}$.

  Portanto, a união de todas essas bolas, isto é,

$$B_1[(00000, 1)] \bigcup B_2[(01101, 1)] \bigcup B_3[(10011, 1)] \bigcup B_4[(11110, 1)],$$

  contém um total de 24 palavras.

Como $\#\mathbb{Z}_2^5 = 2^5 = 32$ palavras, podemos concluir que o código do robô não é perfeito.

Exemplo 4.17. *Considerando ainda o exemplo do robô, vamos aumentar em uma unidade o raio das bolas. Para calcular a cardinalidade de cada bola:*

- *Para as palavras que distam 1 de cada palavra-código:*

$$\binom{5}{1}(2-1) = 5$$

- *Para as palavras que distam 2 de cada palavra-código, teremos:*

$$\binom{5}{2}(2-1)^2 = 10$$

Logo, o total de palavras em cada bola é $5 + 10 = 15$ *palavras mais a palavra-código, o que dá* 16 *palavras por bola. Como temos* 4 *bolas, se elas fossem disjuntas, daria um total de* 64 *palavras. Mas, o código tem um total de* 32 *palavras. Então com o raio igual a* 2*, as bolas se intersectam.*

5

CÓDIGOS LINEARES

Neste capítulo, assumimos que o leitor esteja familiarizado com os seguintes conceitos de Álgebra Linear: espaço vetorial, subespaço vetorial, bases e produto interno. Para um estudo sobre estes tópicos, sugerimos [2, 26]. A principal referência utilizada neste capítulo foi [12].

5.1 CÓDIGOS LINEARES SOBRE $\mathbb{Z}_p$, p PRIMO

Antes de falarmos de códigos lineares, lembremos que o espaço vetorial $\mathbb{Z}_p^n$, p primo, é constituído de todas as possíveis n-uplas sobre $\mathbb{Z}_p$. Além disso, qualquer subespaço vetorial de $\mathbb{Z}_p^n$ possui base sobre $\mathbb{Z}_p$.

Definição 5.1. *Sejam p primo e n um número inteiro positivo. Dizemos que um código de bloco $\mathcal{C} \subseteq \mathbb{Z}_p^n$ é linear se for um $\mathbb{Z}_p$-subespaço vetorial de $\mathbb{Z}_p^n$. Cada elemento de $\mathcal{C}$ é chamado de palavra-código.*

Definição 5.2. *Seja $\mathcal{C} \subseteq \mathbb{Z}_p^n$ um código linear.*

- *A cardinalidade de $\mathcal{C}$ é a quantidade de elementos de $\mathcal{C}$.*
- *A dimensão k de $\mathcal{C}$ é o número de vetores de uma base de $\mathcal{C}$ sobre $\mathbb{Z}_p$.*

Observação 5.3. *Dado um código linear $\mathcal{C}$, ou seja, um subespaço do espaço vetorial $\mathbb{Z}_p^n$, temos que o código $\mathcal{C}$ possui p^k vetores distintos, pois a sua dimensão é k.*

Exemplo 5.4. *Considere o espaço vetorial $\mathbb{Z}_2^5$ sobre $\mathbb{Z}_2$. Temos que o subespaço composto pelos vetores $\{(00000), (10011), (01101), (11110)\}$ define um código linear $\mathcal{C}$. Temos que o comprimento de $\mathcal{C}$ é 5 e a sua dimensão é 2, pois $\mathcal{C}$ tem como base sobre $\mathbb{Z}_2$ o conjunto $\{(10011), (01101)\}$.*

Definição 5.5. *[12, p.86] Seja $x = (x_1, \ldots, x_n) \in \mathbb{Z}_p^n$. Definimos o peso de x como sendo o número inteiro*

$$w(x) := \#\{i; x_i \neq 0\},$$

isto é, $w(x)$ é igual ao número de componentes não nulas na palavra-código x. O peso mínimo de um código $\mathcal{C}$, $w(\mathcal{C})$, é o menor peso de todas as palavras-código de $\mathcal{C}$, exceto a toda nula.

Exemplo 5.6. *Considere o seguinte código linear sobre* $\mathbb{Z}_2$ *dado por*

$$\mathcal{C} = \{(000000), (011011), (110110), (001110), (100011), (111000), (010101), (101101)\}.$$

Temos que os pesos de suas palavras-código são, respectivamente, $0, 4, 4, 3, 3, 3, 3$ *e* 4*. O peso mínimo de* $\mathcal{C}$ *é* $w = 3$*.*

Teorema 5.7. *Dado um código linear* $\mathcal{C} \subseteq \mathbb{Z}_p^n$*, temos que a distância mínima na métrica de Hamming corresponde ao seu peso mínimo, ou seja,* $d_H(\mathcal{C}) = w(\mathcal{C})$*.*

Demonstração. Temos que

$$min_{c_i,c_j \in C, i \neq j} d_H(c_i, c_j) = min_{c_i,c_j \in C, i \neq j} d_H(0, c_i - c_j) = min_{c \in C, c \neq 0} w(\mathcal{C}) = w(\mathcal{C}).$$

□

A partir do teorema anterior, pode-se concluir que, em um código do bloco linear $\mathcal{C}$, determinar a sua distância de Hamming mínima é, essencialmente, o mesmo que determinar seu peso mínimo.

5.2 MATRIZ GERADORA

Uma das principais características dos códigos lineares é sua representação matricial, que simplifica a aplicação prática.

Definição 5.8. *Seja* $\mathcal{C} \subseteq \mathbb{Z}_p^n$ *um código linear de dimensão* k*. Fixada uma base* $\{v_1, v_2, v_3, \ldots, v_k\}$ *de* $\mathcal{C}$ *sobre* $\mathbb{Z}_p$*, chamamos de matriz geradora de* $\mathcal{C}$ *a matriz* $G \in M_{k \times n}(\mathbb{Z}_p)$ *que contém nas suas linhas as coordenadas dos vetores* $v_1, v_2, v_3, \ldots, v_k$*, isto é,*

$$G = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & v_{13} & \cdots & v_{1n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ v_{k1} & v_{k2} & v_{k3} & \cdots & v_{kn} \end{pmatrix}.$$

Dado um código linear $\mathcal{C} \subseteq \mathbb{Z}_p^n$ com matriz geradora $G \in M_{k \times n}(\mathbb{Z}_p)$, temos que as palavras-código de $\mathcal{C}$ são obtidas como combinações lineares das linhas de G, isto é,

$$\mathcal{C} = \left\{ (x_1, \ldots, x_k) \cdot \begin{pmatrix} v_{11} & v_{12} & v_{13} & \cdots & v_{1n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ v_{k1} & v_{k2} & v_{k3} & \cdots & v_{kn} \end{pmatrix} ;\ (x_1, \ldots, x_k) \in \mathbb{Z}_p^k \right\}.$$

A escolha da matriz geradora depende da escolha da base.

Proposição 5.9. *[12, p.90] Duas matrizes geradoras de um mesmo código $\mathcal{C}$ podem ser obtidas uma da outra por meio das seguintes operações elementares nas linhas da matriz:*

- *Troca de linhas.*
- *Multiplicação de uma linha por um elemento não nulo do corpo $\mathbb{Z}_p$.*
- *Adição de qualquer múltiplo de uma linha à outra.*

Definição 5.10. *Dizemos que uma matriz geradora G de um código linear $\mathcal{C}$ está na forma sistemática se $G = [I_k \vdots P_{k\times(n-k)}]$ para alguma matriz $P \in M_{k\times(n-k)}(\mathbb{Z}_p)$.*

Notemos que se $G = [I_k \vdots P_{k\times(n-k)}]$ com $P = (p_{ij})$, $1 \leq i \leq k$, $1 \leq j \leq n-k$, então

$$(x_1, \ldots, x_k) \cdot G = \left(x_1, \ldots, x_k, \sum_{i=1}^{k} x_i p_{i1}, \ldots, \sum_{i=1}^{k} x_i p_{i(n-k)} \right).$$

Definição 5.11. *Seja $G = [I_k \vdots P_{k\times(n-k)}]$ para alguma matriz $P \in M_{k\times(n-k)}(\mathbb{Z}_p)$. Aos usarmos uma matriz geradora na forma sistemática para gerar um código, dizemos que a palavra-código contém k dígitos de informação e $n-k$ dígitos de paridade.*

Exemplo 5.12. *Considere $\mathbb{Z}_2 = \{0, 1\}$ e $\mathcal{C} \subset \mathbb{Z}_2^5$ o código linear com base $\beta = \{(01101), (10011)\}$ (código do robô). A matriz geradora G associada à base β é:*

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Vamos codificar o código da fonte do robô $\{(0,0), (0,1), (1,0), (1,1)\}$ usando a matriz G.

Para isso, devemos multiplicar cada código da fonte pela matriz G. Fazendo as contas:

- *Para a palavra-código $(0,0)$:*

$$\begin{pmatrix} 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

- *Para a palavra-código $(0,1)$:*

$$\begin{pmatrix} 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

- *Para a palavra-código* $(1,0)$*:*

$$\begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

- *Para a palavra-código* $(1,1)$*:*

$$\begin{pmatrix} 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Portanto, obtemos o código do canal do robô, que é

$$\mathcal{C} = \{(00000), (01101), (10011), (11110)\}.$$

Observando as palavras-código geradas, temos que os primeiros 2 *dígitos são herdados do código fonte e os* 3 *últimos são os dígitos de paridade.*

5.3 MATRIZ CONTROLE DE PARIDADE

Uma outra matriz importante associada a um código linear é a matriz controle de paridade, como veremos nesta seção.

Definição 5.13. *Dados* $x = (x_1, \ldots, x_n)$ *e* $y = (y_1, \ldots, y_n)$ *elementos de* $\mathbb{Z}_p^n$*, definimos o produto interno entre* x *e* y *como*

$$\langle x, y \rangle = x_1 y_1 + \cdots + x_n y_n.$$

Proposição 5.14. *[12, p.94] Seja* $\mathcal{C} \subseteq \mathbb{Z}_p^n$ *um código linear. O conjunto*

$$\mathcal{C}^{\perp} = \{x \in \mathbb{Z}_p^n;\ \langle x, c \rangle = 0,\ \forall c \in \mathcal{C}\}$$

é um subespaço vetorial de $\mathbb{Z}_p^n$*.*

Demonstração. Temos que $\mathcal{C}^{\perp} \neq \emptyset$, pois $0 \in \mathcal{C}^{\perp}$. Dados $x, y \in \mathcal{C}^{\perp}$, temos que $\langle x - y, c \rangle = \langle x, c \rangle - \langle y, c \rangle = 0 - 0 = 0$. Portanto, $x - y \in \mathcal{C}^{\perp}$. Agora, dados $x \in \mathcal{C}^{\perp}$ e $\lambda \in \mathbb{Z}_p$, temos que $\langle \lambda x, c \rangle = \lambda \langle x, c \rangle = \lambda \cdot 0 = 0$. Logo, $\lambda x \in \mathcal{C}^{\perp}$. Segue então que $\mathcal{C}^{\perp}$ é um subespaço vetorial. □

Definição 5.15. *Seja* $\mathcal{C}$ *um código linear sobre* $\mathbb{Z}_p$ *com comprimento* n*. O código* $\mathcal{C}^{\perp}$ *composto pelos vetores em* $\mathbb{Z}_p^n$ *que são ortogonais a todas as palavras-código de* $\mathcal{C}$ *é chamado de código dual.*

Proposição 5.16. *[12, p.94] Seja $\mathcal{C} \subseteq \mathbb{Z}_p^n$ um código linear com matriz geradora na forma sistemática $G = [I_k \vdots P_{k\times(n-k)}]$. Então, a dimensão de $\mathcal{C}^\perp$ é $n-k$.*

Demonstração. Se $x = (x_1, \ldots, x_k, x_{k+1}, \ldots, x_n) \in \mathcal{C}^\perp$, então $G \cdot x^t = 0$, ou seja,

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & p_{11} & p_{12} & \cdots & p_{1n-k} \\ 0 & 1 & 0 & \cdots & 0 & p_{21} & p_{22} & \cdots & p_{2n-k} \\ 0 & 0 & 1 & \cdots & 0 & p_{31} & p_{32} & \cdots & p_{3n-k} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & p_{k1} & p_{k2} & \cdots & p_{kn-k} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_k \\ x_{k+1} \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} x_1 + \sum_{j=1}^{n-k} p_{1j}x_{k+j} \\ \vdots \\ x_k + \sum_{j=1}^{n-k} p_{kj}x_{k+j} \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Segue daí que

$$\begin{bmatrix} x_1 \\ \vdots \\ x_k \end{bmatrix} = -P \begin{bmatrix} x_{k+1} \\ \vdots \\ x_n \end{bmatrix}.$$

Portanto, existe uma relação entre as coordenadas de x. A partir das coordenadas $x_{k+1}, \ldots, x_n$, é possível obter as coordenadas $x_1, \ldots, x_k$. Como temos p possibilidades para cada uma das coordenadas $x_{k+1}, \ldots, x_n$, temos que $\mathcal{C}^\perp$ possui p^{n-k} elementos. Logo, $\mathcal{C}^\perp$ possui dimensão $n-k$.

□

Definição 5.17. *Seja $\mathcal{C} \subseteq \mathbb{Z}_p^n$ um código linear. Chamamos de matriz controle de paridade do código $\mathcal{C}$ qualquer matriz geradora do código dual $\mathcal{C}^\perp$.*

Cada palavra-código c do código $\mathcal{C}$ é ortogonal a todos os vetores do código dual $\mathcal{C}^\perp$. Dessa forma, se G é uma matriz geradora de $\mathcal{C}$ e H é uma matriz geradora de $\mathcal{C}^\perp$, então

$$G \cdot H^t = 0,$$

onde H^t representa a matriz transposta de H.

Assim, a matriz controle de paridade simplifica o processo de determinar se um vetor é uma palavra-código ou não.

Definição 5.18. *[12, p.97] Dados um código $\mathcal{C}$ com matriz controle de paridade H e um vetor $v \in k^n$, chamaremos o vetor vH^t de síndrome de v.*

Exemplo 5.19. *Seja $\mathcal{C}$ um código linear sobre $\mathbb{Z}_2$ com matriz geradora*

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Temos que uma matriz controle de paridade H de $\mathcal{C}$ é dada por

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

e é uma matriz geradora do código dual $\mathcal{C}^{\perp}$. Sejam os vetores $u = (10010)$ e $v = (01101)$, temos que $uH^t = (01)$ e $vH^t = (00)$. Logo, v é uma palavra-código e u não.

O próximo teorema nos dá uma forma prática para determinar a matriz controle de paridade de um código.

Teorema 5.20. *[12, p.94] Seja $\mathcal{C} \subseteq \mathbb{Z}_p^n$ um código linear, com matriz geradora $G = (I_{k\times k} \vdots P_{k\times(n-k)})$ na forma sistemática. Então, uma matriz controle de paridade de $\mathcal{C}$ é dada por $H = ((-P^t)_{(n-k)\times k} \vdots I_{(n-k)\times(n-k)})$, onde P^t indica a transposta da matriz P.*

Demonstração. Por meio de cálculos diretos, temos que

$$G \cdot H^t = (I_{k\times k} \vdots P_{k\times(n-k)}) \begin{pmatrix} -P_{k\times(n-k)} \\ \cdots \\ I_{(n-k)\times(n-k)} \end{pmatrix} = -P_{k\times(n-k)} + P_{k\times(n-k)} = 0_{k\times(n-k)}.$$

Além disso, é fácil ver que as linhas de H são linearmente independentes. Portanto, $H = (-P^t \vdots I)$ é uma matriz controle de paridade de $\mathcal{C}$. □

Exemplo 5.21. *Seja $\mathcal{C}$ o código linear sobre $\mathbb{Z}_3$ com matriz geradora G, dada por*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Temos que uma matriz controle de paridade H de $\mathcal{C}$ é dada por

$$H = \begin{pmatrix} 0 & -1 & -1 & 1 & 0 & 0 \\ 0 & -2 & 0 & 0 & 1 & 0 \\ -2 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

O próximo teorema estabelece uma relação direta entre o peso mínimo de um código linear e uma matriz de controle de paridade associada dele.

Teorema 5.22. *[12, p.98] Seja $\mathcal{C}$ um código linear com matriz controle de paridade H. $\mathcal{C}$ contém uma palavra-código de peso de Hamming menor ou igual a w se, e somente se, existe uma relação de dependência linear de w colunas de H.*

Demonstração. Para toda palavra-código c, temos que $c \cdot H^t = 0$.

($\Longrightarrow$) Seja c uma palavra-código de peso w. Logo, c tem exatamente w entradas não nulas. Para facilitar a visualização, suponhamos que as w primeiras entradas de c sejam não nulas e as demais sejam nulas, isto é, $c = (c_1, \ldots, c_w, 0, \ldots, 0)$ com $c_i \neq 0$ para $i = 1, \ldots, w$. Fazendo a multiplicação $c \cdot H^t$, temos que

$$(c_1, \ldots, c_w, 0, \ldots, 0) \cdot \begin{bmatrix} h_{11} & h_{21} & h_{31} & \cdots & h_{(n-k)1} \\ h_{12} & h_{22} & h_{32} & \cdots & h_{(n-k)2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_{1n} & h_{2n} & h_{3n} & \cdots & h_{n(n-k)} \end{bmatrix}$$

$$= c_1 \begin{bmatrix} h_{11} \\ h_{12} \\ \vdots \\ h_{1n} \end{bmatrix} + c_2 \begin{bmatrix} h_{21} \\ h_{22} \\ \vdots \\ h_{2n} \end{bmatrix} + \cdots + c_w \begin{bmatrix} h_{w1} \\ h_{w2} \\ \vdots \\ h_{wn} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Portanto, existe uma relação de dependência linear de w colunas de H.

($\Longleftarrow$) Por outro lado, se H tem w colunas linearmente dependentes então uma combinação de w colunas de H é igual a zero. Para facilitar a visualização suponhas as primeiras w colunas de H linearmente dependentes. Logo, existem $c_1, \ldots, c_w \in \mathbb{Z}_p$ não todos nulos tais que

$$c_1 \begin{bmatrix} h_{11} \\ h_{12} \\ \vdots \\ h_{1n} \end{bmatrix} + c_2 \begin{bmatrix} h_{21} \\ h_{22} \\ \vdots \\ h_{2n} \end{bmatrix} + \cdots + c_w \begin{bmatrix} h_{w1} \\ h_{w2} \\ \vdots \\ h_{wn} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Seja $c = (c_1, \ldots, c_w, 0 \ldots, 0)$. Temos que $c \cdot H^t = 0$. Portanto, $c \in (\mathcal{C}^\perp)^\perp = \mathcal{C}$. Temos que $w(c) \leq w$. □

O próximo corolário de verificação imediata segue do teorema anterior.

Corolário 5.23. *[12, p.98] Um código tem peso mínimo maior ou igual do que w se, e somente se, quaisquer $w-1$ colunas de H são linearmente independentes.*

Demonstração. ($\Longrightarrow$) Se existissem $w-1$ colunas de H linearmente dependentes, existiria uma palavra-código de peso menor ou igual a w. Mas, isso não acontece, pois $w(C) \geq w$.

($\Longleftarrow$) Se existisse uma palavra-código de peso menor do que w, então existiriam $w-1$ colunas de H linearmente dependentes. Mas, isso não ocorre, pois quaisquer $w-1$ colunas são linearmente independentes.

□

Resumidamente, esse resultado estabelece uma relação fundamental entre o peso mínimo de um código linear e as colunas da matriz controle de paridade.

6

CÓDIGOS DE HAMMING BINÁRIOS

Os códigos de Hamming binários constituem uma classe de códigos lineares com distância de Hamming mínima igual a 3, ou seja, são capazes de corrigir um erro. A sua construção é feita através da matriz controle de paridade e é baseada na distância mínima. Como referência para este capítulo utilizamos [12].

A construção de códigos de Hamming se baseia no fato de que um código tem peso mínimo maior ou igual do que w se, e somente se, quaisquer $w-1$ colunas de H são linearmente independentes. (Corolário 5.23). Como os códigos de Hamming possuem distância mínima igual a 3, é necessário que as colunas de sua matriz controle de paridade sejam duas a duas linearmente independentes e que existam 3 linearmente dependentes.

6.1 CONSTRUÇÃO

O processo para se construir um código de Hamming binário é:

- Considere $m \geq 2$ um número natural.
- Seja H a matriz controle de paridade a ser obtida. H possuirá m linhas, ou seja, cada coluna de H terá m dígitos.
- Sobre $\mathbb{Z}_2$ existem 2^m possíveis m-uplas distintas. Consideremos apenas as $2^m - 1$ m-uplas não nulas.
- Como estas m-uplas binárias não nulas são duas a duas distintas, temos que nenhuma é múltipla da outra, sendo assim duas a duas são linearmente independentes.
- Cada coluna da matriz H é preenchida com uma destas m-uplas não nulas, até que todas sejam utilizadas. Para fazer isso, podemos deixar as colunas que formam a matriz identidade por último e assim facilitar o cálculo de uma matriz geradora.
- Obtemos uma matriz com m linhas (linearmente independentes) e $2^m - 1$ colunas que atua como matriz controle de paridade para um código de Hamming.
- A partir da matriz controle de paridade, podemos obter uma matriz geradora.

Com base nessa construção, temos:

- Todo código de Hamming binário possui comprimento igual a $2^m - 1$.
- A dimensão de tais códigos é dada por

$$k = 2^m - 1 - m.$$

De fato, ao considerarmos a matriz controle de paridade H de um código de Hamming binário, podemos afirmar que suas linhas formam um conjunto linearmente independente. Dentre as colunas de H, existem m que formam uma matriz identidade. Sem perda de generalidade, suponhamos que H esteja descrita da seguinte forma:

$$H = \begin{pmatrix} h_{1,1} & h_{1,2} & \dots & h_{1,2^m-1-m} & 1 & 0 & \dots & 0 \\ h_{2,1} & h_{2,2} & \dots & h_{2,2^m-1-m} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ h_{m,1} & h_{m,2} & \dots & h_{m,2^m-1-m} & 0 & 0 & \dots & 1 \end{pmatrix}$$

Portanto, não existe uma combinação linear das linhas de H com coeficientes em $\mathbb{Z}_2$ que resulte no vetor todo nulo.

- A distância mínima de um código de Hamming binário é

$$d = 3$$

e sua capacidade de correção de erros é

$$t = 1.$$

Por construção, quaisquer duas colunas de H são linearmente independentes. Além disso, existem 3 colunas linearmente dependentes.

Exemplo 6.1. *Considere $m = 3$. Obteremos um código de Hamming binário com parâmetros iguais a: comprimento $n = 2^3 - 1 = 7$ e dimensão $k = 2^3 - 1 - 3 = 4$. Uma matriz controle de paridade para tal código é dada por:*

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Uma matriz geradora é:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Vale observar que todo par de colunas de H é linearmente independente e que alguns conjuntos de três colunas são linearmente dependentes, como, por exemplo, a primeira, segunda e última coluna, ou ainda, segunda, terceira e quarta coluna.

Exemplo 6.2. *Considere $m = 4$. Assim temos que os parâmetros de $\mathcal{C}$ são: $n = 2^4 - 1 = 15$ e $k = 2^4 - 1 - 4 = 11$. A matriz controle de paridade de um código de Hamming sobre $\mathbb{Z}_2$ com comprimento $n = 15$ e dimensão $k = 11$ é dada por:*

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Vale observar que todo par de colunas de H é linearmente independente, isto acontece porque não existe um par de colunas binárias de H que dê como resultado de sua soma o valor zero. Observamos também que alguns conjuntos de três colunas são linearmente dependentes, como, por exemplo a primeira, a segunda e a quinta coluna. Assim, a distância mínima é 3.

Exemplo 6.3. *Vamos implementar um código fonte binário para um robô com a funcionalidade dele se mover para leste, oeste, norte e sul e levantar o braço direito e o braço esquerdo. Uma possibilidade de código fonte é:*

- *oeste com o braço direito levantado:* 0011.
- *oeste com o braço esquerdo levantado:* 0010.
- *leste com o braço direito levantado:* 0111.
- *leste com o braço esquerdo levantado:* 0110.
- *sul com o braço direito levantado:* 1011.
- *sul com o braço esquerdo levantado:* 1010.
- *norte com o braço direito levantado:* 1111.
- *norte com o braço esquerdo levantado:* 1110.

Agora, vamos implementar o código de canal usando o código de Hamming de comprimento 7. Para isso, vamos pegar a matriz geradora

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

do Exemplo 6.1 e multiplica cada palavra do código fonte por ela.

Por exemplo, a palavra 1110 *será codificada como a palavra-código* 1110010*, pois*

$$(1\,1\,1\,0) \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} = (1\,1\,1\,0\,0\,1\,0).$$

Palavra do Código de Fonte	Palavra-código do Código de Canal
0011	0011110
0010	0010011
0111	0111000
0110	0110101
1011	1011001
1010	1010100
1111	1111111
1110	1110010

Tabela 14: Código de Fonte e Código de Canal

Teorema 6.4. *[12, p.100] Os códigos de Hamming binários são códigos perfeitos.*

Demonstração. Considere um código de Hamming binário de comprimento $n = 2^m - 1$ e dimensão $k = 2^m - 1 - m$. Os códigos de Hamming binários são capazes de corrigir um erro. Desta forma, as esferas de raio 1 ao redor de cada palavra-código são disjuntas. Considere a esfera centrada na origem. Temos que existem $n + 1$ vetores nesta esfera. Como toda esfera ao redor de cada palavra-código é uma translação da esfera centrada na origem, temos que existem $n + 1$ vetores em cada esfera de raio 1. Como o número de esferas é igual ao número

de palavras-código, temos que existem 2^k esferas. Multiplicando o número de esferas pela quantidade de vetores que cada uma possui, obtemos

$$2^k \cdot (n+1) = 2^k \cdot (2^m - 1 + 1) = 2^k \cdot 2^m = 2^{2^m - 1 - m + m} = 2^{2^m - 1} = 2^n,$$

que corresponde ao número total de vetores de espaço vetorial. Assim, como todo vetor de comprimento n está em uma destas esferas, temos que o código é perfeito. □

6.2 DECODIFICAÇÃO

A seguir vamos apresentar um algoritmo de decodificação de um erro para códigos de Hamming binário. Seja H a matriz controle de paridade do código $\mathcal{C}$ e seja r uma palavra recebida com no máximo um erro. Vamos proceder da seguinte forma:

- Devemos calcular $H \cdot r^t$.
- Se $H \cdot r^t$ for igual a zero, então podemos afirmar que o vetor r pertence ao código $\mathcal{C}$. Caso contrário, ocorreu um erro.
- Definimos o vetor erro com $e = r - c$, onde c é a palavra código enviada. Observamos que:
$$H \cdot e^t = H \cdot (r-c)^t = H \cdot r^t - H \cdot c^t = H \cdot r^t.$$
- Como estamos supondo que ocorreu apenas um erro, e possuirá apenas uma entrada não nula, isto é, $e = (0, 0, \ldots, 0, 1, \ldots, 0)$, com 1 na i-ésima posição onde ocorreu o erro.
- Se $H \cdot e^t = H \cdot r^t$, então $H \cdot r^t$ resulta na i-ésima coluna de H. De fato,
$$\begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1i} & \cdots & v_{1n} \\ h_{21} & h_{22} & \cdots & h_{2i} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ h_{m1} & h_{m2} & \cdots & h_{mi} & \cdots & v_{mn} \end{pmatrix} \cdot \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} h_{1i} \\ h_{2i} \\ \vdots \\ h_{mi} \end{pmatrix}.$$
- Sabendo que o erro ocorreu na i-ésima posição, se o valor for 0 trocamos por 1 e se for 1 trocamos por 0.

Exemplo 6.5. *Consideremos código de Hamming do Exemplo 6.2 com matriz controle de paridade*

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Seja $r = (1\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 1)$ *o vetor recebido. Temos que*

$$s = H \cdot r^t = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix},$$

que corresponde a $8^{\underline{a}}$ *coluna da matriz* H*, ou seja, o erro em* r *ocorreu na* $8^{\underline{a}}$ *posição. Portanto, o vetor enviado é* $v = (1\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1)$.

7

PROPOSTA DIDÁTICA

Como proposta didática, criamos um história em quadrinhos direcionada a alunos dos anos iniciais do ensino fundamental II que propõe atividades explorando os conceitos de códigos, criptografia e dígitos verificadores. A intenção é que os alunos percebam a relevância de aprender, revisar, resgatar e reforçar determinados conceitos, como potenciação, divisão e se engajem nas atividades propostas.

A história em quadrinhos foi desenvolvida na Plataforma Canva de onde algumas imagens foram extraídas. Outras imagens de personagens foram geradas com o auxílio da ferramenta *Big Creator Image*. Além disso, imagens de planetas e sonda espacial foram obtidas dos sites da Wikipedia e da Nasa.

A história em quadrinhos pode ser acessada clicando no link https://heyzine.com/flip-book/82d5ab0324.html ou pode ser visualizada no Apêndice A. A seguir descrevemos as atividades contidas no material.

7.1 ATIVIDADE 1: O DESAFIO DA PORTA E A CIFRA DE CÉSAR

Nesta atividade, os alunos serão levados a compreender o funcionamento da Cifra de César e a praticar a decodificação de mensagens utilizando esse método criptográfico. Os objetivos específicos são:

- Compreender o funcionamento da Cifra de César.
- Praticar a decodificação de mensagens utilizando a Cifra de César.
- Desenvolver habilidades no cálculo lógico e matemático para decifrar mensagens.
- Promover a colaboração e o trabalho em equipe na resolução de problemas e desafios.
- Estimular o interesse e a curiosidade dos alunos pela Matemática.

Estes objetivos têm como foco não só a compreensão da Cifra de César em si, mas também o desenvolvimento das habilidades matemáticas e de lógica dos estudantes.

A atividade começa com os alunos descobrindo o deslocamento, que é de 5 posições. Em seguida, os alunos terão decodificar uma mensagem. Para isso, eles podem construir a tabela

apresentada a seguir, ou seguir a sugestão do livro e fazer os anéis concêntricos. A escolha de qual método utilizar fica a cargo do professor.

ALFABETO	CRIPTOGRAFADO	ALFABETO	CRIPTOGRAFADO
a	F	n	S
b	G	o	T
c	H	p	U
d	I	q	V
e	J	r	W
f	K	s	X
g	L	t	Y
h	M	u	Z
i	N	v	A
j	O	w	B
k	P	x	C
l	Q	y	D
m	R	z	E

Tabela 15: Cifra de César

A mensagem codificada no livro é: **ATHJX JXYFT UWJUFWFIFX UFWF NSNHNFW ZRF JRTHNTSFSYJ ANFLJR WZRT F IJXAJSIFW TX JSNLRFX IT ZSNAJWXT ITX HTINLTX? JSYFT INLIYJ XNR!**

A mensagem decodificada é: **Vocês estão preparadas para iniciar uma emocionante viagem rumo a desvendar os enigmas do universo dos códigos? Então digite SIM!**

Esta atividade está alinhada com a competência específica 1 de Matemática da BNCC que diz:

> Reconhecer que a Matemática é uma ciência humana, fruto das necessidades e preocupações de diferentes culturas, em diferentes momentos históricos, e é uma ciência viva, que contribui para solucionar problemas científicos e tecnológicos e para alicerçar descobertas e construções, inclusive com impactos no mundo do trabalho. [1, p.267]

E nesta atividade podemos citar ainda a competência específica 2 da BNCC.

> Desenvolver o raciocínio lógico, o espírito de investigação e a capacidade de produzir argumentos convincentes, recorrendo aos conhecimentos matemáticos para compreender e atuar no mundo. [1, p.267]

Essa atividade não apenas introduz os alunos ao conceito de criptografia, mas também os envolve em práticas que estimulam o raciocínio lógico e a capacidade de investigação. Além disso, ao proporcionar diferentes formas de decodificar a mensagem, como a construção de tabelas ou o uso de anéis concêntricos, o professor promove a autonomia e a criatividade dos estudantes na resolução de problemas.

Portanto, essa atividade não apenas cumpre com os objetivos específicos da Cifra de César, mas também contribui para o desenvolvimento de habilidades essenciais de pensamento crítico e lógico, alinhadas com as competências da BNCC em Matemática.

7.2 ATIVIDADES 2 E 3: DECIFRANDO MENSAGENS PELA CIFRA DE SUBSTITUIÇÃO SIMPLES

Nessas atividades, os alunos serão levados a compreender o funcionamento da Cifra de Substituição Simples e a praticar a decodificação de mensagens. Os objetivos específicos são:

- Compreender o funcionamento da Cifra de Substituição Simples primeiro utilizando a palavra-chave, e na mensagem seguinte utilizando somente a frequência das letras e as estruturas das palavras.
- Praticar a decodificação de mensagens utilizando a Cifra de Substituição Simples.
- Comparar números racionais.
- Ordenar números em ordem decrescente.
- Interpretar gráficos e tabelas.
- Desenvolver habilidades no cálculo lógico e matemático para decifrar mensagens.
- Promover a colaboração e o trabalho em equipe na resolução de problemas e desafios.
- Estimular o interesse e a curiosidade dos alunos pela Matemática.

Consideremos a primeira mensagem codificada: **FBC KMWB GE KELMKELWIE SBIM MJIBJLCECE AMCCEKMJLEV FECE GMVSMJGEC BV IBGWTBV! VXIMVVB!**

Para decodificá-la, primeiro vamos construir uma tabela, onde na primeira linha devemos colocar as letras do alfabeto em ordem alfabética e na segunda linha começar com a palavra-chave. Neste caso, a palavra-chave será ENIGMA.

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
E	N	I	G	M	A																				

Tabela 16: Alfabeto com a palavra-chave

Vamos construir uma tabela com a mensagem codificada e substituir na mensagem codificada o E pelo a, N pelo b, o I pelo c, o G pelo d e o A pelo f. Aos alunos então tentarão descobrir as demais letras levando em conta apenas palavras conhecidas da língua portuguesa.

F	B	C		K	M	W	B		G	E		K	E	L	M	K	E	L	W	I	E
					E				D	A			A		E		A			C	A
S	B	I	M		M	J	I	B	J	L	C	E	C	E		A	M	C	C	E	-
		C	E		E		C					A		A		F	E			A	
K	M	J	L	E	V		F	E	C	E		G	M	V	S	M	J	G	E	C	
	E			A				A		A		D	E			E		D	a		
B	V		I	B	G	W	T	B	V!		V	X	I	M	V	V	B!				
			C		D								C	E							

Tabela 17: Mensagem com as substituições das letras da palavra-chave

Agora, analisando a estrutura das palavras na língua portuguesa, e com o auxílio do professor dando dicas, é possível decifrar a palavra **KELMKELWIE** como **Matemática**. Assim, descobrimos mais algumas letras e as substituímos em ambas as tabelas. Repetindo esse processo sucessivamente, conseguimos decifrar a mensagem inteira (Tabela 18 e Tabela 19)

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
E	N	I	G	M	A	T	Y	W	Q	U	O	K	J	B	F	Z	C	V	L	X	S
w	x	y	z																		
D	P	R	H																		

Tabela 18: Alfabeto com a palavra-chave

F	B	C		K	M	W	B		G	E		K	E	L	M	K	E	L	W	I	E
P	o	r		m	e	i	o		d	a		M	a	t	e	m	á	t	i	c	a
S	B	I	M		M	J	I	B	J	L	C	E	C	E		A	M	C	C	E	-
v	o	c	e		e	n	c	o	n	t	r	a	r	á		f	e	r	r	a	-
K	M	J	L	E	V		F	E	C	E		G	M	V	S	M	J	G	E	C	
m	e	n	t	a	s		p	a	r	a		d	e	s	v	e	n	d	a	r	
B	V		I	B	G	W	T	B	V!		V	X	I	M	V	V	B!				
o	s		c	o	d	i	g	o	s!		S	u	c	e	s	s	o!				

Tabela 19: Mensagem decifrada com palavra-chave

Portanto, a mensagem decodificada é: **Por meio da Matemática, você encontrará ferramentas para decifrar os códigos! Sucesso!**

Após a realização da atividade, é importante chamar a atenção dos alunos que precisamos de mais ferramentas, pois nem sempre conseguiremos acertar alguma palavra codificada com base no conhecimento de uma palavra-chave apenas.

Na atividade seguinte, vamos trabalhar com a contagem e comparação de números para verificar qual letra tem mais frequência.

A mensagem codificada é: **AJDFKCLO DWLFZCLFDO CD DYKBUZO D UKOGDFKLO,YZL CDOKOGZU CKZYGD CLO SFLTIDUZO, ODMZU BJDFFDKFLO ZSIKEZCLO! SZFZTDYO, DYKBUZ CDEKVFZCL ELU L UZKL FOJEDOOL, UZKO JU CDOLVKLELYEIJKCL D OJSDFZCL! ZBLFZ, FJUL ZL SFLWK UL CDOZVKL SZFZ ELYAJKOGZF Z DYG FZCZ YZ OZIZ ODE FDGZ D CDEKVFZF ODJ O ODBFDCLO. SCFGD CZ ODYNZ ODEFDGZ: JNJJ_UJKGGLLIDZIIII _OEFHSGGLYYKYYMZ_YYKYYMZLUZKLF**.

Primeiro, vamos contar quantas vezes cada letra do alfabeto aparece na mensagem codificada e colocar essa informação em uma tabela:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
2	5	18	34	11	25	12	1	9	13	22	32	3	2	30	0	0	0	8	2	14	S
w	x	y	z																		
4	0	18	38																		

Tabela 20: Quantidade de vezes que cada letra aparece na mensagem codificada

Ao analisar a Tabelas 20, identificamos que a letra mais frequente é o Z. As letras aparecem em ordem decrescente de frequência conforme listadas: Z, D, L, O, F, K, Y, C, U, J, G, E, I, S, B, V, M, W, T, N, A, H.

Agora, analisando a Tabela 11 e o gráfico de frequências 2, temos que a letra A é a letra mais frequente na língua portuguesa, seguida pela letra E. Portanto, substituiremos o Z na mensagem codificada pela letra A e o D pela letra E. Vamos continuar esse processo até a letra C, pois na atividade é dito que a mensagem codificada respeita a frequência das letras em ordem decrescente até a letra C. Neste caso, podemos fazer as seguintes substituições:

Z	D	L	O	F	K	Y	C	U	J	G	E	I	S	B	V	M	W	T	N	A	H
a	e	o	s	r	i	n	d	m	u	t	c										

Tabela 21: Letras decifradas

Depois disso, tentaremos decifrar alguma palavra para encontrar as demais letras.

A	J	D	F	K	C	L	O		D	W	L	F	Z	C	L	F	D	O	C	D	
	u	e	r	i	d	o	s		e				o	r	a	d	o	r	e	s	
C	D		D	Y	K	B	U	Z	O		D		U	K	O	G	D	F	k	L	O
d	e		e	n	i		m	a	s		e		m	i	s	t	e	r	i	o	s
Y	Z	L		C	D	O	K	O	G	Z	U		C	K	Z	Y	G	D			
n	a	o		d	e	s	i	s	t	a	m		d	i	a	n	t	e			
C	L	O		S	F	L	T	I	D	U	Z	O		O	D	M	Z	U			
d	o	s			r	o			e	m	a	s		s	e		a	m			
B	J	D	F	F	D	K	F	L	O		Z	S	I	K	E	Z	C	L	O		
	u	e	r	r	e	i	r	o	s		a			i	c	a	d	o	s		
S	Z	F	Z	T	D	Y	S		D	Y	K	B	U	Z		C	D	E	K	-	
	a	r	a		e	n	s		e	n	i		m	a		d	e	c	i		
V	F	Z	C	L		E	L	U		L		U	Z	K	L	F		O	J	-	
	r	a	d	o		c	o	m		o		m	a	i	o	r		s	u	-	
E	D	O	O	L		U	Z	K	O		J	U		C	D	O	L	V	K	L	
c	e	s	s	o		m	a	i	s		u	m		d	e	s	a		i	o	
E	L	Y	E	I	J	K	C	L		D		O	J	S	D	F	Z	C	L		Z
c	o	n	c		u	i	d	o		e		s	u		e	r	a	d	o		a
B	L	F	Z		F	J	U	L		Z	L		S	F	L	W	K	U	L		
	o	r	a		r	u	m	o		a	o			r	o		i	m	o		
C	D	O	Z	V	K	L		S	Z	F	Z		E	L	Y	A	J	K	O		-
d	e	s	a		i	o		p	a	r	a		c	o	n		u	i	s		-
G	Z	F		Z		D	Y	G	F	Z	C	Z		Y	Z		O	Z	I	Z	
t	a	r		a		e	n	t	r	a	d	a		n	a		s	a		a	
O	D	E	F	D	G	Z		D		C	D	E	K	V	F	Z	F				
s	e	c	r	e	t	a		e		d	e	c	i		r	a	r				
O	D	J	O		O	D	B	F	D	C	L	O		S	Z	F	G	D		C	Z
s	e	u	s		s	e		r	e	d	o	s			a	r	t	e		d	a
O	D	Y	N	Z		O	D	E	F	D	G	Z	:								
s	e	n	h	a		s	e	c	r	e	t	a	:								
J	N	J	J	_	U	J	K	G	G	L	L	I	D	B	Z	I	I	I	I	_	
u		u	u	_	m	u	i	t	t	o	o		e		a					_	
O	E	F	H	S	G	G	L	Y	Y	K	Y	Y	M	Z	_	Y	Y	K	Y	Y	
s	c	r			t	t	o	n	n	i	n	n		a	_	n	n	i	n	n	
M	Z	L	U	Z	K	L	F														
	a	o	m	a	i	o	r														

Tabela 22: Mensagem com as substituições da Tabela 10

Por exemplo, apareceu a palavra “UERIDOS” após as substituições, podemos deduzir que o A representa a letra Q, pois essa letra é comum antes das letras UE seguidas.

Vamos continuar analisando a mensagem para identificar mais padrões e fazer as substituições necessárias para completar as palavras.

A	J	D	F	K	C	L	O		D	W	L	F	Z	C	L	F	D	O	C	D	
Q	u	e	r	i	d	o	s		e	x	p	l	o	r	a	d	o	r	e	s	
C	D		D	Y	K	B	U	Z	O		D		U	K	O	G	D	F	k	L	O
d	e		e	n	i	g	m	a	s		e		m	i	s	t	e	r	i	o	s
Y	Z	L		C	D	O	K	O	G	Z	U		C	K	Z	Y	G	D			
n	a	o		d	e	s	i	s	t	a	m		d	i	a	n	t	e			
C	L	O		S	F	L	T	I	D	U	Z	O		O	D	M	Z	U			
d	o	s		p	r	o	b	l	e	m	a	s		s	e	j	a	m			
B	J	D	F	F	D	K	F	L	O		Z	S	I	K	E	Z	C	L	O		
g	u	e	r	r	e	i	r	o	s		a	p	l	i	c	a	d	o	s		
S	Z	F	Z	T	D	Y	S		D	Y	K	B	U	Z		C	D	E	K	-	
p	a	r	a	b	e	n	s		e	n	i	g	m	a		d	e	c	i		
V	F	Z	C	L		E	L	U		L		U	Z	K	L	F		O	J	-	
f	r	a	d	o		c	o	m		o		m	a	i	o	r		s	u	-	
E	D	O	O	L		U	Z	K	O		J	U		C	D	O	L	V	K	L	
c	e	s	s	o		m	a	i	s		u	m		d	e	s	a	f	i	o	
E	L	Y	E	I	J	K	C	L		D		O	J	S	D	F	Z	C	L		Z
c	o	n	c	l	u	i	d	o		e		s	u	p	e	r	a	d	o		a
B	L	F	Z		F	J	U	L		Z	L		S	F	L	W	K	U	L		
g	o	r	a		r	u	m	o		a	o		p	r	o	x	i	m	o		
C	D	O	Z	V	K	L		S	Z	F	Z		E	L	Y	A	J	K	O		-
d	e	s	a	f	i	o		p	a	r	a		c	o	n	q	u	i	s		-
G	Z	F		Z		D	Y	G	F	Z	C	Z		Y	Z		O	Z	I	Z	
t	a	r		a		e	n	t	r	a	d	a		n	a		s	a	l	a	
O	D	E	F	D	G	Z		D		C	D	E	K	V	F	Z	F				
s	e	c	r	e	t	a		e		d	e	c	i	f	r	a	r				
O	D	J	O		O	D	B	F	D	C	L	O		S	Z	F	G	D		C	Z
s	e	u	s		s	e	g	r	e	d	o	s		p	a	r	t	e		d	a
O	D	Y	N	Z		O	D	E	F	D	G	Z	:								
s	e	n	h	a		s	e	c	r	e	t	a	:								
J	N	J	J	_	U	J	K	G	G	L	L	I	D	B	Z	I	I	I	I	_	
u	h	u	u	_	m	u	i	t	t	o	o	l	e	g	a	l	l	l	l	_	
O	E	F	H	S	G	G	L	Y	Y	K	Y	Y	M	Z	_	Y	Y	K	Y	Y	
s	c	r	y	p	t	t	o	n	n	i	n	n	j	a	_	n	n	i	n	n	
M	Z	L	U	Z	K	L	F														
j	a	o	m	a	i	o	r														

Tabela 23: Mensagem decifrada - sem palavra-chave

A mensagem decodificada é: **Queridos exploradores de enigmas e mistérios, não desistam diante dos problemas, sejam guerreiros aplicados! Parabéns, enigma decifrado com o maior sucesso, mais um desafio concluído e superado! Agora, rumo**

ao próximo desafio para conquistar a entrada na sala secreta e decifrar seus segredos. Parte da senha secreta: uhuu_muittoolegallll_scrypttonninnja_nninnjaomaior.

Após a realização desta atividade, o professor deve observar que quanto maior for o texto, mais a frequência das letras de aproximará da frequência da Tabela 11. No caso da atividade em sala de aula não é factível trabalhar com um texto muito longo.

Estas atividades estão alinhadas não apenas com a competência específica 1, que destaca a importância de identificar os conhecimentos matemáticos como meios para compreender e atuar no mundo, mas também com a competência específica 2 da BNCC. Esta última ressalta a importância da Matemática como uma ferramenta não apenas para o desenvolvimento de habilidades cognitivas, mas também para a resolução de problemas complexos e a promoção do avanço científico e tecnológico.

Ao aplicar atividades que envolvem a compreensão da Cifra de Substituição Simples e a prática de decodificação de mensagens, os alunos têm a oportunidade de explorar a Matemática de maneira prática e contextualizada, desenvolvendo não apenas habilidades numéricas, mas também a capacidade de resolver problemas.

Além disso, as atividades também estão de acordo com as habilidades específicas da BNCC, conforme os códigos EF06MA01 e EF06MA02. Essas habilidades se concentram no sistema de numeração decimal, incluindo suas características, leitura, escrita e comparação de números naturais. Essa conexão entre a atividade proposta e as competências e habilidades da BNCC demonstra a relevância e o alinhamento pedagógico para o desenvolvimento dos estudantes no campo da Matemática.

7.3 ATIVIDADE 4: CRIVO DE ERATÓSTENES

O objetivo da construção do Crivo de Eratóstenes é encontrar todos os números primos até um determinado limite de forma sistemática. Esse método antigo, atribuído ao matemático grego Eratóstenes, permite identificar os números primos de maneira prática.

O processo envolve marcar os números a partir de 2 até o limite estabelecido e, em seguida, eliminar os múltiplos de cada número primo encontrado, pois esses não serão números primos e sim números compostos. Ao final do processo, os números não marcados são os primos dentro do intervalo.

Os objetivos específicos desta atividade são:

- Encontrar os números primos.
- Aplicar o conceito de múltiplos de 2, 3 e 5 para facilitar a identificação dos números primos.
- Compreender o conceito de números primos e números compostos e saber diferenciá-los.

- Entender como encontrar números primos a partir do Crivo de Eratóstenes.

Vamos seguir as instruções do *e-book*:
Instruções para calcular todos os primos menores do que 100:

- Primeiro risque o número 1, porque ele só tem um divisor.
- Faça um quadrado em torno do número 2, porque ele tem somente dois divisores: o 1 e ele mesmo. Em seguida, risque todos os múltiplos de 2.
- Faça um quadrado em torno do número 3, porque ele tem somente dois divisores: o 1 e ele mesmo. Em seguida, risque todos os seus múltiplos que não foram riscados anteriormente.
- Faça um quadrado em torno do número 5, porque ele tem somente dois divisores: o 1 e ele mesmo. Em seguida, risque todos os seus múltiplos que não foram riscados
- Faça um quadrado em torno do número 7, porque ele tem somente dois divisores: o 1 e ele mesmo. Em seguida, risque todos os seus múltiplos que não foram riscados.
- Devemos continuar o processo até o número primo menor ou igual a $\sqrt{100} = 10$.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Tabela 24: Crivo de Eratóstenes

Portanto, os números primos até 100 são: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43,47, 53, 59, 61, 67, 71,73, 79, 83, 89 e 97.

7.3.1 *Desafio - Encontrar dois números primos distintos*

Após aprenderem sobre o Crivo de Eratóstenes, os alunos têm um desafio: encontrar dois números primos distintos cujo produto seja igual a 35, 253 e 1247. A proposta é que eles

resolvam esse desafio por meio de tentativas e erros, de modo a perceberem que conforme aumentamos o valor dos números, a dificuldade também aumenta.

A resposta para este desafio é: $35 = 5 \cdot 7$, $253 = 11 \cdot 23$ e $1247 = 43 \cdot 29$.

Ao desafiá-los a encontrar dois números primos cujo produto seja igual a números específicos, eles são incentivados a desenvolver habilidades de raciocínio lógico e estratégico.

Esta atividade está de acordo com a habilidade da BNCC:

> **EF**06**MA**05 Classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos "é múltiplo de", "é divisor de", "é fator de", e estabelecer, por meio de investigações, critérios de divisibilidade por $2, 3, 4, 5, 6, 8, 9, 10, 100$ e 1000. [1, p.301]

Assim, essa atividade não apenas fortalece o domínio dos conceitos matemáticos, mas também promove o desenvolvimento de habilidades e de resolução de problemas, preparando os alunos para desafios mais complexos e estimulando seu interesse e curiosidade pela Matemática.

7.4 ATIVIDADE 5: CONTANDO POSSIBILIDADES

Esta atividade pretende dar uma ideia de como podemos explorar o conceito da multiplicação através do princípio multiplicativo da contagem, utilizando a ideia de codificação de comandos. Os objetivos específicos do princípio multiplicativo da contagem no sexto ano incluem:

- Compreender e aplicar o princípio multiplicativo para determinar o número total de possibilidades em situações que envolvem contagem.
- Utilizar o princípio multiplicativo para contar o número de maneiras de organizar objetos e eventos.
- Desenvolver habilidades de raciocínio lógico e estratégias de contagem ao resolver problemas que necessitam o uso do principio multiplicativo.

Esses objetivos tem como proposta desenvolver a compreensão dos alunos sobre a multiplicação como uma ferramenta para contar e organizar elementos em diferentes situações, promovendo habilidades matemáticas e de resolução de problemas.

Nesta atividade são perguntadas quantas possibilidades existem para situações específicas. A resposta da atividade proposta é:

- 3 dígitos: $2 \cdot 2 \cdot 2 = 8$ possibilidades.
- 4 dígitos: $2 \cdot 2 \cdot 2 \cdot 2 = 16$ possibilidades.

- 5 dígitos: $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32$ possibilidades.
- 6 dígitos: $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 64$ possibilidades.
- 7 dígitos: $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 128$ possibilidades.

Esta atividade está alinhada com a BNCC conforme habilidade:

> **(EF**06**MA**03**)** Resolver e elaborar problemas que envolvam cálculos (mentais ou escritos, exatos ou aproximados) com números naturais, por meio de estratégias variadas, com compreensão dos processos neles envolvidos com e sem uso de calculadora. [1, p.301]

Essa abordagem não apenas fortalece a compreensão da multiplicação, mas também desenvolve a capacidade dos alunos de pensar estrategicamente ao enfrentar problemas que envolvem cálculos e contagem de possibilidades.

Observação 7.1. *Esta é apenas uma sugestão de uma atividade inicial para introduzir o conceito do princípio multiplicativo, sendo necessário explorar outras situações em que o princípio multiplicativo é aplicado.*

7.5 ATIVIDADE 6: TRANSMITINDO IMAGENS

Esta atividade tem como objetivo desenvolver habilidades como consulta de tabelas, codificação e decodificação utilizando a malha quadriculada, por meio da exploração do processo de transmissão das imagens dos planetas pelas sondas espaciais para a Terra. Os objetivos específicos da atividade são:

- Desenvolver habilidades de codificação e decodificação para representar elementos.
- Compreender e aplicar o conceito de coordenadas cartesianas na codificação de informações.
- Praticar habilidades de codificação e decodificação de dados utilizando coordenadas.
- Estimular o raciocínio lógico ao interpretar e manipular informações codificadas em um sistemas de coordenadas.

As instruções para aplicação da atividade são:

- Separar os alunos em duplas ou trios.
- Cada grupo receberá imagens quadriculadas e uma folha quadriculada para anotar os códigos.

- Atribuir uma letra do alfabeto (A, B, C, etc.) para representar as colunas na imagem quadriculada.
- Atribuir um número para representar as linhas (1, 2, 3, etc.).
- Anotem os códigos das cores na ordem em que aparecem na imagem.
- Utilizar a codificação correta, onde a primeira coordenada representa a coluna, a segunda a linha e a terceira o código da cor. Por exemplo, se o primeiro quadradinho é azul água, a codificação seria (A1,29).
- Certificar-se de seguir as instruções corretamente para codificar os elementos de forma precisa e organizada.
- Depois de codificar a imagem, recortar os quadradinhos e misturar.
- Trocar os quadradinhos entre os grupos para a decodificação da imagem.
- Cada grupo deve receber uma nova folha quadriculada para decodificar a imagem recebida utilizando os quadradinhos com os códigos.

A proposta desta atividade esta alinhada de acordo com a habilidade da BNCC:

> **(EF**06**MA**16**)** Associar pares ordenados de números a pontos do plano cartesiano do 1º quadrante, em situações como a localização dos vértices de um polígono. [1, p.303]

Ao aplicar essa atividade, os alunos não apenas praticam habilidades matemáticas, mas também desenvolvem a capacidade de aplicar conceitos de coordenadas cartesianas de forma prática e contextualizada. As atividades propostas têm como objetivo principal buscar envolver os alunos em desafios divertidos e educativo, explorando conceitos matemáticos, promovendo o trabalho em equipe e estimular o interesse pela Matemática.

8

RELATO DE APLICAÇÃO

Durante o processo de elaboração da dissertação e do *e-book*, foi possível aplicar duas atividades em duas salas do 6º ano de uma escola municipal. As atividades aplicadas foram a Cifra de César e a Transmissão de Imagens.

8.1 ATIVIDADE DA CIFRA DE CÉSAR

Para a atividade da Cifra de César, foram necessárias duas aulas de 50 minutos cada. Na primeira aula, os alunos se organizaram em duplas, os objetivos da atividade foram explicados, assim como o conceito da Cifra de César e seu funcionamento. As duplas então recortaram os anéis e codificaram palavras como "Matemática" e decodificaram palavras como "Enigma" e "Códigos".

Na segunda aula, foi relembrado como decodificar e codificar usando os anéis concêntricos, e as duplas receberam uma folha contendo uma frase para ser decifrada utilizando o mesmo deslocamento usado por César, além da mensagem presente no *e-book* com o enigma para encontrar o deslocamento e quatro perguntas sobre a atividade. Então, as duplas decifraram a frase da dissertação **"Eu adoro Aritmética"** . Elas não tiveram dificuldades para descobrir o deslocamento da mensagem e a mensagem do *e-book* **"Vocês estão preparados para iniciar uma emocionante viagem rumo a desvendar os enigmas do universo dos códigos? Então, digite SIM!"**. Algumas duplas que terminaram a atividade foram incentivadas a criar uma mensagem, codificá-la e trocá-la com outra dupla. Nesse momento, algumas duplas foram criativas e queriam codificar cada letra da mensagem utilizando um deslocamento diferente para dificultar a decodificação. Algumas duplas trouxeram mensagens codificadas na aula seguinte para realizar a troca.

Foi possível verificar que a atividade despertou o interesse dos alunos. Um aluno perguntou se também aprenderíamos sobre o Código Morse.

8.2 ATIVIDADE TRANSMITINDO IMAGENS

Para esta atividade, foram necessárias quatro aulas de 50 minutos cada. Nas duas primeiras aulas, os alunos foram separados em duplas e os objetivos da atividade foram explicados. Também foi explicado como as imagens dos planetas eram transmitidas pelas sondas espaciais,

e a importância de codificar e decodificar corretamente. Na segunda aula deste mesmo dia, foi entregue uma imagem quadriculada para cada dupla, uma tabela com os códigos das cores e uma folha com retângulos para as duplas anotarem os códigos.

Eles tiveram muita dificuldade em codificar as imagens grandes; acabavam se perdendo ao codificar os quadradinhos, repetiam os quadradinhos, trocavam a codificação e perdiam muito tempo para encontrar a cor exata.

Então, nas duas aulas do dia seguinte, fiz algumas mudanças na proposta. Desta vez, entreguei imagens menores, como as imagens da flor, do *cupcake* e do coração que estão no Apêndice B. Eles codificaram, recortaram os retângulos onde tinham anotado os códigos e trocaram entre as duplas para fazer a decodificação.

Entreguei para cada dupla uma folha com um quadriculado maior e outra com um quadriculado menor para eles decodificarem as imagens. O resultado foi que algumas imagens decodificadas deram certo e outras não. Os alunos perceberam quando a dupla havia codificado errado e chamaram a atenção para isso, mostrando empenho e preocupação em fazer certo. No geral, apesar das dificuldades nas duas primeiras aulas, com os ajustes realizados, a atividade deu certo e os alunos gostaram. Depois da aplicação, na sexta-feira, eles me pediram qual atividade diferente faríamos em seguida.

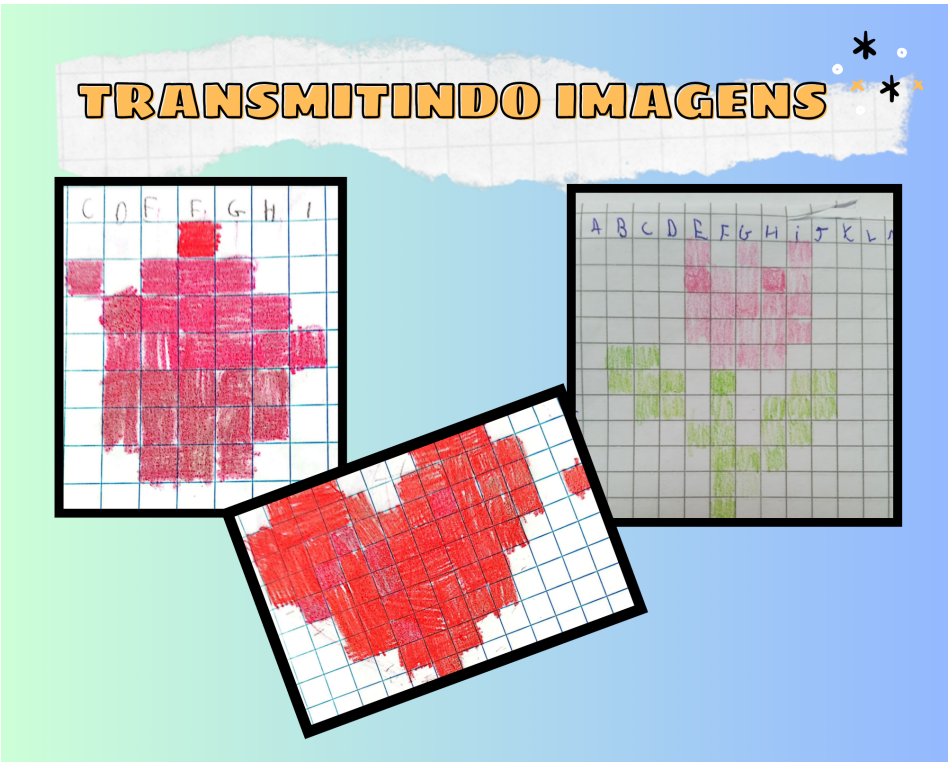


Figura 17: Imagens com erro de codificação ou decodificação

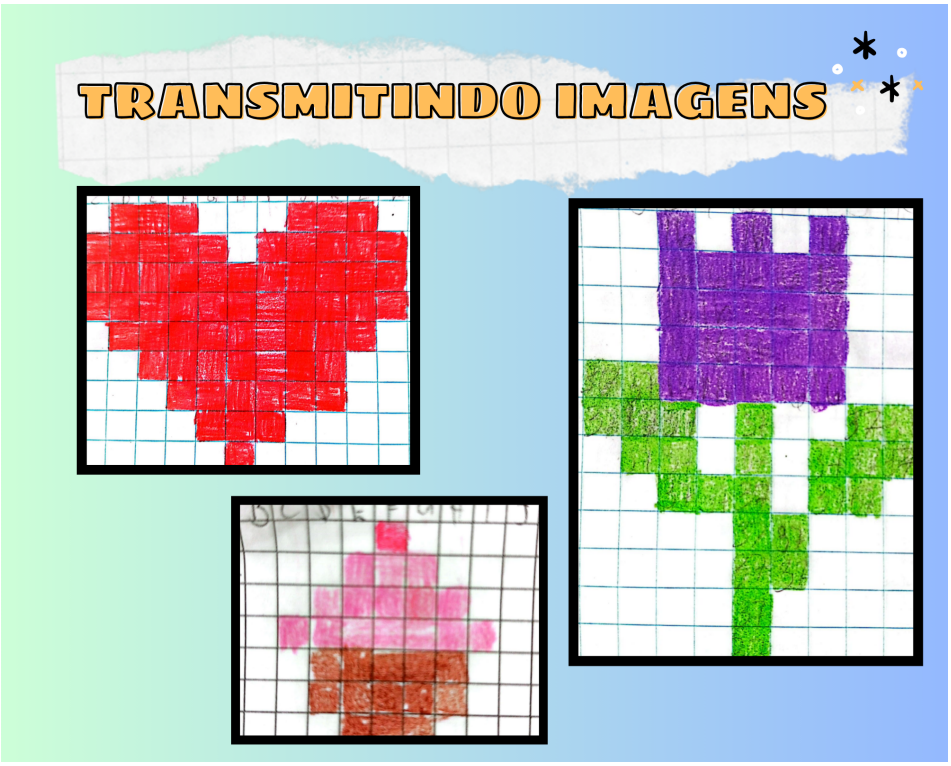


Figura 18: Imagens sem erro de codificação ou decodificação

8.3 CONCLUSÃO

Na atividade da Cifra de César, as duplas demonstraram entendimento e habilidade ao codificar e decodificar palavras, mostrando interesse e participação ao longo das duas aulas. A segunda parte da atividade, envolvendo a decifração da frase da dissertação e da mensagem do *e-book*, foi realizada com sucesso, evidenciando a compreensão do conceito de deslocamento na cifra. A iniciativa de criar mensagens codificadas adicionais e a troca entre as duplas demonstraram criatividade e aprofundamento na compreensão do método de César.

Já na atividade de transmitir imagens, os alunos enfrentaram desafios na codificação de imagens com mais quadradinhos, mas mostraram persistência ao tentar encontrar a codificação correta. As adaptações feitas nas aulas seguintes, ao reduzir o tamanho das imagens e incentivar a troca entre as duplas, resultaram em uma melhor compreensão e sucesso na decodificação das imagens. O envolvimento dos alunos em corrigir os erros de codificação e o interesse em fazer a atividade corretamente refletiram o engajamento e a aprendizagem alcançada.

Em resumo, mesmo com desafios iniciais, as atividades proporcionaram uma experiência de aprendizado significativa para os alunos, estimulando o interesse, a participação ativa e o aprimoramento das habilidades de codificação e decodificação. O *feedback* positivo dos alunos ao final das atividades indica a eficácia das estratégias empregadas e abre espaço para novas atividades criativas e desafiadoras no futuro.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] BRASIL. Ministério da Educação. Base Nacional Comum Curricular. Brasília. (2017).

http://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf.

[2] BOLDRINI, José Luiz; Costa, Sueli I. Rodrigues; Figueiredo, Vera Lúcia; Wetzler, Henry George. Álgebra Linear. São Paulo: Harper & Row do Brasil. (1980).

[3] COUTINHO, Severino Collier. Criptografia. Programa de Iniciação Científica da OBMEP. IMPA. (2015).

https://cdnportaldaobmep.impa.br/portaldaobmep/uploads/material_teorico/83bhrw1mjmgwo.pdf. Acesso em: 30/11/23.

[4] DE MELO, Lais Aline Casagrande Pires. Decifrando a Aritmética para o Ensino Fundamental. Dissertação de Mestrado. Mestrado Profissional em Matemática em Rede Nacional - PROFMAT. UNIFESP. São José dos Campos. (2017).

https://sca.profmat-sbm.org.br/profmat_tcc.php?id1=3196&id2=150870749. Acesso em 02/12/23.

[5] DE MORAIS, George Absalão Pandino. Códigos Perfeitos na Métrica de Lee e a Conjectura de Golomb-Welch. Dissertação de Mestrado. Mestrado em Matemática Aplicada. UNIFESP. São José dos Campos. (2017).

https://repositorio.unifesp.br/items/a1c2d791-8c84-4633-be40-2a6e0047dd2d. Acesso em 27/05/24.

[6] FALEIROS, Antonio Cândido. Criptografia. Notas em Matemática Aplicada. SBMAC. (2011).

https://www.sbmac.org.br/wp-content/uploads/2022/08/livro_52.pdf. Acesso em 27/05/24.

[7] FIARRESGA, Victor Manuel Calhabrês. Criptografia e Matemática. Dissertação de Mestrado. Faculdade de Ciências, Universidade de Lisboa. Portugal. (2010).

https://repositorio.ul.pt/bitstream/10451/3647/1/ulfc055857_tm_Victor_Fiarresga.pdf Acesso em: 15/05/2024.

[8] GOLAY, Marcel Jacques Émile. A Note on Coding for Error Detection. Proc. IRE. v. 37. p. 657. (1949).

[9] HAMMING, Richard Wesley. Error Detecting and Error Correcting Codes. The Bell System Technical Journal. (1950).

[10] HEFEZ, Abramo. Aritmética. SBM. Coleção PROFMAT. (2014).

[11] HEFEZ, Abramo. Iniciação à Aritmética. Rio de Janeiro: IMPA, (2015).

http://www.obmep.org.br/docs/apostila1.pdf.

[12] HEFEZ, Abramo; Villela, Maria Lúcia Torres. Códigos Corretores de Erros. Rio de Janeiro: IMPA, (2008).

[13] IUSENKO, Konstiantyn. Álgebra I para Licenciatura. Notas de aula. IME-USP. São Paulo. (2021).

https://www.ime.usp.br/~iusenko/ensino_2021_1/index.php. Acesso em 08/09/23.

[14] JORDÃO, Edmarcos Martins. RSA-Crypta: Uma Aplicação da Criptografia no Ensino Médio. Dissertação de Mestrado. Mestrado Profissional em Matemática em Rede Nacional - PROFMAT. Universidade Federal Vale do São Francisco. Juazeiro. (2023).

https://sca.profmat-sbm.org.br/profmat_tcc.php?id1=7171&id2=171055450.

[15] LAVOR, Carlile Campos; Alves, Marcelo Muniz Silva; de Siqueira, Rogério Monteiro; Costa, Sueli Irene Rodrigues. Uma Introdução à Teoria de Códigos. Notas em Matemática Aplicada. SBMAC. (2012).

https://www.sbmac.org.br/wp-content/uploads/2022/08/livro_21.pdf.

[16] LEMOS, Manoel. Criptografia, Números Primos e Algoritmos. Rio de Janeiro, IMPA. (2010).

https://impa.br/wp-content/uploads/2017/04/PM_04.pdf. Acesso em 17/05/24.

[17] MORGADO, Augusto Cezar de Oliveira; Carvalho, Paulo Cezar Pinto Carvalho. Matemática Discreta. SBM. Coleção PROFMAT. (2015).

[18] NICOLETTI, Everton Rodrigo. Aplicações de Álgebra Linear aos Códigos Corretores de Erros e ao Ensino Médio. Dissertação de Mestrado. Mestrado Profissional em Matemática em Rede Nacional - PROFMAT. UNESP. Rio Claro. (2015).

https://sca.profmat-sbm.org.br/profmat_tcc.php?id1=1638&id2=507. Acesso em: 13/04/2023.

[19] PAAR, Christof; Pelzl, Jan. Understanding Cryptography: A Textbook for Students and Practitioners. Springer. (2010).

[20] RIBEIRO, Roberta Alves do Nascimento. Os Códigos de Barras como Temas Geradores no Ensino de Matemática. Trabalho de Conclusão de Curso. UNESP. Faculdade de Engenharia e Ciências de Guaratinguetá, (2021).

https://repositorio.unesp.br/server/api/core/bitstreams/89d6a986-0dbc-4daa-a275-8afb5fbee3c6/content. Acesso em: 05/05/2023.

[21] SABADIN, Graça Aparecida Prestes. Códigos Corretores de Erros. Dissertação de Mestrado. Mestrado Profissional em Matemática em Rede Nacional - PROFMAT. Universidade Federal de Santa Catarina. (2019).

https://sca.profmat-sbm.org.br/profmat_tcc.php?id1=4936&id2=170660171. Acesso em: 13/04/2023.

[22] SANTO, Paulo César. Códigos Verificadores e Corretores de Erros. Dissertação de Mestrado. Mestrado Profissional em Matemática em Rede Nacional - PROFMAT. Universidade Federal do ABC. Santo André. (2018).

https://sca.profmat-sbm.org.br/profmat_tcc.php?id1=4256&id2=150530085. Acesso em: 09/05/2023.

[23] SANTOS, José Plínio de Oliveira. Introdução à Teoria dos Números. 3 ed. IMPA. Coleção Matemática Universitária. (2011).

[24] SHANNON, Claude E., A Mathematical Theory of Communication, Bell System Technical Journal, v. 27, n. 3, p. 379-423, (1948).

[25] SINGH, Simon. O livro dos códigos. Tradução de Jorge Calife. Rio de Janeiro: Record (2022).

[26] STEINBRUCH, Alfredo; Winterle, Paulo. Álgebra Linear 2. São Paulo: Pearson/Makron Books. (1987).

[27] Wikipédia, A Enciclopédia Livre. Mariner 9.(2022).

https://gl.wikipedia.org/wiki/Mariner_9. Acesso em 07/09/2023.

[28] Wikipédia, A Enciclopédia Livre. Voyager 1.(2022).

https://pt.wikipedia.org/wiki/Voyager_1. Acesso em 07/09/2023.

APÊNDICE A: *E-BOOK*

No que segue apresentamos todas as páginas do *e-book* intitulado “A incrível viagem pelo universo dos códigos”.

Figura 19: Capa do *e-book*

Figura 20: Contra capa

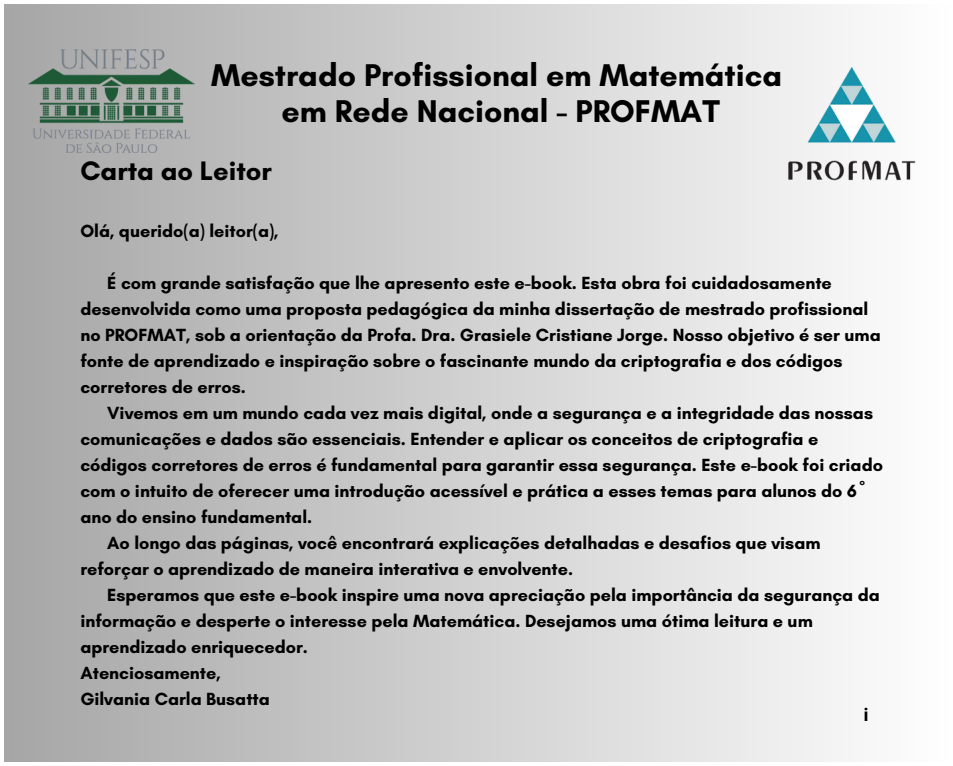


Figura 21: Carta ao Leitor

Figura 22: Índice

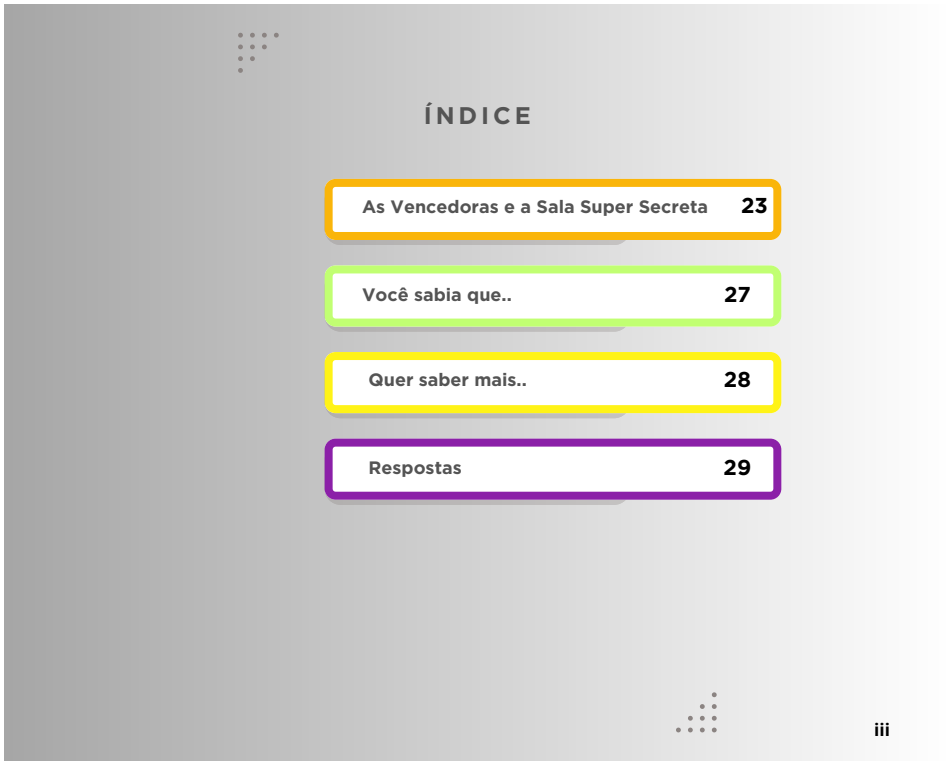


Figura 23: Índice

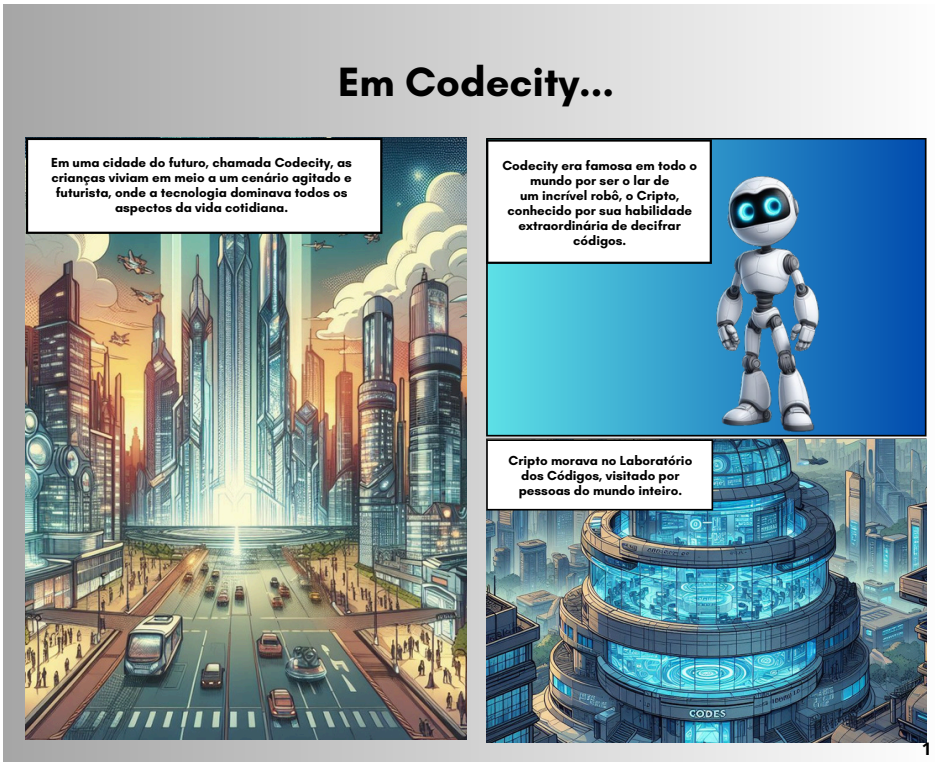


Figura 24: Página 1

Figura 25: Página 2

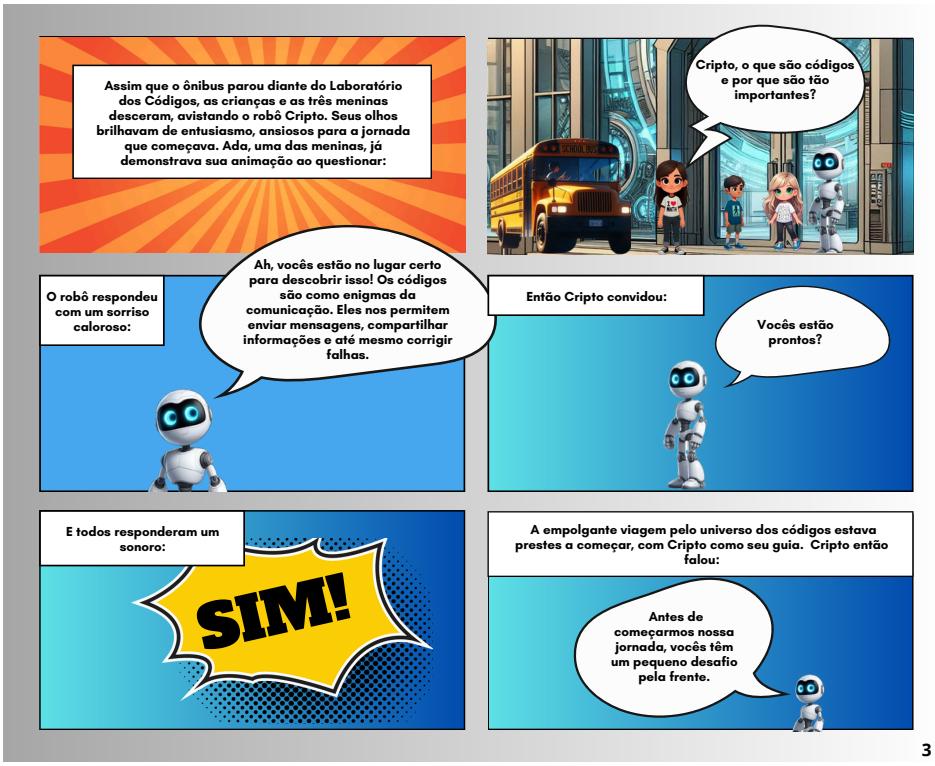


Figura 26: Página 3

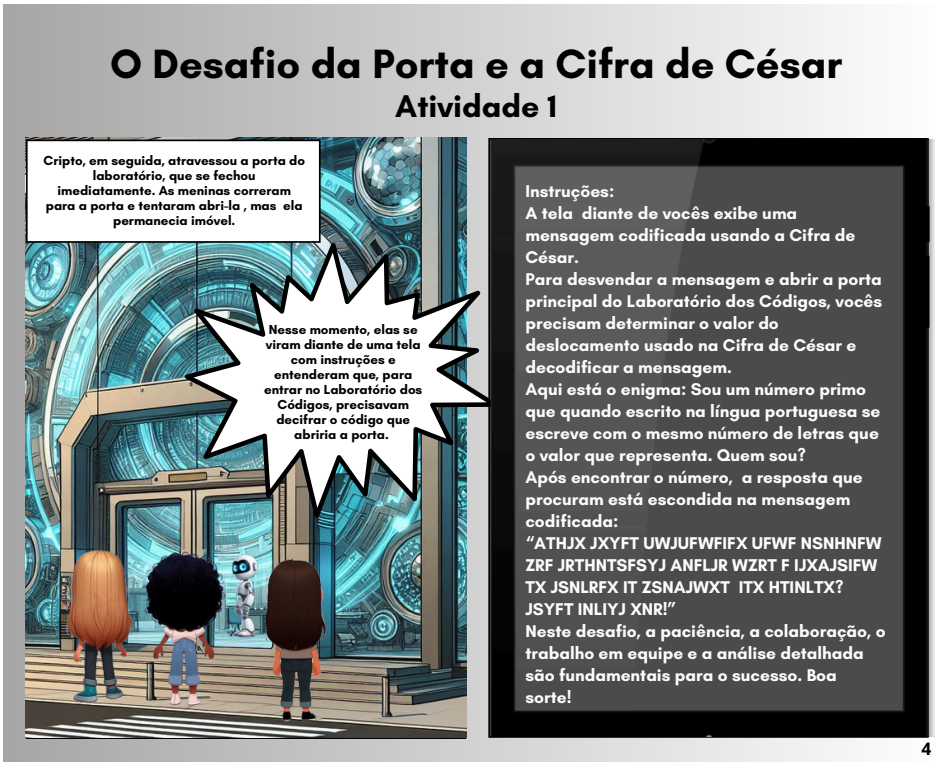


Figura 27: Página 4

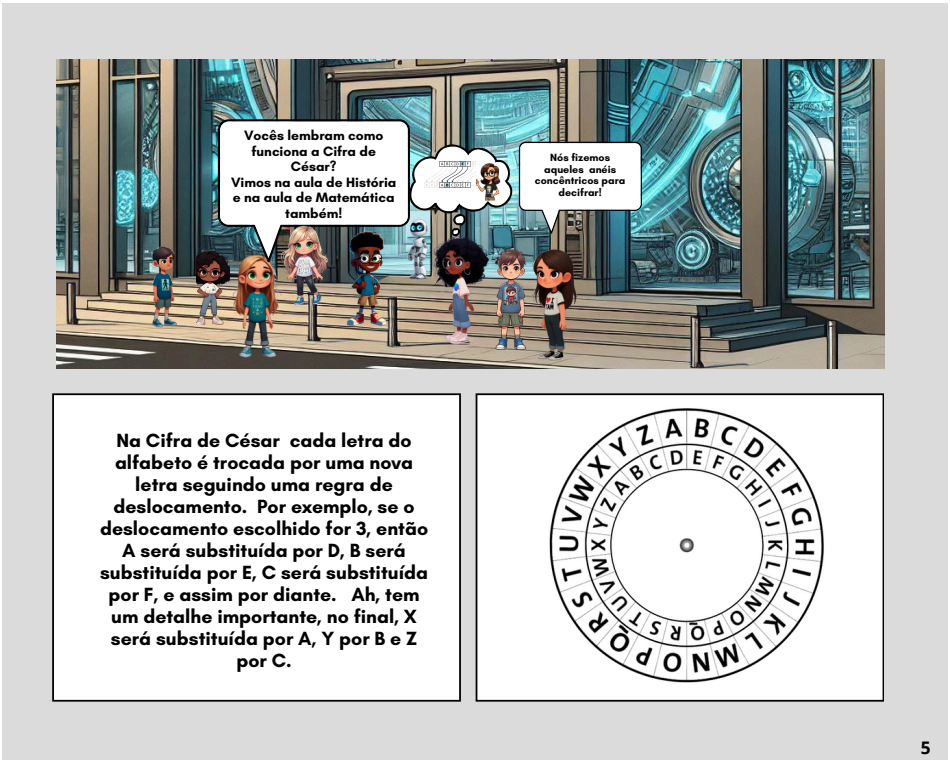


Figura 28: Página 5

Figura 29: Página 6

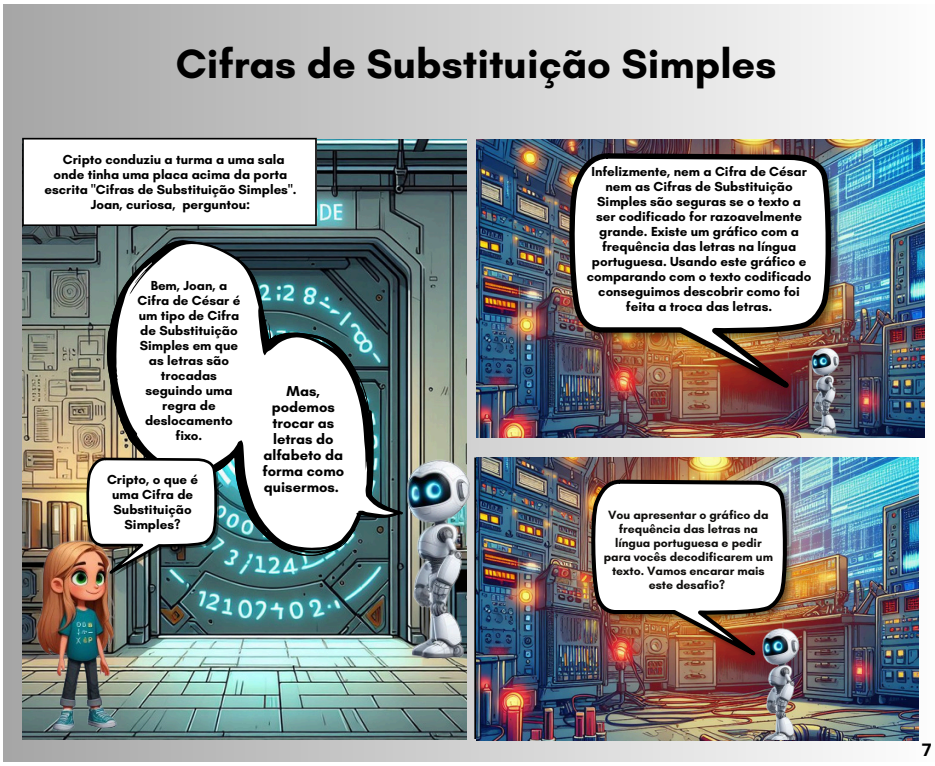


Figura 30: Página 7

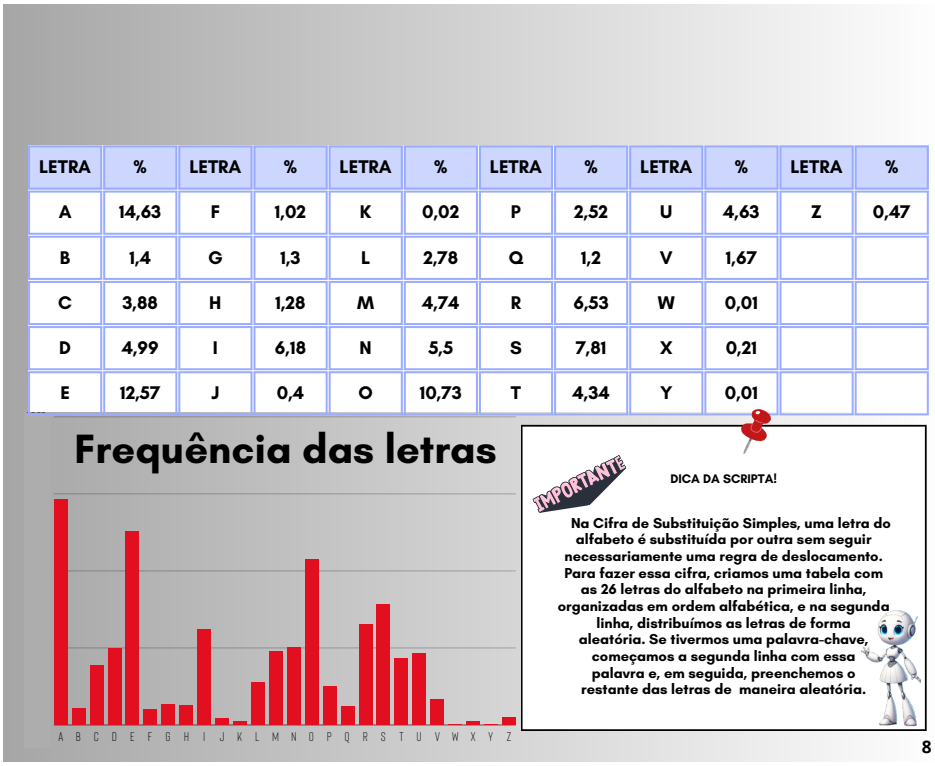


Figura 31: Página 8

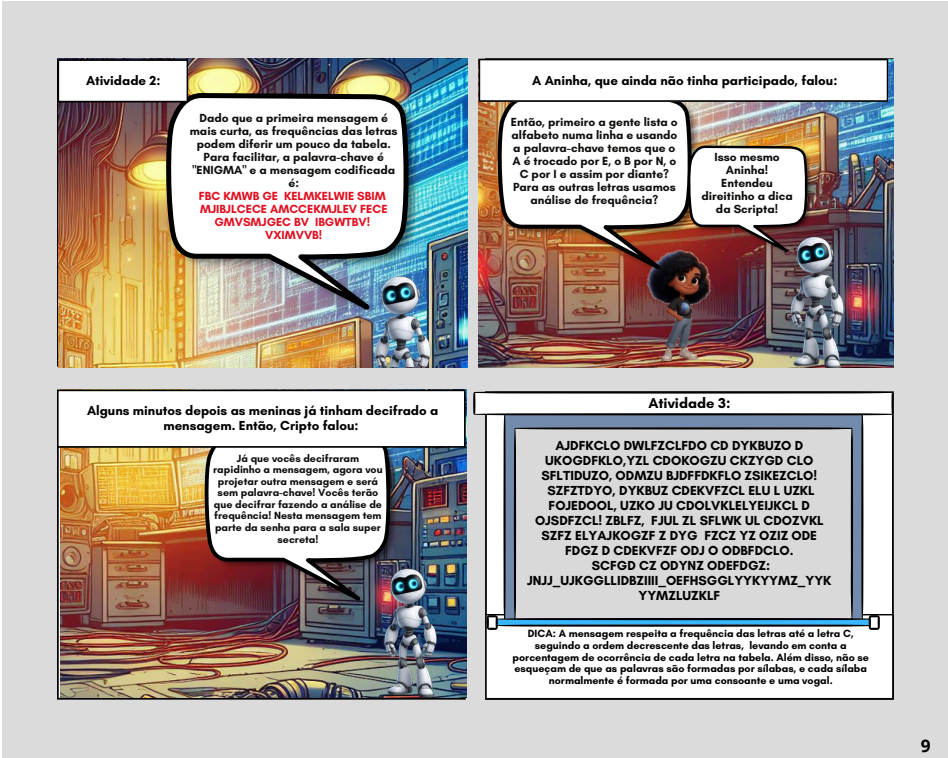


Figura 32: Página 9

Figura 33: Página 10

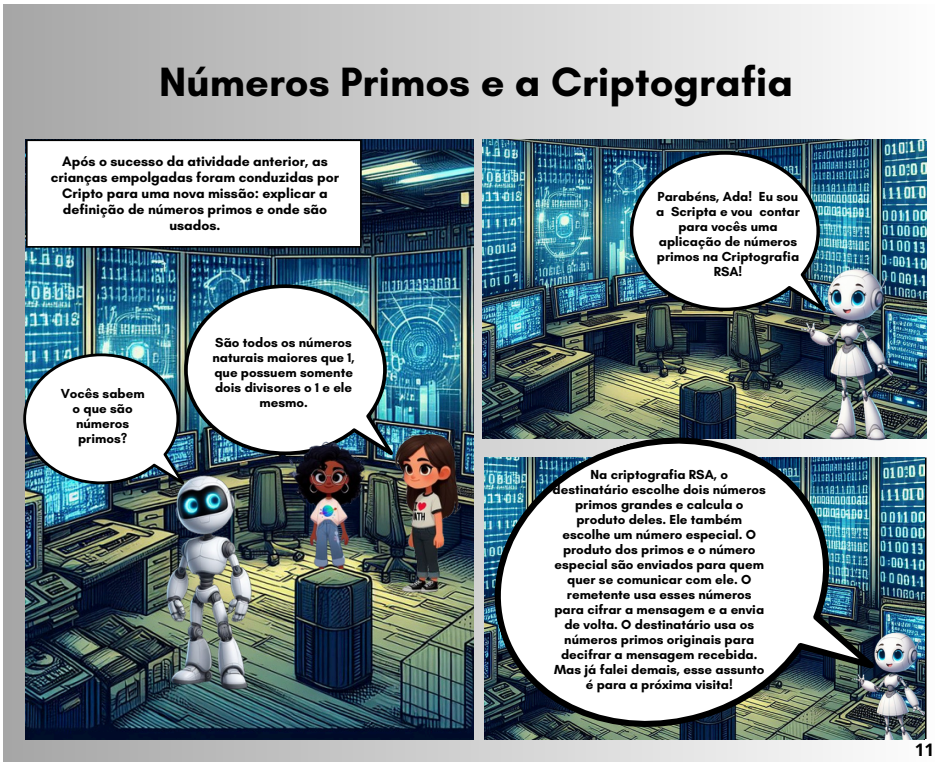


Figura 34: Página 11

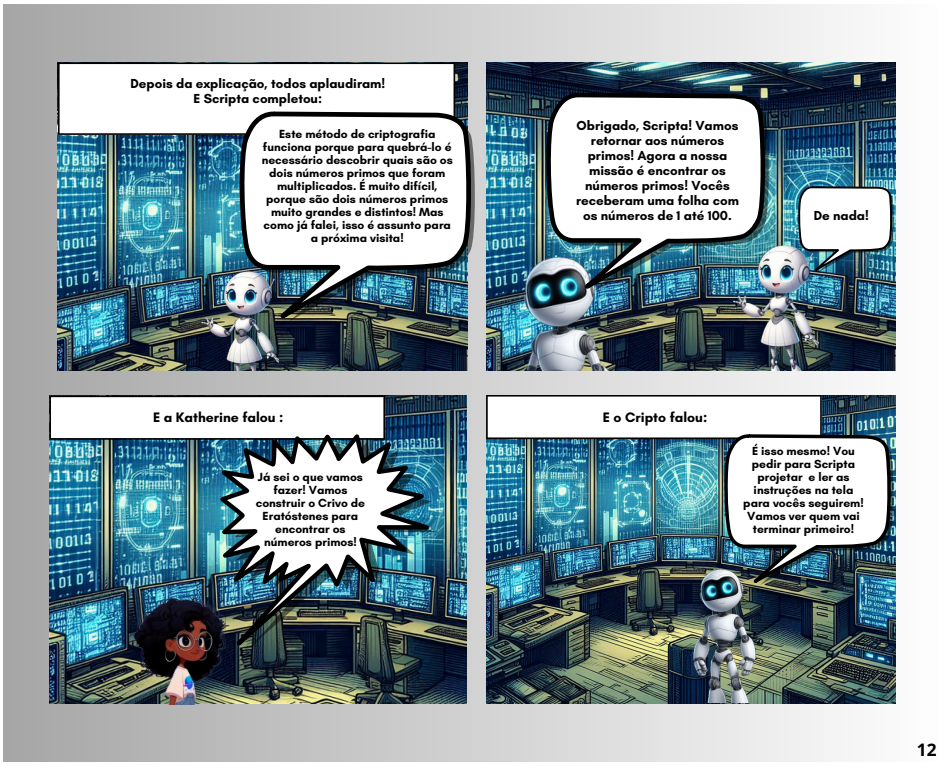


Figura 35: Página 12

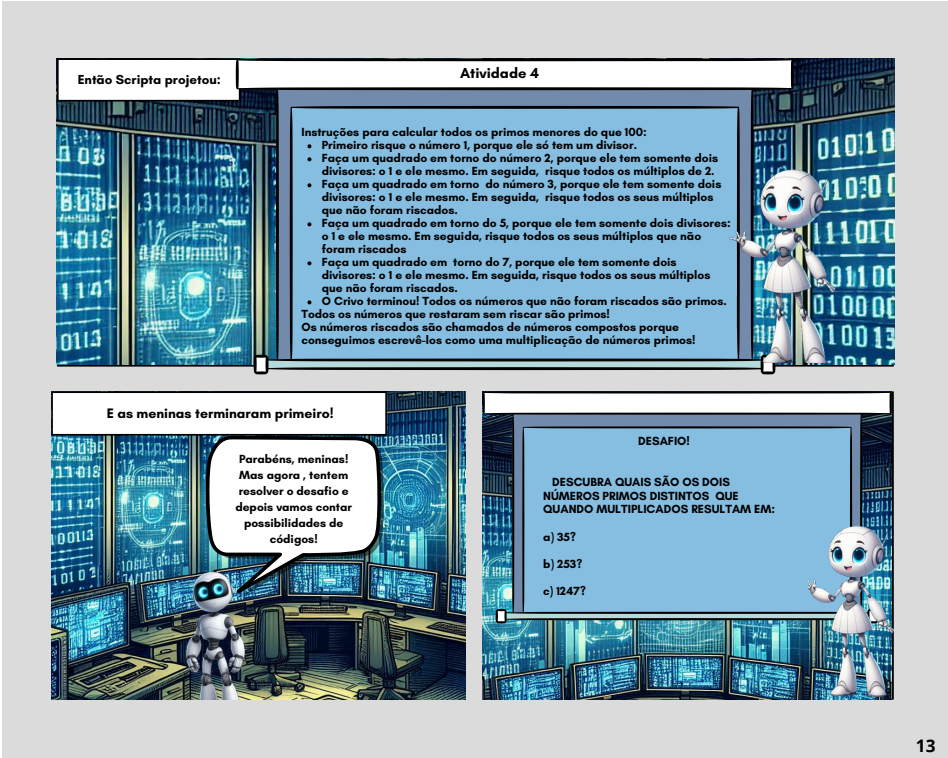


Figura 36: Página 13

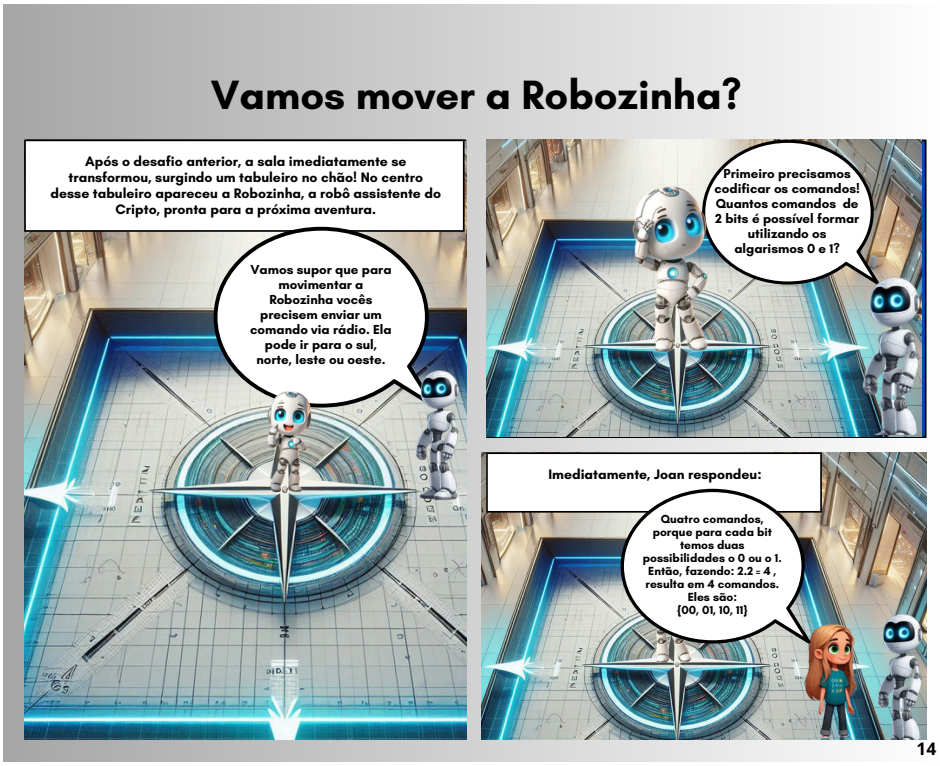


Figura 37: Página 14

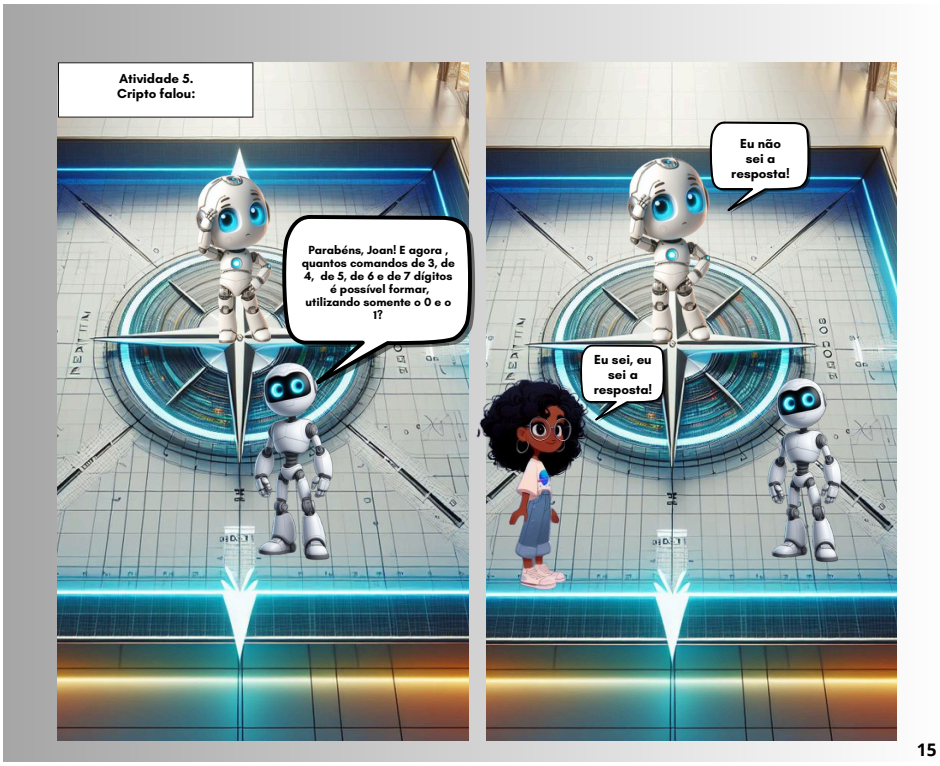


Figura 38: Página 15

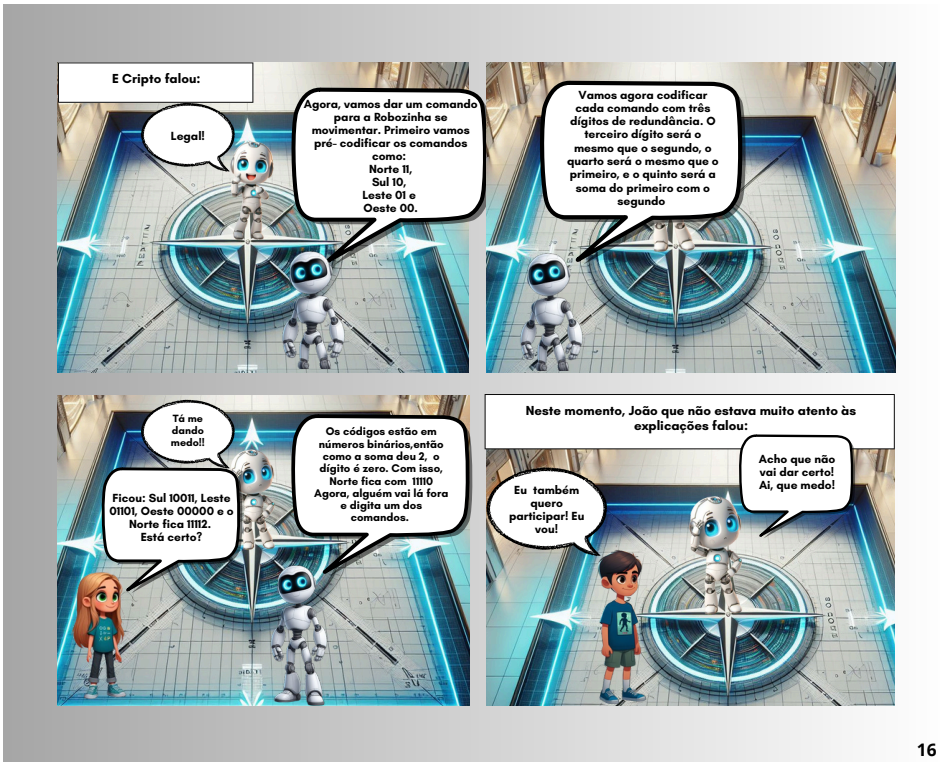


Figura 39: Página 16

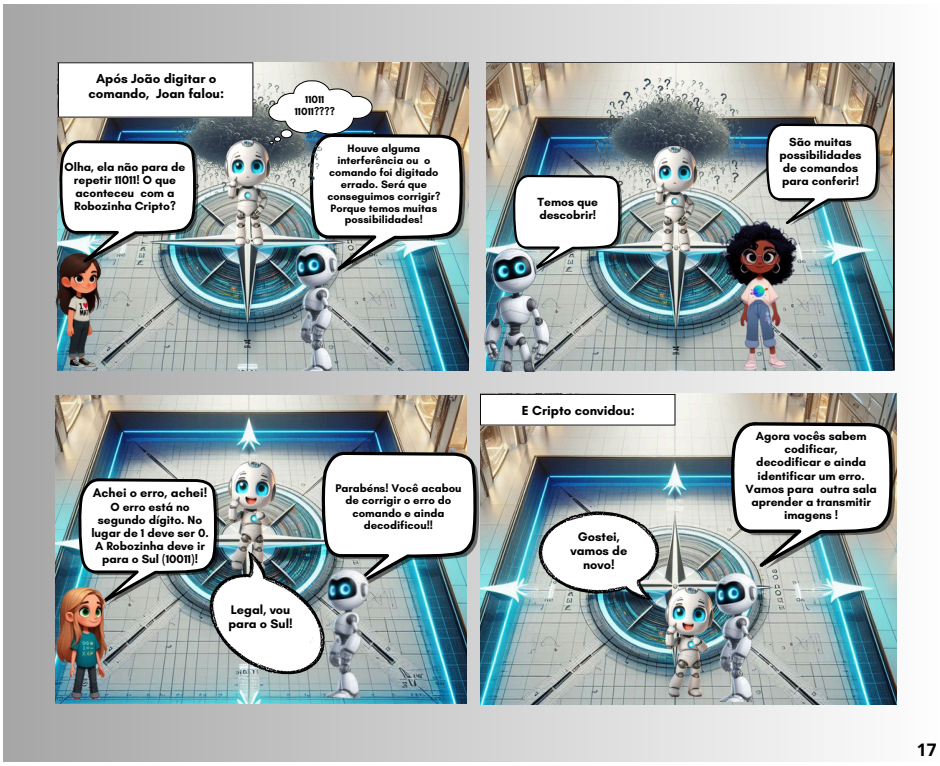


Figura 40: Página 17

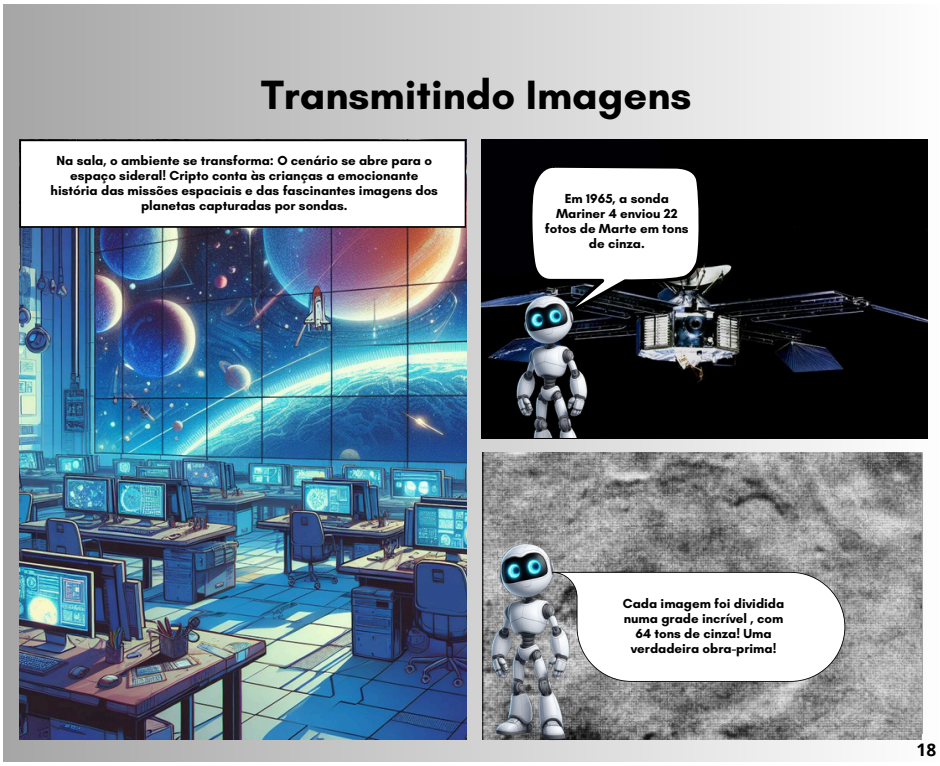


Figura 41: Página 18

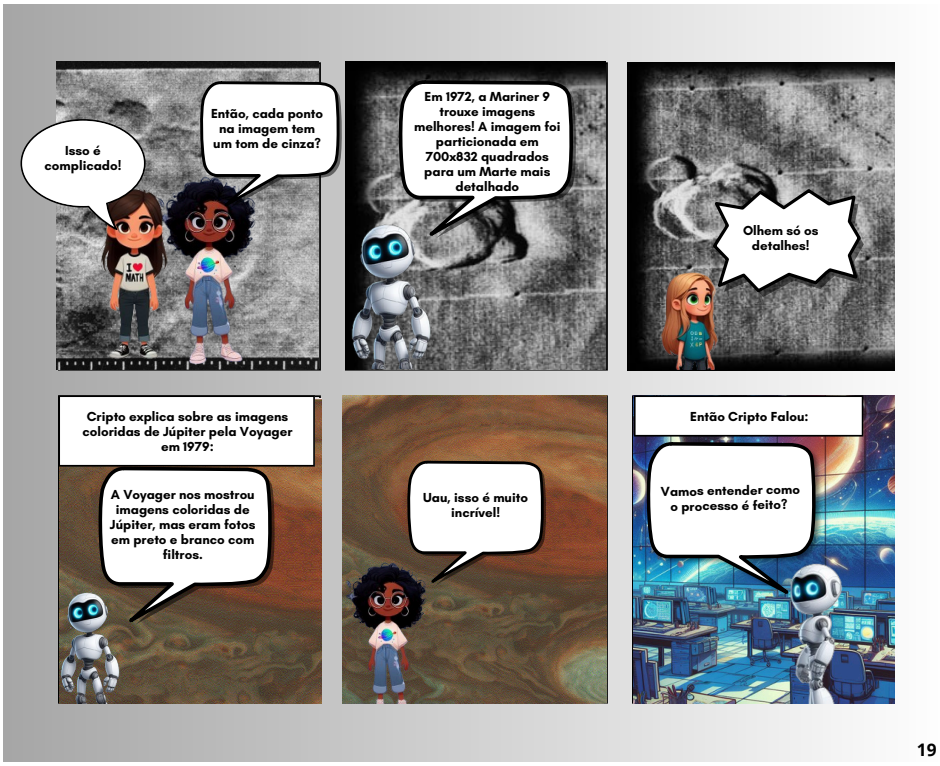


Figura 42: Página 19

Figura 43: Página 20

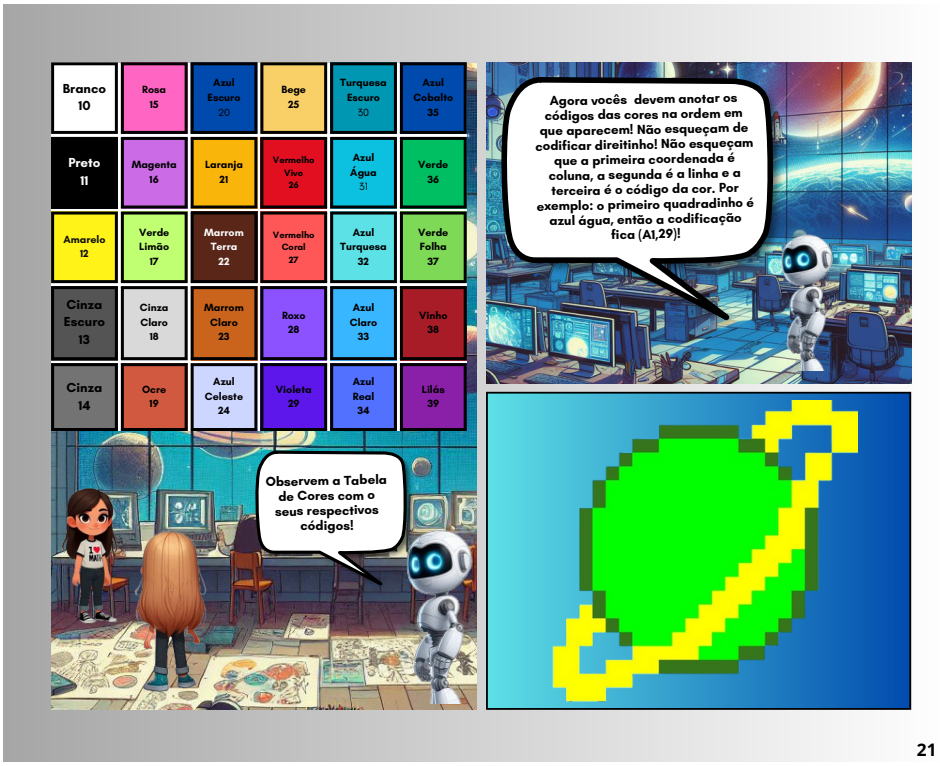


Figura 44: Página 21

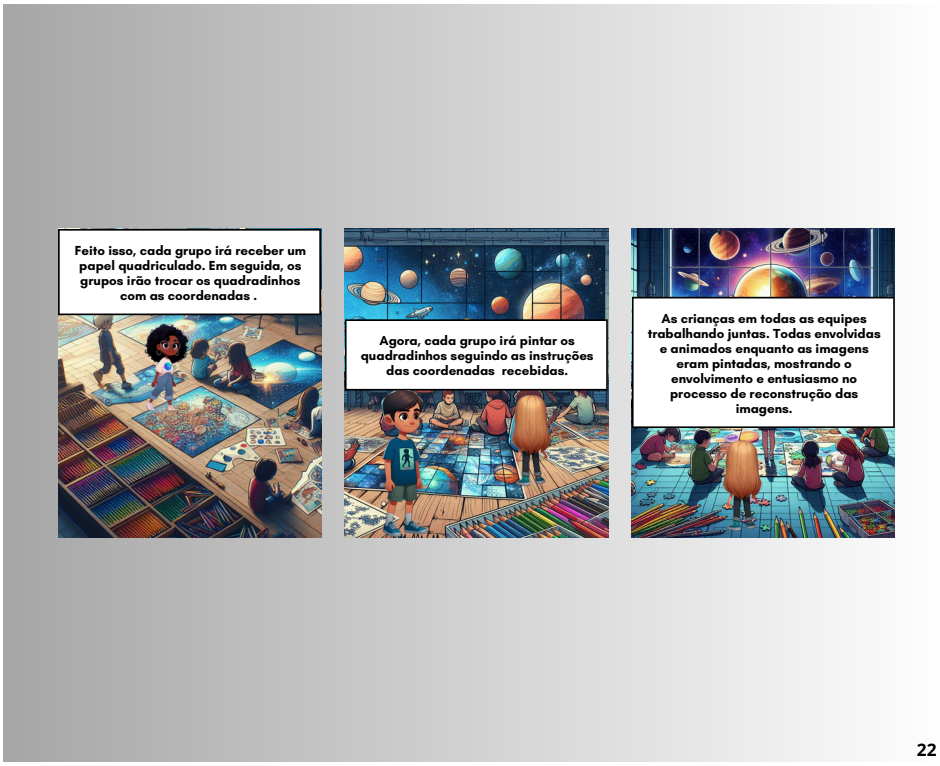


Figura 45: Página 22

Figura 46: Página 23

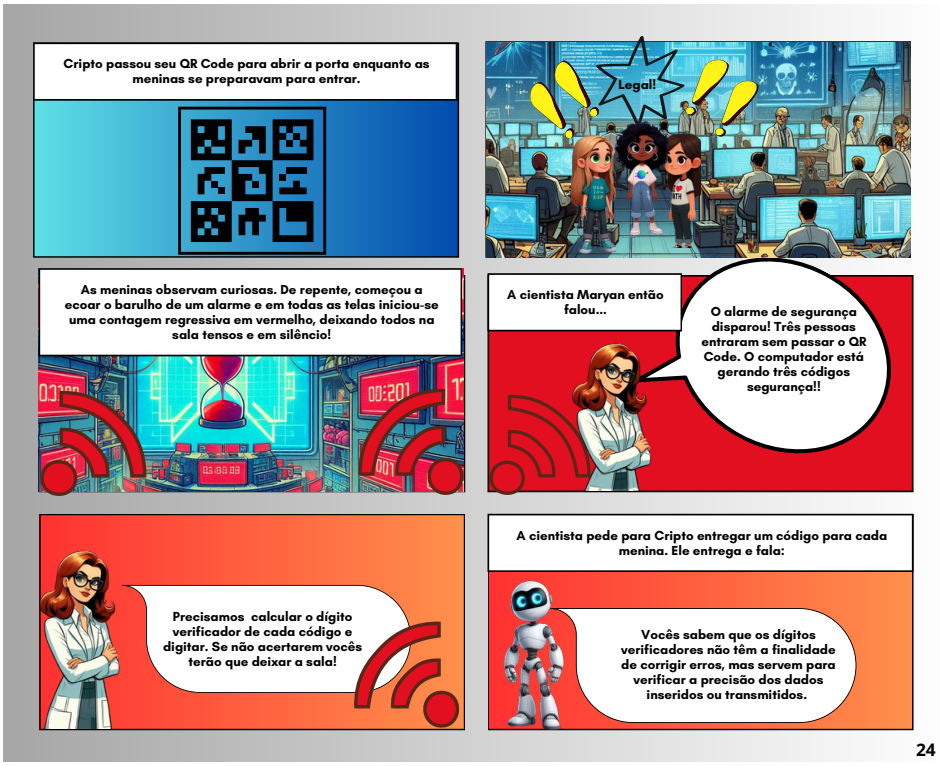


Figura 47: Página 24

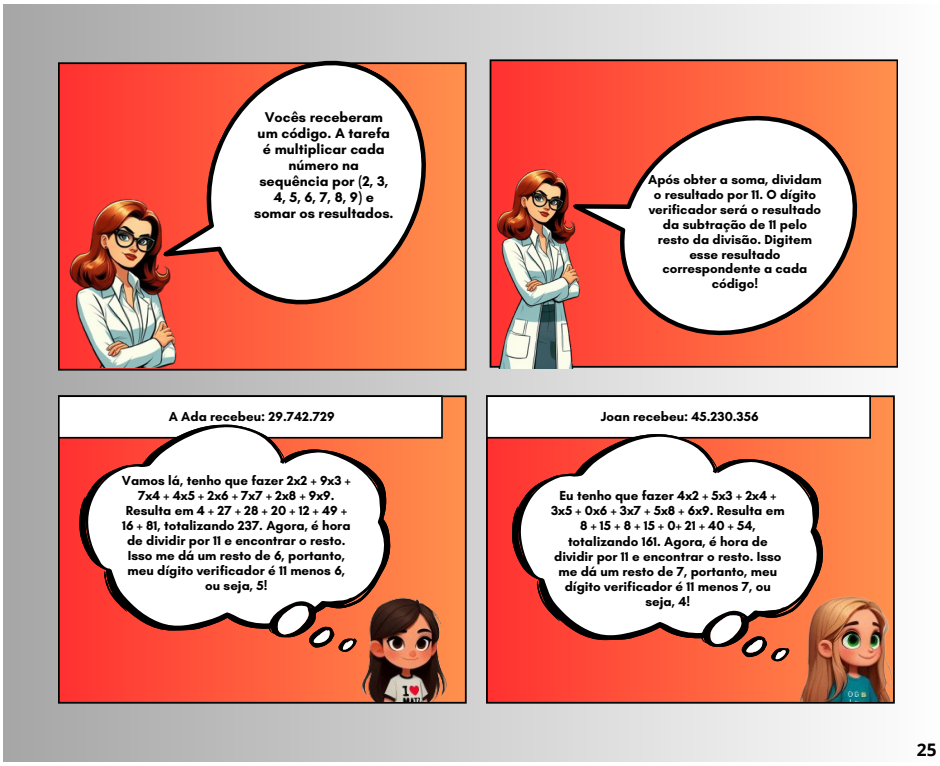


Figura 48: Página 25

Figura 49: Página 26

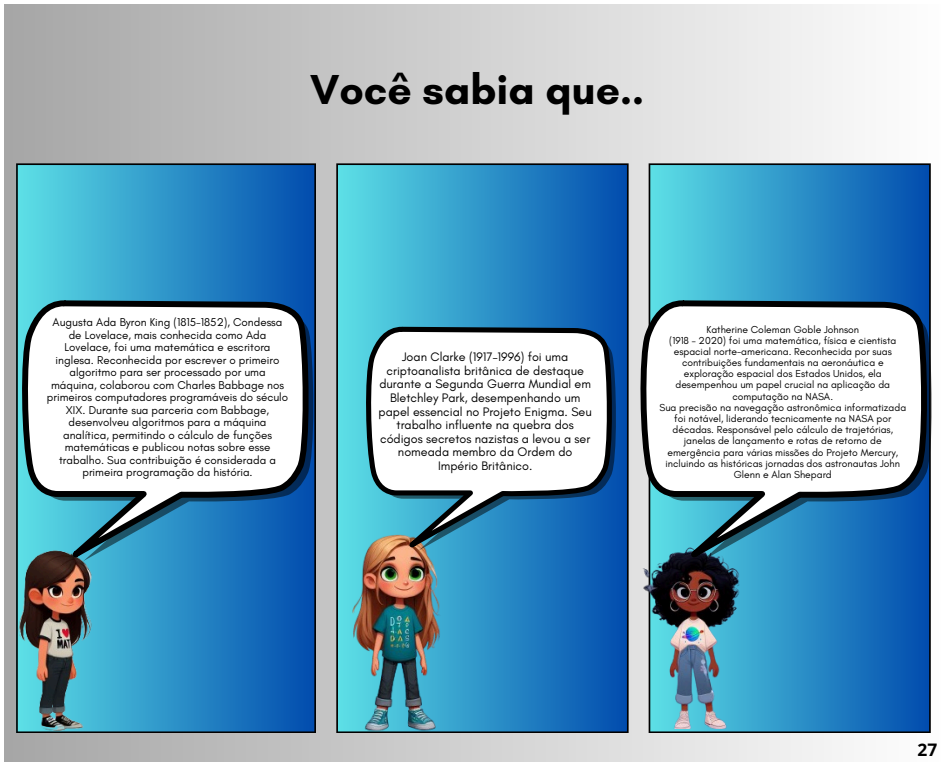


Figura 50: Página 27

Figura 51: Página 28

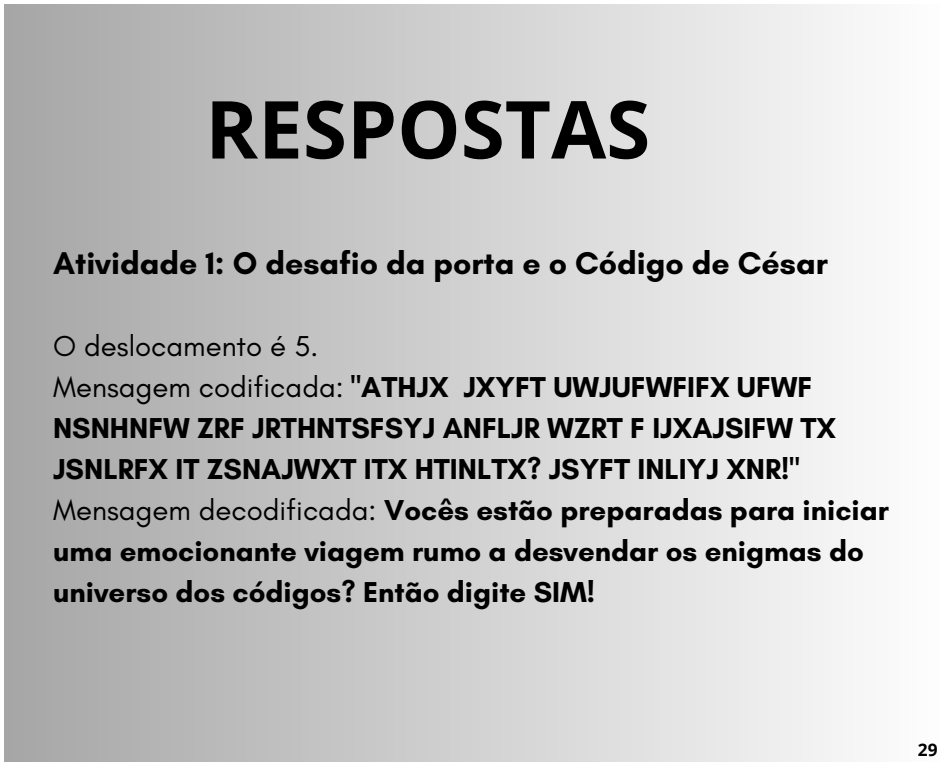


Figura 52: Página 29

Figura 53: Página 30

RESPOSTAS

Atividade 3: Cifra de Substituição Sem Palavra Chave

Tabela :

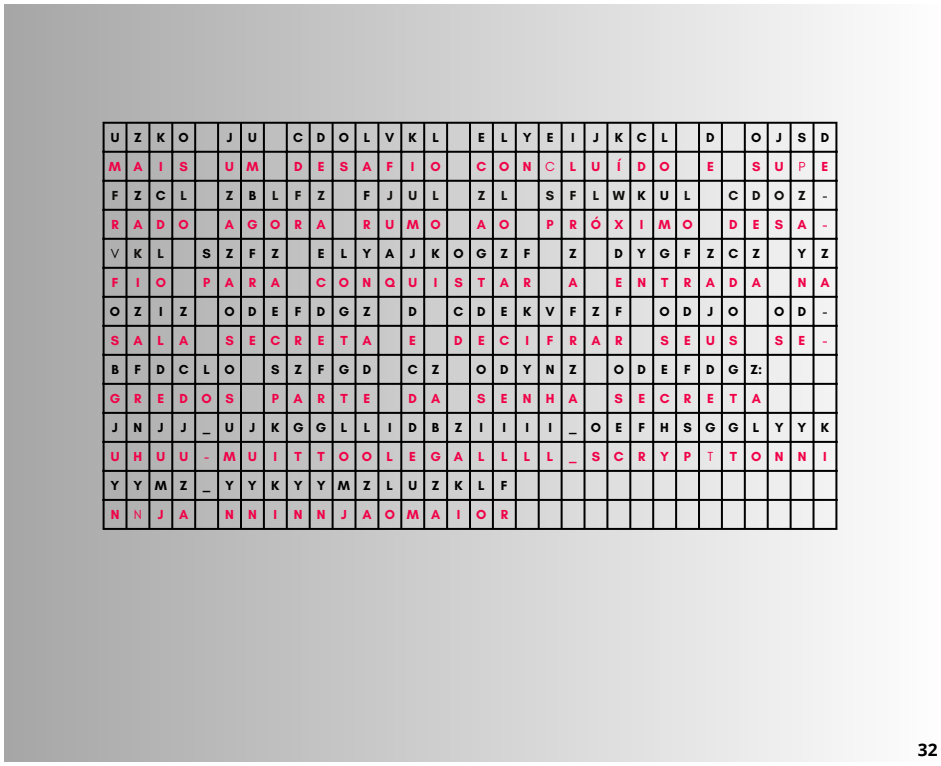
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Z	T	E	C	D	V	B	N	K	M	P	I	U	Y	L	S	A	F	O	G	J	R	X	W	H	Q

Mensagem decodificada:

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

31

Figura 54: Página 31



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

32

Figura 55: Página 32

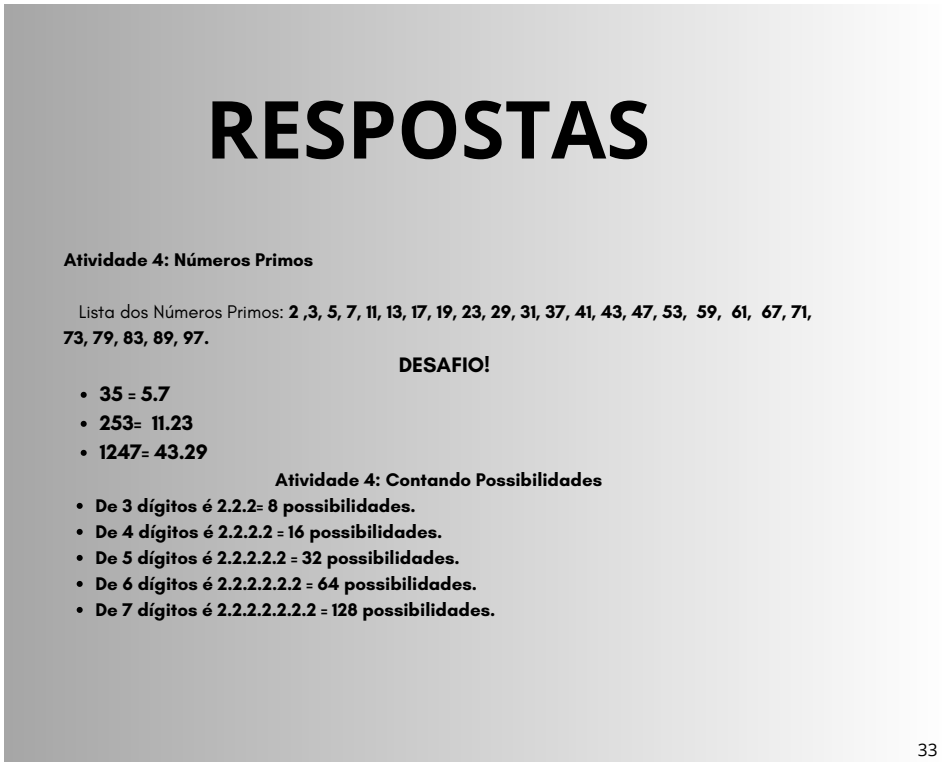


Figura 56: Página 33

APÊNDICE B: DESENHOS PARA A ATIVIDADE DE TRANSMISSÃO DE IMAGENS

Figura 57

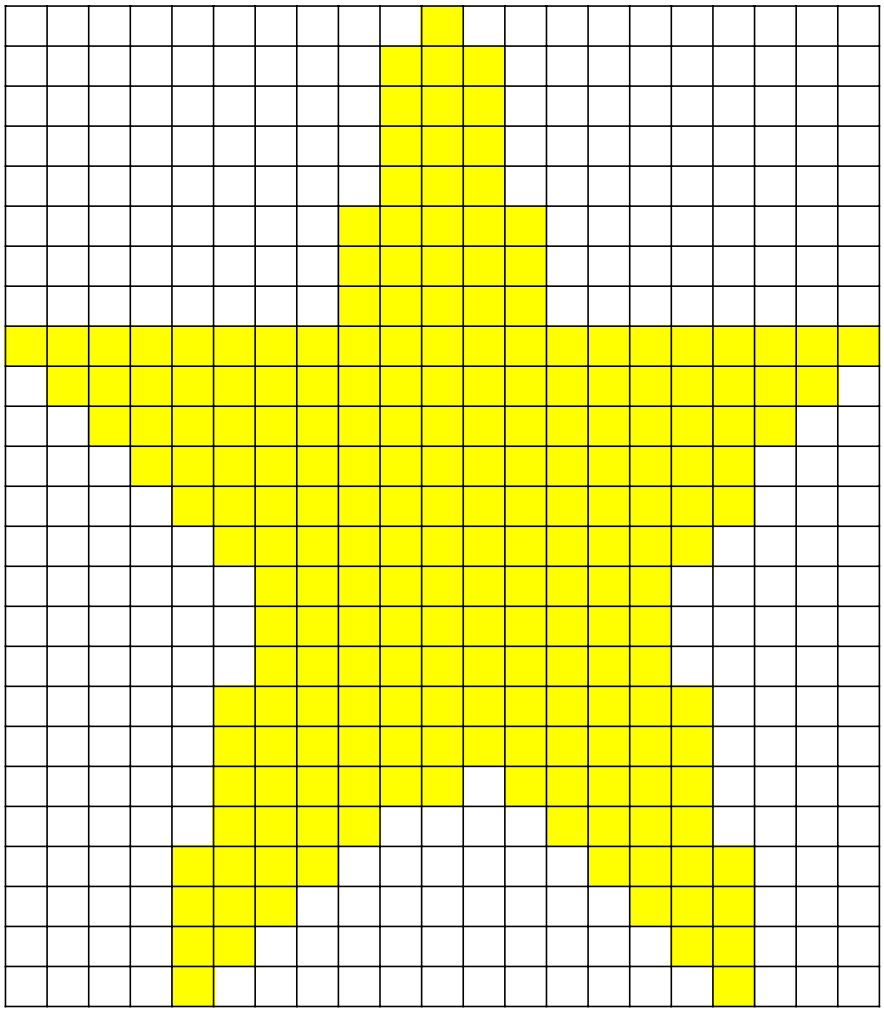


Figura 58

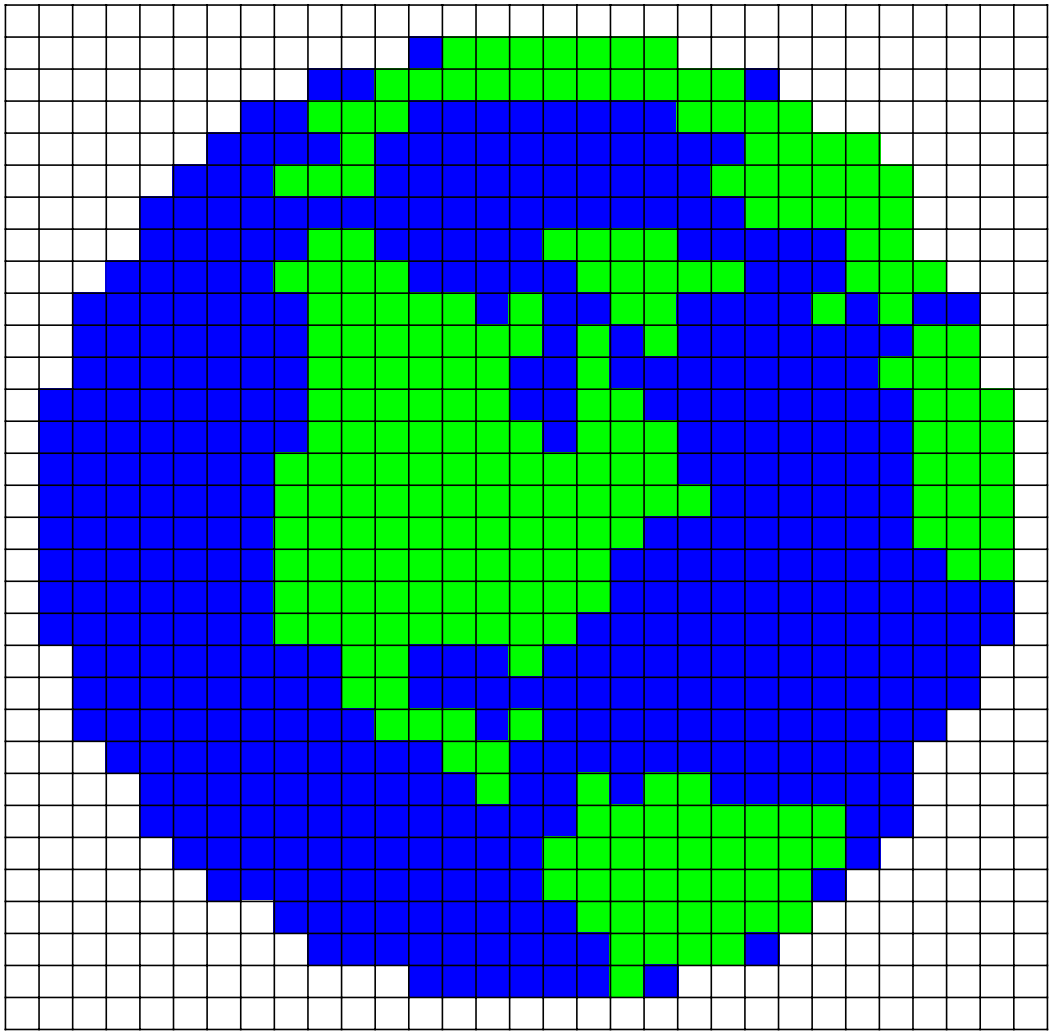


Figura 59

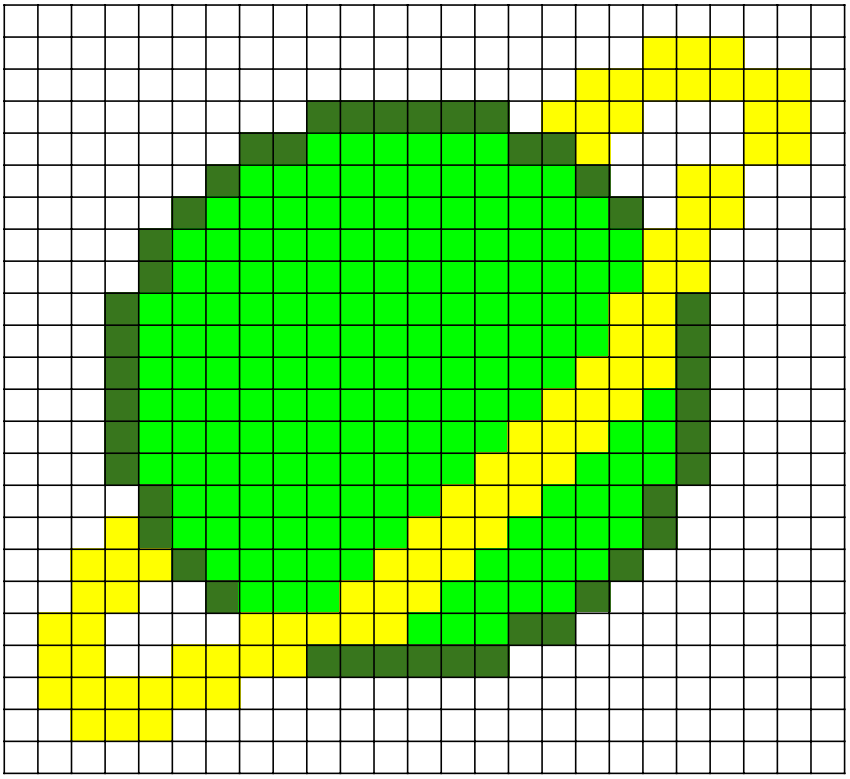


Figura 60

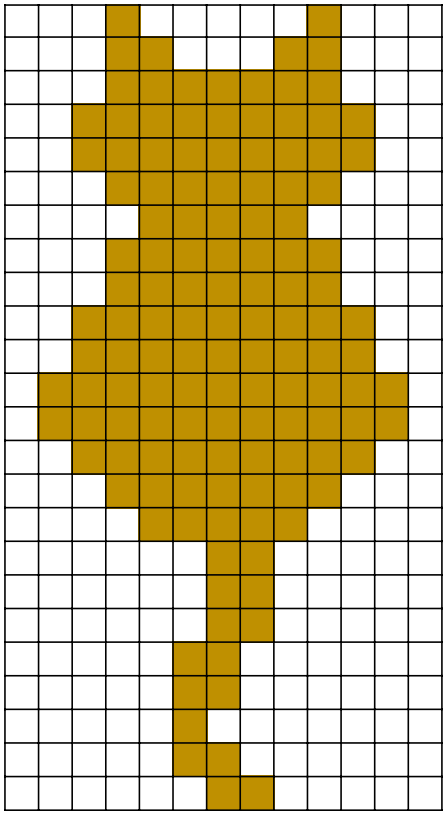


Figura 61

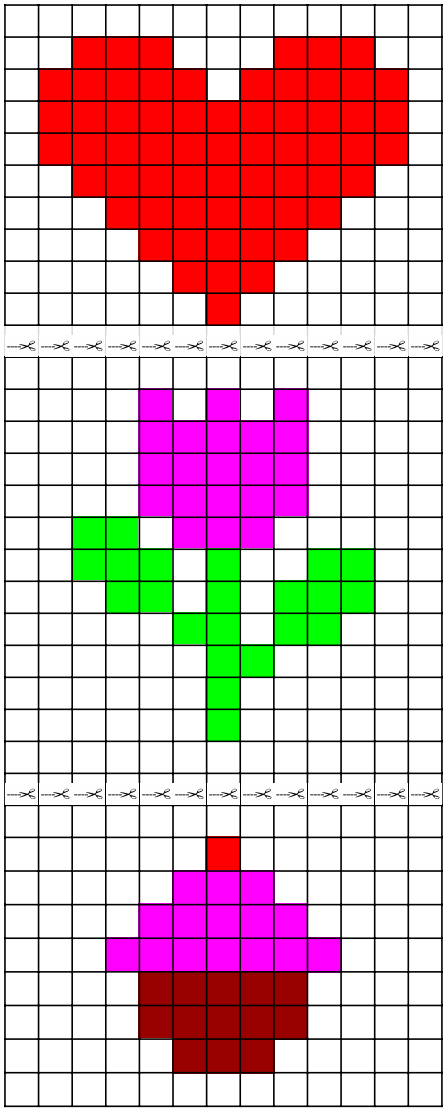


Figura 62