Universidade Federal de Uberlândia
Faculdade de Matemática
Programa de Mestrado Profissional em Matemática em Rede Nacional

CRIPTOGRAFIA: A TEORIA E A PRÁTICA EM SALA DE AULA

Matheus Alves Machado Reis

Uberlândia-MG
2023

Matheus Alves Machado Reis

CRIPTOGRAFIA: A TEORIA E A PRÁTICA EM SALA DE AULA

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional da Universidade Federal de Uberlândia, como parte dos requisitos para a obtenção de título de **MESTRE EM MATEMÁTICA**.

Área de concentração: Matemática
Linha de pesquisa: Álgebra

Orientador(a): Francielle Rodrigues de Castro Coelho

Uberlândia-MG
2023

Ficha Catalográfica Online do Sistema de Bibliotecas da UFU
com dados informados pelo(a) próprio(a) autor(a).

R375 Reis, Matheus Alves Machado, 1988-
2023 CRIPTOGRAFIA: A TEORIA E A PRÁTICA EM SALA DE AULA [recurso eletrônico] / Matheus Alves Machado Reis. - 2023.

Orientadora: Francielle Rodrigues de Castro Coelho.
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Matemática.
Modo de acesso: Internet.
Disponível em: http://doi.org/10.14393/ufu.di.2023.517
Inclui bibliografia.

1. Matemática. I. Coelho, Francielle Rodrigues de Castro,1981-, (Orient.). II. Universidade Federal de Uberlândia. Pós-graduação em Matemática. III. Título.

CDU: 51

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:
Gizele Cristine Nunes do Couto - CRB6/2091
Nelson Marcos Ferreira - CRB6/3074

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Coordenação do Programa de Pós-Graduação em Matemática em Rede Nacional
Av. João Naves de Ávila, 2121, Bloco 1F - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3230-9452 - www.famat.ufu.br - profmat@famat.ufu.br

ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Mestrado Profissional em Matemática em Rede Nacional - PROFMAT UFU				
Defesa de:	Dissertação de Mestrado Profissional, 08, PROFMAT				
Data:	Treze de setembro de dois mil e vinte e três	Hora de início:	15:00	Hora de encerramento:	17:00
Matrícula do Discente:	12112PFT011				
Nome do Discente:	Matheus Alves Machado Reis				
Título do Trabalho:	Criptografia: a teoria e a prática em sala de aula				
Área de concentração:	Matemática				
Linha de pesquisa:	Álgebra				
Projeto de Pesquisa de vinculação:	Não há				

Reuniu-se em webconferência pela plataforma *Microsoft Teams* a Banca Examinadora, aprovada pelo Colegiado do Programa de Pós-graduação em Matemática - Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), assim composta pelas professoras doutoras: Flávia Souza Machado da Silva - UNESP; Ana Paula Tremura Galves - FAMAT/UFU e Francielle Rodrigues de Castro Coelho - FAMAT/UFU, orientadora do candidato.

Iniciando os trabalhos, a presidente da mesa, Profa. Dra. Francielle Rodrigues de Castro Coelho, apresentou a Comissão Examinadora e juntamente com o candidato agradeceram a presença de todas. Posteriormente, a presidente concedeu ao Discente a palavra para a exposição do seu trabalho. A duração da apresentação do Discente e o tempo de arguição e resposta foram conforme as normas do Programa.

Dando continuidade, a senhora presidente concedeu a palavra para as examinadoras que passaram a arguir o candidato. Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final considerando o candidato:

Aprovado

Esta defesa faz parte dos requisitos necessários à obtenção do título de Mestre.

O competente diploma será expedido após cumprimento dos demais requisitos, conforme as normas do Programa, a legislação pertinente e a regulamentação interna da UFU

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.

Documento assinado eletronicamente por **Flávia Souza Machado da Silva**, **Usuário Externo**, em 13/09/2023, às 16:38, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Francielle Rodrigues de Castro Coelho**, **Professor(a) do Magistério Superior**, em 13/09/2023, às 16:39, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Ana Paula Tremura Galves**, **Professor(a) do Magistério Superior**, em 13/09/2023, às 16:39, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4811244** e o código CRC **111E7C2C**.

Referência: Processo nº 23117.065696/2023-11 SEI nº 4811244

Dedico ao meu querido filho que em breve chegará. Que este trabalho possa inspirá-lo a buscar o conhecimento com paixão e motivação.

Agradecimentos

Agradeço a Deus primeiramente por me acompanhar e nortear meus passos no âmbito profissional e pessoal.

Agradeço a minha esposa Lorrayne Reis por me incentivar nos momentos difíceis e aos meus pais Marcia e Vanderley Reis que estiveram presentes na minha vida e me incentivaram aos estudos desde que nasci, deixando sempre claro que "o conhecimento é algo que ninguém pode lhe tirar".

A professora Dra. Francielle Rodrigues de Castro Coelho que me orientou com excelência, paciência e tranquilidade. Sem dúvida alguma a realização deste não seria possível sem ela.

Por fim, agradeço a todos aqueles que direta ou indiretamente contribuíram para a realização deste trabalho, o qual é a realização de um sonho.

REIS, M. A. M. .*Criptografia: a teoria e a prática em sala de aula*. 2023. 74p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Os métodos criptográficos desempenham um papel crucial na proteção da privacidade e segurança das comunicações digitais, garantindo que informações sensíveis permaneçam confidenciais em um mundo cada vez mais conectado. Com o intuito de obter um melhor entendimento sobre alguns desses métodos, os objetivos deste trabalho são estudar os métodos criptográficos Cifra de César e Criptografia RSA, além de apresentar uma proposta e aplicar uma atividade sobre Cifra de César em sala de aula.

Palavras-chave: Congruência modular, Função phi de Euler, Cifra de César, Criptografia RSA.

REIS, M. A. M..*Cryptography: theory and practice in the classroom*. 2023. 74p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

Cryptographic methods play a crucial role in protecting the privacy and security of digital communications, ensuring that sensitive information remains confidential in an increasingly connected world. In order to obtain a better understanding of some of these methods, the objectives of this work are to study the cryptographic methods Caesar Cipher and RSA Cryptography, in addition to presenting a proposal and applying an activity on Caesar Cipher in the classroom.

Keywords: Modular congruence, Euler's phi function, Caesar's cipher, RSA cryptography.

Sumário

Introdução

Em grego, *cryptos* significa secreto, oculto. A criptografia estuda os métodos para codificar (reduzir a um conjunto de símbolos que nos permite representar uma informação) uma mensagem de modo que somente seu destinatário legítimo consiga interpretá-la.

Um exemplo de código simples é o que consiste em substituir uma letra do alfabeto pela próxima, semelhante ao que foi usado por Júlio César (seção 2.1 deste trabalho), por volta de 50 a.C., para comunicar-se com as legiões em combate pela Europa.

Todo código vem acompanhado de duas receitas: uma para codificar uma mensagem e outra para decodificar uma mensagem codificada, o que o destinatário legítimo do código faz quando recebe uma mensagem codificada. Neste contexto, aparece a palavra decifrar, que significa ler uma mensagem codificada sem ser um destinatário legítimo. Para decifrar é preciso entender o código.

Observe que códigos como o de Júlio César são simples de decifrar. Na realidade, códigos que envolvem substituir cada letra sistematicamente por outro símbolo qualquer possui o mesmo problema. Isto se deve ao fato de que a frequência média com que cada letra é usada em uma determinada língua é mais ou menos constante. Logo, quando a mensagem for longa, contar a frequência de cada símbolo na mensagem pode ajudar a descobrir a que letra corresponde os símbolos mais frequentes.

No computador, decifrar uma mensagem por contagem de frequência é mais simples ainda e isto torna inviável os códigos que envolvem substituição de letras. Alguns dos primeiros computadores foram criados para auxiliar na decifração dos códigos usados pelos alemães na segunda guerra mundial e Alan Turing, idealizador da máquina de Turing, foi um dos cientistas responsáveis por isso.

Atualmente, para se realizar transações bancárias e comerciais ou fazer uma compra com cartão de crédito, é necessário codificar as mensagens enviadas por conter informações importantes. Desse modo, tornou-se necessário a criação de novos códigos para uso em aplicações comerciais (e não mais na comunicação entre espiões), difíceis de decifrar, mesmo com a ajuda de um computador. Por este motivo, estes códigos são todos de chave pública e foram introduzidos, em 1976, por W. Diffie e M. E. Hellman da Universidade de Stanford e por R. C. Merkle da Universidade da Califórnia. Em um código de chave pública saber codificar não implica saber decodificar.

O mais conhecido dos métodos de criptografia de chave pública é o RSA, que foi inventado por três matemáticos: Ron Rivest, Adi Shamir e Leonard Adleman, daí a sigla RSA (Rivest-Shamir-Adleman). Eles desenvolveram o algoritmo em 1977, publicaram no artigo [8] e desde então, tornou-se um dos sistemas criptográficos mais amplamente utilizados em todo o mundo. Este método será bastante explorado no capítulo 2 deste trabalho.

Neste trabalho estudamos conceitos e resultados de Teoria dos Números a fim de compreender melhor os métodos criptográficos Cifra de César e RSA, mas vale ressaltar que existem outros métodos criptográficos que não foram explorados ao longo deste trabalho. A seguir, alguns destes métodos serão mencionados.

- Cifra de Vigenère (século XVI): desenvolvida por Blaise de Vigenère no século XVI, é um método de criptografia por substituição polialfabética, essa cifra é uma evolução da Cifra de César. Nela, uma palavra-chave é escolhida, e cada letra da mensagem original é deslocada por um valor determinado pela posição da letra correspondente na palavra-chave. A palavra-chave é repetida ao longo da mesagem original de modo a cobrir todas as letras. Essa repetição torna a cifra mais segura, pois cada letra pode ser deslocada por um valor diferente, dificultando a análise estatística e a quebra do código. A Cifra de Vigenère foi considerada bastante segura em sua época mas com o avanço das técnicas de criptoanálise, a cifra se tornou vulnerável, especialmente quando a extensão da palavra-chave era pequena. ([11], Singh, 2001)

- Cifra de Playfair (1854): é um método de criptografia de substituição que foi inventado pelo cientista Sir Charles Wheatstone, embora tenha sido nomeada em homenagem ao seu colega Sir Lyon Playfair. Ela é uma cifra de substituição polialfabética que utiliza uma matriz 5×5 preenchida com letras do alfabeto para cifrar pares

de letras da mensagem original. Esta cifra ofereceu um nível de segurança maior em relação a métodos mais simples de substituição, como a Cifra de César. No entanto, a cifra não era totalmente segura e com o desenvolvimento de técnicas mais avançadas de criptoanálise, a Cifra de Playfair foi superada e não é considerada segura o suficiente para uso prático em situações de segurança modernas. ([4], Kahn, 1996)

• Enigma (início do século XX): A Enigma foi uma máquina de criptografia eletromecânica usada principalmente durante a Segunda Guerra Mundial. Desenvolvida inicialmente para fins comerciais, a máquina foi posteriormente adotada pelos militares alemães, consistia em uma série de rotores giratórios, que eram configurados de várias maneiras para substituir cada letra do alfabeto. Essa substituição ocorria através de um conjunto complexo de fiações elétricas internas, que criavam uma espécie de circuito elétrico fechado para cada tecla pressionada. A Enigma possuía um teclado para inserir as letras da mensagem original e uma lâmpada indicadora que acendia para mostrar a letra cifrada correspondente. Essa máquina foi amplamente utilizada pelos nazistas para comunicações criptografadas e foi decifrada pelos esforços combinados dos aliados, incluindo o matemático Alan Turing e a equipe de criptoanálise em Bletchley Park. Após a guerra, a Enigma deixou de ser uma ferramenta de segurança e passou a ser estudada como um marco histórico e tecnológico no desenvolvimento da criptografia e da computação. ([11], Singh, 2001)

• AES (Advanced Encryption Standard, 2001): o AES é um algoritmo de criptografia simétrica, isto é, algoritmo onde a mesma chave é usada tanto para cifrar quanto para decifrar os dados e neste caso a chave é mantida em segredo para garantir a segurança do método. A principal característica do AES é a sua estrutura de blocos, o que significa que ele cifra os dados em blocos fixos de tamanho específico (geralmente 128 bits). Ele opera em várias etapas de substituição e permutação, aplicando transformações matemáticas complexas aos dados. O número de rodadas varia dependendo do tamanho da chave utilizada (128, 192 ou 256 bits), garantindo maior segurança quanto maior o tamanho da chave. O AES é amplamente utilizado em diversas aplicações e setores, incluindo segurança de comunicações, criptografia de dados em sistemas de armazenamento, transações financeiras online, segurança em redes sem fio, proteção de informações em dispositivos móveis, entre outros. ([2], Daemen e Rijmen, 2002)

Este trabalho foi dividido em quatro partes: capítulo 1, capítulo 2, capítulo 3 e

considerações finais. A seguir, faremos um breve resumo do que foi abordado em cada capítulo.

No capítulo 1, apresentamos alguns requisitos de Teoria dos Números que serão de fundamental importância para o desenvolvimento deste trabalho. Mais especificamente, recordamos conceitos e resultados sobre máximo divisor comum, números primos, congruência modular e funções aritméticas, além de apresentar as demonstrações dos teoremas de Wilson, Fermat e Euler. As referências para este capítulo foram [6] e [10].

No capítulo 2, estudamos detalhadamente dois métodos de criptografia: Cifra de César e Criptografia RSA. Da Cifra de César exploramos seu conceito e sua relação com a congruência modular. Do método RSA apresentamos os processos de codificação e decodificação, e explicamos o porquê da segurança do método. As referências utilizadas foram [1], [5] e [8].

Finalmente, no capítulo 3, apresentamos uma proposta de aplicação em sala de aula do tema Cifra de César e descrevemos o desenvolvimento da mesma em uma turma de primeiro ano do ensino médio de uma escola.

CAPÍTULO 1

Preliminares

Neste capítulo apresentamos alguns conceitos e resultados que serviram de base para a teoria dos números e que serão importantes para o desenvolvimento deste trabalho. A maioria dos resultados deste capítulo foi introduzido por Gauss em um trabalho publicado em 1801.

1.1 O máximo divisor comum e números primos

Definição 1.1 *Se a e b são números inteiros, dizemos que a divide b, e denotamos por $a|b$, se existe $c \in \mathbb{Z}$ tal que $b = ac$. Se a não divide b, escrevemos $a \nmid b$.*

Observação 1.2 *Com relação à divisibilidade, são válidos os seguintes resultados:*

1. $n|n$, *para todo* $n \in \mathbb{Z}$.
2. $d|n$ *implica que* $ad|an$, *para todo* $a, d, n \in \mathbb{Z}$.
3. $ad|an$ *e* $a \neq 0$ *implicam que* $d|n$, *para todo* $a, d, n \in \mathbb{Z}$.
4. $1|n$, *para todo* $n \in \mathbb{Z}$.
5. $n|0$, *para todo* $n \in \mathbb{Z}$.
6. $d|n$ *e* $n \neq 0$ *implicam que* $|d| \leq |n|$.
7. $d|n$ *e* $n|d$ *implicam que* $|d| = |n|$.

8. *$a, b, c \in \mathbb{Z}$ tais que $a|b$ e $b|c$ implicam que $a|c$.*

9. *$a, b, c, m, n \in \mathbb{Z}$, onde $c|a$ e $c|b$, implicam que $c|(am + bn)$.*

Teorema 1.3 (Algoritmo da Divisão) *Sejam a e b números inteiros. Então, existem únicos números inteiros q e r tais que*

$$a = bq + r,$$

com $0 \leq r < |b|$, q é chamado de quociente e r de resto da divisão de a por b.

Demonstração: A demonstração pode ser encontrada em [10] (Teorema 1.2).

■

Definição 1.4 *O máximo divisor comum de dois inteiros a e b (a ou b diferente de zero), denotado por $mdc(a, b)$, é o maior inteiro que divide a e b.*

Teorema 1.5 *Sejam a e b números inteiros e $d = mdc(a, b)$. Então, existem inteiros n_0 e m_0 tais que $d = n_0a + m_0b$.*

Demonstração: Considere $B = \{na+mb| \ n, m \in \mathbb{Z}\}$. Note que B contém números negativos, números positivos e o 0.

Suponhamos que n_0 e m_0 são tais que $c = n_0a+m_0b$ é o menor inteiro positivo pertencente ao conjunto B. Vamos provar que $c|a$ e $c|b$.

Por contradição, suponhamos que $c \nmid a$. Neste caso, pelo teorema 1.3, existem q e r tais que $a = cq + r$, onde $0 < r < c$. Portanto,

$$r = a - qc = a - q(n_0a + m_0b) = (1 - qn_0)a + (-qm_0)b,$$

o que nos permite concluir que $r \in B$, o que é uma contradição, pois $0 < r < c$ e c é menor elemento positivo de B.

Logo, $c|a$ e de forma análoga prova-se que $c|b$.

Como d é um divisor comum de a e b, exsitem inteiros k_1 e k_2 tais que $a = k_1d$ e $b = k_2d$ e assim,

$$c = n_0a + m_0b = n_0k_1d + m_0k_2d = d(n_0k_1 + m_0k_2),$$

o que implica que $d|c$. Da observação 1.2(6), temos que $d \leq c$ (d e c são positivos). Como $d < c$ não é possível, pois $d = mdc(a,b)$, concluímos que $d = n_0a + m_0b$.

■

Teorema 1.6 *Sejam a e b números inteiros e $d = mdc(a,b)$. Então, d é o único divisor positivo de a e b o qual é divisível por todo divisor comum de a e b.*

Demonstração: Primeiro, note que $d > 0$ pois $1|a$ e $1|b$ implicam que $d \geq 1 > 0$.

Agora, seja d_1 um divisor comum qualquer de a e b.

Do teorema 1.5 e pela observação 1.2(9), segue que $d_1|d$.

Por último, mostremos que d é o único com a propriedade de ser maior que 0 e ser divisível por todo divisor comum de a e b. De fato, se d_1 possui esta propriedade então $d_1|d$ e $d|d_1$. Como $d, d_1 > 0$, pela observação 1.2(7), obtemos que $d_1 = d$. Logo, d é único.

■

Proposição 1.7 *Para todo inteiro positivo t, $mdc(ta,tb) = t \cdot mdc(a,b)$.*

Demonstração: Consideremos os conjuntos $A = \{mta + ntb |\ m,n \in \mathbb{Z}\}$ e $B = \{ma + nb |\ m,n \in \mathbb{Z}\}$. Observe que, $A = tB$.

Pelo teorema 1.5, $mdc(ta,tb)$ é o menor valor positivo de A e $mdc(a,b)$ é o menor valor positivo de B. Logo,

$$mdc(ta,tb) = t \cdot mdc(a,b).$$

■

Proposição 1.8 *Se $c > 0$ e a e b são divisíveis por c, então*

$$mdc\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c} \cdot mdc(a,b)$$

Demonstração: Como c divide a e b, temos que a/c e b/c são números inteiros. Tomando $t = c$, $a = a/c$ e $b = b/c$ na proposição 1.7, segue o resultado.

■

Corolário 1.9 *Se $d = mdc(a,b)$ então $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.*

Demonstração: Pela proposição 1.8, como d é um divisor comum de a e b, obtemos

$$mdc\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d} \cdot d = 1.$$

■

Exemplo 1.10 *Como $mdc(25,35) = 5$, segue que $mdc(5,7) = 1$.*

Definição 1.11 *Dizemos que os números inteiros a e b são relativamente primos sempre que $mdc(a,b) = 1$.*

Teorema 1.12 *Para quaisquer números inteiros a, b e x, temos que $mdc(a,b) = mdc(a, b+ax)$.*

Demonstração: Sejam $d = mdc(a,b)$ e $f = mdc(a, b+ax)$. Pelo teorema 1.5, existem inteiros n_0 e m_0 tais que $d = n_0a + m_0b$. Observe que

$$\begin{aligned} d &= n_0a + m_0b \\ &= n_0a - xm_0a + xm_0a + m_0b \\ &= a(n_0 - xm_0) + (b+ax)m_0. \end{aligned}$$

Assim, $f = mdc(a, b+ax)$ divide d.

Agora, vamos provar que $d|f$.

Pela observação 1.2(9), $d|(b + ax)$ e pelo teorema 1.6, temos que $d|mdc(a, b+ax) = f$.

Logo, como d e f são positivos, concluímos que $d = f$ (pela observação 1.2(7)).

■

Exemplo 1.13 *Temos que* $mdc(4, 12) = mdc(4, 12 + 3 \cdot 4) = mdc(4, 12 + 7 \cdot 4)$.

Proposição 1.14 *Sejam* a, b *e* c *números inteiros tais que* $mdc(a, c) = mdc(b, c) = 1$. *Então,* $mdc(ab, c) = 1$.

Demonstração: Pelo teorema 1.5, como $mdc(a, c) = 1$ e $mdc(b, c) = 1$, segue que existem $m_0, m_1, n_0, n_1 \in \mathbb{Z}$ tais que $1 = m_0a + n_0c = m_1b + n_1c$. Assim,

$$\begin{aligned} 1 &= (m_0a + n_0c)(m_1b + n_1c) \\ 1 &= m_0m_1ab + m_0n_1ac + n_0m_1bc + n_0n_1c^2 \\ &= m_0m_1ab + (m_0n_1a + n_0m_1b + n_0n_1c)c. \end{aligned}$$

Seja $d = mdc(ab, c)$. Temos que

$$d|ab \text{ e } d|c \implies d|[m_0m_1ab + (m_0n_1a + n_0m_1b + n_0n_1c)c] \implies d|1 \implies d = \pm 1.$$

Como d é o maior inteiro que divide ab e c, temos que $d = 1$, como queríamos demonstrar.

■

Teorema 1.15 *Se* $a|bc$ *e* $mdc(a, b) = 1$ *então* $a|c$.

Demonstração: Como $mdc(a, b) = 1$, pelo teorema 1.5, existem números inteiros m e n tais que

$$na + mb = 1. \tag{1.1}$$

Multiplicando a equação (1.1) por c, obtemos

$$nac + mbc = c.$$

Como $a|ac$ e $a|bc$ então, pela observação 1.2(9), $a|c$.

■

Teorema 1.16 *Se a e b são números inteiros e $a = qb + r$ onde q e r são números inteiros, então $mdc(a, b) = mdc(b, r)$.*

Demonstração: Sejam A o conjunto dos divisores de a e b e B o conjunto dos divisores de b e r.

Da relação

$$a = bq + r \tag{1.2}$$

podemos concluir que todo elemento de B pertence a A.

Isolando r em (1.2), obtemos

$$r = a - bq,$$

e daí, conclui-se que todo elemento de A pertence a B.

Logo, $A = B$ e portanto, $mdc(a, b) = mdc(b, r)$.

■

Teorema 1.17 (Algoritmo de Euclides) *Sejam $r_0 = a$ e $r_1 = b$ números inteiros não-negativos com $b \neq 0$. Se o algoritmo da divisão for aplicado sucessivamente para se obter*

$$r_j = q_{j+1} r_{j+1} + r_{j+2},$$

$0 \leq r_{j+2} < r_{j+1}$, *para* $j = 0, 1, 2, \ldots, n-1$ *e* $r_{n+1} = 0$ *então* $mdc(a, b) = r_n$, *o último resto não nulo.*

Demonstração: Aplicando o teorema 1.3 a $r_0 = a$ e $r_1 = b$, existem $q_1, r_2 \in \mathbb{Z}$ tais que $r_0 = q_1 r_1 + r_2$, onde $0 \leq r_2 < r_1$. Em seguida, dividimos r_1 por r_2 obtendo $r_1 = q_2 r_2 + r_3$, com $q_2, r_3 \in \mathbb{Z}$ e $0 \leq r_3 < r_2$. Seguimos aplicando o teorema 1.3 sucessivamente até obter o resto $r_{n+1} = 0$ (isto ocorrerá após um número finito de aplicações do teorema 1.3 pois a cada passo o resto é sempre menor do que o anterior). Portanto, obtemos a sequência de equações

$$\begin{aligned} r_0 &= q_1 r_1 + r_2, & 0 \leq r_2 < r_1 \\ r_1 &= q_2 r_2 + r_3, & 0 \leq r_3 < r_2 \\ &\vdots & \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n, & 0 \leq r_n < r_{n-1} \\ r_{n-1} &= q_n r_n + 0. & \end{aligned}$$

Assim, da última equação temos que $mdc(r_{n-1}, r_n) = r_n$. Pelo teorema 1.16, concluímos que $d = mdc(r_{n-2}, r_{n-1})$. Prosseguindo aplicando o teorema 1.16 às demais equações, obtemos

$$r_n = mdc(r_{n-1}, r_n) = mdc(r_{n-2}, r_{n-1}) = \ldots = mdc(r_1, r_2) = mdc(r_0, r_1) = mdc(a, b).$$

Logo, o $mdc(a, b)$ é o último resto não nulo da sequência de divisões realizadas.

■

Observação 1.18 *O algoritmo que, além de calcular o máximo divisor comum entre a e b, fornece os coeficientes $m_0, n_0 \in \mathbb{Z}$ tais que $am_0 + bn_0 = mdc(a, b)$, é chamado de Algoritmo de Euclides estendido. Este algoritmo é usado, em especial, para o cálculo do inverso modular* (*definição* 1.45)*, que será importante na decodificação de uma mensagem no sistema RSA* (*seção* 2.5)*. Vejamos como proceder para encontrar m_0 e n_0 através de um exemplo* (*exemplo* 1.19)*.*

Exemplo 1.19 *Vamos calcular $mdc(84, 128)$ usando o Algoritmo de Euclides* (*teorema* 1.17) :

$$\begin{aligned} 128 &= 84 \cdot 1 + 44 \\ 84 &= 44 \cdot 1 + 40 \\ 44 &= 40 \cdot 1 + 4 \\ 40 &= 4 \cdot 10. \end{aligned}$$

Assim, $mdc(84, 128) = 4$.

Agora, usando o Algoritmo de Euclides estendido vamos encontrar $m_0, n_0 \in \mathbb{Z}$ tais

que $84m_0 + 128n_0 = 4$*. Das equações anteriores, obtemos*

$$\begin{aligned} 4 &= 44 - 1 \cdot 40 \\ &= 44 - 1 \cdot (84 - 1 \cdot 44) \\ &= 2 \cdot 44 - 1 \cdot 84 \\ &= 2 \cdot (128 - 1 \cdot 84) - 1 \cdot 84 \\ &= -3 \cdot 84 + 2 \cdot 128. \end{aligned}$$

Logo, $m_0 = -3$ *e* $n_0 = 2$*.*

Definição 1.20 *Um número inteiro* n ($n > 1$) *que possui somente dois divisores positivos* n *e* 1 *é chamado primo. Se* $n > 1$ *não é primo, dizemos que* n *é composto.*

Proposição 1.21 *Se* $p|ab$ *e* p *é um número primo, então* $p|a$ *ou* $p|b$*.*

Demonstração: Suponha que $p \not| a$. Como $mdc(a, p) = 1$, pelo teorema 1.15, segue que $p|b$.

■

Teorema 1.22 (Teorema Fundamental da Aritmética) *Todo número inteiro maior que* 1 *pode ser representado de modo único* (*a menos da ordem*) *como um produto de fatores primos.*

Demonstração: No caso em que n é um número primo, o resultado é válido.

Agora vamos considerar o caso em que n é um número composto.

Seja p_1 ($p_1 > 1$) o menor dos divisores positivos de n. Temos que p_1 é primo, pois caso contrário, existiria p, $1 < p < p_1$ com $p|n$, contradizendo a escolha de p_1. Logo, $n = p_1 n_1$.

Se n_1 for primo a prova está completa. Caso contrário, tomamos p_2 como sendo o menor fator de n_1. Pelo argumento anterior, p_2 é primo e temos que $n = p_1 n_1 = p_1 p_2 n_2$.

Continuando este procedimento, podemos obter uma sequência decrescente de números inteiros positivos $n_1, n_2, n_3, \ldots, n_r$, todos eles maiores do que 1 e

portanto, este processo deve terminar. Como os números primos na sequência $p_1, p_2, \cdots, p_k$ não são necessariamente distintos, então n terá a seguinte forma:

$$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_k^{a_k}$$

Para provarmos a unicidade usamos indução sobre n. Para $n = 2$, a unicidade é válida. Assumimos então que a unicidade se verifica para todos os inteiros maiores do que 1 e menores do que n.

Vamos provar que também vale a unicidade para n. Se n é primo não há nada a provar. Vamos supor então, que n seja composto e que tenha duas fatorações, isto é,

$$n = p_1 p_2 p_3 \cdots p_s = q_1 q_2 q_3 \cdots q_r.$$

Mostremos que $s = r$ e que cada $p_i = q_j$. Como p_1 divide o produto $q_1 q_2 \cdots q_r$ ele divide pelo menos um dos fatores q_j. Sem perda de generalidade podemos supor que $p_1 | q_1$. Como são ambos primos, isto implica $p_1 = q_1$. Logo,

$$\frac{n}{p_1} = p_2 p_3 \cdots p_s = q_2 q_3 \cdots q_r. \tag{1.3}$$

Como $1 < n/p_1 < n$, a hipótese de indução nos diz que as duas fatorações de (1.3) são idênticas, isto é, $s = r$ e, a menos da ordem, as fatorações $p_1 p_2 p_3 \cdots p_s$ e $q_1 q_2 q_3 \cdots q_r$ são iguais, como queríamos provar.

■

Teorema 1.23 *Se $n = \prod_{i=1}^{r} p_i^{a_i}$, então o conjunto dos divisores positivos de n é o conjunto de todos os números da forma*

$$\prod_{i=1}^{r} p_i^{c_i}, \ 0 \leq c_i \leq a_i, \ i = 1, 2, 3, \ldots, r.$$

Demonstração: É claro que os divisores positivos de n devem ser da forma $\prod_{i=1}^{r} p_i^{c_i}, 0 \leq c_i \leq a_i, i = 1, 2, 3, \ldots, r,$ pois se c_i não tiver no intervalo mencionado, o

produto acima não será um divisor de n.

■

Teorema 1.24 *O conjunto de todos os números primos é infinito.*

Demonstração: Suponhamos que o conjuntos de todos os números primos seja finito. Consideremos $p_1, p_2, \ldots, p_n$ a lista de todos os números primos.

Tomando $R = p_1 p_2 \cdots p_n + 1$, temos que R não é divisível por nenhum dos p_i da lista e R é maior do que qualquer p_i.

Mas, pelo teorema 1.22, ou R é primo ou possui algum fator primo. Como nenhum p_i da lista divide R, segue que R é um número primo, o que é um absurdo pois R é maior do que qualquer p_i da lista.

Portanto, o conjunto de todos os números primos é infinito.

■

Teorema 1.25 *Se n não é um número primo, então n possui um fator primo menor do que ou igual a* $\sqrt{n}$.

Demonstração: Como n é composto segue que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Suponhamos que $n_1 \leq n_2$.

Logo, $n_1 \leq \sqrt{n}$, pois caso contrário teríamos $n = n_1 n_2 > \sqrt{n} \cdot \sqrt{n} = n$, o que é uma contradição.

Pelo teorema 1.22, n_1 possui algum fator primo p e $p \leq \sqrt{n}$. Como p é um fator primo de n_1 então p também é um fator primo de n, o que conclui a demonstração.

■

Observação 1.26 *Na prática, o resultado anterior é bastante importante pois ele nos diz que para testarmos se um número n é primo, basta testarmos a divisibilidade de n apenas pelos números primos menores do que ou iguais a* $\sqrt{n}$.

Proposição 1.27 *Sejam a e b números inteiros positivos relativamente primos entre si. Se d é divisor de ab, então existe um único par de divisores positivos* d_1 *de a e* d_2

de b tais que $d = d_1 d_2$. Reciprocamente, se d_1 e d_2 são divisores positivos de a e b, respectivamente, então $d = d_1 d_2$ é um divisor positivo de ab.

Demonstração: Consideremos as fatorações de a e b dadas por

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \text{ e } b = q_1^{b_1} q_2^{b_2} \cdots q_m^{b_m}$$

Como $mdc(a, b) = 1$, temos que $p_i \neq q_j$, para todo $i \in \{1, 2, \ldots, n\}$ e para todo $j \in \{1, 2, \ldots, m\}$. Logo, a fatoração de ab é dada por

$$ab = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} q_1^{b_1} q_2^{b_2} \cdots q_m^{b_m}.$$

Assim, se d é um divisor positivo de ab, então

$$d = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} q_1^{\beta_1} q_2^{\beta_2} \ldots q_m^{\beta_m},$$

com $0 \leq \alpha_i \leq a_i, i = 1, 2, 3, \ldots, n$ e $0 \leq \beta_i \leq b_j, j = 1, 2, 3, \ldots, m$.

Defina $d_1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ e $d_2 = q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m}$.

Temos que $mdc(d_1, d_2) = 1$ e $d_1 d_2 = d$.

Reciprocamente, consideremos d_1 e d_2 como divisores positivos de a e b, respectivamente. Logo,

$$d_1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \text{ e } d_2 = q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m},$$

onde $0 \leq \alpha_i \leq a_i, i = 1, 2, 3, \ldots, n$ e $0 \leq \beta_i \leq b_j, j = 1, 2, 3, \ldots, m$.

Portanto,

$$d = d_1 d_2 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m}$$

é um divisor de ab.

■

1.2 Congruência modular

Ao longo deste trabalho, o assunto Congruência Modular é muito importante. Nesta seção, vamos apresentar conceitos e resultados sobre este assunto que serão muito utilizados no decorrer dele.

Definição 1.28 *Sejam a e b números inteiros e $m \in \mathbb{Z}, m > 0$. Dizemos que a é congruente a b módulo m, e denotamos $a \equiv b \pmod{m}$, se $m|(a-b)$. Se $m \nmid (a-b)$, dizemos que a é incongruente a b módulo m e denotamos por $a \not\equiv b \pmod{m}$.*

Proposição 1.29 *Para todos $a, b, c, m \in \mathbb{Z}$, $m > 0$,*

$$a \equiv b \pmod{m} \iff \exists\, x \in \mathbb{Z} \text{ tal que } a = mx + b.$$

Demonstração: Basta observar que,

$a \equiv b \pmod{m} \iff m|(a-b) \iff \exists\, x \in \mathbb{Z}$ tal que $a - b = mx \iff \exists\, x \in \mathbb{Z}$ tal que $a = mx + b$.

■

Proposição 1.30 *Se a, b, m e d são números inteiros, $m > 0$, as seguintes sentenças são verdadeiras:*

1. *(Reflexiva) $a \equiv a \pmod{m}$.*
2. *(Simétrica) Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.*
3. *(Transitiva) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.*

Demonstração:

1. Como $m|(a-a)$, segue que $a \equiv a \pmod{m}$.
2. Por hipótese, $a \equiv b \pmod{m}$, isto é, $m|(a-b)$. Logo, $m|(b-a)$ e consequentemente, $b \equiv a \pmod{m}$.
3. Como $m|(a-b)$, $m|(b-c)$ e $a - c = (a-b) + (b-c)$, temos que $m|(a-c)$. Portanto, $a \equiv c \pmod{m}$.

■

Teorema 1.31 *Para todos $a, b, c, m \in \mathbb{Z}$, $m > 0$, com $a \equiv b \ (mod\ m)$ tem-se:*

1. $a + c \equiv b + c \ (mod\ m)$;
2. $a - c \equiv b - c \ (mod\ m)$;
3. $ac \equiv bc \ (mod\ m)$.

Demonstração:

1. Como $a \equiv b \ (mod\ m)$ temos que $m|(a-b)$. Assim, $a = mx + b$, para algum $x \in \mathbb{Z}$. Deste modo, somando c em ambos os lados da igualdade, segue que

$$a + c = mx + (b + c) \Longrightarrow a + c \equiv b + c \ (mod\ m).$$

2. De maneira análoga ao item anterior, prova-se que $a - c \equiv b - c \ (mod\ m)$.
3. Sabendo que $a \equiv b \ (mod\ m)$, podemos afirmar que $m|(a-b)$. Temos que, $a = mx + b$, para algum $x \in \mathbb{Z}$. Deste modo, multiplicando ambos os lados da igualdade por c, segue que

$$ac = mcx + bc \Longrightarrow \exists\ \bar{x} = cx \in \mathbb{Z} \text{ tal que } ac = m\bar{x} + bc \Longrightarrow ac \equiv bc \ (mod\ m).$$

■

Teorema 1.32 *Se a, b, c e m são números inteiros, com $m > 0$, e $ac \equiv bc \ (mod\ m)$, então $a \equiv b \ (mod\ m/d)$, onde $d = mdc(c, m)$.*

Demonstração: Como $ac \equiv bc \ (mod\ m)$ e $d|c$ e $d|m$ (pois $d = mdc(c, m)$), temos

$$m|(ac - bc) \implies \exists\ k \in \mathbb{Z} \text{ tal que } c(a-b) = km \implies \exists\ k \in \mathbb{Z} \text{ tal que}$$
$$(c/d)(a-b) = k(m/d).$$

Pelo corolário 1.9, segue que $mdc(c/d, m/d) = 1$. Assim,

$$(m/d)|(c/d)(a-b) \overset{Teo.1.15}{\Longrightarrow} (m/d)|(a-b).$$

Portanto, $a \equiv b \ (mod\ m/d)$.

■

Teorema 1.33 *Para todos $a, b, k, m \in \mathbb{Z}$, com $k, m > 0$ onde $a \equiv b \ (mod\ m)$, tem-se:*

$$a^k \equiv b^k \ (mod\ m).$$

Demonstração: Como sabemos que $a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \ldots + b^{k-1})$ e $m|(a-b)$, segue o resultado.

■

Teorema 1.34 *Sejam $m_1, m_2, \ldots, m_k \in \mathbb{N}^*$ e $a, b \in \mathbb{Z}$, onde $a \equiv b \ (mod\ m_1)$, $a \equiv b \ (mod\ m_2), \ldots, a \equiv b \ (mod\ m_k)$. Então,*

$$a \equiv b \ (mod\ [m_1, m_2, \ldots, m_k]),$$

onde $[m_1, m_2, \ldots, m_k]$ é o mínimo múltiplo comum de $m_1, m_2, \ldots, m_k$.

Demonstração: Considere p_n o maior número primo que aparece nas fatorações de $m_1, m_2, \ldots, m_k$. Cada m_i pode ser expresso como

$$m_i = p_1^{\alpha_{1i}} \cdot p_2^{\alpha_{2i}} \cdot \ldots \cdot p_n^{\alpha_{ni}},$$

alguns α_{ji} podem ser nulos.

Como $a \equiv b \ (mod\ m_i)$, com $i \in \{1, 2, \ldots, k\}$, temos que $m_i|(a-b)$, para todo $i \in \{1, 2, \ldots, k\}$. Logo, $p_j^{\alpha_{ji}}|(a-b), i = 1, 2, \ldots, k,\ j = 1, 2, \ldots, n$.

Tomando $\alpha_j = \max\{\alpha_{ji} | \ i = 1, \ldots, k\}$, obtemos

$$p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n} | (a-b).$$

Mas $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n} = [m_1, m_2, \ldots, m_k]$, o que implica que $a \equiv b \ (mod\ [m_1, m_2, \ldots, m_k])$.

■

Definição 1.35 *Se h e k são dois inteiros com $h \equiv k \ (mod\ m)$, dizemos que k é um resíduo de h módulo m.*

Definição 1.36 *O conjunto dos inteiros* $\{r_1, r_2, \ldots, r_s\}$ *é um sistema completo de resíduos módulo* m *se:*

1. $r_i \not\equiv r_j \pmod{m}$, *para* $i \neq j$;
2. *para todo inteiro* n *existe* r_i *tal que* $n \equiv r_i \pmod{m}$.

Exemplo 1.37 *É fácil ver que* $\{0, 1, 2, \ldots, m-1\}$ *é um sistema completo de resíduos módulo* m.

Teorema 1.38 *Se* k *inteiros* $r_1, r_2, \ldots, r_k$ *formam um sistema completo de resíduos módulo* m *então* $k = m$.

Demonstração: Pelo exemplo 1.37, $\{0, 1, 2, \ldots, m-1\}$ é um sistema completo de resíduos módulo m. Assim, cada r_i é congruente a exatamente um dos $i \in \{0, 1, 2, \ldots, m-1\}$, o que nos permite concluir que $k \leq m$. Como, por hipótese, $\{r_1, r_2, \ldots, r_k\}$ forma um sistema completo de resíduos módulo m, cada $i \in \{0, 1, 2, \ldots, m-1\}$ é congruente a exatamente um dos $r_i's$ e portanto, $m \leq k$. Logo, $k = m$.

■

Teorema 1.39 *Se* $r_1, r_2, \ldots, r_m$ *é um sistema completo de resíduos módulo* m *e* a *e* b *são números inteiros tais que* $mdc(a, b) = 1$, *então*

$$ar_1 + b, ar_2 + b, \ldots, ar_m + b$$

também é um sistema completo de resíduos módulo m.

Demonstração: Considerando a demonstração do teorema 1.38, basta mostrar que quaisquer dois elementos do conjunto $\{ar_1 + b, ar_2 + b, \ldots, ar_m + b\}$ são incongruentes módulo m.

Suponhamos que $ar_i + b \equiv ar_j + b \pmod{m}, i \neq j$. Do teorema 1.31(2), temos

$$ar_i \equiv ar_j \pmod{m}.$$

Como $mdc(a, m) = 1$, pelo teorema 1.32, segue que

$$r_i \equiv r_j \ (mod\ m),$$

o que é um absurdo pois $\{r_1, r_2, \ldots, r_m\}$ é um sistema completo de resíduos módulo m.

■

1.3 Congruência linear

Definição 1.40 *Chamamos de congruência linear em uma variável a uma congruência da forma* $ax \equiv b \ (mod\ m)$, *onde* x *é uma incógnita.*

Observação 1.41 *Se* x_0 *é uma solução de* $ax \equiv b \ (mod\ m)$ *(ou seja,* $ax_0 \equiv b \ (mod\ m)$*) e* $x_1 \equiv x_0 \ (mod\ m)$, *então* x_1 *também é solução de* $ax \equiv b \ (mod\ m)$.

Teorema 1.42 *Sejam* a, b *e* m *inteiros tais que* $m > 0$ *e* $mdc(a, b) = d$.

1. *Se* $d \nmid c$, *então a equação* $ax + by = c$ *não possui solução inteira.*
2. *Se* $d|c$, *então a equação* $ax + by = c$ *possui infinitas soluções. Se* $x = x_0$ *e* $y = y_0$ *é uma solução particular, então todas as soluções são dadas por*

$$x = x_0 + (b/d)k$$
$$y = y_0 - (a/d)k,$$

onde k *é um número inteiro.*

Demonstração:

1. Suponhamos que $ax + by = c$ possui solução inteira (x_0, y_0), ou seja, $ax_0 + by_0 = c$. Como $d = mdc(a, b)$ segue que $d|ax_0 + by_0$. Logo, $d|c$, o que é um absurdo.
2. Como $d = mdc(a, b)$, pelo teorema 1.5, temos que existem inteiros n_0 e m_0 tais que $an_0 + bm_0 = d$.

   Por hipótese, $d|c$ e então existe $l \in \mathbb{Z}$ tal que $c = ld$. Assim,

$$a(n_0 l) + b(m_0 l) = ld = c.$$

Portanto, o par (x_0, y_0) com $x_0 = n_0 l$ e $y_0 = m_0 l$ é uma solução particular da equação $ax + by = c$.

Agora, para todo $k \in \mathbb{Z}$, observe que

$$x = x_0 + (b/d)k \quad \text{e} \quad y = y_0 - (a/d)k$$

são soluções da equação $ax + by = c$ uma vez que $a(x_0 + (b/d)k) + b(y_0 - (a/d)k) = c$.

Logo, a partir de uma solução particular (x_0, y_0), podemos gerar infinitas soluções inteiras para a equação $ax + by = c$.

Falta mostrar que toda solução da equação $ax + by = c$ é da forma $x = x_0 + (b/d)k, y = y_0 - (a/d)k$. Suponhamos que (x, y) seja uma solução, isto é, $ax + by = c$. Como $ax_0 + by_0 = c$, obtemos

$$\begin{aligned} 0 &= c - c \\ &= ax + by - (ax_0 + by_0) \\ &= a(x - x_0) + b(y - y_0), \end{aligned}$$

o que implica que $a(x - x_0) = b(y_0 - y)$.

Sabemos que $d = mdc(a, b)$ e daí, pelo corolário 1.9, $mdc(a/d, b/d) = 1$. Assim,

$$a(x - x_0) = b(y_0 - y) \implies (a/d)(x - x_0) = (b/d)(y_0 - y).$$

Logo,

$$(b/d)|(a/d)(x - x_0) \overset{teo.1.15}{\implies} (b/d)|(x - x_0) \implies \exists\ k \in \mathbb{Z} \text{ tal que } x = x_0 + (b/d)k.$$

Substituindo $x = x_0 + (b/d)k$ na equação $(a/d)(x - x_0) = (b/d)(y_0 - y)$, obtemos $y = y_0 - (a/d)k$, o que conclui a demonstração.

■

Teorema 1.43 *Sejam a, b e m números inteiros tais que $m > 0$ e $mdc(a, m) = d$. No caso em que $d \nmid b$ a congruência $ax \equiv b \pmod{m}$ não possui nenhuma solução e*

quando $d|b$, possui exatamente d soluções incongruentes módulo m.

Demonstração: Pela proposição 1.29, x é solução de $ax \equiv b \ (mod \ m)$ se, e somente se, existe $y \in \mathbb{Z}$ tal que $ax = b+my$. Logo, existe $y \in \mathbb{Z}$ tal que $ax-my = b$.

Primeiro, suponhamos que $d \nmid b$.

Neste caso, pelo teorema anterior, temos que a equação $ax - my = b$ não possui solução.

Agora, suponhamos que $d|b$.

Do teorema anterior concluímos que $ax - my = b$ possui infinitas soluções dadas por

$$x = x_0 - (m/d)k \ \text{ e } \ y = y_0 - (a/d)k,$$

onde (x_0, y_0) é uma solução particular de $ax - my = b$ e k é um inteiro qualquer. Assim, a congruência $ax \equiv b \ (mod \ m)$ possui infinitas soluções dadas por

$$x = x_0 - (m/d)k.$$

Falta mostrar que existem exatamente d soluções incongruentes módulo m para a congruência $ax \equiv b \ (mod \ m)$.

Mostremos que duas soluções $x_1 = x_0 - (m/d)k_1$ e $x_2 = x_0 - (m/d)k_2$ são congruentes se, e somente se, $k_1 \equiv k_2 \ (mod \ d)$. De fato,

$$x_1 \equiv x_2 \ (mod \ m) \iff (m/d)k_1 \equiv (m/d)k_2 \ (mod \ m).$$

Como $mdc(m/d, m) = m/d$ e $m/(m/d) = d$, pelo teorema 1.32, obtemos

$$(m/d)k_1 \equiv (m/d)k_2 \ (mod \ m) \iff k_1 \equiv k_2 \ (mod \ d).$$

Isto nos mostra que as soluções incongruentes são da forma $x = x_0 - (m/d)k$, onde k percorre um sistema completo de resíduos módulo d, o que conclui a demonstração.

■

Definição 1.44 *Dizemos que uma solução x_0 de $ax \equiv b \ (mod\ m)$ é única módulo m quando qualquer solução x_1 for congruente a x_0 módulo m.*

Definição 1.45 *Uma solução $\overline{a}$ de $ax \equiv 1 \ (mod\ m)$ é chamada de um inverso de a módulo m.*

Observação 1.46

1. *No caso em que existe uma solução para a congruência $ax \equiv 1 \ (mod\ m)$, dizemos que a é inversível módulo m.*
2. *A próxima proposição nos diz quando um inteiro x é o seu próprio inverso módulo p.*

Proposição 1.47 *Seja p um número primo. O inteiro positivo x é tal que $x^2 \equiv 1 \ (mod\ p)$ se, e somente se, $x \equiv 1 \ (mod\ p)$ ou $x \equiv -1 \ (mod\ p)$.*

Demonstração: Se x é tal que $x^2 \equiv 1 \ (mod\ p)$, então $p|(x^2-1)$. Logo,

$$p|(x-1)(x+1) \overset{prop.1.21}{\Longrightarrow} x \equiv 1 \ (mod\ p) \text{ ou } x \equiv -1 \ (mod\ p).$$

A recíproca é de simples verificação pois

$$x \equiv 1 \ (mod\ p) \text{ ou } x \equiv -1 \ (mod\ p) \Longrightarrow p|(x-1)(x+1) \Longrightarrow x^2 \equiv 1 \ (mod\ p).$$

■

Proposição 1.48 *Sejam a e m números inteiros, com $m > 0$. Então, a é inversível módulo m se, e somente se, $mdc(a,m) = 1$.*

Demonstração: Seja $d = mdc(a,m)$. Mostremos que $d = 1$.

Sabemos que existe $b \in \mathbb{Z}$ tal que $ab \equiv 1 \ (mod\ m)$. Assim,

$$m|(ab-1) \implies \exists\ x \in \mathbb{Z} \text{ tal que } ab - mx = 1.$$

Como $d = mdc(a,m)$ segue que $d|a$ e $d|m$. Logo, $d|(ab-mx) = 1$ e então, $d = 1$.

Reciprocamente, suponhamos que $mdc(a,m) = 1$.

Pelo teorema 1.5, temos que existem $x, y \in \mathbb{Z}$ tais que $ax + my = 1$. Então, existem $x, y \in \mathbb{Z}$ tais que $ax - 1 = m(-y)$.

Logo, $m|(ax-1)$ e portanto, $ax \equiv 1\ (mod\ m)$.

■

Observação 1.49 *Pela proposição anterior, no caso em que a é inversível módulo m, como $mdc(a, m) = 1$ segue que existem $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + my_0 = 1$. Temos que x_0 é um inverso de a módulo m pois*

$$ax_0 + my_0 = 1 \implies m(-y_0) = ax_0 - 1 \implies m|(ax_0 - 1) \implies ax_0 \equiv 1\ (mod\ m).$$

Lembrando que x_0 deve ser encontrado utilizando o Algoritmo de Euclides estendido (observação 1.18).

1.4 Teoremas de Wilson, Fermat e Euler

Teorema 1.50 (Teorema de Wilson) *Se p é um número primo, então $(p-1)! \equiv -1\ (mod\ p)$.*

Demonstração: Para $p = 2$ e $p = 3$, o resultado é válido pois $(2-1)! \equiv 1 \equiv -1\ (mod\ 2)$ e $(3-1)! \equiv 2 \equiv -1\ (mod\ 3)$.

Pelo teorema 1.43, a congruência $ax \equiv 1\ (mod\ p)$ tem uma única solução para todo $a \in \{1, 2, 3, \ldots, p-1\}$. Observe que, no conjunto $\{1, 2, 3, \ldots, p-1\}$, apenas 1 e $p-1$ são seus próprios inversos módulo p. Então, podemos agrupar os números $2, 3, 4, \ldots, p-2$ em $(p-3)/2$ pares cujo produto seja congruente a 1 módulo p. Multiplicando estas congruências, membro a membro, obtemos

$$2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-2) \equiv 1\ (mod\ p).$$

Multiplicando ambos os lados desta congruência por $p-1$ teremos

$$2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-2) \cdot (p-1) \equiv p-1\ (mod\ p).$$

Portanto, como $p - 1 \equiv -1\ (mod\ p)$ segue que $(p-1)! \equiv -1\ (mod\ p)$.

■

Teorema 1.51 *Se n é número inteiro positivo para o qual $(n-1)! \equiv -1 \ (mod \ n)$, então n é um número primo.*

Demonstração: Suponhamos que n não seja um número primo. Então, $n = r \cdot s$, com $1 < r < n$ e $1 < s < n$. Daí, $r|(n-1)!$ pois $1 < r < n$.

Como $(n-1)! \equiv -1 \ (mod \ n)$ segue que $n|[(n-1)!+1]$. Assim, $r|[(n-1)!+1]$. Logo,

$$r|[(n-1)!+1] \text{ e } r|(n-1)! \implies r|1,$$

o que é uma contradição pois $r > 1$.

■

Teorema 1.52 (Pequeno Teorema de Fermat) *Seja p um número primo. Se $p \nmid a$, então $a^{p-1} \equiv 1 \ (mod \ p)$.*

Demonstração: Pelo exemplo 1.37, sabemos que o conjunto $\{0, 1, 2, \ldots, p-1\}$ é um sistema completo de resíduos módulo p.

Como $mdc(a, p) = 1$, nenhum dos números $1a, 2a, \ldots, (p-1)a$ é divisível por p, ou seja, nenhum deles é congruente a 0 módulo p. Além disso, quaisquer ja e ka, com $j, k \in \{1, 2, \ldots, p-1\}$ e $j \neq k$, são incongruentes (entre si) módulo p, pois

$$ja \equiv ka \ (mod \ p) \implies p|(j-k)a \overset{teo.1.15}{\implies} p|(j-k) \implies j = k,$$

o que é uma contradição.

Logo, cada elemento de $\{1a, 2a, \ldots, (p-1)a\}$ é congruente a exatamente um elemento de $\{1, 2, \ldots, p-1\}$. Assim,

$$1a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \ (mod \ p) \implies a^{p-1}(p-1)! \equiv (p-1)! \ (mod \ p).$$

Portanto,

$$p|(a^{p-1}-1)(p-1)! \overset{teo.1.15}{\implies} p|(a^{p-1}-1) \implies a^{p-1} \equiv 1 \ (mod \ p).$$

■

Corolário 1.53 *Se p é um número primo e a é um número inteiro positivo, então $a^p \equiv a \pmod{p}$.*

Demonstração: Vamos separar a demonstração em dois casos:

1. $p|a$.

   Neste caso, $p|a(a^{p-1}-1)$ e portanto, $a^p \equiv a \pmod{p}$.

2. $p \nmid a$.

   Neste caso, pelo teorema 1.52, $p|(a^{p-1}-1)$ e então, $p|a(a^{p-1}-1)$. Desse modo, $a^p \equiv a \pmod{p}$.

■

Definição 1.54 *Se n é um inteiro positivo, a função ϕ de Euler, denotada por $\phi(n)$, é definida como sendo o número de inteiros positivos menores do que ou iguais a n que são relativamente primos com n.*

Exemplo 1.55 *Se p é um número inteiro positivo e primo então $\phi(p) = p - 1$.*

Definição 1.56 *Um sistema reduzido de resíduos módulo m é um conjunto de $\phi(m)$ inteiros $r_1, r_2, \ldots, r_{\phi(m)}$ tais que cada elemento do conjunto é relativamente primo com m, e se $i \neq j$, então $r_i \not\equiv r_j \pmod{m}$.*

Exemplo 1.57 *O conjunto $\{0, 1, 2, 3, 4, 5, 6, 7\}$ é um sistema completo de resíduos módulo 8, portanto $\{1, 3, 5, 7\}$ é um sistema reduzido de resíduos módulo 8. Para se obter um sistema reduzido de resíduos de um sistema completo módulo m, basta retirar os elementos do sistema completo que não são relativamente primos com m.*

Teorema 1.58 *Seja a um inteiro positivo tal que $mdc(a, m) = 1$. Se $r_1, r_2, r_3, \ldots, r_{\phi(m)}$ é um sistema reduzido de resíduos módulo m, então $ar_1, ar_2, \ldots, ar_{\phi(m)}$ também é um sistema reduzido de resíduos módulo m.*

Demonstração: Na sequência $ar_1, ar_2, \ldots, ar_{\phi(m)}$ temos $\phi(m)$ elementos, então devemos mostrar que todos eles são relativamente primos com m e, dois a dois, incongruentes módulo m.

Pela proposição 1.14, como $mdc(a,m) = 1$ e $mdc(r_i, m) = 1$, temos que $mdc(ar_i, m) = 1$. Falta mostrar que $ar_i \not\equiv ar_j \ (mod\ m)$, se $i \neq j$. Note que

$$ar_i \equiv ar_j \ (mod\ m) \implies m|a(r_i - r_j) \overset{teo.1.15}{\implies} m|(r_i - r_j) \implies r_i \equiv r_j \ (mod\ m).$$

Portanto, $i = j$, pois $r_1, r_2, \ldots, r_{\phi(m)}$ é um sistema reduzido de resíduos módulo m, o que conclui a demonstração.

■

Teorema 1.59 (Teorema de Euler) *Se m é um inteiro positivo e a é número inteiro tal que $mdc(a,m) = 1$ então $a^{\phi(m)} \equiv 1 \ (mod\ m)$.*

Demonstração: No teorema anterior mostramos que os elementos $ar_1, ar_2, \ldots, ar_{\phi(m)}$ formam um sistema reduzido de resíduos módulo m se $mdc(a,m) = 1$ e $r_1, r_2, \ldots, r_{\phi(m)}$ for um sistema reduzido de resíduos módulo m. Logo, ar_i é congruente a exatamente um $r_j, 1 \leq j \leq \phi(m)$. Assim,

$$ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\phi(m)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(m)} \ (mod\ m),$$

ou seja,

$$a^{\phi(m)} r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(m)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(m)} \ (mod\ m).$$

Então, $m|r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(m)}(a^{\phi(m)} - 1)$. Como $mdc(r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(m)}, m) = 1$ (pela proposição 1.14), segue que $a^{\phi(m)} \equiv 1 \ (mod\ m)$.

■

Observação 1.60 *É importante ressaltar que o teorema 1.59 é uma generalização do teorema 1.52.*

1.5 Funções aritméticas

Nesta seção, estudamos funções aritméticas e apresentamos alguns resultados sobre funções aritméticas multiplicativas. Veremos que para avaliar uma função multiplicativa basta conhecer seu valor em potências de números primos.

Definição 1.61 *Chamamos de função aritmética uma função definida para todos os inteiros positivos.*

Definição 1.62 *$\tau(n)$ é o número de divisores positivos de n e $\sigma(n)$ a soma dos divisores positivos de n. Usando a notação de somatório podemos definir estas funções da seguinte maneira:*

$$\tau(n) = \sum_{d|n} 1 \quad e \quad \sigma(n) = \sum_{d|n} d.$$

Proposição 1.63 *Se a decomposição em fatores primos de n é $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, então $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)\dots(\alpha_r + 1)$.*

Demonstração: Primeiro, observe que todo número da forma p_1^t, com $0 \leq t \leq \alpha_1$, é um divisor de $p_1^{\alpha_1}$. Então, $\tau(p_1^{\alpha_1}) = \alpha_1 + 1$.

Caso $n = p_1^{\alpha_1} p_2^{\alpha_2}$, com p_1 e p_2 primos distintos, temos que $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)$. O caso geral segue por indução.

■

Definição 1.64 *Uma função multiplicativa f é uma função aritmética (não-nula) tal que $f(mn) = f(m)f(n)$, para todo par de inteiros positivos m e n relativamente primos.*

Teorema 1.65 *Se $f(n)$ é uma função multiplicativa então*

$$F(n) = \sum_{d|n} f(d)$$

é também multiplicativa.

Demonstração: Devemos mostrar que $F(mn) = F(m)F(n)$, para todo par m e n relativamente primos. Pela definição de $F(n)$ temos

$$F(mn) = \sum_{d|mn} f(d).$$

Como $mdc(m,n) = 1$, pela proposição 1.27, segue que todo divisor de mn pode ser expresso, de modo único, como o produto de d_1 e d_2, com $d_1|m, d_2|n$ e $mdc(d_1,d_2) = 1$ e cada par de divisores d_1 de m e d_2 de n corresponde um único divisor $d = d_1d_2$ de mn. Logo,

$$\begin{aligned} F(mn) &= \sum_{d|mn} f(d) \\ &= \sum_{d_1|m, d_2|n} f(d_1d_2). \end{aligned}$$

Por hipótese, f é multiplicativa e daí,

$$\begin{aligned} F(mn) &= \sum_{d_1|m, d_2|n} f(d_1)f(d_2) \\ &= \sum_{d_1|m} \sum_{d_2|n} f(d_1)f(d_2) \\ &= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) \\ &= F(m)F(n). \end{aligned}$$

■

Corolário 1.66 *As funções $\tau(n)$ e $\sigma(n)$ são multiplicativas.*

Demonstração: Como

$$\tau(n) = \sum_{d|n} 1 \quad \text{e} \quad \sigma(n) = \sum_{d|n} d,$$

e $f(d) = 1$ e $f(d) = d$ são funções multiplicativas, segue o resultado.

■

Proposição 1.67 *Sejam p um número primo e a um número inteiro positivo. Então,*

$$\sigma(p^\alpha) = \frac{p^{\alpha+1}-1}{p-1} \quad e \quad \tau(p^\alpha) = \alpha + 1.$$

Demonstração: Como os divisores positivos de p^α são $1, p, p^2, \ldots, p^\alpha$ segue que

$$\tau(p^\alpha) = \alpha + 1 \quad \text{e} \quad \sigma(p^\alpha) = 1 + p + p^2 + \ldots + p^\alpha.$$

Por indução sobre α, como $p \neq 1$, prova-se que $1 + p + p^2 + \ldots + p^\alpha = \frac{p^{\alpha+1}-1}{p-1}$.

Portanto,

$$\tau(p^\alpha) = \alpha + 1 \quad \text{e} \quad \sigma(p^\alpha) = \frac{p^{\alpha+1}-1}{p-1}.$$

■

Proposição 1.68 *Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, então*

$$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1}-1}{p_i-1} \quad e \quad \tau(n) = \prod_{i=1}^{r} (\alpha_i + 1).$$

Demonstração: Como $\tau(n)$ e $\sigma(n)$ são funções multiplicativas, pela proposição 1.67, temos que

$$\begin{aligned}
\tau(n) &= \tau(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}) \\
&= \tau(p_1^{\alpha_1})\tau(p_2^{\alpha_2}) \cdots \tau(p_r^{\alpha_r}) \\
&= (\alpha_1 + 1)(\alpha_2 + 2) \cdots (\alpha_r + 1) \\
&= \prod_{i=1}^{r} (\alpha_i + 1)
\end{aligned}$$

e

$$\begin{aligned}
\sigma(n) &= \sigma(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}) \\
&= \sigma(p_1^{\alpha_1})\sigma(p_2^{\alpha_2}) \cdots \sigma(p_r^{\alpha_r}) \\
&= \left(\frac{p_1^{\alpha_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{\alpha_2+1}-1}{p_2-1}\right) \cdots \left(\frac{p_r^{\alpha_r+1}-1}{p_r-1}\right) \\
&= \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1}-1}{p_i-1}.
\end{aligned}$$

■

Na definição 1.54, apresentamos a função ϕ de Euler. Vamos mostrar que esta função aritmética é multiplicativa (Teorema 1.71). Para isto, antes precisamos provar o seguinte teorema.

Teorema 1.69 *Para p um número primo e α um inteiro positivo, temos*

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

Demonstração: Pela definição 1.54, sabemos que $\phi(p^\alpha)$ é o número de inteiros positivos não superiores a p^α que são relativamente primos com p^α. Como p é primo, os únicos números que não são relativamente primos com p^α são os múltiplos de p. A quantidade de múltiplos de p entre 1 e p^α é

$$p^\alpha \div p = p^{\alpha-1}.$$

Portanto,

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

■

Exemplo 1.70 $\phi(125) = \phi(5^3) = 5^3 - 5^2 = 100,\ \ \phi(128) = \phi(2^7) = 2^7 - 2^6 = 64.$

Teorema 1.71 *A função ϕ de Euler é multiplicativa, isto é, $\phi(mn) = \phi(m)\phi(n)$, para m e n inteiros positivos tais que $mdc(m,n) = 1$.*

Demonstração: Segue abaixo uma tabela com todos os números de 1 a mn.

1	m+1	2m+1	...	(n-1)m+1
2	m+2	2m+2	...	(n-1)m+2
3	m+3	2m+3	...	(n-1)m+3
⋮	⋮	⋮	⋮	⋮
m	2m	3m	...	nm

Se na linha r, onde estão os termos $r, m+r, 2m+r, \ldots, (n-1)m+r$, tivermos $mdc(m,r) = d > 1$, então nenhum termo nesta linha será relativamente primo

com mn pois como estes termos são da forma $km + r, 0 \leq k \leq n-1$, temos que são divisíveipor $d = mdc(m, r)$.

Assim, para encontrarmos inteiros nesta tabela que são relativamente primos com mn, devemos olhar na linha r somente se $mdc(m, r) = 1$. Logo, temos $\phi(m)$ linhas onde todos os elementos são relativamente primos com m.

Como $mdc(m, n) = 1$, devemos procurar em cada uma dessas $\phi(m)$ linhas quantos elementos são relativamente primos com n, uma vez que todos são relativamente primos com m. Desse modo, cada uma destas $\phi(m)$ linhas possui $\phi(n)$ elementos relativamente primos com m e com n e portanto, eles são relativamente primos com mn. Isso nos permite concluir que

$$\phi(mn) = \phi(m)\phi(n).$$

■

Teorema 1.72 *Para $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, temos*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

Demonstração: Do teorema 1.69 segue que

$$\begin{aligned}\phi(p_i^{\alpha_i}) &= p_i^{\alpha_i} - p_i^{\alpha_i - 1} \\ &= p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right).\end{aligned}$$

Pelo teorema 1.71, temos

$$\begin{aligned}\phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}) &= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right)\cdots p_r^{\alpha_r}\left(1 - \frac{1}{p_r}\right) \\ &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).\end{aligned}$$

■

CAPÍTULO 2

Criptografia

O foco deste trabalho é o estudo sobre criptografia. Neste capítulo, vamos destacar dois sistemas criptográficos, a saber, Cifra de César (seções 2.1 e 2.2) e Criptografia RSA (seções 2.3, 2.4, 2.5 e 2.6).

2.1 Cifra de César: conceito

Uma cifra é um sistema que transforma um texto simples em um texto cifrado aplicando um conjunto de transformações a cada caractere (ou letra) do texto simples. As transformações particulares empregadas em qualquer momento são controladas por uma chave de criptografia usada naquele momento. A segurança do texto cifrado depende fortemente do sigilo da chave de criptografia. O objetivo de quem quer decifrar o texto cifrado é encontrar a chave de criptografia e consequentemente quebrar o sistema.

Um dos primeiros sistemas criptográficos conhecidos foi usado por Júlio César e é chamado de *Cifra de César*. É um tipo de cifra na qual cada letra do texto é substituída por outra, que se apresenta no alfabeto após ela um número fixo de vezes. A esse número fixo de vezes chamamos de chave de criptografia e denotamos por β. No exemplo a seguir, usamos $\beta = 3$.

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

Este tipo de criptografia foi a maneira encontrada por Júlio César para se comunicar com as tropas por toda a Europa de modo que as informações se mantivessem sigilosas e foi eficaz na época uma vez que o analfabetismo e a confusão com um idioma desconhecido era comum quando o código era interceptado.

Exemplo 2.1 *Utilizando a Cifra de César e $\beta = 3$, a frase cifrada relativa à frase simples*

VENCEMOS EM MONTEVIDÉU

é

YHQFHPRV HP PRQWHYLGHX.

2.2 Congruência modular e a Cifra de César

Uma outra maneira de compreender a Cifra de César é analisando-a via congruências modulares de modo que cada letra do alfabeto é associada a um dos números do conjunto $\{0, 1, 2, \ldots, 25\}$ (conjunto dos possíveis restos da divisão de um número inteiro por 26) como segue.

Tabela 2.1: Correspondência Cifra de César

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

Após a realização da correspondência entre as letras da mensagem simples e os respectivos números de acordo com a tabela anterior, teremos uma mensagem simples composta por uma sequência numérica.

Considere β a chave de criptografia. Então, $\beta \in \mathbb{Z}, 0 \leq \beta \leq 25$.

Sejam M o número correspondente de uma letra da mensagem simples de acordo com a tabela anterior e $E_\beta(M)$ o número M cifrado. Calculamos $E_\beta(M)$ da seguinte maneira:

$$(M + \beta) \equiv E_\beta(M) \ (mod\ 26),$$

onde $0 \leq E_\beta(M) \leq 25$.

Exemplo 2.2 *Considerando a mensagem simples*

VENCEMOS EM MONTEVIDÉU,

e $\beta = 5$*, vamos obter a mensagem cifrada usando congruência modular. De acordo com a tabela* 2.1*, temos a seguinte correspondência entre as letras da mensagem simples e os números:*

V	*E*	*N*	*C*	*E*	*M*	*O*	*S*	*E*	*M*	*M*	*O*	*N*	*T*	*E*	*V*	*I*	*D*	*E*	*U*
21	4	13	2	4	12	14	18	4	12	12	14	13	19	4	21	8	3	4	20

Realizando as congruências, obtemos

1. $M = 21 \implies E_5(M) = 0$ *pois*

$$21 + 5 = 26 \equiv 0 \ (mod\ 26).$$

2. $M = 4 \implies E_5(M) = 9$ *pois*

$$4 + 5 = 9 \equiv 9 \ (mod\ 26).$$

3. $M = 13 \implies E_5(M) = 18$ *pois*

$$13 + 5 = 18 \equiv 18 \ (mod\ 26).$$

4. $M = 2 \implies E_5(M) = 7$ *pois*

$$2 + 5 = 7 \equiv 7 \ (mod\ 26).$$

5. $M = 12 \implies E_5(M) = 17$ *pois*

$$12 + 5 = 17 \equiv 17 \ (mod\ 26).$$

6. $M = 14 \implies E_5(M) = 19$ *pois*

$$14 + 5 = 19 \equiv 19 \ (mod\ 26).$$

7. $M = 18 \implies E_5(M) = 23$ *pois*

$$18 + 5 = 23 \equiv 23 \ (mod\ 26).$$

8. $M = 19 \implies E_5(M) = 24$ *pois*

$$19 + 5 = 24 \equiv 24 \ (mod\ 26).$$

9. $M = 8 \implies E_5(M) = 13$ *pois*

$$8 + 5 = 13 \equiv 13 \ (mod\ 26).$$

10. $M = 3 \implies E_5(M) = 8$ *pois*

$$3 + 5 = 8 \equiv 8 \ (mod\ 26).$$

11. $M = 20 \implies E_5(M) = 25$ *pois*

$$20 + 5 = 25 \equiv 25 \ (mod\ 26).$$

Logo, de acordo com a tabela 2.1, a correspondência entre números e letras da mensagem cifrada é a seguinte

0	9	18	7	9	17	19	23	9	17	17	19	18	24	9	0	13	8	9	25
A	*J*	*S*	*H*	*J*	*R*	*T*	*X*	*J*	*R*	*R*	*T*	*S*	*Y*	*J*	*A*	*N*	*I*	*J*	*Z*

Portanto, a mensagem cifrada é

AJSHJRTX JR RTSYJANIJZ.

Observação 2.3 *Conhecendo a chave de criptografia β é possível decifrar uma mensagem cifrada também usando congruência modular. Para isto, sejam C um número cifrado e $D_\beta(C)$ o número C decifrado. Podemos calcular $D_\beta(C)$ através da relação de congruência que segue:*

$$(C + 26 - \beta) \equiv D_\beta(C) \ (mod\ 26),$$

onde $0 \leq D_\beta(C) \leq 25$.

Exemplo 2.4 *Considerando a mensagem numérica cifrada do exemplo 2.2, vamos decifrá-la usando a relação de congruência dada na observação 2.3. Sabemos que $\beta = 5$ e temos que*

1. $C = 0 \implies D_5(C) = 21$ *pois*

$$0 + 26 - 5 = 21 \equiv 21 \ (mod\ 26).$$

2. $C = 9 \implies D_5(C) = 4$ *pois*

$$9 + 26 - 5 = 30 \equiv 4 \ (mod\ 26).$$

3. $C = 18 \implies D_5(C) = 13$ *pois*

$$18 + 26 - 5 = 39 \equiv 13 \ (mod\ 26).$$

4. $C = 7 \implies D_5(C) = 2$ *pois*

$$7 + 26 - 5 = 28 \equiv 2 \ (mod\ 26).$$

5. $C = 17 \implies D_5(C) = 12$ *pois*

$$17 + 26 - 5 = 38 \equiv 12 \ (mod\ 26).$$

6. $C = 19 \implies D_5(C) = 14$ *pois*

$$19 + 26 - 5 = 40 \equiv 14 \ (mod\ 26).$$

7. $C = 23 \implies D_5(C) = 18$ *pois*

$$23 + 26 - 5 = 44 \equiv 18 \ (mod\ 26).$$

8. $C = 24 \implies D_5(C) = 19$ *pois*

$$24 + 26 - 5 = 45 \equiv 19 \ (mod\ 26).$$

9. $C = 13 \implies D_5(C) = 8$ *pois*

$$13 + 26 - 5 = 34 \equiv 8 \ (mod\ 26).$$

10. $C = 8 \implies D_5(C) = 3$ *pois*

$$8 + 26 - 5 = 29 \equiv 3 \ (mod\ 26).$$

11. $C = 25 \implies D_5(C) = 20$ *pois*

$$25 + 26 - 5 = 46 \equiv 20 \ (mod\ 26).$$

De acordo com os resultados das congruências e a tabela 2.1, obtemos a mensagem

VENCEMOS EM MONTEVIDÉU.

Observação 2.5 *1. Segundo [5], é conhecido que, na sua época, Júlio César usou $\beta = 3$ como a chave de criptografia para o seu sistema de cifras. Não é conhecido o motivo dessa escolha. Como, neste sistema, operamos com congruência módulo 26, ele poderia ter escolhido como chave de criptografia qualquer inteiro β, $0 \leq \beta \leq 25$, sendo que uma dessas chaves ($\beta = 0$) é a identidade e não oferece nenhum sigilo.*

2. É importante ressaltar que uma mensagem cifrada por uma Cifra de César é extremamente insegura, pois a análise criptográfica exaustiva usando as 25 chaves de criptografia não triviais é facilmente realizada.

2.3 Introdução ao método RSA

O método RSA é o mais conhecido dos métodos de criptografia de chave pública. Foi inventado em 1977 por R. Rivest, A. Shamir e L. Adleman que trabalhavam no Massachussets Institute of Technology (M.I.T.). Atualmente, é um código de chave pública bastante utilizado em aplicações comerciais, no processo de criptografia de dados envolvendo e-mail, e-commerce e assinaturas digitais.

Para usar o método RSA é necessário converter a mensagem em uma sequência de números. Para simplificar, vamos supor que a mensagem original é um texto que possui somente letras. Assim, a mensagem é constituída pelas letras que formam as palavras e pelos espaços entre palavras. Chamaremos esta etapa de pré-codificação.

Na pré-codificação fazemos cada letra do alfabeto corresponder a um número conforme a seguinte tabela:

Tabela 2.2: Correspondência Criptografia RSA

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

Quando for feita a correspondência entre letra e número, o espaço entre duas palavras será substituído pelo número 99.

Observação 2.6 *Observe que é importante fazer cada letra corresponder a um número de dois algarismos pois isso evita ambiguidades. Por exemplo, se A correspondesse ao número* 1*, B correspondesse ao número* 2 *e assim por diante, então L corresponderia ao número* 12*. Neste caso o número* 12 *poderia ser AB ou L.*

Exemplo 2.7 *De acordo com a tabela* 2.2*, a frase PALMEIRAS É CAMPEÃO é convertida no número:*

25102122141827102899149912102225141024

Para dar continuidade ao processo de pré-codificação precisamos determinar os parâmetros do sistema RSA que vamos usar. Estes parâmetros são dois números primos distintos p e q.

Seja $n = pq$. Utilizando o exemplo 2.7, vamos separar em blocos o longo número produzido nele. Os blocos devem conter números menores que n e não podem começar por 0. Além disso, é bom que os blocos não correspondam a alguma unidade linguística (palavra, letra ou qualquer outra) pois isso torna a decodificação por contagem de frequência praticamente impossível.

Vamos escolher $p = 17$ e $q = 23$. Logo, $n = 391$.

A mensagem pode ser separada em blocos da seguinte maneira:

$$2-5-102-122-141-82-7-102-89-91-49-91-2-102-225-1-4-102-4 \tag{2.1}$$

Desse modo, encerramos a etapa de pré-codificação. Vamos passar às etapas de codificação (seção 2.4) e decodificação (seção 2.5).

2.4 Codificação

A fim de codificar a mensagem precisamos de $n = pq$ e de um número inteiro positivo e que seja inversível módulo $\phi(n)$ (ou seja, $mdc(e, \phi(n)) = 1$ (proposição 1.48)). Pelo teorema 1.71 e exemplo 1.55, sabemos que

$$\phi(n) = (p-1)(q-1).$$

Definição 2.8 *Chamamos o par (n, e) de chave de codificação do sistema RSA.*

Observação 2.9 *O processo de codificação da mensagem seguirá os seguintes passos:*

1. *Tendo a mensagem passado pelo processo de pré-codificação, temos uma sequência de blocos. A codificação de cada bloco será feita separadamente e a mensagem codificada será uma sequência dos blocos codificados. Os blocos codificados não podem ser reunidos formando um longo número pois, neste caso, ficaria impossível decodificar a mensagem.*

2. *A chave de codificação é o par* (n, e)*. Sejam* b *um bloco, onde* b *é um inteiro positivo menor que* n*, e* $C(b)$ *o bloco* b *codificado. Calculamos* $C(b)$ *da seguinte maneira:*

$$b^e \equiv C(b) \ (mod\ n),$$

com $0 \leq C(b) < n$*.*

Agora, vamos realizar a codificação de cada bloco obtido no processo de pré-codificação considerando o exemplo 2.7. Lembrando que $p = 17$, $q = 23$ e $n = 391$. Neste caso, $\phi(n) = 352$.

Para este exemplo, vamos escolher $e = 3$, que é o menor número primo tal que $mdc(e, \phi(n)) = 1$. A seguir, codificaremos cada bloco b da mensagem pré-codificada (2.1).

1. $b = 2 \implies C(b) = 8$ pois

$$2^3 = 8 \equiv 8 \ (mod\ 391).$$

2. $b = 5 \implies C(b) = 125$ pois

$$5^3 = 125 \equiv 125 \ (mod\ 391).$$

3. $b = 102 \implies C(b) = 34$ pois

$$102^3 = 102^2 \cdot 102 = 10404 \cdot 102 \equiv 238 \cdot 102 \equiv 34 \ (mod\ 391).$$

4. $b = 122 \implies C(b) = 44$ pois

$$122^3 = 122^2 \cdot 122 = 14884 \cdot 122 \equiv 26 \cdot 122 \equiv 44 \ (mod\ 391).$$

5. $b = 141 \implies C(b) = 142$ pois

$$141^3 = 141^2 \cdot 141 = 19881 \cdot 141 \equiv 331 \cdot 141 \equiv 142 \ (mod\ 391).$$

6. $b = 82 \implies C(b) = 58$ pois

$$82^3 = 82^2 \cdot 82 = 6724 \cdot 82 \equiv 77 \cdot 82 \equiv 58 \ (mod\ 391).$$

7. $b = 7 \implies C(b) = 343$ pois

$$7^3 = 343 \equiv 343 \ (mod\ 391).$$

8. $b = 89 \implies C(b) = 387$ pois

$$89^3 = 89^2 \cdot 89 = 7921 \cdot 89 \equiv 101 \cdot 89 \equiv 387 \ (mod\ 391).$$

9. $b = 91 \implies C(b) = 114$ pois

$$91^3 = 91^2 \cdot 91 = 8281 \cdot 91 \equiv 70 \cdot 91 \equiv 114 \ (mod\ 391).$$

10. $b = 49 \implies C(b) = 349$ pois

$$49^3 = 49^2 \cdot 49 = 2401 \cdot 49 \equiv 55 \cdot 49 \equiv 349 \ (mod\ 391).$$

11. $b = 225 \implies C(b) = 13$ pois

$$225^3 = 225^2 \cdot 225 = 50625 \cdot 225 \equiv 186 \cdot 225 \equiv 13 \ (mod\ 391).$$

12. $b = 1 \implies C(b) = 1$ pois

$$1^3 \equiv 1 \ (mod\ 391).$$

13. $b = 4 \implies C(b) = 64$ pois

$$4^3 = 64 \equiv 64 \ (mod\ 391).$$

Portanto, obtemos a seguinte sequência de blocos codificados:

8−125−34−44−142−58−343−34−387−114−349−114−8−34−13−1−64−34−64

2.5 Decodificação

Nesta seção veremos como fazer para decodificar os blocos de uma mensagem codificada.

Para isto, precisamos considerar dois números, a saber, $n = pq$ e o inverso de e módulo $\phi(n)$, que denotaremos por d.

Definição 2.10 *Chamamos o par (n, d) de chave de decodificação do sistema RSA.*

Observação 2.11 *O processo de decodificação da mensagem codificada seguirá os seguintes passos:*

1. *Tendo a mensagem passado pelo processo de codificação, temos uma sequência de blocos. A decodificação de cada bloco será feita separadamente e a mensagem decodificada será uma sequência dos blocos decodificados.*

2. *A chave de decodificação é o par (n, d). Sejam a um bloco da mensagem codificada e $D(a)$ o bloco a decodificado. Calculamos $D(a)$ da seguinte maneira:*

$$a^d \equiv D(a) \ (mod\ n),$$

onde $0 \leq D(a) < n$.

Agora, vamos decodificar a mensagem codificada do exemplo 2.7:

$$8-125-34-44-142-58-343-34-387-114-349-114-8-34-13-1-64-34-64 \tag{2.2}$$

Neste caso, $\phi(n) = 352$ e $e = 3$. Utilizando o Algoritmo de Euclides estendido (observação 1.18), podemos obter d :

$$352 = 3 \cdot 117 + 1 \implies 1 = 352 + (-117) \cdot 3.$$

Logo, $(-117) \cdot 3 \equiv 1 \ (mod\ 352)$ e daí, o inverso de 3 módulo 352 é -117.

Como vamos usar d como expoente de potências ($d > 0$) e

$$-117 \equiv 235 \ (mod\ 352),$$

segue que $d = 235$ (que é o menor inteiro positivo congruente a -117 módulo 352).

Agora, faremos os cálculos de $D(a)$, onde a é um bloco de (2.2). São eles:

1. $a = 8 \implies D(a) = 2$.

   De fato, primeiro note que $8^{235} = (2^3)^{235} = 2^{705}$. Pelo Teorema de Euler (teorema 1.59), como $mdc(2, 391) = 1$ então $2^{\phi(391)} \equiv 1 \ (mod\ 391)$. Logo,

$$2^{352} \equiv 1 \ (mod\ 391) \overset{Teo.1.33}{\Longrightarrow} 2^{704} \equiv 1 \ (mod\ 391) \overset{Teo.1.31(3)}{\Longrightarrow} 2^{705} \equiv 2 \ (mod\ 391).$$

2. $a = 125 \implies D(a) = 5$.

   De fato, note que $125^{235} = (5^3)^{235} = 5^{705}$. Pelo Teorema de Euler (teorema 1.59), como $mdc(5, 391) = 1$ então $5^{\phi(391)} \equiv 1 \ (mod\ 391)$. Logo,

$$5^{352} \equiv 1 \ (mod\ 391) \overset{Teo.1.33}{\Longrightarrow} 5^{704} \equiv 1 \ (mod\ 391) \overset{Teo.1.31(3)}{\Longrightarrow} 5^{705} \equiv 5 \ (mod\ 391).$$

3. $a = 34 \implies D(a) = 102$.

   De fato, observe que $34^{235} = 2^{235} \cdot 17^{235}$.

   Usando os teoremas 1.31(3) e 1.33, podemos concluir que

$$2^{235} \equiv 246 \ (mod\ 391), \tag{2.3}$$

$$17^{235} \equiv 153 \ (mod\ 391). \tag{2.4}$$

   De (2.3), (2.4) e do teorema 1.31(3), obtemos

$$34^{235} \equiv 102 \ (mod\ 391).$$

4. $a = 44 \implies D(a) = 122$.

   De (2.3) (do item 3) e do teorema 1.33, podemos concluir que

$$2^{470} \equiv 302 \ (mod\ 391). \tag{2.5}$$

   Utilizando os teoremas 1.31(3) e 1.33 e fazendo alguns cálculos, pode-se provar que

$$11^{235} \equiv 148 \ (mod\ 391). \tag{2.6}$$

   De (2.5), (2.6) e do teorema 1.31(3), obtemos

$$44^{235} \equiv 122 \ (mod\ 391).$$

5. $a = 142 \implies D(a) = 141$.

   De fato, note que $142^{235} = 2^{235} \cdot 71^{235}$.

Utilizando os teoremas 1.31(3) e 1.33 e fazendo alguns cálculos, pode-se provar que

$$71^{235} \equiv 177 \ (mod\ 391). \tag{2.7}$$

De (2.3) (do item 3), (2.7) e do teorema 1.31(3), temos

$$142^{235} \equiv 141 \ (mod\ 391).$$

6. $a = 58 \implies D(a) = 82$.

   De fato, note que $58^{235} = 2^{235} \cdot 29^{235}$.

   Utilizando os teoremas 1.31(3) e 1.33 e fazendo alguns cálculos, pode-se provar que

   $$29^{235} \equiv 261 \ (mod\ 391). \tag{2.8}$$

   De (2.3) (do item 3), (2.8) e do teorema 1.31(3), temos

   $$58^{235} \equiv 82 \ (mod\ 391).$$

7. $a = 343 \implies D(a) = 7$.

   De fato, note que $343^{235} = (7^3)^{235} = 7^{705}$. Pelo Teorema de Euler (teorema 1.59), como $mdc(7, 391) = 1$ então $7^{\phi(391)} \equiv 1 \ (mod\ 391)$. Portanto,

   $$7^{352} \equiv 1 \ (mod\ 391) \overset{Teo.1.33}{\implies} 7^{704} \equiv 1 \ (mod\ 391) \overset{Teo.1.31(3)}{\implies} 7^{705} \equiv 7 \ (mod\ 391).$$

8. $a = 387 \implies D(a) = 89$.

   De fato, note que $387^{235} = (3^2)^{235} \cdot 43^{235} = 3^{470} \cdot 43^{235}$.

   Dos teoremas 1.31(3) e 1.33 e realizando alguns cálculos, obtemos

   $$3^{235} \equiv 58 \ (mod\ 391), \tag{2.9}$$

   $$43^{235} \equiv 287 \ (mod\ 391). \tag{2.10}$$

   Aplicando os teoremas 1.31(3) e 1.33 às equações (2.9) e (2.10), concluímos que

   $$387^{235} \equiv 89 \ (mod\ 391).$$

9. $a = 114 \implies D(a) = 91$.

   De fato, observe que $114^{235} = 2^{235} \cdot 3^{235} \cdot 19^{235}$.

   Pelos teoremas 1.31(3) e 1.33 e realizando alguns cálculos, obtemos

   $$19^{235} \equiv 365 \ (mod\ 391). \tag{2.11}$$

   Das equações (2.3), (2.9), (2.11) e do teorema 1.31(3), segue que

   $$114^{235} \equiv 91 \ (mod\ 391).$$

10. $a = 349 \implies D(a) = 49$.

    De fato, usando os teoremas 1.31(3) e 1.33 e realizando alguns cálculos, podemos concluir que

    $$349^{235} \equiv 49 \ (mod\ 391).$$

11. $a = 13 \implies D(a) = 225$.

    De fato, dos teoremas 1.31(3) e 1.33 e fazendo alguns cálculos, podemos concluir que

    $$13^{235} \equiv 225 \ (mod\ 391).$$

12. $a = 1 \implies D(a) = 1$.

    De fato, $1^{235} \equiv 1 \ (mod\ 391)$.

13. $a = 64 \implies D(a) = 4$.

    De fato, observe que $64^{235} = (2^3)^{235} \cdot (2^3)^{235} = 2^{705} \cdot 2^{705}$.

    Pelo item 1, segue que $2^{705} \equiv 2 \ (mod\ 391)$. Do teorema 1.33, concluímos que

    $$64^{235} \equiv 4 \ (mod\ 391).$$

Portanto, obtemos a seguinte sequência de blocos decodificados:

$$2-5-102-122-141-82-7-102-89-91-49-91-2-102-225-1-4-102-4$$

Observação 2.12 *É claro que se b é um bloco da mensagem original pré-codificada, então é esperado que $D(C(b)) = b$. Sem isto não teríamos um código útil. Veremos que isto sempre ocorre no próximo resultado.*

Teorema 2.13 *Sejam p e q números primos distintos, $n = pq$, e um número inteiro positivo tal que $mdc(e, \phi(n)) = 1$ e d o inverso de e módulo $\phi(n)$. Se b é um número inteiro tal que $1 \leq b \leq n-1$, então $D(C(b)) = b$.*

Demonstração: Primeiro, note que é suficiente provar que $D(C(b)) \equiv b \ (mod\ n)$ pois tanto $D(C(b))$ quanto b pertencem ao intervalo que vai de 1 a $n-1$ e assim, são congruentes se, e somente se, são iguais.

Da definição de $C(b)$, temos que $b^e \equiv C(b) \ (mod\ n)$. Pelo teorema 1.33, segue que

$$(b^e)^d \equiv C(b)^d \ (mod\ n). \tag{2.12}$$

Agora, da definição de D, sabemos que $D(C(b))$ é tal que

$$C(b)^d \equiv D(C(b)) \ (mod\ n). \tag{2.13}$$

Considerando a transitividade e a simetria da relação de congruência, de (2.13) e (2.12) obtemos

$$D(C(b)) \equiv b^{ed} \ (mod\ n). \tag{2.14}$$

Como d é o inverso de e módulo $\phi(n)$, então $ed \equiv 1 \ (mod\ \phi(n))$. Assim, existe $k \in \mathbb{Z}$ de modo que $ed = 1 + k\phi(n)$. Observe que, como $e > 2, d > 2$ e $\phi(n) > 0$, temos que $k > 0$.

Lembrando que $n = pq$, vamos calcular $r, s \in \mathbb{Z}$, com $1 \leq r \leq p$ e $1 \leq s \leq q$, tais que $b^{ed} \equiv r \ (mod\ p)$ e $b^{ed} \equiv s \ (mod\ q)$. Os cálculos de r e s são análogos, por isso vamos calcular apenas r.

Como $ed = 1 + k\phi(n)$ e $\phi(n) = (p-1)(q-1)$ então $ed = 1 + k(p-1)(q-1)$. Logo,

$$b^{ed} \equiv b(b^{p-1})^{k(q-1)} \ (mod\ p). \tag{2.15}$$

Precisamos separar em dois casos:

1. $p \nmid b$.

Neste caso, pelo Pequeno Teorema de Fermat (teorema 1.52),

$$b^{p-1} \equiv 1 \ (mod\ p). \tag{2.16}$$

Assim, de (2.15) e (2.16), concluímos que

$$b^{ed} \equiv b \ (mod\ p).$$

2. $p|b$.

Neste caso, $p|b(b^{ed-1}-1)$ e daí, $p|(b^{ed}-b)$. Logo,

$$b^{ed} \equiv b \ (mod\ p).$$

Nos dois casos, mostramos que

$$b^{ed} \equiv b \ (mod\ p),$$

ou seja, $r = b$.

Analogamente, podemos mostrar também que $s = b$.

Logo, tanto p quanto q dividem $b^{ed}-b$. Como $mdc(p,q) = 1$ (pois p e q são primos distintos), segue que $n = pq$ divide $b^{ed}-b$. Assim,

$$b^{ed} \equiv b \ (mod\ n). \tag{2.17}$$

Portanto, de (2.14) e (2.17),

$$D(C(b)) \equiv b \ (mod\ n),$$

como queríamos demonstrar.

■

2.6 A segurança do método RSA

Sejam p e q os números primos que são os parâmetros do sistema RSA e $n = pq$. Como o método RSA é um método de chave pública então a chave de codificação

(n, e) corresponde à chave pública do sistema. Portanto, somente o par (n, e) é acessível a qualquer usuário.

O método RSA só será seguro se for difícil calcular d quando somente n e e são conhecidos. Observe que, na prática, só conseguimos calcular d usando o algoritmo euclidiano estendido a $\phi(n)$ e e, e só conseguimos calcular $\phi(n)$ se soubermos fatorar n para obter p e q. Logo, na prática, só quebramos o código se conseguirmos fatorar n. Então, se n é muito grande, esse problema se torna muito difícil e neste caso, o sistema RSA é bem seguro.

Acredita-se que quebrar um código no sistema RSA é equivalente ao problema de fatorar n. Vale ressaltar que isto não foi provado ainda. A seguir veremos um exemplo desta situação.

Exemplo 2.14 *Suponhamos a situação hipotética de que conhecemos $\phi(n)$ a partir de n e e. Neste caso, afirmamos que conhecemos a fatoração de n.*

De fato, sabemos que $n = pq$ e $\phi(n) = (p-1)(q-1)$ são conhecidos. Vamos determinar p e q a partir disso. Temos

$$\phi(n) = (p-1)(q-1) = pq - (p+q) + 1 = n - (p+q) + 1.$$

Logo, $p + q = n - \phi(n) + 1$.

Note que,

$$(p+q)^2 - 4n = p^2 + 2pq + q^2 - 4pq = p^2 - 2pq + q^2 = (p-q)^2,$$

ou seja, $p - q = \sqrt{(p+q)^2 - 4n}$.

Como conhecemos $p + q$ e $p - q$, podemos calcular p e q. Portanto, fatoramos n.

Desse modo, é difícil imaginar a situação de que conhecemos $\phi(n)$ sem fatorar n pois conhecendo $\phi(n)$ e n chegamos aos fatores de n.

Exemplo 2.15 *Usando a ideia do exemplo anterior, vamos fatorar $n = pq$, onde p e q são números primos, sabendo que $n = 3552377$ e $\phi(n) = 3548580$. Temos*

$$p + q = 3552377 - 3548580 + 1 = 3798, \tag{2.18}$$

$$p - q = \sqrt{3798^2 - 4 \cdot 3552377} = 464. \tag{2.19}$$

De (2.18) *e* (2.19)*, obtemos*

$$p = 2131 \;\; e \;\; q = 1667.$$

Observação 2.16 *No método RSA é muito importante escolher bem os parâmetros p e q pois senão pode ser fácil decodificar uma mensagem neste sistema. É claro que se p e q forem pequenos, a quebra pode ser simples. Então, para garantir a eficácia deste método, p e q devem ser números primos bem grandes desde que* $|p-q|$ *não seja pequeno* (*pois neste caso poderíamos encontrar p e q de maneira fácil usando o algoritmo de Fermat* (*[1], seção* 4*, capítulo* 2)).

CAPÍTULO 3

Aplicação em sala de aula

3.1 Sobre a atividade

A maneira como abordamos pedagogicamente determinado assunto em sala de aula desempenha um papel crucial, pois influencia diretamente a qualidade e eficácia do processo de ensino-aprendizagem. Ele permite ao educador adaptar sua instrução para atender às necessidades e estilos de aprendizagem dos variados alunos. Alguns autores apresentam contribuições valiosas sobre o processo de ensino-aprendizagem e são citados a seguir.

Nas palavras de Paulo Freire, “Ensinar não é transferir conhecimento, mas criar as possibilidades para a sua produção ou a sua construção.” ([3], Freire)

Observe que a frase de Paulo Freire destaca a importância de um papel ativo do educador no processo de aprendizagem e rejeita a visão tradicional de ensino como uma mera transferência unilateral de informações.

Segundo Santos em [9],

> Sob a perspectiva da teoria sociocultural de Vygotsky, o ensino de matemática deve, primordialmente, mostrar a relação direta do que se está estudando com a realidade de vida do aluno, evitando que o saber matemático continue aparentando estar na contramão do saber da vida. ([9], Santos, 2016, p.43)

No entanto, ainda em [9], Santos comenta como deve ser colocada em prática esta relação:

> A sala de aula de matemática deve criar condições para que a apren-

> dizagem seja um processo ativo de elaboração, com o aluno construindo seu conhecimento. Então, se o professor de matemática, ao planejar sua aula, procurar motivar o aluno, desafiá-lo intelectualmente, quando leva em consideração sua maturação biológica, o impacto sofrido por suas experiências de vidas, as trocas interpessoais aluno/professor – aluno/aluno e as transmissões culturais baseadas no meio em que vive, ele está pondo em prática as ideias construtivistas de Piaget. ([9], Santos, 2016, p.41)

Noe, em [7], reforça a relevância de se trabalhar conteúdos matemáticos valorizando o raciocínio lógico:

> Segundo Piaget, a Matemática é resultado do processo mental da criança em relação ao cotidiano, arquitetado mediante atividades de se pensar o mundo por meio da relação com objetos. Dessa forma, não podemos pensar o ensino da Matemática de acordo com o sistema tradicional de educação, caracterizado pela repetição e verbalização de conteúdos. Piaget considera o método tradicional fracassado, pois o mesmo trata a criança como um ser apático e vago. Suas ideias refletem sobre um ensino formador de um raciocínio lógico matemático que conduz à interpretação e compreensão, em detrimento da memorização. ([7], Noe, 2015)

Assim, realizamos a atividade proposta na seção 3.2 levando em conta as seguintes orientações:

- A atuação como moderador no processo é de suma importância, uma vez que o conhecimento não está centrado na figura do professor.
- As vontades e vivências dos alunos devem ser consideradas durante a realização da atividade.
- A relevância na sociedade do tema abordado na atividade deve ser mostrada a fim de relacionar o que se está estudando com a realidade vivida pelo aluno.
- Valorização do raciocínio lógico em detrimento da memorização de conteúdos.

Nas próximas seções, procedemos à exposição do projeto e do desenvolvimento de uma atividade em sala de aula e dos resultados alcançados com ela. A atividade em questão foi realizada durante o primeiro semestre do ano de 2023 em uma turma de primeiro ano do ensino médio de uma escola, situada no município de Uberlândia, no estado de Minas Gerais.

A execução da atividade proposta em ambiente de sala de aula se deu no decorrer do ano letivo em uma disciplina do itinerário formativo que visa aprofundar nos conhecimentos da área do conhecimento *Matemática e suas Tecnologias*.

O conteúdo abordado, os recursos materiais empregados, bem como os métodos de avaliação relacionados à referida atividade foram informados à supervisão da escola e estão inseridos no planejamento anual da disciplina.

3.2 Projeto

Tema

Criptografia de César.

Competências

- Compreender a ideia de chave de criptografia;
- Compreender e fazer uso de estratégias criptográficas;
- Identificar padrões em textos e sequências numéricas.

Objetivos

- Geral:

Promover o debate e o uso da lógica como ferramenta na resolução de problemas. Estimular os(as) alunos(as) a avaliar suas repostas em outros conteúdos a fim de se assegurarem de que elas têm sentido.

- Específicos:

Ao final da atividade o(a) aluno(a) deverá ser capaz de:

- enviar mensagens criptografadas para outros(as) colegas;

- avaliar se as escolhas dele foram corretas com relação à construção de uma frase;

- identificar as diferentes técnicas usadas por outros grupos e avaliá-las;

- descriptografar mensagens sem o conhecimento da chave.

Justificativa

A escolha deste tema para ser trabalhado em sala de aula se deu por cumprir um dos objetivos da disciplina do itinerário formativo da escola, que é compreender sobre as tecnologias digitais da informação e das técnicas de comunicação por ela empregada, além de ser um assunto de mais fácil compreensão do que outros assuntos abordados nesta dissertação.

Recursos didáticos

Os recursos didáticos a serem utilizados são:

- quadro negro;
- giz;
- celular ou computador que tenha acesso a internet;
- site mathcryptosite.wixsite.com/mathcrypto.

Avaliação

A avaliação será feita levando-se em consideração a participação e empenho dos(as) estudantes no desenvolvimento das atividades propostas em sala de aula analisando se os objetivos propostos foram cumpridos.

3.3 Desenvolvimento do projeto em sala de aula

A atividade foi realizada durante três aulas de 50 minutos de uma disciplina do itinerário formativo de uma turma do primeiro ano do ensino médio. A carga horária total da atividade foi de 150 minutos. Vamos separar a descrição da atividade em três momentos: Primeira aula, Segunda aula e Terceira aula.

Primeira aula

Na primeira aula de 50 minutos, o professor iniciou apresentando e explicando a Cifra de César. Além disso, a turma foi dividida em onze duplas.

A atividade proposta foi que cada dupla escolhesse/criasse uma frase simples para que a mesma fosse cifrada usando como chave de criptografia $\beta = 4$. Em seguida, as duplas deveriam trocar suas frases cifradas de modo que a mensagem cifrada recebida por cada dupla não fosse a sua original. O objetivo desta atividade era que cada dupla decifrasse a frase cifrada por outra dupla de maneira correta, sabendo que $\beta = 4$.

Para a escolha da frase simples, algumas duplas fizeram pesquisa na internet através de seus celulares, outras escolheram frases que faziam parte de músicas ou do cotidiano.

Após a escolha da frase, em um papel, cada dupla cifrou usando chave de criptografia $\beta = 4$.

Em seguida, as frases cifradas foram trocadas pelas duplas para a decifração. Neste momento, observou-se que muitas duplas cometeram erros ortográficos ao escolher a frase simples, o que poderia ser uma dificuldade a mais para a dupla que decifraria esse tipo de frase cifrada. Outro problema encontrado foi que algumas duplas cifraram algumas letras de modo equivocado.

Entretanto, nos dois casos (erros ortográficos e letras cifradas erradas), foi possível decifrar o que se queria transmitir.

De modo geral, os(as) estudantes da turma acharam a atividade fácil, apesar de esboçarem estranhamento com a utilização de muito raciocínio lógico na realização da mesma. Eles entendem que em uma aula de Matemática deve ter sempre "muita conta".

Os minutos finais dessa primeira aula foram utilizados para mostrar a relevância do raciocínio lógico na Matemática, para explicar para os(as) estudantes que existem outros tipos de criptografia e também foi lançado o seguinte desafio: “Ao decifrar as frases, se não conhecessem a chave de criptografia, ainda seriam capazes de decifrá-las?" O desafio foi lançado pois na próxima aula os(as) estudantes iriam se deparar com este tipo de situação.

Segunda aula

Na segunda aula de 50 minutos, a turma foi novamente dividida em duplas, mas por conta de estudantes faltosos foram formadas dez duplas.

A atividade proposta era que cada dupla escolhesse uma frase simples e a cifrasse usando uma chave de criptografia β da sua escolha. Em seguida, como na primeira atividade, as duplas deveriam trocar suas frases cifradas de modo que a mensagem cifrada recebida por cada dupla não fosse a sua original, e o objetivo era que cada dupla decifrasse a frase cifrada por outra dupla de maneira correta, agora sem saber a chave de criptografia que foi usada no momento em que a frase foi cifrada.

Nesta atividade, no momento de decifrar as frases cifradas, muitos grupos tiveram dificuldades. As principais dificuldades relatadas foram as seguintes:

- a atividade era diferente de qualquer outra que já tinham realizado na vida escolar;
- por causa da pandemia, não estavam habituados a trabalhar em grupo;
- tiveram dificuldade em experimentar um valor plausível para a chave de criptografia β.

Apesar das frases a se decifrar serem compostas por, em média, dez palavras, nesta atividade somente um grupo conseguiu decifrar a frase cifrada e por consequência, finalizar a atividade em 50 minutos. Os grupos que não terminaram, trouxeram as frases decifradas na semana seguinte, antes da realização da terceira aula.

Terceira aula

Na terceira aula, o professor iniciou comentando sobre a frequência com que algumas letras do nosso alfabeto aparecem nas palavras da língua portuguesa. Por exemplo, as vogais A, E e O aparecem em uma frequência bem maior do que as vogais I e U nas palavras.

Além disso, explicou que é praticamente impossível uma palavra com três ou mais letras não ter uma vogal como sendo uma das três primeiras letras. Assim, ao invés de 25 valores possíveis para a chave de criptografia β, os(as) estudantes teriam 15

valores possíveis para β (considerando as 3 primeiras letras da palavra cifrada, cada uma com 5 possibilidades de ser vogal).

Com estas orientações, utilizando as mesmas frases cifradas pelos grupos durante a segunda aula, cada grupo deveria decifrar uma frase diferente daquela que já havia decifrado.

A atividade se iniciou, não sendo necessário mais que 15 minutos para que quase todos os grupos conseguissem decifrar sua frase cifrada. Houve grupos que não tinham decifrado nesse tempo, mas pelo menos já conheciam a chave de criptografia β relativa às suas frases. Apenas um grupo não conseguiu descobrir a chave de criptografia e então fez uso do site https://mathcryptosite.wixsite.com/mathcrypto que foi criado pelo autor deste trabalho para esta finalidade.

No final desta atividade, foi solicitado aos(às) estudantes um relatório em que deveria constar os procedimentos que utilizaram para cifrar e decifrar as frases propostas por eles(as).

Com relação à avaliação dos(as) estudantes nas atividades propostas, foi realizada valorizando o empenho de cada estudante em cada grupo, considerando principalmente como cada um avaliava suas tentativas de solução nos momentos de cifrar e decifrar as frases. É interessante ressaltar que foi discutido em aulas posteriores com a turma a relevância de se autoavaliar com relação às respostas em atividades avaliativas para que não ocorram afirmações como "*o copo tem* 300 *metros quadrados*" ou ainda, "*minha mãe tem* -33 *anos de idade*".

Sobre o site

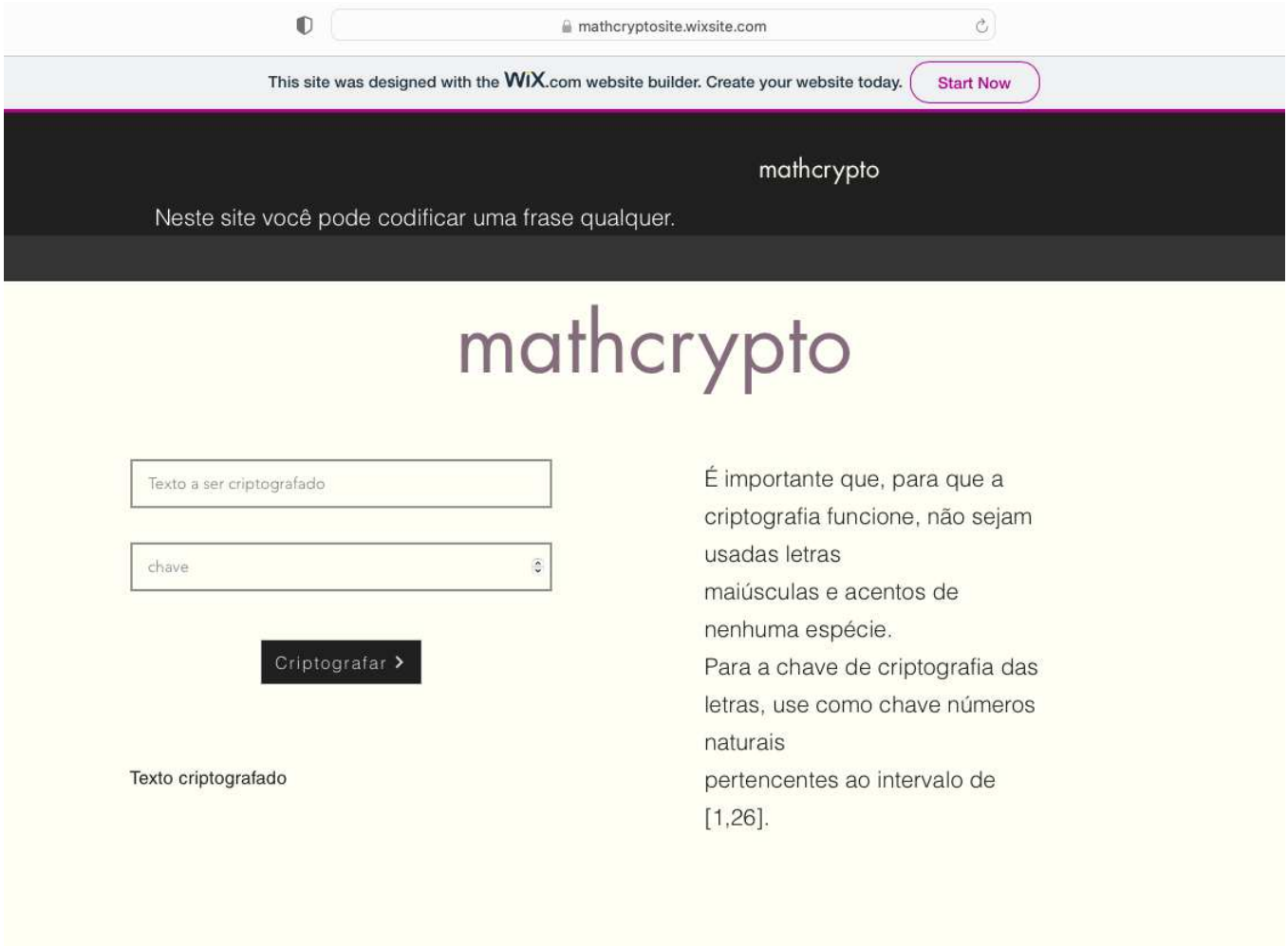
O site https://mathcryptosite.wixsite.com/mathcrypto foi desenvolvido e criado pelo autor deste trabalho com a finalidade de cifrar ou decifrar frases usando Cifra de César.

O site possui duas caixas de entrada: na primeira delas o usuário deve escrever uma frase em letras minúsculas e na segunda delas o usuário deve selecionar um número inteiro β tal que $1 \leq \beta \leq 26$, onde β é a chave de criptografia do sistema Cifra de César.

A partir da inserção dos dados nas duas caixas de entrada, o usuário deve clicar

no botão CRIPTOGRAFAR e então o algoritmo identifica cada letra da frase simples (respectivamente, cifrada) com uma outra letra da frase cifrada (respectivamente, decifrada) levando-se em conta a chave de criptografia que foi selecionada na segunda caixa de entrada.

Figura 3.1: Site criado pelo autor.



Fonte: Criptografia. Acesso em 26/09/2023.

3.4 Conclusão

As atividades desenvolvidas nas três aulas tiveram como um dos objetivos estimular os(as) alunos(as) a fazerem uso da lógica como ferramenta para que criassem um senso crítico das respostas obtidas em exercícios além de obviamente ensiná-los uma aplicação moderna da matemática no ramo da segurança da informação.

A atividade da primeira aula consistiu em cada dupla criar ou buscar na internet uma frase e criptografá-la via Cifra de César com chave de criptografia fixada

pelo professor, permutando a frase com outra dupla e ambas as duplas realizaram o processo de descriptografar.

Ao não informar a chave de criptografia, a atividade da segunda aula foi mais complexa. As duplas tiveram que descobrir, por meio do raciocínio lógico e tentativas, a chave de criptografia para, em seguida, decifrar a frase cifrada.

A maioria das duplas perceberam que é possível reduzir o espaço amostral das possíveis chaves de criptografia analisando as vogais mais usadas e qual das primeiras letras seria uma vogal. Aquelas duplas que não tiveram essa percepção fizeram uso de um site, desenvolvido pelo autor deste trabalho, que os posssibilitou análises mais rápidas. Levando em conta que cada aluno(a) teve seu tempo respeitado, alguns concluíram a atividade em casa.

Ainda assim, ressalto que ficou claro aos(às) alunos(as) que a criptografia desempenha um papel de extrema relevância na era digital atual e que pelo seu dinamismo evoluiu muito ao longo dos anos. Se isso não tivesse ocorrido, nos dias atuais, ainda haveria apenas 25 possibilidades para descriptografar mensagens importantes no âmbito militar, digital e comercial.

A pandemia ocorrida recentemente impediu que os(as) estudantes, em sua maioria, tivessem oportunidades de realizar trabalhos em grupos por um longo tempo e isso foi um problema no decorrer da atividade, uma vez que ao invés de dividir as tarefas relativas à cada atividade, muitas vezes cada aluno(a) da dupla fazia do seu modo o exercício proposto.

Contudo, as atividades em questão revelaram-se altamente proveitosas, trazendo consigo uma gama significativa de benefícios e aprendizados. Ao promover a participação ativa dos envolvidos, proporcionou que os objetivos fossem alcançados. Ademais, a atividade serviu como um meio eficaz para estimular a colaboração e a interação entre os(as) membros(as) do grupo, favorecendo a troca de ideias e o desenvolvimento de competências interpessoais, o que não foi estimulado e realizado com os estudantes ao longo dos dois anos de pandemia.

CAPÍTULO 4

Considerações finais

A criptografia é vital para guardar e transmitir informações sensíveis desde o Império Romano, garantindo a segurança de dados. Ela é essencial nos tempos modernos. Na era digital é utilizada para proteger transações financeiras, dados médicos e informações confidenciais, preservando a confiança na sociedade digital. Neste contexto, tentamos escrever neste trabalho tanto sobre algumas formas de criptografia, quanto sobre uma forma de transmissão de informação criptografada em sala de aula no intuito de mostrar aos alunos uma aplicação da matemática e despertar neles o interesse na disciplina (além de outros objetivos listados anteriormente no capítulo 3).

Ao aplicar a Cifra de César em sala de aula, o professor deve se mostrar ativo e perceptivo às inúmeras técnicas dos alunos de encontrarem uma solução para a descriptografia das mensagens, que vão desde tentativa e erro até a análise de qual a letra mais usada. Ainda assim existem alunos que vão de modo criativo encontrar soluções "fora da caixa" e o contrário, aqueles que terão dificuldades em encontrar a chave da criptografia. Para estes, neste trabalho, usamos um site como auxílio no processo, a fim de que todos os objetivos fossem alcançados.

Gostaríamos de propor aos educadores da área de Matemática, independente do grau de ensino, que refletissem sobre a importância de se conectar os tópicos ensinados em sala de aula com elementos do dia a dia dos alunos e sobre a relevância que possuem neste processo.

Para finalizar, como nossos alunos estão inseridos em uma realidade em que a

criptografia ocupa um local de destaque, acreditamos que eles não só devem ser instigados a pensar sobre seu funcionamento mas também a pensar em como melhorá-lo.

Referências Bibliográficas

[1] COUTINHO, S.C. **Números Inteiros e Criptografia RSA**. Rio de Janeiro: IMPA/SBM, 1997.

[2] DAEMEN, J. and RIJMEN, V. **The design of Rijndael: AES - The Advanced Encryption Standard.** Berlin: Springer Verlag, 2002.

[3] FREIRE, P. **O educador da liberdade.** Disponível em: < https://acervoapi.paulofreire.org/server/api/core/bitstreams/eb339075-b34a-409f-a2cf-86330ee42631/content >. Acesso em 10 jul. 2023.

[4] KAHN, D. **The codebreakers.** New York: The New American Library, Inc., 1996.

[5] LUCIANO, D. and PRICHETT, G., **Cryptology: From Caesar Ciphers to Public-Key Cryptosystems**. Mathematical Association of America, v. 18, n. 01, 1987, p.2-17.

[6] MUNIZ NETO, A.C. **Tópicos de Matemática Elementar: teoria dos números**, vol 5. Rio de Janeiro: SBM, 2012.

[7] NOE, M. **O ensino da Matemática sob a visão de Piaget.** Disponível em: 2015. < http://educador.brasilescola.uol.com.br/estrategias-ensino/o-ensino-matematica-sob-visao-piaget.htm >. Acesso em 06 jul. 2023.

[8] RIVEST, R.L., SHAMIR, A. and ADLEMAN, L. **A method for obtaining digital signatures and public-key cryptosystems**. Communications of the ACM, v. 21, n. 02, 1978, p.120-126.

[9] SANTOS, A.P.F. **A Criptografia no ensino fundamental II: contexto histórico, cifras simétricas, aplicações de conteúdos matemáticos e muitas**

outras curiosidades. Dissertação (Mestrado em Matemática) - Centro de Ciências e Tecnologia da Universidade Estadual do Norte Fluminense Darcy Ribeiro, p.131. 2016.

[10] SANTOS, J.P.O. **Introdução à Teoria dos Números**. Rio de Janeiro: IMPA, 2009.

[11] SINGH, S. **O livro dos códigos**. São Paulo: Editora Record, 2001.