UNIVERSIDADE ESTADUAL DO OESTE DO PARANÁ
PROGRAMA DE PÓS GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONAL EM REDE NACIONAL

Introdução à criptografia e atividades para a Educação Básica

Setembro de 2021

UNIVERSIDADE ESTADUAL DO OESTE DO PARANÁ
PROGRAMA DE PÓS GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONAL EM REDE NACIONAL - PROFMAT

Introdução à criptografia e atividades para a Educação Básica

Dafne de Moraes Deparis

Dissertação apresentada ao programa de pós graduação em matemática como parte dos requisitos para obtenção do título de Mestre pelo Mestrado Profissional em Matemática em Rede Nacional - PROFMAT.

Banca examinadora:
Orientadora Profa. Dra. Raquel Lehrer - UNIOESTE
Prof. Dr. Jhone Caldeira Silva - UFG
Prof. Dr. Clézio Aparecido Braga - UNIOESTE

Cascavel, Setembro de 2021.

Ficha de identificação da obra elaborada através do Formulário de Geração Automática do Sistema de Bibliotecas da Unioeste.

Deparis, Dafne de Moraes
Introdução à criptografia e atividades para a Educação Básica / Dafne de Moraes Deparis; orientadora Raquel Lehrer. -- Cascavel, 2021.
103 p.

Dissertação (Mestrado Profissional Campus de Cascavel) -- Universidade Estadual do Oeste do Paraná, Centro de Ciências Exatas e Tecnológicas, Programa de Pós-Graduação em Matemática - Mestrado Profissional, 2021.

1. Criptografia RSA. 2. Sequências Didáticas. 3. Pequeno Teorema de Fermat. I. Lehrer, Raquel, orient. II. Título.

Dafne de Moraes Deparis

Introdução à Criptografia e Atividades para a Educação Básica

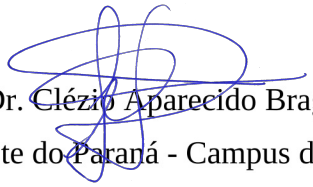
Trabalho Final de Conclusão apresentado ao Programa de Pós-graduação em Matemática - PROFMAT em cumprimento parcial aos requisitos para obtenção do título de Mestre em Ensino de Matemática, área de concentração Ensino de matemática, linha de pesquisa Ensino básico de matemática, APROVADO pela seguinte banca examinadora:

Orientadora – Profa. Dra. Raquel Lehrer

Universidade Estadual do Oeste do Paraná - Campus de Cascavel (UNIOESTE)

Prof. Dr. Jhone Caldeira Silva

Universidade Federal de Goiás - UFG



Prof. Dr. Clézio Aparecido Braga

Universidade Estadual do Oeste do Paraná - Campus de Cascavel (UNIOESTE)

Cascavel, 23 de setembro de 2021.

Agradecimentos

Agradeço à minha orientadora, Profa. Dra. Raquel Lehrer, pelos ensinamentos e pela paciência.

Aos meus professores e ao coordenador do programa Prof. Dr. André Vicente.

Aos colegas de curso, pela ajuda e companheirismo.

Ao meu esposo Maiko Teixeira, pelo apoio, pelo incentivo a estudar e por acreditar em mim.

Aos meus pais Irony Antonia de Moraes Deparis e Clovis Roque Deparis, e à minha irmã, Karlize de Moraes Deparis, pelo incentivo a estudar, pelas palavras de apoio e força.

Aos meus colegas de trabalho, em especial, aos meus chefes, pela compreensão.

À instituição de ensino, na qual trabalho, pela possibilidade de estudar.

E, principalmente, agradeço à Deus.

Resumo

O objetivo do trabalho foi estudar aspectos da Criptografia, como seu significado, história e métodos criptográficos, em especial a Criptografia RSA, incluindo definições, teoremas, proposições e exemplos sobre a Aritmética dos números inteiros, ou seja, a matemática envolvida no funcionamento da Criptografia RSA. Finalizando, fizemos algumas sugestões de atividades para aplicação no Ensino Fundamental e Médio, envolvendo criptografia.

Palavras-chave: Criptografia RSA, Sequências Didáticas e Pequeno Teorema de Fermat.

Abstract

The objective of the work was to study aspects of Cryptography, such as its meaning, history and cryptographic methods, especially RSA Cryptography, including definitions, theorems, propositions and examples about integer arithmetic, that is, the mathematics involved in the functioning of RSA Cryptography. Finally, we made some suggestions to activities with application in Elementary and High School, involving cryptography.

Keywords: RSA Encryption, Didactic Sequences and Fermat's Little Theorem.

Sumário

Introdução

A necessidade da escrita secreta para o homem é um ponto indiscutível; desde a antiguidade até os dias atuais, o sigilo na comunicação deve ser tão velho quanto o surgimento da escrita. Por anos, reis e rainhas necessitavam da comunicação secreta para assuntos de disputa de território; manutenção de segredos de estado; transações militares com seus exércitos. No decorrer da história da Criptografia, é possível perceber a evolução de códigos e cifras, que foram impulsionados pela ameaça de informações importantes e secretas acabarem nas mãos de inimigos, e também devido aos decifradores que ao descobrirem o funcionamento de uma cifra, obrigavam os cifradores a inventarem uma nova cifra desconhecida e mais segura. Isso trouxe avanços tecnológicos, que começaram com a invenção de instrumentos criptográficos como o Disco de Alberti, que facilitavam a cifragem; e posteriormente, a invenção do telégrafo, do rádio e de máquinas que evoluíram até chegarem ao ilustre computador. Hoje, a comunicação está extremamente rápida e facilitada, o que nos deixa dependentes da Criptografia para desempenharmos nossas atividades diárias, porque ela está presente na conversa de WhatsApp com a amiga ou com o chefe do seu trabalho, no comércio eletrônico, operações bancárias, nas transações de uma empresa, cartão de crédito, entre outras aplicações.

Conforme Carneiro (2017, p. 4), a palavra criptografia tem origem grega, *kryptos* significa oculto, escondido, secreto, e *graphein*, escrita. Apenas ocultar a mensagem, trata-se do método chamado esteganografia, já a criptografia esconde o significado da mensagem, tornando um texto legível em um texto ilegível, para isso utiliza-se códigos ou cifras, de modo que apenas a pessoa (remente e destinatário) que possuir a chave transformará o texto ilegível em legível novamente. As cifras podem ser classificadas em cifras de transposição e cifras de substituição. Na cifra de transposição, as letras da mensagem são reordenadas. A cifra de substituição consiste em trocar palavras, frases, sentenças ou até mesmo códigos, por outras palavras, frases, sentenças, ou códigos; ou ainda trocar as letras da mensagem por outras letras. Para cifrar o transmissor aplica um algoritmo, composto por uma chave, na mensagem original transformando-a no texto cifrado, o receptor da mensagem fará o caminho inverso para decifra-lá, mas para isso precisa conhecer o algoritmo e a chave, que podem ser combinados previamente. As cifras de substituição,

de acordo com Carneiro (2017, p. 6-9), podem ser monoalfabéticas, sendo a Cifra de César um exemplo, ou polialfabéticas, como a Cifra de Vigenère.

A chave é um elemento confidencial que cifra e decifra a mensagem, ela pode ser simétrica e assimétrica. Nas cifras que usam chave simétrica, geralmente, no processo de decifragem é aplicado o oposto da chave de cifragem, ou ainda, se sabemos a chave para cifrar obtemos, facilmente, a chave para decifrar. Já a cifra com chave assimétrica seria uma chave para cifragem e outra diferente para decifragem, o que nos leva ao conceito de chave pública. Um exemplo de método criptográfico de chave pública é a Criptografia RSA, desenvolvida em 1977, por Ron Rivest, Adi Shamir e Leonard Adleman, trata-se de uma função matemática que satisfaz os requisitos do sistema de chaves assimétricas. Os conteúdos matemáticos envolvidos no processo de codificação, decodificação, na demonstração do funcionamento e relacionados a segurança do método de criptografia RSA são resultados da Teoria dos Números, como máximo divisor comum, números primos, fatoração, aritmética modular e o Pequeno Teorema de Fermat.

Diante disso, no Capítulo 1 deste trabalho temos cenários da história da Criptografia, trazendo seus significados e avanços. No Capítulo 2 procuramos apresentar os resultados matemáticos que fundamentam o funcionamento e a segurança da Criptografia RSA. O Capítulo 3 descreve o processo de codificação e decodificação de uma mensagem através da Criptografia RSA, explica porque ela funciona e é segura até hoje, e para finalizá-lo fazemos um exemplo do método. E com o intuito de tornar a matemática na sala de aula dinâmica e significativa, no Capítulo 4 trazemos três atividades, em que os conteúdos matemáticos são desenvolvidos empregando criptografia.

Capítulo 1

A história da Criptografia

"A necessidade de sigilo na comunicação escrita deve ser tão velha como a própria escrita"(Fiarresga, 2010, p. 3).

Desde os tempos antigos e, principalmente, na realidade atual, com os diversos meios de comunicação e uma comunicação extremamente facilitada e rápida, a escrita secreta é uma necessidade da humanidade. O objetivo de ocultar as mensagens é proteger seu conteúdo, significado, caso ela for interceptada por uma pessoa que não é o destinatário certo, e os motivos são diversos: informações de guerra; disputa de território; manutenção de segredos de estado; nas transações de uma empresa; segurança de dados pessoais, senhas, cartões de crédito, transações bancárias; origem e autenticidade de documentos; conexões Wi-Fi, codificação de HD de computador ou, simplesmente, uma conversa com uma amiga no WhatsApp. A escrita secreta pode ser dividida em duas ciências, a esteganografia e a criptografia. A partir da criptografia, surge a criptoanálise, e o estudo de ambas é chamado de criptologia.

A escrita secreta através do método chamado esteganografia busca a ocultar a mensagem e não torná-la ilegível. Singh (2020, p. 20) conta como o uso da esteganografia evitou a conquista da Grécia pela Pérsia: Demerato avisou os gregos sobre o plano de ataque dos persas. Para isso, raspou a cera de um par de tabuletas, escrevendo a mensagem, que foi coberta com cera novamente. Outros relatos de Singh (2020, p. 21) foram de mensagens gravadas no couro cabeludo do mensageiro, e ocultada pelo crescimento do cabelo, quando o mensageiro chega ao destino, o cabelo era raspado. Temos também, as tintas invisíveis, "substâncias transparentes que submetidas a determinadas condições de temperatura, a certos tipos de luz ou postas em contato com determinados reagentes químicos, adquirem coloração e se tornam visíveis"(Tkotz, 2005, p. 75). Outro exemplo apresentado por Tkotz (2005, p. 97) é a microfotografia, redução da mensagem a um ponto, colocado como ponto final em outro texto qualquer, e tal formato foi aplicado pe-

los alemães na Segunda Guerra Mundial. Se o esconderijo da mensagem for encontrado, a informação sigilosa será imediatamente revelada, sendo essa a maior desvantagem da esteganografia.

Conforme Carneiro (2017, p. 4), a palavra criptografia tem origem grega, *kryptos* significa oculto, escondido, secreto, e *graphein*, escrita. Segundo S. C. Coutinho (2009, p. 1), "a criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. É a arte dos códigos secretos". A criptografia transforma um texto legível em um texto ilegível, para isso utiliza códigos ou cifras, de modo que apenas a pessoa que possuir a chave poderá, novamente, transformar o texto ilegível em legível.

Na história da humanidade aparecem várias cifras, que podem ser divididas em cifras de substituição e cifras de transposição; isso mostra a evolução da criptografia ao longo dos anos, sempre que uma cifra deixava de cumprir seu papel de proteger uma mensagem dentro da escrita secreta, outra mais forte era criada. O que originou a Criptoanálise, que estuda maneiras de entender e quebrar as cifras. Essa batalha entre cifradores e decifradores, resultou em grande avanço tecnológico, na criação dos computadores, e é também o que nos possibilita realizar compras pela internet, realizar transações bancárias com garantia de confidencialidade, integridade e disponibilidade. Segundo Stallings (2014, p. 26),

> "os três conceitos envolvem os objetivos fundamentais da segurança tanto para dados quanto para serviços de informação e computação [...]:
>
> - Confidencialidade: preservar restrições autorizadas sobre acesso e divulgação de informação, incluindo meios para proteger a privacidade de indivíduos e informações privadas. Uma perda de confidencialidade seria a divulgação não autorizada de informação.
> - Integridade: prevenir-se contra a modificação ou destruição imprópria de informação, incluindo a irretratabilidade e autenticidade dela. Uma perda de integridade seria a modificação ou destruição não autorizada de informação.
> - Disponibilidade: assegurar acesso e uso rápido e confiável da informação. Uma perda de disponibilidade é a perda de acesso ou de uso da informação ou sistema de informação."

1.1 A cifra de transposição

A cifra de transposição consiste em reordenar as letras da mensagem, isto é, são construídos anagramas. Por exemplo, da palavra "LER", é possível obter os seguintes anagramas "LER", "LRE", "ELR", "ERL", "RLE" e "REL". O ponto fraco da cifra de transposição é quando a mensagem é curta e o número de combinações é baixo, facilmente testável, o que não acontece no caso de uma mensagem extensa. Segundo Singh (2020, p. 24), um exemplo, é o citale espartano, que é considerado o primeiro aparelho criptográfico militar. Ele consiste num bastão de madeira em volta do qual é enrolada uma tira de

couro, onde o remetente escreve a mensagem no sentido longitudinal, ao desenrolar a tira a mensagem parece uma série de letras sem sentido, o mensageiro usa a tira como cinto, com as letras viradas para o corpo, o destinatário precisará de um bastão de mesmo diâmetro para entender a mensagem.

Figura 1.1: Citale espartano
Fonte: *https* : *//www.teses.usp.br/teses/disponiveis/*55/55136/*tde* − 06042017 − 164507/*publico/DanieleHelenaBonfim_revisada.pdf*

1.2 A cifra de substituição

A cifra de substituição, de acordo com Singh (2020, p. 14), pode ocorrer através do uso de códigos, o que consiste em trocar palavras, frases, sentenças ou até mesmo códigos, por outra palavras, frases, sentenças, ou códigos; geralmente ocorre a redução do tamanho da mensagem e não é mantido o significado dela. Um exemplo, para um comandante transmitir aos seus soldados a ordem "Ataquem ao meio dia", garantindo que os seus planos sejam mantidos em segredo, ele codifica a frase para "maçã", no caso de necessitar alterar para "Ataquem ao entardecer", ele precisará de outro código, o que torna a criptografia através de códigos inviável, pois receptor e transmissor precisam possuir um livro de códigos e sempre que alguma palavra ou frase não constar nesse livro, a comunicação ficará comprometida. No caso da cifra, as letras da ordem "Ataquem ao meio dia" são reordenadas ou substituídas, letra por letra, por outras letras do alfabeto cifrado. Segundo Singh (2020, p. 28), para cifrar o transmissor aplica no texto original um algoritmo, composto por uma chave, transformando-o no texto cifrado, o receptor da mensagem ao recebê-la, precisa conhecer o algoritmo e a chave para obter o texto original, ou ainda, decifrá-lo. Nesse caso, transmissor e receptor precisam, previamente, combinar o algoritmo e a chave.

Figura 1.2: Modelo genérico de um sistema criptográfico
Fonte: *http* : *//www.comp.ime.eb.br/graduacao/pfc/repositorio − pfc/*2013/2013 − *Guimaraes_Tannus.pdf*

A cifra de César é como ficou conhecida a cifra de substituição simples, pois era a cifra que o imperador romano Júlio César usava, conforme é descrito em "As vidas dos Césares", por Suetônio no século II. Nessa cifra, de acordo com Singh (2020, p. 26), o alfabeto cifrado é deslocado três casas em relação ao alfabeto original, sendo assim, o algoritmo consiste em substituir cada letra do alfabeto original pela letra correspondente no alfabeto cifrado; a chave desse algoritmo é o deslocamento de três casas. Por exemplo,

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

Tabela 1.1: Cifra de César

Texto original	p	r	o	f	m	a	t
Texto cifrado	S	U	R	I	P	D	W

Tabela 1.2: Um exemplo utilizando a cifra de César

Como o alfabeto possui 26 letras, podemos realizar 25 descolocamentos diferentes, o que resulta em 25 cifras, o que torna a Cifra de César um alvo fácil para os

criptoanalistas. No entanto, se em vez de deslocar em algumas casas o alfabeto cifrado em relação ao original, "o alfabeto cifrado consista em qualquer rearranjo do alfabeto original, então existem 400.000.000.000.000.000.000.000.000 de chaves possíveis para se escolher" (Singh, 2020, p. 28), o que dificultaria bastante o trabalho do criptoanalista, pois não teria tempo hábil para testar todas as possibilidades, obrigando-o a aprimorar sua técnica. A cifra *atbash*, é um rearranjo do alfabeto, em que letra "a" é substituída pela letra "z", a letra "b" é substituída pela letra "y", a letra "c" é substituída pela letra "w", e assim sucessivamente, ou seja, para cifrar uma letra da mensagem é levado em conta a distância que ela está do início do alfabeto,"g" é a sétima letra do alfabeto, no alfabeto cifrado sua correspondente será "t", pois "t" é a sétima letra considerando o final do alfabeto. A *atbash* é uma cifra de substituição simples hebraica, que foi encontrada no livro de Jeremias do Antigo Testamento da Bíblia, conforme Tkotz (2005, p. 181), "em Jeremias 25:26 e 51:41,..., aparece Sheshach no lugar de Babel, o que levou alguns a pensarem que se tratava de um bairro da Babilônia".

Texto original	p	r	o	f	m	a	t
Texto cifrado	K	I	L	U	N	Z	G

Tabela 1.3: Um exemplo utilizando a cifra *atbash*

Os árabes foram responsáveis por provar a fragilidade de uma cifra de substituição monoalfabética, pois eles descobriram como decifrá-la sem o conhecimento da chave e do algoritmo, o que é chamado de criptoanálise. O povo árabe inventou a criptoanálise, "a ciência da dedução do texto original a partir do texto cifrado, sem o conhecimento da chave"(Carneiro, 2017, p. 7). Eles obtiveram um método para quebrar a cifra de substituição monoalfabética, e esse método é baseado na análise de frequência das letras no texto. O método não parece ter surgido da necessidade de quebrar cifras, e sim da busca para entender o Alcorão. Nas escolas em Basra, Kufa e Bagdá, estudiosos analisavam a frequência e a fonética das palavras para ordenar, cronologicamente, os capítulos do Alcorão e saber a origem das palavras, e isso fez com que percebessem que algumas letras são mais comuns no idioma árabe. No entanto, o registro mais antigo desta técnica relacionada à criptoanálise é oriundo do cientista Abu Yusef Ya'qub ibn Is-haq ibn as-Sabbah ibn omran ibn Ismail al-Kindi, que viveu durante o século IX e era conhecido como "o filósofo dos árabes". De acordo com Singh (2020, p. 32), "a criptoanálise só pôde ser inventada depois que a civilização atingiu um nível suficientemente sofisticado de estudo, em várias disciplinas, incluindo matemática, estatística e linguística".

Assim como no idioma árabe, a frequência média das letras nos textos da língua portuguesa é quase constante, conforme a tabela abaixo mostra, as cinco letras usadas com maior frequência são: as vogais A, E e O, e na sequência as consoantes S e R.

A tabela abaixo foi extraída do livro Criptografia - Segredos embalados para viagem de Viktoria Tkotz, e segundo a autora, para obtê-la foram analisadas 157.764 palavras com 725.511 letras dos cinquenta primeiros capítulos de Memórias Póstumas de Brás Cubas, de Machado de Assis, Os Bruzundangas, de Lima Barreto, obras selecionadas de Rui Barbosa, A profissão de Jacques Pedreira, de João do Rio, e Contos Gauchescos, de João Simões Lopes Neto e o texto lido na cerimônia de encerramento do Fórum Social Mundial de 2002 por Saramago.

Letra	%	Letra	%	Letra	%
A	14,63	J	0,40	S	7,81
B	1,04	K	0,02	T	4,34
C	3,88	L	2,78	U	4,63
D	4,99	M	4,74	V	1,67
E	12,57	N	5,05	W	0,01
F	1,02	O	10,73	X	0,21
G	1,30	P	2,52	Y	0,01
H	1,28	Q	1,20	Z	0,47
I	6,18	R	6,53		

Tabela 1.4: Frequências de ocorrência das letras no português do Brasil

Por exemplo, ao analisar um texto cifrado pela cifra de substituição monoalfabética na língua portuguesa, e identificar que a letra P aparece com maior frequência, tem grandes chances da letra P do alfabeto cifrado fazer correspondência com a letra A no alfabeto original, e assim, sucessivamente, o segundo símbolo mais frequente no texto cifrado corresponderá a segunda letra mais frequente do alfabeto original.

Um ponto negativo da análise de frequência é o fato de não funcionar bem com textos curtos, o que pode ser verificado com o trava-línguas: "Três tigres tristes para três pratos de trigo. Três pratos de trigo para três tigres tristes", que cifrado usando a cifra de César fica: "Wuhv wljuhv wulvwhv sdud wuhv sudwrv gh wuljr. Wuhv sudwrv gh wuljr sdud wuhv wljuhv wulvwhv". Para decifrar, o primeiro impasse é que as letras W e U, as mais frequentes da frase, aparecem quatorze vezes cada uma, então seria necessário fazer uma escolha aleatória entre elas para associar com a letra A, que é a letra mais frequente do alfabeto original, chegando assim no segundo impasse, as letras W e U correspondem as letras T e R, respectivamente. Por sua vez, a letra A aparece apenas seis vezes, e corresponde a letra D no alfabeto cifrado.

As características da língua portuguesa como possuir palavras de duas letras, tal como, de, da, do, os, as, eu, entre outras; palavras de três letras, que, com, não, ele, seu, sua; os dígrafos, rr, ss, nh, ch, qu, somadas à análise de frequência, facilitam a

decifração de mensagens secretas.

Uma história que evidencia a insegurança para envio de mensagens secretas trazida pela análise de frequência, é a de Maria, rainha da Escócia. Singh (2020, p. 51-56) conta que ela foi mantida presa na Inglaterra e assassinada por sua prima Elizabeth I, rainha da Inglaterra. Maria representava uma ameaça para o trono de Elizabeth I, pois era admirada pelos católicos, por isso foi acusada de planejar o assassinato de Elizabeth I. Enquanto Maria estava presa no Chartley Hall, ela trocou cartas com Anthony Babington, que planejava seu resgate, as cartas chegavam ao destino com ajuda de Gilbert Gifford. Gifford usava esteganografia para esconder as cartas, ele colocava-as na tampa de um barril de cerveja, e Babington ainda cifrava as mensagens, usando vinte e três símbolos no lugar das letras do alfabeto, juntamente, com trinta e seis símbolos representando palavras e frases, quatro nulos e um símbolo para indicar uma letra dupla. Mas Gifford traiu Maria e Babington, entregando as cartas para sir Francis Walsingham, primeiro secretário da rainha Elizabeth. Walsingham conseguia ler as cartas com a ajuda de Thomas Phelippes, o qual decifrava-as pela análise de frequência. Maria foi decapitada no dia 8 de fevereiro de 1587.

O enfraquecimento da cifra de substituição monoalfabética trouxe insegurança para o envio de mensagens secretas através dela, e a ideia de driblar a análise de frequência das letras do idioma foi o estímulo para criação de novas cifras. Um aprimoramento da cifra de substituição monoalfabética são as cifras de substituição polialfabética, que fazem uso de mais de um alfabeto cifrado, isso implica que a mesma letra será cifrada de maneiras diferentes no decorrer do texto, uma delas foi a chamada Cifra de Vigenère.

> "Quanto maior for o número de equivalentes de uma letra, maior será a sua "despersonalização", e, quanto maior a "despersonalização", maior a segurança do sistema. [...] Pelo mesmo motivo exposto anteriormente, quanto maior for o número de alfabetos cifrantes, maior será a segurança da cifra. Se o número de alfabetos cifrantes depender de uma palavra ou frase-chave, quanto maior for a chave, maior será a segurança da cifra porque os ciclos cifrantes se repetem menos. Se o tamanho da chave for igual ao comprimento do texto que deve ser cifrado, então a cifra será extremamente segura e, como só existe um ciclo cifrante, essa cifra só poderá ser quebrada se os analistas possuírem vários criptogramas cifrados com a mesma chave (Tkotz, 2005, p. 221)."

Apesar de receber o nome de Cifra de Vigenère, segundo Carneiro (2017, p. 8-9) a primeira proposta para a cifra de substituição polialfabética partiu de Leon Battista Alberti. Ele viveu no século XV, e ficou mais conhecido por projetar a primeira fonte de Trevi em Roma e por ter escrito um livro sobre arquitetura. Posteriormente, a cifra recebeu contribuições do abade alemão Johannes Trithemius e do cientista italiano Giovanni Porta. Contudo, foi o diplomata francês Blaise de Vigenère, que compilou as ideias de Alberti, Trithemius e Porta, e transformou-as em um sistema completo de cifragem, descrita no seu tratado "Traicté des chiffres", publicado em 1586.

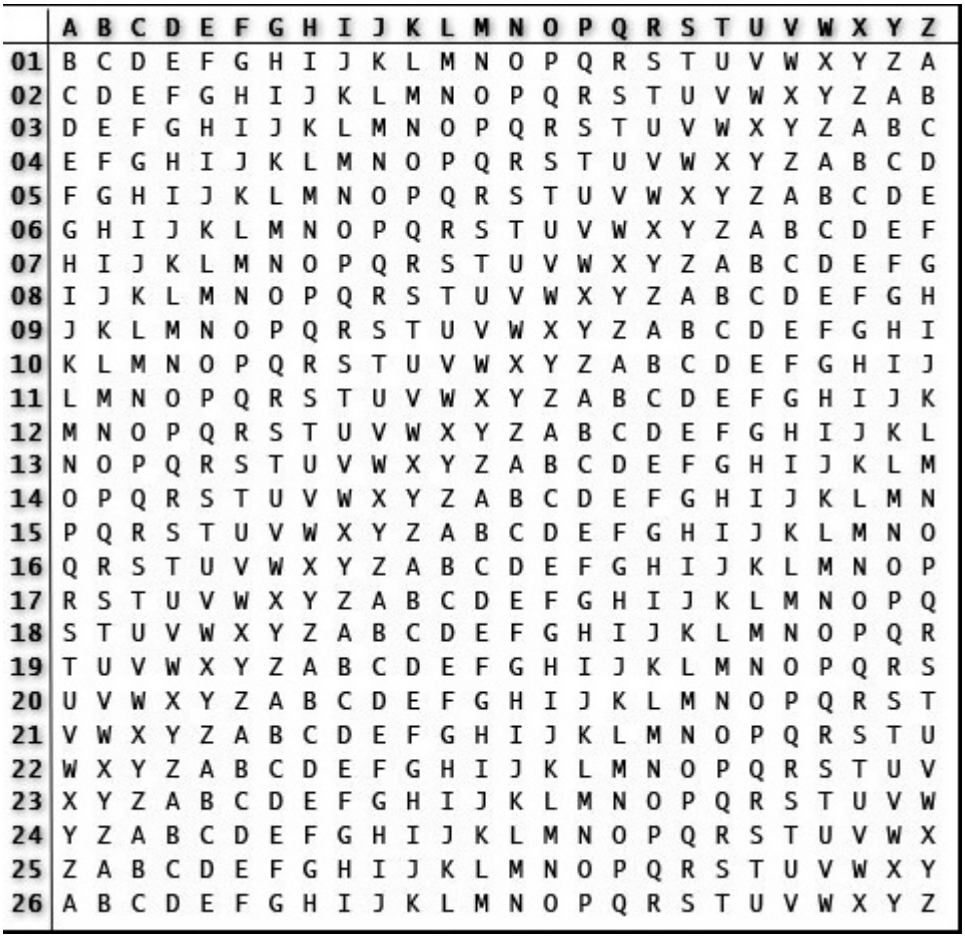
A cifra de Vigenère é formada por vinte e seis alfabetos cifrados pela Cifra de

César, mas com diferentes deslocamentos do alfabeto, conforme Figura 1.3. O processo de cifragem descrito por Carneiro (2017, p. 10) é o seguinte: escolhe-se uma palavra que será a chave, escreve-se a chave acima do texto que será cifrado, repetindo-se a chave até o fim do texto, assim cada letra do texto terá sua letra correspondente na palavra-chave. Fazendo isso, o processo continua no quadrado de Vigenére, a letra do texto cifrado será a letra que encontra-se na interseção da coluna que corresponde a letra do texto original com a linha que corresponde a letra da palavra-chave, segue-se com o mesmo processo até o fim do texto original. Para decifrar, de acordo com Carneiro (2017, p. 10), escreve-se a palavra-chave acima do texto cifrado, repetindo-se a chave até terminar o texto, no quadrado de Vigenère, segue-se a linha correspondente a letra da palavra-chave até encontrar-se a letra do texto cifrado. Feito isso, é só verificar a letra dessa coluna. O número de letras da palavra-chave corresponderá ao número de modos diferentes que cada letra do texto será cifrada, por exemplo, se a palavra-chave possuir cinco letras, a letra A poderá ser cifrada de cinco modos diferentes.

Chave	L	A	R	A	N	J	A
Texto original	p	r	o	f	m	a	t
Texto cifrado	A	R	F	F	Z	J	T

Tabela 1.5: Um exemplo da cifra de Vigenère

No exemplo da Cifra de Vigenère, Tabela 1.5, estamos cifrando a palavra profmat. Inicialmente, adotamos LARANJA como nossa palavra-chave e escrevemos ela acima da palavra profmat, caso a palavra ou frase a ser cifrada tivesse mais de sete letras, precisaríamos repetir a palava-chave ou escolher outra. Prosseguindo, continuamos o processo no quadrado de Vigenère (Figura 1.3), tomamos "p" a primeira letra do texto original e localizamos a coluna correspondente a letra "p" no quadrado de Vigenère (décima sexta coluna), em seguida, tomamos a letra "L" que é a primeira letra da palavra-chave e localizamos sua linha no quadrado de Vigenère (décima primeira linha). A primeira letra do texto cifrado será "A", que é a interseção da coluna correspondente a primeira letra do texto original e da linha correspondente a primeira letra da palavra-chave na Figura 1.3. Agora, vamos cifrar a letra "r", segunda letra do texto original, usando a letra "A" da palavra-chave; a letra cifrada será "R", que é a interseção entre a coluna correspondente a "r" e a linha correspondente a "A" na Figura 1.3. A terceira letra do texto cifrado é "F", pois ela encontra-se na interseção entre a coluna correspondente "o", terceira letra do texto original, e a linha correspondente a "R", terceira letra da palavra-chave. E assim, seguimos cifrando as próximas letras do texto original profmat.



	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
01	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
02	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
03	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
04	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
05	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
06	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
07	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
08	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
09	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	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

Figura 1.3: Quadrado de Vigenère
Fonte: $https://danieldonda.wordpress.com/2007/10/31/cifra-de-vigenere-le-chiffre-indechiffrable/$

Outra contribuição de Leon Battista Alberti, de acordo com Carneiro (2017, p. 11-12), foi o disco de Alberti no século XV, o primeiro artefato criptográfico. Funcionava como a cifra de César e era composto por dois círculos de cobre concêntricos de raios diferentes, com o alfabeto gravado ao longo das borda de cada círculo, os dois círculos giravam independentemente, de modo que o círculo maior correspondia ao alfabeto original e o outro ao alfabeto cifrado, então era só escolher o deslocamento, posicionar o círculo menor, assim facilitando a cifragem e decifragem.

Figura 1.4: Disco de Alberti
Fonte:
$https://horaciobacon.wordpress.com/2014/01/03/la-escritura-secreta-parte-iv/$

De acordo com Tkotz (2005, p. 222), outro artifício para fortalecer uma cifra é usar vários substitutivos para a mesma letra, o que faz com que ela perca suas características. Quando as letras do texto original são manipuladas em grupos de duas ou mais, a segurança do sistema também aumenta, isso se explica devido ao número de digramas possíveis que é muito maior do que o número de letras do alfabeto, ou seja, $26 \cdot 26 = 676$, o que implica que sua ocorrência torna-se relativamente menor. Um exemplo de cifra que divide o texto em grupos de letras para criptografar é a Cifra de Hill, criada em 1929, por Lester S. Hill, um professor de matemática norte-americano. Ela é baseada em transformações matriciais. A seguir temos um exemplo da cifra de Hill, com $n = 2$, aplicando o procedimento descrito no livro "Álgebra Linear com Aplicações" escrito por Howard Anton e Chris Rorres. Vamos criptografar a palavra PROFMAT.

Primeiramente, será estabelecido uma relação biunívoca abaixo entre as letras do alfabeto e os números inteiros de 0 a 25.

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

Tabela 1.6: Relação biunívoca entre as letras do alfabeto e os números inteiros de 0 a 25

O segundo passo é escolher uma matriz quadrada de ordem 2, cujos elementos

são números inteiros, além disso, a matriz deverá ter inversa em $\mathbb{Z}_{26}$ (classe residual módulo 26). Com essas especificações, temos a seguinte matriz A

$$A = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}.$$

O terceiro passo é fazer grupos de duas letras sucessivas da palavra PROFMAT, para fechar o último grupo será necessário adicionar uma letra fictícia que será a letra T, ou seja, PR OF MA TT que corresponde aos seguintes vetores colunas, usando a tabela 1.6:

$$P_1 = \begin{bmatrix} 15 \\ 17 \end{bmatrix},\ P_2 = \begin{bmatrix} 14 \\ 5 \end{bmatrix},\ P_3 = \begin{bmatrix} 12 \\ 0 \end{bmatrix},\ P_4 = \begin{bmatrix} 19 \\ 19 \end{bmatrix}.$$

Para codificar, são efetuados os seguintes produtos matriciais:

$$A * P_1 = \begin{bmatrix} 177 \\ 81 \end{bmatrix},\ A * P_2 = \begin{bmatrix} 100 \\ 43 \end{bmatrix},\ A * P_3 = \begin{bmatrix} 60 \\ 24 \end{bmatrix},\ A * P_4 = \begin{bmatrix} 209 \\ 95 \end{bmatrix},$$

resultando no que chamamos de vetores cifrados. Mas os elementos dos vetores cifrados não possuem correspondentes no alfabeto. Quando isso ocorrer, ou seja, quando o elemento do vetor cifrado for um número inteiro maior do que 25, ele será substituído pelo resto da divisão deste inteiro por 26. Sendo assim:

$$A * P_1 = \begin{bmatrix} 21 \\ 3 \end{bmatrix},\ A * P_2 = \begin{bmatrix} 22 \\ 17 \end{bmatrix},\ A * P_3 = \begin{bmatrix} 8 \\ 24 \end{bmatrix},\ A * P_4 = \begin{bmatrix} 1 \\ 17 \end{bmatrix},$$

ou ainda, usando a Tabela 1.6, VD - WR - IY - BR. Logo, a mensagem que será transmitida é VDWRIYBR.

O número de letras por grupo é a ordem da matriz, no caso apresentado acima, o texto foi agrupado em pares, então dizemos que é uma 2-cifra de Hill.

O destinatário da mensagem precisa da matriz inversa módulo 26 da matriz A, que denotamos por A^{-1}. A matriz inversa módulo 26 da matriz A, sendo

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

será

$$A^{-1} = (a \cdot d - b \cdot c)^{-1} \cdot \begin{bmatrix} d & -b \\ -c & a \end{bmatrix},$$

onde $(a \cdot d - b \cdot c)^{-1}$ é o recíproco ou inverso multiplicativo do resíduo $det(A) = a \cdot d - b \cdot c (\text{mod } 26)$.

No nosso exemplo, temos:

$$A^{-1} = \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix}.$$

Então, o destinatário recebe a mensagem cifrada, VDWRIYBR, divide a mensagem em grupos compostos por duas letras VD - WR - IY - BR, cujos vetores cifrados correspondentes são:

$$C_1 = \begin{bmatrix} 21 \\ 3 \end{bmatrix},\ C_2 = \begin{bmatrix} 22 \\ 17 \end{bmatrix},\ C_3 = \begin{bmatrix} 8 \\ 24 \end{bmatrix},\ C_4 = \begin{bmatrix} 1 \\ 17 \end{bmatrix}.$$

Então, realiza os produtos abaixo:

$$A^{-1} * C_1 = \begin{bmatrix} 93 \\ 225 \end{bmatrix},\ A^{-1} * C_2 = \begin{bmatrix} 430 \\ 499 \end{bmatrix},\ A^{-1} * C_3 = \begin{bmatrix} 584 \\ 520 \end{bmatrix},\ A^{-1} * C_4 = \begin{bmatrix} 409 \\ 331 \end{bmatrix}.$$

Como são números maiores que 25, para encontrar as letras correspondentes na Tabela 1.6 é necessário dividir os elementos dos vetores colunas por 26, com isso temos os seguintes vetores colunas:

$$A^{-1} * C_1 = \begin{bmatrix} 15 \\ 17 \end{bmatrix},\ A^{-1} * C_2 = \begin{bmatrix} 14 \\ 5 \end{bmatrix},\ A^{-1} * C_3 = \begin{bmatrix} 12 \\ 0 \end{bmatrix},\ A^{-1} * C_4 = \begin{bmatrix} 19 \\ 19 \end{bmatrix}$$

e pela Tabela 1.6, temos PR - OF - MA - TT. Portanto, a mensagem transmitida foi PROFMAT.

O livro "Álgebra Linear com Aplicações", escrito por Howard Anton e Chris Rorres, traz uma maneira de quebrar a cifra de Hill, através da obtenção da matriz decodificadora. Nesse método é necessário possuir um texto cifrado e o seu correspondente texto original. Ou então, que você tenha um texto cifrado, no qual consiga deduzir algumas palavras, o que permitirá determinar a matriz decodificadora da cifra de Hill. Isso é baseado em um resultado de Álgebra Linear, que nos diz que conseguimos determinar

uma transformação conhecendo-a em uma base. Ou seja, supondo que a mensagem interceptada foi cifrada utilizando n-cifra de Hill, e que sejam conhecidos os vetores comuns p_1, p_2, ..., p_n, linearmente independentes, cujos correspondentes vetores cifrados, também conhecidos, sejam $A * p_1$, $A * p_2$, ..., $A * p_n$, então é possível determinar a matriz A e, consequentemente, sua inversa $A^{-1}(\text{mod } m)$. O processo para encontrar a matriz A consiste em aplicar operações elementares sobre as linhas da matriz C até reduzi-la na matriz identidade I (C é uma matriz $n \times n$, cujas linhas são as matrizes transpostas das matrizes $A * p_1$, $A * p_2$, ..., $A * p_n$), e então aplicar estas mesmas operações elementares sobre as linhas da matriz P, que será transformada na matriz $(A^{-1})^T$. (P é uma matriz $n \times n$, cujas linhas são as matrizes transpostas das matrizes p_1, p_2, ..., p_n)

A complexidade da cifra polialfabética gerou resistência entre os criptógrafos profissionais em adotá-la, apesar deles necessitarem de cifras mais fortes para, principalmente, atividades militares, ou seja, continuar preservando os interesses de uma nação em segredo. Então surgiram variações de cifras monoalfabéticas, como a cifra de substituição homofônica, na qual cada letra poderia ter mais de um substitutivo, o que variava conforme a frequência da letra no texto, então cada símbolo corresponderia a um por cento do texto. Ainda que cada letra fosse substituída por vários símbolos, trata-se de uma cifra de substituição monoalfabética, porque um mesmo símbolo representa um única letra, diferente da polialfabética, em que um símbolo poderá representar mais de uma letra. Entretanto, depois de 1830, segundo Carneiro (2017, p. 12) além da eficiência da criptoanálise, houve um avanço na comunicação, com o desenvolvimento do telégrafo e do código Morse, e os criptógrafos sentiram-se pressionados a adotarem a cifra de substituição polialfabética, uma vez que para enviar mensagens pelo telégrafo era necessário entregar a mensagem para o telegrafista, que lia a mensagem, antes de transmiti-la ao destino em código Morse.

O prestígio da cifra de Vigenère, considerada indecifrável, chegou ao fim no século XIX, conforme conta Singh (2020, p. 85), sendo quebrada pelo cientista britânico Charles Babbage e pelo comandante prussiano Friedrich Kasiski. Nascido em 1791, Charles Babbage era professor de matemática em Cambridge, Inglaterra, e tinha grande interesse na quebra de cifras desde criança. O interesse por quebrar a cifra de Vigenère surgiu quando o dentista John Hall Brock Thwaites afirmou ter inventado uma nova cifra, que Babbage identificou como sendo a cifra de Vigenère, escrevendo isso para sociedade. Thwaites não aceitou as afirmações de Babbage e o desafiou a decifrá-la. Babbage aceitou o desafio e, por volta de 1854, obteve êxito na sua criptoanálise. O método de Babbage consistia em identificar sequências idênticas de letras no texto cifrado, depois verificava a distância entre essas sequências, o que auxiliava na determinação do comprimento da palavra-chave, ou seja, no número de letras dessa palavra; essa distância pode ser, exatamente, o comprimento n da chave ou um múltiplo do comprimento da chave;

o passo seguinte é descobrir as letras que compõe a chave. Cada letra da palavra-chave corresponde a um alfabeto cifrado diferente, ou seja, são n alfabetos cifrados através da cifra de substituição monoalfabética, então dividindo o texto nas n partes é possível aplicar a análise de frequência em cada uma dessas partes, separadamente. Infelizmente, de acordo com Singh (2020, p. 96), Babbage não publicou seus estudos. Na época, Kasiski ficou com o mérito, detalhando sua técnica descoberta, independentemente, para quebrar a cifra de Vigenère no trabalho intitulado "Die Geheimschriften und die Dechiffrer-Kunst" (A Escrita Secreta e a Arte de Decifrá-la), publicado em 1863.

Consequentemente, no final do século XIX, a criptografia passava por momentos difíceis, pois não existia uma cifra segura, somado a isso a telecomunicação deu outro salto com a criação do rádio pelo físico italiano Guglielmo Marconi. O rádio possibilitou comunicar-se entre dois locais quaisquer, sem a necessidade de ter um fio ligando esses locais. Conforme Singh (2020, p. 121) descreveu, o rádio facilitou a comunicação e a interceptação, características colocadas em evidência com o início da Primeira Guerra Mundial.

> "A associação de métodos é um procedimento que pode aumentar muito a segurança de um texto cifrado. A ideia de associar métodos não é nova e persiste até os dias de hoje. As cifras mais modernas, dentre as quais se destacam DES, DES triplo e RSA, antes de qualquer classificação mais técnica, podem ser consideradas como cifras baseadas na associação de métodos. E os métodos que são associados com mais frequência, como não poderia deixar de ser, são os de transposição, de substituição e de esteganografia." (Tkotz, 2005, p. 230)

Outro exemplo é a cifra *ADFGVX*, que esteve presente na Primeira Guerra Mundial. Ela consiste em um método de cifragem que une substituição e transposição. Para Singh (2020, p. 121-122), a comunicação através do rádio, o contínuo sucesso dos criptoanalistas, e a necessidade de trazer de volta o sigilo para os comandantes, fez crescer a busca por uma nova cifra segura. Por esses motivos e para manter em segredo um novo ataque, pois os aliados desconheciam a nova cifra, em 5 de março de 1918, os alemães adotaram a cifra *ADFGVX*. Porém, os aliados contavam com um talentoso criptoanalista, o francês George Painvin, que não sossegou até quebrar a *ADFGVX*, então os aliados conseguiram preparar-se para o ataque alemão, fazendo os inimigos recuarem após cinco dias de batalha.

Conforme apêndice F do livro "O livro dos códigos", de Simon Singh, a primeira etapa da *ADFGVX* é a construção da grade abaixo (Figura 1.5), a distribuição das 26 letras e dos dígitos de 0 a 9 é aleatória, a disposição desses elementos faz parte da chave e deve ser conhecida pelo destinatário. Na sequência, é necessário identificar a posição das letras do texto original na grade, e depois substituí-las pelas letras que identificam a linha e a coluna da sua posição, sendo assim o texto cifrado será composto por digramas formados apenas pelas letras A, D, F, G, V e X. A escolha das letras A, D, F, G, V e X deve-se ao Código Morse usado nas transmissões telegráficas, elas dificilmente são

confundidas quando traduzidas para pontos e traços, o que reduz as chances de erros na transmissão telegráfica.

	A	D	F	G	V	X
A	8	p	3	d	1	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

Figura 1.5: A grade de substituição para a primeira etapa da cifra ADFGVX
Fonte: Arquivo pessoal do autor

Na segunda etapa da cifragem, é aplicado a transposição, para isso escolhe-se uma palavra-chave, conhecida pelo remetente e pelo destinatário, que é escrita na primeira linha de uma nova grade. Em seguida, o texto cifrado na primeira etapa, será escrito nas linhas posteriores da grade de cima para baixo. Então, as colunas da grade são reordenadas para que as letras da palavra-chave fiquem em ordem alfabética, o criptograma final é a extração das letras por coluna de cima para baixo, conforme a ordem alfabética das letras da palavra-chave.

Para facilitar a visualização do procedimento descrito acima, vamos fazer um exemplo cifrando a palavra MESTRADO (texto original), usando a grade da Figura 1.5. Nesse caso, para cifrar as letras do texto original precisamos localizá-las na grade. Começando a cifragem, a letra M encontra-se na interseção da linha correspondente a letra G com a coluna corresponde a letra X, logo M será substituído por GX no texto cifrado. Continuando com E, a segunda letra do texto original, ela encontra-se na interseção entre a linha correspondente a letra X e a coluna correspondente a letra D da Figura 1.5, ou seja, o texto cifrado referente a letra E será XD. Fazemos esse processo até cifrar todas as letras do texto original. Após isso, obtemos o seguinte texto cifrado GX - XD - VD - DD - VV - DV - AG - DG, ou ainda, GXXDVDDDVVDVAGDG. Na fase da

transposição, empregamos a palavra-chave SOMA, que foi escrita na primeira linha da grade à esquerda da Figura 1.6, nas linhas seguintes da grade foram escritas as letras texto cifrado GXXDVDDDVVDVAGDG (obtido acima), começamos escrevendo abaixo da letra S em direção a letra A, e assim, sucessivamente, até terminar o texto cifrado. E então, reordenamos as colunas da grade à esquerda da Figura 1.6, para que as letras da palavra-chave SOMA fiquem em ordem alfabética, conforme a grade à direita na Figura 1.6.

S	O	M	A
G	X	X	D
V	D	D	D
V	V	D	V
A	G	D	G

A	M	O	S
D	X	X	G
D	D	D	V
V	D	V	V
G	D	G	A

Figura 1.6: Segunda etapa do exemplo da cifra ADFGVX
Fonte: Arquivo pessoal do autor

Portanto, o texto cifrado final que será entregue ao destinatário é DDVGXDDDXDVGGVVA, finalmente, obtido pela extração das letras da coluna A, depois as letras da coluna M, coluna O, e, por último da coluna S da grade à direita.

Segundo Carneiro (2017, p. 15), entre os anos de 1914 e 1918, não há registro de avanços na criptografia. Em contrapartida, nos anos seguintes, foram inventadas máquinas para cifrar e decifrar mensagens. Uma máquina cifrante que ficou bastante conhecida foi a Enigma, Singh (2020, p. 146) diz que ela foi desenvolvida pelo alemão Arthur Scherbius, engenheiro elétrico, que junto com seu amigo Richard Ritter possuía uma empresa de engenharia inovadora, a Scherbius & Ritter. O funcionamento da Enigma era baseado no disco de cifras de Alberti, ou melhor, basicamente tratava-se de uma versão elétrica do disco de Alberti. A forma primária da Enigma era composta por um teclado destinado para digitação das letras do texto original, um misturador responsável pela cifragem, e um quadro de lâmpadas que exibia os caracteres cifrados, esses elementos ficavam ligados

através de fios elétricos. Singh (2020, p. 146-147) define misturador como

> "um espesso disco de borracha cheio de fios, é a parte mais importante da máquina. Partindo do teclado, os fios entram no misturador em seis pontos diferentes e fazem uma série de voltas e torções dentro do misturador antes de emergirem de outros seis pontos no lado oposto. A fiação interna do misturador determina como as letras serão cifradas."

Demorou um pouco, mas Scherbius conseguiu encontrar um mercado para suas máquinas. Em 1925, os militares alemães começaram a usá-las, e posteriormente, o governo e empresas estatais. A versão da máquina Enigma adquirida pelos militares não era a mesma versão das poucas máquinas que Scherbius vendera para os empresários.

> "Nas duas décadas seguintes os militares alemães compraram 30 mil máquinas Enigma. E a invenção de Scherbius deu aos alemães o sistema mais seguro de criptografia do mundo. Com ele, no início da Segunda Guerra Mundial, as comunicações estavam protegidas por um nível sem igual de cifragem. Naquela época parecia que a máquina Enigma desempenharia um papel vital na vitória nazista, mas ela acabou ajudando na queda de Hitler. Scherbius não viveu o suficiente para ver os sucessos e os fracassos do seu sistema de cifras. Em 1929, enquanto dirigia uma parelha de cavalos, ele perdeu o controle da carruagem e colidiu contra um muro, morrendo das lesões internas no dia 13 de maio (Singh, 2020, p. 161)."

Após a Primeira Guerra Mundial, os britânicos continuaram atentos as comunicações alemãs, mas em 1926, perceberam que algo havia mudado, foi quando os alemães começaram a usar a máquina Enigma para cifrar as mensagens. Inicialmente, os britânicos, os americanos e os franceses não obtiveram sucesso na tarefa de desvendar a cifra Enigma.

Como foi bem colocado por Singh (2020, p. 164), "se a necessidade é a mãe das invenções, então a adversidade é a mãe da criptoánalise". A Polônia não encontrava-se em posição de segurança e temia pela sua soberania, a Rússia e a Alemanha representavam uma ameça para seus territórios. Movidos por essa insegurança, os poloneses fundaram o Biuro Szyfrów, um departamento de cifras.

A Enigma não foi invicta, isso graças aos esforços, principalmente, de Marian Rejewski do Biuro, e Alan Turing da Escola de Cifras e Códigos do Governo, localizada em Bletchley Park, de Buckinghamshire. Contudo, segundo Singh (2020, p. 166), o primeiro passo para quebra da cifra Enigma foi um alemão descontente com seu país, que em 1931 vendeu informações sobre os segredos da Enigma para um agente francês. Isso possibilitou aos aliados a construção de um réplica da Enigma, mas não era suficiente, eles precisavam do ajuste inicial da máquina, ou seja, a chave da cifra. Para essa tarefa árdua, os poloneses selecionaram alguns matemáticos, entre eles estava Marian Rejewski, que foi capaz de desvendar os segredos da Enigma e então conseguir entender as mensagens alemãs por vários anos. Porém, os inimigos tomavam alguns cuidados, e de vez em quando faziam alterações no modo como transmitiam as mensagens. Em consequência, conforme Singh (2020, p. 177) escreveu, Rejewski inventou as bombas, que eram adaptações da

máquina Enigma que verificavam os ajustes corretos dos misturadores, para cada arranjo possível de misturador, era necessário uma bomba.

Em 1938, Singh (2020, p. 178) conta que os alemães acrescentaram misturadores, aumentando muito o número de arranjos, o que inviabilizou para os poloneses a construção da quantidade necessária de bombas para decifrar as comunicações alemãs. A partir disso, Singh (2020, p. 181) relata que os poloneses compartilharam suas descobertas com os ingleses, porque até então os avanços poloneses na criptoanálise eram desconhecidos pelos franceses e ingleses.

Os criptoanalistas da Bletchley Park dominaram as técnicas polonesas de criptoanálise da Enigma, onde Alan Turing foi um dos destaques, pois inventou a máquina de Turing, que era um princípio para criação do computador de hoje. "Turing fora além e fornecera uma sólida base teórica para a computação, dando ao computador um potencial até então não imaginado" (Singh, 2020, p. 190). Na luta contra a Enigma, Turing seguiu os passos de Rejewski através do aprimoramento das bombas e, somado aos esforços dos outros pesquisadores de Bletchley Park, finalmente, a Enigma foi decifrada, terminando com a guerra em 1945.

Após a guerra, os criptoanalistas continuaram usufruindo da tecnologia dos computadores, que permitia mais agilidade para testar todas as chaves possíveis, mas os criptógrafos não ficaram em desvantagem, enxergando o potencial de criar cifras ainda mais poderosas através dos computadores. Além do campo militar e do governo, o computador acabou conquistando novos espaços, como o campo comercial, na década de 1960. Para Carneiro (2017, p. 18-19), graças a algumas invenções, ele tornou-se um produto mais potente, e também surgiram versões de valores mais baixos, e por essa e outras mudanças tornou-se acessível às pessoas comuns. O advento dos computadores trouxe algumas questões a serem resolvidas pela criptografia, entre elas estava a distribuição de chaves.

É possível observar, ao longo da história da criptografia, que a distribuição de chaves sempre foi um ponto crítico, os criptógrafos conviviam com o risco da chave parar em mãos erradas. Além disso, o crescente uso dos computadores para cifrar comunicações importantes, implicou no aumento da demanda por distribuição de chaves, o que tornou-se impraticável tanto logisticamente quanto pelos custos exorbitantes. Mas a melhor e mais segura opção para entrega das chaves ainda era pessoalmente. Por exemplo, uma empresa necessita encaminhar informações confidenciais para seus clientes, sendo assim, ela cifra as informações. Os clientes precisarão usar a mesma cifra (nesse ponto, entra a questão da padronização) e também a chave para decifrar, o funcionário da empresa poderia passar a chave através de ligação telefônica, porém o telefone pode estar grampeado, então a empresa organiza-se para que um funcionário de confiança, pessoalmente, entregue a

chave para cada um de seus clientes.

Segundo Singh (2020, p. 277-279), o criptógrafo Whitfield Diffie tinha grande interesse pelo problema da distribuição de chaves. Nascido em 1944, graduou-se em matemática no Massachusetts Institute of Technology, em 1965. Ele possuía uma visão de mundo conectado, onde pessoas comuns com seus computadores interligados por linhas telefônicas nas suas casas pudessem trocar informações através de e-mails, comprar produtos pela internet, realizar transações bancárias, mas isso implicaria na necessidade de privacidade digital. Diffie teve sua visão de mundo concretizada com a ARPANet em 1969, evoluindo para Internet em 1982.

> "No final dos anos 80 os usuários não-acadêmicos e não-governamentais tiveram acesso à Internet, e daí em diante o número de usuários cresceu explosivamente. Hoje, mais de cem milhões de pessoas usam a Internet para trocar informações e enviar mensagens pelo correio eletrônico, os e-mails (Singh, 2020, p. 279)."

Diffie conheceu Hellman e Merkle, e os três vislumbravam resolver o problema da distribuição de chaves. De acordo com Singh (2020, p. 280-281), Martin Hellman, nascido em 1945, era professor da Universidade de Stanford na Califórnia, e Ralph Merkle um refugiado intelectual. Juntos concluíram que a solução para o problema da distribuição de chaves era uma função matemática de mão única, ou seja, difícil de reverter. Após uma busca incessante, Hellman conseguiu chegar a um esquema, usando a função modular $Y^x (\text{mod } P)$, no qual não era necessária a troca de chaves, o receptor e o emissor apenas precisam decidir juntos os valores de Y e P, sendo Y menor que P, podendo fazer isso por telefone, pois esses valores não são a chave, portanto não são sigilosos. O esquema de Hellman não será descrito nesse trabalho, pois nosso objetivo é a criptografia RSA, caso alguém tenha interesse, ele encontra-se na página 290 de "O livro dos códigos", do autor Simon Singh. O trabalho de Diffie-Hellman-Merkle mostra a ausência da necessidade da troca de chaves, entretanto, ainda existe uma troca de informações entre receptor e emissor para a cifragem de um segredo, o que prejudicava uma forma de comunicação imediata, como um e-mail.

Entretanto, Diffie foi além do conquistado pelos três, ele chegou ao conceito de chave assimétrica. Até o momento, todas as cifras eram formadas por chaves simétricas, ou seja, para o processo de decifragem era aplicado o oposto da chave de cifragem. Já na cifra com chave assimétrica seria uma chave para cifragem e outra diferente para decifragem. A partir do conceito de chave assimétrica, podemos falar sobre o conceito de chave pública. Para exemplificar, imagine a troca de informações por Alice e Bob, através do computador.

> "[...] a chave de cifragem de Alice será um número e sua chave de decifragem um outro número diferente. Alice mantém em segredo sua chave de decifragem, de modo que a chamamos de chave particular de Alice. Contudo ela divulga sua chave de cifragem de modo

> que todos tenham acesso a ela, e é por isso que a chamamos comumente de chave pública de Alice. Se Bob deseja mandar uma mensagem para Alice, ele simplesmente procura sua chave pública, que poderia estar em uma lista, semelhante a uma lista telefônica. Bob então usa a chave pública de Alice para cifrar sua mensagem. Ele envia para Alice e ela pode decifrá-la usando sua chave de decifragem particular (Singh, 2020, p. 295)."

Em 1975, Diffie publicou seu trabalho sobre o sistema de chaves assimétricas, porém ele ainda não havia descoberto uma cifra que preenchesse os requisitos do seu sistema.

A descoberta da função matemática que satisfaz os requisitos do sistema de chaves assimétricas foi realizada, em 1977, por Ron Rivest, Leonard Adleman e Adi Shamir, dois cientistas da computação e um matemático, respectivamente. Eles eram pesquisadores do Laboratório de Ciência da Computação do MIT, Estados Unidos. Por isso, o método de cifra de chave pública mais influente da criptografia moderna ficou conhecido como RSA.

Conforme descreveu Singh (2020, p. 300), a RSA é baseada em uma função modular, na qual é colocado um número, que corresponde a mensagem a ser cifrada, o resultado disso é um texto cifrado, ou seja, outro número. Um aspecto importante dessa função de mão única é a possibilidade de escolha do valor de N, cada pessoa para personalizar sua função pode escolher um valor de N diferente. A flexibilidade de N é o que torna-a uma função de mão única reversível sob certas circunstâncias.

O valor de N é obtido através da multiplicação de dois números primos p e q, o número N é a chave pública de uma pessoa, e os números p e q correspondem à chave particular dela. A pessoa pode divulgar sua chave pública, por exemplo, colocá-la em um lista pública de chaves, onde constem as chaves de diversas pessoas. Para cifrar uma mensagem, obtemos a chave pública N do destinatário e colocamos na forma geral da função de mão única, então temos a função de mão única do destinatário. O destinatário receberá o resultado da aplicação da mensagem na sua função personalizada, ele usará sua chave particular p e q para decifrá-la.

A segurança da RSA reside no fato que os valores de p e q não são públicos, e apenas eles revertem a função de mão única utilizada. E a força da RSA reside na escolha de p e q suficientemente grandes, gerando N ainda maior, para que seja virtualmente impossível fatorar N para chegar na chave particular p e q, capaz de decifrar as mensagens. "O único problema para a segurança da criptografia de chave pública RSA é que, em alguma época no futuro, alguém possa encontrar um modo rápido de fatorar N" (Singh, 2020, p. 303).

Segundo Singh (2020, p. 314), a cifra RSA e os fundamentos da chave pública também foram descobertos na Europa, de forma independente do trabalho conquistado por Rivest, Adleman e Shamir. Mas como os responsáveis foram James Ellis, Clifford

Clocks e Malcolm Williamson, funcionários do governo britânico no Quartel-General de Comunicações do Governo (GCHQ), a descoberta foi mantida em sigilo por alguns anos.

Anteriormente à descrição da criptografia de chave pública RSA, no próximo capítulo deste trabalho, vamos abordar os conteúdos matemáticos envolvidos e necessários para compreensão desse método.

Capítulo 2

Aritmética dos números inteiros

Nesse capítulo, vamos abordar alguns resultados da Teoria dos Números que auxiliarão no entendimento de certos conceitos de criptografia e, inclusive, do algoritmo de Criptografia RSA. E também, teoremas, proposições, lemas, necessários para demonstração deles. Para isso, serão usados os livros "Números Inteiros e Criptografia RSA", do Severino Collier Coutinho, "Álgebra Moderna", do autor Hygino H. Domingues e Gelson Iezzi, "Estruturas Algébricas para Licenciatura", de Jhone Caldeira Silva e Olimpio Ribeiro Gomes e "Introdução à Teoria dos Números", de José Plínio de Oliveira Santos.

Os conjuntos numéricos utilizados serão os seguintes:

$\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$ o conjunto dos números naturais;

$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$ o conjunto dos números inteiros.

Denotaremos por $\mathbb{N}^*$, quando $\mathbb{N} \setminus \{0\}$. E também $\mathbb{Z}^*$, quando for $\mathbb{Z} \setminus \{0\}$.

Definição 2.1. *Sejam a, $b \in \mathbb{Z}$. Dizemos que b divide a se existir algum $q \in \mathbb{Z}$ tal que $a = b \cdot q$.*

Quando falamos de divisão exata no conjunto dos números inteiros, dizemos que o número inteiro b é divisor do número inteiro a ou que o número a é divisível por b, ou ainda, que a é um múltiplo de b, se para algum $q \in \mathbb{Z}$ temos $a = b \cdot q$. Quando b divide a, denotaremos por $b \mid a$, ou se b não divide a, denotaremos por $b \nmid a$. O número inteiro q é chamado quociente de a por b.

Exemplo 2.2. *Dados os números inteiros* 3 *e* 12, 3 *divide* 12, *pois* $12 = 3 \cdot 4$.

Agora, vamos apresentar algumas propriedades do conceito de divisibilidade no conjunto dos números inteiros.

Proposição 2.3. *Sejam a, b, c, $d \in \mathbb{Z}$. Então são válidas as afirmações a seguir:*

(a) $d \mid d$. *(reflexividade)*

(b) Se $a, b \geq 0$, $a \mid b$ *e* $b \mid a$, *então* $a = b$.

(c) Se $d \mid a$ *e* $d \mid b$, *então* $d^2 \mid a \cdot b$.

(d) Se $d \mid a$ *e* $a \mid b$, *então* $d \mid b$. *(transitividade)*

(e) Se $d \mid a$ *e* $d \mid b$, *então* $d \mid (x \cdot a + y \cdot b)$, *para quaisquer inteiros* x *e* y.

(f) Se $d \mid a$ *e* $b \mid c$, *então* $d \cdot b \mid a \cdot c$.

Demonstração. (a) Pela definição de divisibilidade, devemos mostrar que existe um número inteiro q tal que $d = d \cdot q$. Pela neutralidade multiplicativa do número 1, basta tomar $q = 1$.

(b) Por hipótese, existem q_1 e $q_2 \in \mathbb{Z}$ tais que

$$b = a \cdot q_1 \tag{2.1}$$

e

$$a = b \cdot q_2 \tag{2.2}$$

Se $a = 0$ ($b = 0$), então $b = 0$ ($a = 0$). Suponhamos pois, a, $b > 0$. De (2.1) e (2.2), temos $a = a \cdot q_1 \cdot q_2$, e segue, pela lei do cancelamento, que $q_1 \cdot q_2 = 1$. Mas q_1 e q_2 são positivos e, portanto, essa igualdade só é possível para $q_1 = q_2 = 1$. Portanto, $a = b$.

(c) Pela hipótese de que $d \mid a$ temos que existe um inteiro q_1 tal que

$$a = d \cdot q_1 \tag{2.3}$$

e pela hipótese de que $d \mid b$, temos que existe um inteiro q_2 tal que

$$b = d \cdot q_2 \tag{2.4}$$

Bem, para concluir que $d^2 \mid a \cdot b$, devemos mostrar que é possível encontrar um inteiro q_3, tal que $a \cdot b = d^2 \cdot q_3$. Para isso substituímos as expressões de a e b dadas pelas equações (2.3) e (2.4) no produto $a \cdot b$ e teremos

$$a \cdot b = (d \cdot q_1) \cdot (d \cdot q_2). \tag{2.5}$$

Agora usamos as propriedades associativa e comutativa da multiplicação para reagrupar os termos obtendo

$$a \cdot b = d^2 \cdot (q_1 \cdot q_2). \tag{2.6}$$

Observando, esta última igualdade, vemos que o número procurado é $q_3 = q_1 \cdot q_2$.

(d) Pela hipótese de que $d \mid a$, temos que existe um inteiro q_1 tal que

$$a = d \cdot q_1 \tag{2.7}$$

e, pela hipótese de que $a \mid b$, temos que existe um inteiro q_2 tal que

$$b = a \cdot q_2 \tag{2.8}$$

Agora, substituindo o valor de a dado pela expressão (2.7) na expressão (2.8), e usando a propriedade associativa da multiplicação temos

$$b = d \cdot (q_1 \cdot q_2). \tag{2.9}$$

Finalmente, observando a igualdade (2.9), vemos que bastar tomar o número inteiro q_3 como $q_3 = q_1 \cdot q_2$ e teremos $d \mid b$, que é o resultado desejado.

(e) Pela hipótese de que $d \mid a$, existe um inteiro q_1 tal que

$$a = d \cdot q_1 \tag{2.10}$$

e, pela hipótese de que $d \mid b$, existe um inteiro q_2 tal que

$$b = d \cdot q_2. \tag{2.11}$$

A fim de obter $d \mid (x \cdot a + y \cdot b)$, o que precisamos demonstrar é que é possível encontrar um inteiro q_3 tal que $d \cdot q_3 = x \cdot a + y \cdot b$, quaisquer que sejam os números inteiros x e y. Procedemos como anteriormente e substituímos as expressões de a e b dadas pelas igualdades (2.10) e (2.11) em $x \cdot a + y \cdot b$, obtendo

$$x \cdot a + y \cdot b = x \cdot (d \cdot q_1) + y \cdot (d \cdot q_2) \tag{2.12}$$

Agora, usando a propriedade associativa da multiplicação seguida da propriedade distributiva da multiplicação em relação à adição, podemos reescrever a igualdade (2.12) da forma

$$x \cdot a + y \cdot b = (x \cdot q_1 + y \cdot q_2) \cdot d. \tag{2.13}$$

Finalmente, observando a igualdade (2.13), vemos que encontramos um inteiro q_3, a saber, $q_3 = x \cdot q_1 + y \cdot q_2$, com a propriedade que $d \cdot q_3 = x \cdot a + y \cdot b$, que é exatamente o que desejávamos.

(f) Pela hipótese de que $d \mid a$, existe um inteiro q_1 tal que

$$a = d \cdot q_1 \tag{2.14}$$

e pela hipótese de que $b \mid c$, temos que existe um inteiro q_2 tal que

$$c = b \cdot q_2. \tag{2.15}$$

Multiplicando-se membro a membro as igualdades (2.14) e (2.15), obtém-se

$$a \cdot c = (d \cdot b) \cdot (q_1 \cdot q_2). \tag{2.16}$$

De (2.16), concluímos que $d \cdot b \mid a \cdot c$. □

Até agora falamos sobre divisão exata, mas não é sempre que isso acontece, vejamos o exemplo abaixo.

Exemplo 2.4. *Dados* 3 *e* 16, 3 *não divide* 16, *pois não existe* $q \in \mathbb{Z}$ *tal que* $16 = 3 \cdot q$.

Assim como o par de números 3 e 16, em que um não divide o outro, há infinitos pares de números inteiros tais que nenhum dos dois é divisor do outro. Considerando esses casos, vamos estabelecer uma "divisão com resto", através do Algoritmo da Divisão (ele aparece no livro VII dos "Elementos" de Euclides). Antes disso, enunciemos o chamado Teorema de Eudoxius:

Teorema 2.5. *Dados* a *e* b *inteiros, com* $b \neq 0$, *então* a *é um múltiplo de* b *ou se encontra entre dois múltiplos consecutivos de* b, *isto é, correspondendo a cada par de inteiros* a *e* $b \neq 0$ *existe um inteiro* q *tal que, para* $b > 0$,

$$q \cdot b \leq a < (q+1) \cdot b$$

e para $b < 0$,

$$q \cdot b \leq a < (q-1) \cdot b.$$

Exemplo 2.6. *Se* $a = 11$ *e* $b = 4$, *devemos tomar* $q = 2$,

$$2 \cdot 4 \leq 11 < 3 \cdot 4.$$

Para $a = -11$ *e* $b = 4$, *tomamos* $q = -3$,

$$-3 \cdot 4 \leq -11 < (-3+1) \cdot 4.$$

Exemplo 2.7. *Se* $a = 11$ *e* $b = -4$, *tomamos* $q = -2$,

$$(-2) \cdot (-4) \leq 11 < (-2-1) \cdot (-4)$$

Para $a = -11$ *e* $b = -4$, *tomamos* $q = 3$,

$$3 \cdot (-4) \leq -11 < (3-1) \cdot (-4).$$

Teorema 2.8. *(Algoritmo da Divisão) Dados dois inteiros* a *e* b, *com* $b \neq 0$, *existe um único par de inteiros* q *e* r *tais que*

$$a = b \cdot q + r \qquad com \qquad 0 \leq r < |b|.$$

Demonstração. Pelo Teorema de Eudoxius, como $b > 0$, existe q satisfazendo:

$$q \cdot b \leq a < (q+1) \cdot b$$

o que implica $0 \leq a - q \cdot b$ e $a - q \cdot b < b$. Desta forma, se definirmos $r = a - q \cdot b$, teremos, garantida, a existência de q e r. Ou ainda, pelo Teorema de Eudoxius, tomando $b < 0$, existe q satisfazendo:

$$q \cdot b \leq a < (q-1) \cdot b$$

o que implica $0 \neq a - q \cdot b$ e $a - q \cdot b < -b$. Definindo $r = a - q \cdot b$, teremos, garantida, a existência q e r. A fim de mostrarmos a unicidade, vamos supor a existência de outro par q_1 e r_1 verificando:

$$a = b \cdot q_1 + r_1 \qquad \text{com} \qquad 0 \leq r_1 < b.$$

Disto temos $(b \cdot q + r) - (b \cdot q_1 + r_1) = 0$, o que implica em $b \cdot (q - q_1) = r_1 - r$, logo $b \mid (r_1 - r)$. Mas, como $r_1 < b$ e $r < b$, temos $|r_1 - r| < b$ e, portanto, como $b \mid (r_1 - r)$ devemos ter $r_1 - r = 0$. Logo, $q_1 \cdot b = q \cdot b$, então $q_1 = q$, uma vez que $b \neq 0$. □

Os elementos a, b, q e r são chamados dividendo, divisor, quociente e resto, respectivamente, da divisão de a por b.

Exemplo 2.9. *Dados $a = 34$ e $b = 3$ temos que existem $q = 11$ e $r = 1$, tais que $34 = 3 \cdot 11 + 1$ e $0 \leq 1 < 3$.*

Exemplo 2.10. *Dados $a = -144$ e $b = 11$ temos que existem $q = -13$ e $r = 3$, tais que $-140 = 11 \cdot (-13) + 3$ e $0 \leq 3 < 11$.*

Em particular, quando b divide a, o resto é 0.

Observação 2.11. *Seja a um inteiro qualquer e $b = 4$, utilizando o Algoritmo da Divisão, podemos escrever*

$$a = 4 \cdot q + r, \quad \textit{onde} \quad 0 \leq r < 4.$$

Nesse caso, os valores possíveis de r são 0, 1, 2 e 3. Ou seja, o número inteiro a pode ser escrito somente de uma das seguintes formas

$$4 \cdot q, \quad 4 \cdot q + 1, \quad 4 \cdot q + 2, \quad 4 \cdot q + 3, \quad \textit{com} \quad q \in \mathbb{Z}.$$

Observe que se considerarmos os conjuntos

$$\begin{aligned} \{4 \cdot q | q \in \mathbb{Z}\} &= \{\ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\}, \\ \{4 \cdot q + 1 | q \in \mathbb{Z}\} &= \{\ldots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\}, \end{aligned}$$

$$\begin{aligned}\{4\cdot q+2|q\in\mathbb{Z}\} &= \{\ldots,-14,-10,-6,-2,2,6,10,14,18,\ldots\},\\ \{4\cdot q+3|q\in\mathbb{Z}\} &= \{\ldots,-13,-9,-5,-1,3,7,11,15,19,\ldots\},\end{aligned}$$

obteremos uma partição do conjunto $\mathbb{Z}$. Ou seja, qualquer elemento de $\mathbb{Z}$ pertence a um único desses conjuntos e a união disjunta desses quatro conjuntos resulta em todo o conjunto $\mathbb{Z}$.

2.1 Máximo Divisor Comum

Seja $a\in\mathbb{Z}^*$; o conjunto dos números inteiros divisores de a será denotado por $D(a)$. Considerando os números inteiros 6 e 8, o conjunto dos números divisores de 6 é $D(6)=\{\pm1,\pm2,\pm3,\pm6\}$ e o conjunto dos divisores de 8 é $D(8)=\{\pm1,\pm2,\pm4,\pm8\}$. Os divisores comuns de 6 e 8 são elementos da interseção dos conjuntos $D(6)$ e $D(8)$:

$$D(6)\cap D(8)=\{\pm1,\pm2\}$$

O maior elemento dessa interseção, ou seja, o número 2, é o máximo divisor comum de 6 e 8.

Definição 2.12. *Sejam a e b dois números inteiros, $a\neq0$ ou $b\neq0$. Dizemos que $d\in\mathbb{Z}$ é o máximo divisor comum de a e b se cumpre as seguintes condições:*

i) $d>0$

ii) $d\mid a$ *e* $d\mid b$

iii) Se d' é um inteiro tal que $d'\mid a$ e $d'\mid b$, então $d'\mid d$ (ou seja, todo divisor comum de a e b também é divisor de d).

Denotaremos o máximo divisor comum entre os números inteiros a e b por $mdc(a,b)$.

Note que $mdc(0,0)$ não está definido, uma vez que o número zero é divisível por qualquer inteiro não nulo.

Observação 2.13. *Se d é o máximo divisor comum de a e b, então d também é máximo divisor comum de $-a$ e b, a e $-b$ e $-a$ e $-b$, pois todo divisor de x é divisor de $-x$, e vice-versa.*

O próximo teorema nos diz que o $mdc(a,b)$ sempre existe, que pode ser escrito como uma combinação linear entre a e b com coeficientes inteiros. Por exemplo,

$mdc(12, 27) = 3 = 12 \cdot (-2) + 27 \cdot 1$. Vale salientar que essa combinação não é única, por exemplo, $mdc(12, 27) = 3 = 12 \cdot (-11) + 27 \cdot 5$. E que escrever um número inteiro k como uma combinação linear com coeficientes inteiros entre a e b, não significa que k seja o $mdc(a, b)$, por exemplo, $12 \cdot 3 + 27 \cdot (-1) = 9 \neq 3 = mdc(12, 27)$.

Proposição 2.14. *Para quaisquer inteiros a e b, existem inteiros x_0 e y_0 tais que $d = a \cdot x_0 + b \cdot y_0$ é o máximo divisor comum de a e b.*

Demonstração. Sejam a e b inteiros, tais que $a > 0$ e $b > 0$, o que é possível devido à Observação 2.13. Consideremos o conjunto $L = \{a \cdot x + b \cdot y \mid x, y \in \mathbb{Z}\}$. L possui elementos estritamente positivos, por exemplo, $a + b$, obtido ao se fazer $x = y = 1$. Seja d o menor entre todos os elementos estritamente positivos de L. Portanto, $d = a \cdot x_0 + b \cdot y_0$, para convenientes elementos $x_0, y_0 \in \mathbb{Z}$. Mostremos que d é o máximo divisor comum de a e b. De fato:

1. Obviamente $d > 0$.

2. Aplicando o Algoritmo da Divisão a a e d, o que é possível, pois $d > 0$, então temos $a = d \cdot q + r$ $(0 \leq r < d)$. Mas, como já vimos, $d = a \cdot x_0 + b \cdot y_0$ e, então:

   $$a = (a \cdot x_0 + b \cdot y_0) \cdot q + r$$

   o que resulta em,

   $$r = a \cdot (1 - q \cdot x_0) + b \cdot (-q \cdot y_0)$$

   o que mostra que r é um elemento de L. Então r, não pode ser estritamente positivo, pois é menor que d (= mínimo de L). Logo, $r = 0$ e, portanto, $a = d \cdot q$. Ou seja: $d \mid a$. De maneira análoga se demonstra que $d \mid b$.

3. Se $d' \mid a$ e $d' \mid b$, então $d' \mid d$, uma vez que $d = a \cdot x_0 + b \cdot y_0$, pela Proposição 2.3 (e).

□

Lema 2.15. *Sejam a, $b \in \mathbb{Z}$. Se $a \mid b$, então $mdc(a, b) = |a|$.*

Demonstração. Pela Observação 2.13, sem perda de generalidade, podemos nos ater a números inteiros estritamente positivos. Depois $a \mid a$ e $a \mid b$ (hipótese). E se $d' \mid a$ e $d' \mid b$, é claro que $d' \mid a$. □

Lema 2.16. *Sejam a, $b \in \mathbb{Z}$. Se $a = b \cdot q + r$, então $d = mdc(a, b)$ se, e somente se, $d = mdc(b, r)$.*

Demonstração. Suponhamos $d = mdc(a, b)$ e provemos que $d = mdc(b, r)$. Primeiro, $d > 0$, por hipótese. Depois, como $d \mid a$ e $d \mid b$, então $d \mid b$ e $d \mid (a - b \cdot q)$. Ou seja, $d \mid b$ e $d \mid r$. Por último, se $d' \mid b$ e $d' \mid r$, então $d' \mid b$ e $d' \mid (b \cdot q + r)$, ou seja, $d' \mid b$ e $d' \mid a$; mas, como $d = mdc(a, b)$, então $d' \mid d$.

Agora, demonstrando a recíproca. Suponhamos que $d = mdc(b, r)$ e provemos que $d = mdc(a, b)$. Primeiro, $d > 0$, por hipótese. Depois $d \mid b$ e $d \mid r$, então $d \mid b$ e $d \mid b \cdot q + r$. Ou seja, $d \mid b$ e $d \mid a$. Por último, se $d' \mid b$ e $d' \mid a$, então $d' \mid b$ e $d' \mid a - b \cdot q$, ou seja, $d' \mid b$ e $d' \mid r$, mas como $d = mdc(b, r)$, então $d' \mid d$. □

O mecanismo para calcular o máximo divisor comum em que encontramos todos os divisores dos números, depois fazemos a interseção desses conjuntos e então identificamos o maior número da interseção é muito trabalhoso, e por vezes impraticável, quando trata-se de números muito grandes. Na sequência, vamos descrever o método de Euclides, ou ainda, o método das divisões sucessivas para encontrar o máximo divisor comum dos números inteiros a e b:

$$\begin{array}{rcll} a & = & b \cdot q_1 + r_1 & (0 \leq r_1 < b) \\ b & = & r_1 \cdot q_2 + r_2 & (r_2 < r_1) \\ r_1 & = & r_2 \cdot q_3 + r_3 & (r_3 < r_2) \\ ..... & & ..... & \end{array}$$

O algoritmo euclidiano consiste em dividir a por b. Se $r_1 = 0$, então $b = mdc(a, b)$, devido ao Lema 2.15, e o processo termina na primeira etapa. Se $r_1 \neq 0$, dividimos b por r_1. Se $r_2 = 0$, então $r_1 = mdc(b, r_1)$, devido ao Lema 2.15; mas, devido ao Lema 2.16, $mdc(b, r_1) = mdc(a, b)$, ou seja, segue que $r_1 = mdc(a, b)$. E assim por diante.

Ocorre que, como $b > r_1 > r_2 > \cdots \geq 0$, então para algum índice n teremos certeza que $r_{n+1} = 0$. De fato, se todos os elementos de $\{r_1, r_2, r_3, ...\}$ fossem não nulos, então esse conjunto, que é limitado inferiormente, não teria mínimo, o que é impossível. Assim, para o índice n referido:

$$\begin{array}{rcl} r_{n-2} & = & r_{n-1} \cdot q_n + r_n \\ r_{n-1} & = & r_n \cdot q_{n+1}. \end{array}$$

Portanto, o último resto diferente de zero desta sequência de divisões é o máximo divisor comum de a e b, em virtude dos lemas demonstrados:

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

Exemplo 2.17. *Usando o algoritmo de Euclides, vamos determinar o máximo divisor comum entre 2021 e 32.*

Pelas divisões sucessivas, temos:

$$\begin{aligned} 2021 &= 32 \cdot 63 + 5 \quad \text{e} \quad 0 \leq 5 < 32 \\ 32 &= 5 \cdot 6 + 2 \quad \text{e} \quad 2 < 5 \\ 5 &= 2 \cdot 2 + 1 \quad \text{e} \quad 1 < 2 \\ 2 &= 1 \cdot 2 + 0. \end{aligned}$$

Portanto, o $mdc(2021, 32) = 1$, pois foi o último resto não nulo encontrado no processo de divisões sucessivas.

As divisões sucessivas também são representadas através da grade abaixo, onde são escritos apenas a e b e os restos das divisões.

2021	32	5	2	1
5	2	1	0	

Além disso, a partir das divisões sucessivas, é possível determinar os inteiros x_0 e y_0 tais que $a \cdot x_0 + b \cdot y_0 = d$ em que $d = mdc(a, b)$:

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 = 5 - (32 - 5 \cdot 6) \cdot 2 = 5 \cdot 13 + 32 \cdot (-2) \\ &= (2021 - 32 \cdot 63) \cdot 13 + 32 \cdot (-2) \\ &= 2021 \cdot 13 + 32 \cdot (-821). \end{aligned}$$

Logo, temos que $mdc(2021, 32) = 1 = 2021 \cdot 13 + 32 \cdot (-821)$.

2.2 Números Primos

Definição 2.18. *Um número inteiro p é chamado número primo se as seguintes condições se verificam:*

(i) $p \neq 0$

(ii) $p \neq \pm 1$

(iii) Os únicos divisores de p são ± 1, $\pm p$.

Se um número inteiro $n \neq \{0, \pm 1\}$ não é primo, então dizemos que n é composto. Nesse caso, n não possui apenas os divisores ± 1 e $\pm n$. Dessa maneira, devem existir números inteiros u e v tais que $1 < u < n$ e $1 < v < n$ e $n = u \cdot v$.

Exemplo 2.19. *O número 2 é primo, pois seus únicos divisores são -2, -1, 1, 2, inclusive ele é o único número primo, que também é um número par. Já o número 15 é composto, pois seus divisores são ± 1, ± 3, ± 5, ± 15.*

Definição 2.20. *Sejam a e b dois inteiros, $a \neq 0$ ou $b \neq 0$. Dizemos que a e b são primos entre si (ou coprimos) quando $mdc(a, b) = 1$.*

Exemplo 2.21. *São inteiros primos entre si: 2 e 3, 9 e 25, -9 e 22, -18 e -55, pois temos*

$$1 = mdc(2, 3) = mdc(9, 25) = mdc(-9, 22) = mdc(-18, -55).$$

Teorema 2.22. *Dois inteiros a e b, $a \neq 0$ ou $b \neq 0$, são primos entre si se, e somente se, existem inteiros x e y tais que $a \cdot x + b \cdot y = 1$.*

Demonstração. (i) Suponhamos que a e b sejam primos entre si. Então $mdc(a, b) = 1$ e, pela Proposição 2.14, existem x e y tais que $a \cdot x + b \cdot y = 1$.

(ii) Agora, suponhamos que existam inteiros x e y tais que $a \cdot x + b \cdot y = 1$ e seja $d = mdc(a, b)$. Assim, $d \mid a$ e $d \mid b$, o que implica $d \mid (a \cdot x + b \cdot y)$ (Proposição 2.3 (e)), ou seja, $d \mid 1$. Sendo $d > 0$, concluímos que $d = 1$ e, portanto, a e b são primos entre si. □

Corolário 2.23. *Se a e b são inteiros não simultaneamente nulos e se $d = mdc(a, b)$, então $mdc(a/d, b/d) = 1$.*

Demonstração. Como $d = mdc(a, b)$, pela Proposição 2.14, existem x_0 e y_0 tais que $a \cdot x_0 + b \cdot y_0 = d$. Daí, dividindo ambos os membros por d, $(a/d) \cdot x_0 + (b/d) \cdot y_0 = 1$. Logo, pelo Teorema 2.22, a/d e b/d são primos entre si. □

Teorema 2.24. *Sejam a, b, $c \in \mathbb{Z}$. Se $a \mid b \cdot c$ e $mdc(a, b) = 1$, então $a \mid c$.*

Demonstração. Como $mdc(a, b) = 1$ pelo Teorema 2.22 existem inteiros x e y tais que $a \cdot x + b \cdot y = 1$. Multiplicando-se os dois lados desta igualdade por c temos: $(a \cdot c) \cdot x + (b \cdot c) \cdot y = c$. Como $a \mid a \cdot c$ e, por hipótese, $a \mid b \cdot c$ então, pela Proposição 2.3(e), $a \mid c$. □

Proposição 2.25. *Sejam a, b, $c \in \mathbb{Z}$. Se $mdc(a, b) = 1$ e a e b dividem c então o produto $a \cdot b$ divide c.*

Demonstração. Por hipótese, a divide c, ou seja,

$$c = a \cdot q \text{ para algum inteiro } q. \tag{2.17}$$

Mas b também divide c. Como $mdc(a, b) = 1$, segue do Teorema 2.24, que b divide q. Assim temos que

$$q = b \cdot t \text{ para algum inteiro } t. \tag{2.18}$$

De (2.17) e (2.18), segue que

$$c = a \cdot q = a \cdot (b \cdot t) = (a \cdot b) \cdot t.$$

Portanto, podemos concluir que $a \cdot b$ divide c. □

Proposição 2.26. *Sejam a, b e c inteiros, então temos que $mdc(a \cdot c, b) = 1$ se, e somente se, $mdc(a, b) = mdc(c, b) = 1$.*

Demonstração. Temos que $mdc(a \cdot c, b) = 1$ implica que existem m, $n \in \mathbb{Z}$ tais que $m \cdot a \cdot c + n \cdot b = 1$, logo $(m \cdot c) \cdot a + n \cdot b = 1$ e $(m \cdot a) \cdot c + n \cdot b = 1$, o que implica que $mdc(a, b) = mdc(c, b) = 1$. Reciprocamente, tomamos $d = mdc(c, b)$, logo, pela definição de máximo divisor comum, $d \mid c$ e $d \mid b$ e, portanto $d \mid a \cdot c$ e $d \mid b$. Precisamos mostrar que d é divisível por todo divisor comum de $a \cdot c$ e b. Seja e um divisor comum de $a \cdot c$ e b. Como $mdc(e, a) \mid a$ e $mdc(e, a) \mid e$ e e divide b, temos que $mdc(e, a) \mid mdc(a, b)$; logo sendo $mdc(a, b) = 1$, temos que $mdc(e, a) = 1$. Como $e \mid a \cdot c$ e $mdc(e, a) = 1$, pelo Teorema 2.24, temos que $e \mid c$. Portanto, $e \mid c$ e $e \mid b$ e, consequentemente, $e \mid d$, e como por hipótese $d = 1$, pois $mdc(c, b) = 1$, $e = 1$. Então concluímos $mdc(a \cdot c, b) = 1$. □

2.3 O Teorema Fundamental da Aritmética

A seguir apresentaremos dois lemas que auxiliam na demonstração de um importante teorema, o Teorema Fundamental da Aritmética. Ele possibilita decompor em números primos qualquer número inteiro maior que um. Também, várias propriedades interessantes dos número inteiros derivam dele. Mas, infelizmente, é um processo lento para números grandes. O processo de escrever números inteiros maiores que um através de números primos é denominada fatoração.

Lema 2.27. *Sejam a, b, $p \in \mathbb{Z}$. Se $p \mid a \cdot b$, p primo, então $p \mid a$ ou $p \mid b$.*

Demonstração. Suponhamos que p não seja um divisor de a. Logo, $-p$ também não é divisor de a. Como os divisores de p são apenas ± 1 e $\pm p$, então os divisores comuns a p e a são apenas ± 1. Daí, $mdc(p, a) = 1$ e, portanto, existem x_0 e $y_0 \in \mathbb{Z}$ tais que $p \cdot x_0 + a \cdot y_0 = 1$. Multiplicando-se ambos os membros dessa igualdade por b, obtém-se:

$$p \cdot (b \cdot x_0) + (a \cdot b) \cdot y_0 = b.$$

Como $p \mid p$ e $p \mid a \cdot b$, então $p \mid [p \cdot (b \cdot x_0) + (a \cdot b) \cdot y_0]$, ou seja, $p \mid b$. Analogamente, se mostra que, se p não divide b, então p divide a. □

Por indução, pode-se demonstrar sem dificuldades maiores que, se p é primo e divide $a_1 \cdot a_2 \ldots a_n$ $(n \geq 1)$, então p divide um dos fatores a_i.

Lema 2.28. *Sejam p, q_1, q_2, ..., q_n, números primos e suponhamos que p divida o produto $q_1 \cdot q_2 \dots q_n$. Então $p = q_j$, para algum $j \in \{1, 2, \dots, n\}$.*

Demonstração. A demonstração será por indução sobre o número n de primos presentes no produto $q_1 \cdot q_2 \dots q_n$. Seja f a função proposicional correspondente a propriedade que desejamos demonstrar.

O primeiro passo de indução é provar para $n = 1$, ou seja, que $f(1)$ é verdadeira. Temos que o número p é divisor de q_1 e é diferente de 1, como p e q_1 são números primos, então $p = q_1$ e, de fato, $f(1)$ é verdadeira.

Vamos supor que $f(r)$ seja verdadeira, onde $r \geq 1$. Ou seja, para $n = r$, é válido que, sendo p um número primo divisor do produto $q_1 \cdot q_2 \dots q_r$, temos $p = q_j$, para algum $j \in \{1, 2, \dots, r\}$.

E então devemos mostrar que para $n = r+1$ a propriedade também é satisfeita, ou seja, que $f(r+1)$ é verdadeira. Para isso, é necessário provar que, sendo p um número primo divisor do produto $q_1 \cdot q_2 \dots q_r \cdot q_{r+1}$, temos $p = q_j$, para algum $j \in \{1, 2, \dots, r, r+1\}$. Separamos o produto $q_1 \cdot q_2 \dots q_r \cdot q_{r+1}$ da seguinte forma:

$$q_1 \cdot q_2 \dots q_r \cdot q_{r+1} = (q_1 \cdot q_2 \dots q_r) \cdot q_{r+1}.$$

Pelo Lema 2.27, temos que p divide $q_1 \cdot q_2 \dots q_r$ ou p divide q_{r+1}. Caso $p \mid q_{r+1}$, então como p e q_{r+1} são números primos, concluímos que $p = q_{r+1}$ e está encerrada a demonstração. Caso $p \mid q_1 \cdot q_2 \dots q_r$, pela hipótese de indução $p = q_j$, para algum $j \in \{1, 2, \dots, r\}$. Logo, $f(r+1)$ é verdadeira.

Portanto, pelo Princípio de Indução, concluímos que $f(n)$ é verdadeira para todo $n \geq 1$. □

Teorema 2.29. *(Teorema Fundamental da Aritmética) Seja $n > 1$ um número inteiro. Então existem números primos p_1, p_2, ..., p_k (não necessariamente distintos) tais que $n = p_1 \cdot p_2 \dots p_k$ e tal fatoração é única, a menos da ordem de seus fatores.*

Demonstração. (Existência)

Vamos demonstrar usando o Princípio de Indução, e f denotará a função proposicional correspondente à propriedade que desejamos demonstrar.

Primeiramente, precisamos mostrar que $f(2)$ é verdadeira. Mas $n = 2$ já um número primo, de modo que a igualdade $n = 2$ coincide com a fatoração do enunciado e, assim, $f(2)$ é verdadeira.

Suponhamos que $f(s)$ seja verdadeira para todo $2 \leq s < r$. Ou seja, é válido que existem números primos p_1, p_2, ..., p_k tais que $s = p_1 \cdot p_2 \dots p_k$ para todo $2 \leq s < r$.

Então mostraremos que a afirmação é válida para r, ou seja, que $f(r)$ é verdadeira. Isto implica em mostrar que existem números primos q_1, q_2, ..., q_l tais que $r = q_1 \cdot q_2 \dots q_l$. Se o número r for um número primo, basta escolhermos $p_1 = r$. Caso contrário, r será um número composto e, como já afirmamos anteriormente, existem inteiros u e v tais que $r = u \cdot v$, com $1 < u < r$ e $1 < v < r$. Pela hipótese de indução, resulta que existem primos w_1, w_2, ..., w_i e t_1, t_2, ..., t_j tais que

$$u = w_1 \cdot w_2 \dots w_i \qquad \text{e} \qquad v = t_1 \cdot t_2 \dots t_j.$$

Assim, $r = w_1 \cdot w_2 \dots w_i \cdot t_1 \cdot t_2 \dots t_j$, ou seja, r também pode ser escrito como um produto de números primos. Logo $f(r)$ é também verdadeira.

Portanto, pelo Princípio de Indução, $f(n)$ é verdadeira para todo $n \geq 2$.

(Unicidade)

Vamos supor que n possui duas decomposições em fatores primos, ou seja,

$$n = p_1 \cdot p_2 \dots p_k = q_1 \cdot q_2 \dots q_l.$$

E, sem perda de generalidade, suponhamos que $l \geq k$. Pela igualdade anterior, temos que p_1 divide $q_1 \cdot q_2 \dots q_l$, e pelo Lema 2.28, concluímos que $p_1 = q_j$, para algum $j \in \{1, 2, \dots, l\}$. Reordenando os índices dos $q_j's$, se necessário, podemos supor que $p_1 = q_1$, obtendo

$$p_1 \cdot p_2 \dots p_k = p_1 \cdot q_2 \dots q_l.$$

Logo, $p_2 \dots p_k = q_2 \dots q_l$. Repetindo esse processo k vezes, teremos que $p_j = q_j$, para todo $j \in \{1, 2, \dots, k\}$. Agora afirmamos que $l = k$, pois caso fosse $l > k$, teríamos

$$p_1 \cdot p_2 \dots p_k = p_1 \cdot p_2 \dots p_k \dots q_{k+1} \dots q_l,$$

o que implicaria $1 = q_{k+1} \dots q_l$, ou seja, para algum $j \in \{k+1, \dots, l\}$, q_j seria um divisor de 1, o que é impossível. Logo, $p_j = q_j$ para todo $j \in \{1, 2, \dots, k\}$ e $l = k$, o que prova que a fatoração de n é única. □

2.3.1 Fatoração-padrão

Já sabemos que todo número inteiro $n > 1$ pode ser escrito como produto de números primos. Para apresentar o método para obter essa decomposição de n em primos são necessárias as proposições a seguir. A primeira proposição diz que entre todos os divisores maiores que 1 de n, o menor deles é um número primo.

Proposição 2.30. *Seja n um número composto. Então o menor divisor de n maior que 1 é um número primo.*

Demonstração. Seja u o menor divisor de n satisfazendo $1 < u < n$, e seja d um divisor (maior que 1) de u. Pela definição de divisibilidade, existem inteiros v e q tais que

$$n = u \cdot v \qquad \text{e} \qquad u = d \cdot q.$$

Disso, $n = d \cdot q \cdot v$, o que significa que d também é um divisor de n. Mas como u é o menor divisor (maior que 1) de n, devemos ter $u \leq d$ e, como d é um divisor de u, devemos ter $d \leq u$. Essas duas desigualdades mostram que $d = u$. Logo, o único divisor de u maior que 1 é o próprio u, o que significa que u é primo. □

Teorema 2.31. *O conjunto $\mathbb{P}$ dos números primos é infinito.*

Demonstração. Vamos supor, por contradição, que $\mathbb{P}$ seja um conjunto finito com n elementos e coloquemos $\mathbb{P} = \{p_1 = 2, p_2 = 3, p_3 = 5, \ldots, p_n\}$ onde os números primos estão organizados em ordem crescente, ou seja, p_n é o maior de todos os números primos. Agora, consideremos o número inteiro

$$u = p_1 \cdot p_2 \cdot p_3 \ldots p_n + 1, \tag{2.19}$$

que não pode ser primo, pois claramente $u > p_n$. Assim pelo Teorema Fundamental da Aritmética, existe algum primo $p_j \in \mathbb{P}$ tal que p_j divide u. Logo, podemos escrever

$$u = p_j \cdot q, \tag{2.20}$$

para algum inteiro q. Pelas igualdades (2.19) e (2.20), vemos que

$$p_j \cdot q = p_1 \cdot p_2 \cdot p_3 \ldots p_n + 1,$$

o que implica que $1 = p_j \cdot (q - p_1 \cdot p_2 \cdot p_3 \ldots p_{j-1} \cdot p_{j+1} \ldots p_n)$. Isso é o mesmo que dizer que o primo p_j é um divisor do número 1. Mas isso é impossível, pois os únicos números que são divisores de 1 são 1 e -1. Essa contradição mostra que $\mathbb{P}$ é um conjunto infinito. □

A próxima proposição reduz o número de tentativas para encontrarmos os divisores primos de n, ou seja, veremos que para encontrar esses divisores de n não precisamos dividi-lo pelos primos de 2 a $n - 1$, basta que façamos isso apenas para os números primos menores ou iguais ao número $\sqrt{n}$.

Proposição 2.32. *Se n é um número composto e p é o menor divisor primo de n, então $p \leq \sqrt{n}$.*

Demonstração. Como p é um divisor de n, existe um inteiro q tal que

$$n = p \cdot q, \tag{2.21}$$

que, por sua vez, também é um divisor de n. Como p é o menor divisor (maior que 1) de n e $q > 1$ (senão teríamos $n = p$), devemos ter

$$p \leq q. \tag{2.22}$$

Mas de (2.21) obtemos $q = \dfrac{n}{p}$, o que junto com (2.22), nos dá $p \leq \dfrac{n}{p}$. Disso segue imediatamente que $p^2 \leq n$ ou, equivalentemente, $p \leq \sqrt{n}$, que é o resultado desejado. □

A Proposição 2.32 tem uma importante aplicação, trata-se de um teste de primalidade. Ela nos diz que, para testarmos se um número n é primo, é suficiente testarmos apenas pelos primos menores ou iguais a $\sqrt{n}$. Portanto, para obter a lista de todos os números primos menores que 60, devemos excluir dentre os números de 2 a 60 aqueles que são múltiplos de 2, 3, 5 e 7, pois estes são primos menores ou iguais a $\sqrt{60} = 7,74\ldots$. Este processo é chamado de *Crivo de Eratóstenes*. Detalhadamente, o processo consiste em fazer uma tabela de todos os números de 2 a 60 e, de maneira sistemática, exlcuir todos os números compostos da tabela. Começando, mantemos o 2 e excluímos todos os múltiplos de 2 da tabela. Feito isso, mantemos o 3 e excluímos todos os múltiplos de 3 da tabela. Agora mantemos o 5 e excluímos todos os múltiplos de 5 da tabela. E por último, mantemos o 7 e excluímos seus múltiplos, pois esses e os múltiplos de 2, 3 e 5 não são números primos.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~

Portanto, os primos entre 2 e 60 são todos aqueles que não foram eliminados pelo processo descrito, isto é,

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,29,\ 31,\ 37,\ 41,\ 43,\ 47,\ 53,\ 59.$$

Neste momento, já estamos aptos a apresentar o algoritmo da decomposição de um número inteiro n em números primos, o que faremos através da decomposição de $n = 60$ em números primos. Já sabemos que não é necessário dividi-lo pelos primos de 2 a 59, mas sim começando do 2 até $\sqrt{60}$.

(a) Sabemos que 60 é um número composto, então temos que o menor divisor (maior que 1) de 60 é o primo $p_1 = 2$. Porém, tratando-se de outro n, se as divisões de n pelos primos de 2 a $n-1$ não forem exatas, concluímos que n é um número primo.

(b) Em seguida, repetimos o passo anterior para o quociente $\frac{60}{2} = 30$, que é um inteiro e composto, ou seja, o menor divisor de $\frac{60}{2} = 30$ é o número primo $p_2 = 2$ e, pela propriedade transitiva, é o segundo divisor primo de 60. Observemos que $p_1 \leq p_2$, no caso analisado $p_1 = p_2$. Se $\frac{n}{p_1} = q_1$ for primo, então encerramos o processo e teremos $n = p_1 \cdot q_1$ e $p_1 \leq q_1$.

(c) Repetimos o processo para o número inteiro e composto $\frac{60}{2\cdot 2} = 15$, e obtemos $p_3 = 3$ como terceiro divisor de 60. Se $\frac{n}{p_1 \cdot p_2} = q_2$ for primo, então teremos $n = p_1 \cdot p_2 \cdot q_2$ e $p_1 \leq p_2 \leq q_2$.

(d) E finalmente, chegamos que $q_3 = \frac{60}{2\cdot 2\cdot 3} = 5$ é um número primo, ou ainda, $\frac{60}{2\cdot 2\cdot 3\cdot 5} = 1$, então temos $60 = 2 \cdot 2 \cdot 3 \cdot 5$. No caso genérico, repita até que

$$\frac{n}{p_1 \cdot p_2 \ldots p_k} = 1 \qquad \text{com} \qquad p_1 \leq p_2 \leq \ldots \leq p_k.$$

O que implica no resultado desejado $n = p_1 \cdot p_2 \ldots p_k$.

É possível observar através da decomposição de $60 = 2^2 \cdot 3 \cdot 5$ em fatores primos, conforme Teorema Fundamental da Aritmética, que o 2 aparece duas vezes, isto é, que acontecerá repetição de alguns primos. Por conseguinte, escrevemos $n = p_1^{a_1} \cdot p_2^{a_2} \ldots p_t^{a_t}$, onde p_i são primos distintos e cada a_i é um inteiro não negativo que indica a quantidade de vezes que o primo p_i aparece na decomposição de n, que chamamos de fatoração-padrão da decomposição de n ou decomposição canônica de n.

Dado um número inteiro que não tenha um fator primo pequeno, a Fatoração-padrão é ineficiente. Conforme exemplifica Coutinho (2005, p. 39), considerando um número primo $n \geq 10^{100}$, temos $\sqrt{n} \geq 10^{50}$, ou seja, será necessário executar pelo menos 10^{50} vezes o algoritmo da fatoração-padrão para determinar que n é primo. Digamos que um computador execute 10^{10} divisões por segundo, ele demoraria 10^{40} segundos para determinar que n é primo, o que corresponde a 10^{31} anos, se comparado com a idade do Universo desde o Big Bang que é estimada em 20 bilhões de anos, ou seja, $2 \cdot 10^{11}$ anos, isso é impossível de ser realizado.

É importante ressaltar que a segurança da criptografia RSA depende da inexistência de um algoritmo de fatoração que tenha um bom funcionamento para todos os números inteiros.

Exemplo 2.33. *Vamos decompor o número inteiro 9828 em números primos. É usual representar a decomposição através da tabela abaixo:*

9828	2
4914	2
2457	3
819	3
273	3
91	7
13	13
1	
	$2^2 \cdot 3^3 \cdot 7 \cdot 13$

Logo, $9828 = 2^2 \cdot 3^3 \cdot 7 \cdot 13$ *é a fatoração-padrão de 9828.*

A seguir uma das aplicações do Teorema Fundamental da Aritmética, trata-se da obtenção de uma fórmula para o número de divisores positivos de um inteiro n. Consideremos $n = 12 = 2^2 \cdot 3^1$, sendo que $D_+(12) = \{1, 2, 3, 4, 6, 12\}$ ($D_+(n)$ denota o conjunto dos divisores positivos de n). Os divisores positivos de 12 podem ser escritos da seguinte maneira:

$$1 = 2^0 \cdot 3^0, \qquad 2 = 2^1 \cdot 3^0, \qquad 3 = 2^0 \cdot 3^1$$
$$4 = 2^2 \cdot 3^0, \qquad 6 = 2^1 \cdot 3^1, \qquad 12 = 2^2 \cdot 3^1.$$

Diante disso, é possível afirmar que os divisores de 12 têm a forma $d = 2^r \cdot 3^s$, onde $r, s \in \mathbb{N}$, $0 \leq r \leq 2$ e $0 \leq s \leq 1$.

Proposição 2.34. *Se* $n = p_1^{a_1} \cdot p_2^{a_2} \dots p_t^{a_t}$ *é a fatoração-padrão de* n*, então a quantidade de divisores positivos de* n *é dada por*

$$\tau(n) = (a_1 + 1) \cdot (a_2 + 1) \dots (a_t + 1).$$

Demonstração. Seja n um inteiro e $n = p_1^{a_1} \cdot p_2^{a_2} \dots p_t^{a_t}$ sua fatoração-padrão, um inteiro d é divisor de n se, e somente se, d divide o produto $p_1^{a_1} \cdot p_2^{a_2} \dots p_t^{a_t}$, o que implica que, para d positivo, a fatoração-padrão de d deve ser $d = p_1^{b_1} \cdot p_2^{b_2} \dots p_t^{b_t}$, onde $b_i \in \mathbb{N}$ e $0 \leq b_i \leq a_i$ para todo $i \in \{1, 2, \dots, t\}$. Assim, a totalidade de divisores positivos é obtida quando cada b_i varia de 0 até a_i, ou seja, existem $a_i + 1$ possibilidades para cada b_i. Então, pelo Princípio Multiplicativo de Contagem, o total de divisores positivos de n é a igual:

$$\tau(n) = (a_1 + 1) \cdot (a_2 + 1) \dots (a_t + 1).$$

□

Exemplo 2.35. *Aplicando a Proposição 2.34, o número de divisores positivos de 12, cuja fatoração-padrão é* $12 = 2^2 \cdot 3^1$*, é igual a* $\tau(12) = (2+1) \cdot (1+1) = 6$*, conferindo com o resultado obtido anteriormente.*

Exemplo 2.36. *Queremos determinar o número de divisores positivos de 176. Primeiramente, obtemos* $176 = 2^4 \cdot 11^1$ *sua fatoração-padrão. Assim, pela Proposição 2.34, temos* $\tau(176) = (4+1) \cdot (1+1) = 10$*, ainda é razoável encontrarmos os divisores para depois contá-los. Entretanto, para o número* $720 = 2^4 \cdot 3^2 \cdot 5^1$*, que possui* $\tau(720) = (4+1) \cdot (2+1) \cdot (1+1) = 30$ *divisores positivos, a tarefa de encontrar os divisores torna-se exaustiva.*

2.3.2 Fatoração pelo método de Fermat

O método de fatoração que apresentaremos a seguir não é amplamente conhecido como o método da fatoração-padrão. Entretanto, segundo Antunes (2002, p. 19), o método é executado extremamente rápido, porque os laços não possuem multiplicações e divisões, o que torna a execução rápida, o inconveniente está no número de execuções. Além disso, ele contém a ideia por trás do método da Peneira Quadrática, que trata-se de um dos mais poderosos algoritmos para fatorar números compostos por números primos grandes.

A eficiência da fatoração pelo método de Fermat depende do inteiro n a ser fatorado, ter um divisor primo que não é muito menor que $\sqrt{n}$. Ainda, de acordo com Antunes (2002, p. 19), ele funciona no sentido contrário ao da fatoração-padrão, pois começa procurando fatores próximos a raiz quadrada de n, e segue procurando fatores decrescentes.

O objetivo do algoritmo é encontrar números inteiros positivos x e y tais que $n = x^2 - y^2 = (x-y) \cdot (x+y)$, onde $x-y$ e $x+y$ são fatores de n.

Para começar o algoritmo, é necessário supor que n é um número ímpar, pois sendo n par então 2 é um de seus fatores. Na sequência, determinamos a parte inteira da raiz quadrada de n.

Observação 2.37. *Se* $r \in \mathbb{R}$*, denotaremos sua parte inteira por* $[r]$*. Por exemplo,* $[\sqrt{125}] = 11$*,* $[\sqrt{\pi}] = 1$ *e* $[\sqrt{49}] = 7$*.*

Caso n seja um quadrado perfeito, ou seja, quando existe algum inteiro r tal que $n = r^2$, então r é fator de n, e ainda $x = r$ e $y = 0$.

Caso contrário, se $y > 0$, então $x = \sqrt{n + y^2} > \sqrt{n}$. Dessa forma, x é incrementado de 1 a 1, até encontrar um valor inteiro para $y = \sqrt{x^2 - n}$, o que implica $n = (x + y) \cdot (x - y)$. Ou até que x seja igual a $\frac{(n+1)}{2}$, e então n é primo.

Não faremos a demonstração, o leitor pode consultar sobre o assunto em Coutinho (2005, p. 41).

Exemplo 2.38. *Vamos fatorar o número inteiro* $n = 32881$ *pelo algoritmo de Fermat. Primeiramente, calculamos* $\sqrt{32881} = 181,3311887\ldots$, *assim* $x = [181,3311887\ldots] = 181$. *Porém,*

$$x^2 = 181^2 = 32761 < 32881,$$

por isso, incrementamos x *de 1 em 1, até que* $\sqrt{x^2 - n}$ *seja inteiro, ou* x *seja igual a* $\frac{(n+1)}{2}$, *que neste caso vale 16441. Isso será resumido através da tabela a seguir:*

x	$y = \sqrt{x^2 - n}$
182	15,58
183	24,65
184	31,22
185	36,66
186	41,41
187	45,69
188	49,62
189	53,29
190	56,73
191	60

Logo, $x = 191$ *e* $y = 60$ *são os valores desejados. E, portanto, os fatores correspondentes são* $x + y = 191 + 60 = 251$ *e* $x - y = 191 - 60 = 131$.

2.3.3 Números de Fermat e Números de Mersenne

Os números da forma $F_n = 2^{2^n} + 1$ são chamados números de Fermat, em homenagem ao matemático francês Pierre de Fermat.

Proposição 2.39. *Se* $2^m + 1$ *é um número primo, então existe* $n \in \mathbb{N}$ *tal que* $m = 2^n$.

Demonstração. Se m não fosse uma potência de 2, m deveria possuir um divisor q ímpar, ou seja, $m = q \cdot s$ com $s \in \mathbb{Z}$. Portanto, teríamos

$$2^m + 1 = (2^s)^q + 1 = (2^s + 1) \cdot (2^{s\cdot(q-1)} - 2^{s\cdot(q-2)} + 2^{s\cdot(q-3)} - \ldots + 1),$$

o que mostra que $2^s + 1$ seria um divisor não trivial de $2^m + 1$, contradizendo a hipótese de $2^m + 1$ ser primo. □

De fato, os números da forma $F_n = 2^{2^n} + 1$ para $n = 0, 1, 2, 3,$ e, 4 são primos. Os números são $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$. Fermat conjecturou que todos os números desta forma são primos. Entretanto, em 1732, Leonhard Euler mostrou que para $n = 5$, $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 641 \cdot 6700417$, ou seja, é um número composto.

Os números da forma $M_n = 2^n - 1$, onde n é um número primo, são chamados de números de Mersenne, em homenagem ao matemático Marin Mersenne (1588-1648).

Proposição 2.40. *Se $n > 1$ e $a^n - 1$ é um número primo, então $a = 2$ e n é também primo.*

Demonstração. Para demonstrar usaremos que a soma dos m primeiros termos da Progressão Geométrica (PG) $(1, x, x^2, x^3, \ldots, x^{m-1})$ é dada por

$$S_m = 1 + x + x^2 + x^3 + \ldots + x^{m-1} = \frac{x^m - 1}{x - 1}. \tag{2.23}$$

Em (2.23), se x é um inteiro, então $x - 1$ é um divisor de $x^m - 1$ para qualquer inteiro positivo m. Isso justifica o fato de ser $a = 2$, pois, do contrário, teríamos $a - 1 \neq 1$ e, então, fazendo a substituição de x por a e de m por n na igualdade (2.23), veríamos que $a^n - 1$ teria um divisor não trivial, a saber, $a - 1$. Logo, $a^n - 1$ não poderia ser primo, contradizendo a hipótese. Ainda precisamos provar que n deve ser primo. Supondo que n não seja primo, haveria u e v tais que $n = u \cdot v$. Então, substituindo x por a^v e m por u na igualdade (2.23), teríamos que $a^v - 1$ seria um divisor não trivial de $a^{u \cdot v} - 1 = a^n - 1$, contradizendo novamente a hipótese de ser $a^n - 1$ um número primo. □

De fato, os números da forma $M_n = 2^n - 1$ para $n = 2, 3, 5,$ e, 7 são primos. Os números são $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$. Mas, para $n = 11$, $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$ é composto.

2.4 Mínimo Múltiplo Comum

Seja $a \in \mathbb{Z}^*$, o conjunto dos números inteiros múltiplos de a será denotado por $M(a)$. Considerando os números 6 e 8, o conjunto dos números múltiplos de 6 é $M(6) = \{0, \pm 6, \pm 12, \pm 18, \pm 24, \pm 30, \pm 36, \pm 42, \pm 48, \pm 54, \pm 60, \ldots\}$ e o conjunto dos múltiplos de 8 é $M(8) = \{0, \pm 8, \pm 16, \pm 24, \pm 32, \pm 40, \pm 48, \pm 56, \pm 64, \pm 72, \pm 80, \ldots\}$. Os números 6 e 8 possuem números múltiplos positivos comuns, por exemplo, 24 e 48, mas o menor deles é o 24. Portanto, o mínimo múltiplo comum entre 6 e 8 é 24.

Definição 2.41. *Sejam a e b dois inteiros, $a \neq 0$ e $b \neq 0$. O mínimo múltiplo comum entre a e b é o número inteiro positivo m que satisfaz as seguintes condições:*

(i) $a \mid m$ *e* $b \mid m$;

(ii) Se existe $m_1 \in \mathbb{Z}$ *tal que* $a \mid m_1$ *e* $b \mid m_1$, *então* $m \mid m_1$.

O mínimo múltiplo comum entre os números inteiros a e b será denotado por $mmc(a, b)$.

O próximo teorema apresenta uma maneira de obter o $mmc(a, b)$ através de uma relação entre o $mdc(a, b)$ e o $mmc(a, b)$.

Teorema 2.42. *Para quaisquer inteiros a e b, $a \neq 0$ e $b \neq 0$, é válida a seguinte relação:*

$$mdc(a, b) \cdot mmc(a, b) = |a \cdot b|.$$

Demonstração. Pela definição de mínimo múltiplo comum, concluímos que $mmc(a, b) = mmc(|a|, |b|)$. Desse modo, sem perda de generalidade, consideremos a e b números inteiros positivos. Então, vamos demonstrar que

$$mdc(a, b) \cdot mmc(a, b) = a \cdot b.$$

Sejam $d = mdc(a, b)$ e $m = mmc(a, b)$. Pela definição de máximo divisor comum, $\frac{a}{d}$ e $\frac{b}{d}$ são números inteiros; e pela definição de mínimo múltiplo comum, $\frac{m}{a}$ e $\frac{m}{b}$ são números inteiros. Note também que $a \mid a \cdot \frac{b}{d}$ e $b \mid b \cdot \frac{a}{d}$. Assim, $\frac{a \cdot b}{d}$ é um múltiplo comum de a e b. Logo, existe $q \in \mathbb{Z}$ tal que $\frac{a \cdot b}{d} = m \cdot q$, já que $m = mmc(a, b)$. Isso implica que

$$\frac{a}{d} = \frac{m}{b} \cdot q \qquad \text{e} \qquad \frac{b}{d} = \frac{m}{a} \cdot q.$$

Ou seja, q é divisor comum de $\frac{a}{d}$ e $\frac{b}{d}$. Mas, observe que $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si, pois pela Proposição 2.14, $a \cdot x + b \cdot y = d$, como $d \neq 0$, é possível escrever $\frac{a}{d} \cdot x + \frac{b}{d} \cdot y = 1$, ou seja, pelo Teorema 2.22, $mdc(\frac{a}{d}, \frac{b}{d}) = 1$. Logo, $q = 1$. Portanto, $\frac{a \cdot b}{d} = m$, ou seja, $a \cdot b = m \cdot d$. □

Exemplo 2.43. *Determinemos o $mmc(20, 24)$. Sendo $mdc(20, 24) = 4$, utilizando o Teorema 2.42, temos*

$$mdc(20, 24) \cdot mmc(20, 24) = |20 \cdot 24|.$$

Assim, $mmc(20, 24) = \frac{480}{4} = 120$.

O Teorema Fundamental da Aritmética possui outra aplicação importante que é o cálculo do máximo divisor comum e do mínimo múltiplo comum de dois números dados a partir de suas decomposições em fatores primos.

Proposição 2.44. *Sejam a e b inteiros positivos e sejam p_1, p_2, ..., p_t os primos que dividem a ou b:*

$$a = p_1^{a_1} \cdot p_2^{a_2} \dots p_t^{a_t} \qquad e \qquad b = p_1^{b_1} \cdot p_2^{b_2} \dots p_t^{b_t}$$

onde os $a_i's$ e os $b_i's$ são inteiros não negativos. Então

$$mdc(a,b) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_t^{\alpha_t} \qquad e \qquad mmc(a,b) = p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_t^{\beta_t},$$

onde $\alpha_t = min\{a_t, b_t\}$ e $\beta_t = max\{a_t, b_t\}$.

Demonstração. Vamos iniciar mostrando o *mdc*. É fácil perceber que o número $d = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_t^{\alpha_t}$ é um divisor de a e b. Se $n = p_1^{d_1} \cdot p_2^{d_2} \dots p_t^{d_t}$ é outro divisor de a e b, então $d_i \leq a_i$ e $d_i \leq b_i$, de modo que $d_i \leq \alpha_i$. Assim, n é divisor de d, ou seja, d é o maior divisor comum de a e b. Agora, para o *mmc* temos que o número $m = p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_t^{\beta_t}$ é um múltiplo de a e b. Além disso, se o número $n = p_1^{m_1} \cdot p_2^{m_2} \dots p_t^{m_t}$ for um múltiplo comum de a e b, então $a_i \leq m_i$ e $b_i \leq m_i$, de modo que $\beta_i \leq m_i$. Assim, n é múltiplo de m, ou seja, m é o menor múltiplo comum de a e b. □

Observação 2.45. *A Proposição 2.44 diz que o mdc entre dois números a e b é o produto das menores potências dos primos que dividem ambos os números. Enquanto o mmc é produto das maiores potências dos primos que dividem pelo menos um dos números a e b.*

Exemplo 2.46. *Vamos exemplificar calculando o mdc e o mmc entre os números 120 e 140. Sendo assim, temos que $140 = 2^2 \cdot 3^0 \cdot 5^1 \cdot 7^1$ e $120 = 2^3 \cdot 3^1 \cdot 5^1 \cdot 7^0$ são as fatorações de 140 e 120. E pela Proposição 2.44, $mdc(120, 140) = 2^2 \cdot 3^0 \cdot 5^1 \cdot 7^0 = 20$, e o $mmc(120, 140) = 2^3 \cdot 3^1 \cdot 5^1 \cdot 7^1 = 840$.*

Assim como a decomposição de um número em fatores primos é ilustrada por uma tabela, o *mdc* e o *mmc* também podem ser ilustrados através de uma tabela:

140	120	2
70	60	2
35	30	2
35	15	3
35	5	5
7	1	7
1	1	
		$mdc(120, 140) = 2^2 \cdot 5^1 = 20$ e
		$mmc(120, 140) = 2^3 \cdot 3^1 \cdot 5^1 \cdot 7^1 = 840$

onde o *mdc* é o produto dos primos da terceira coluna da tabela que dividem simultaneamente 120 e 140, e o *mmc* é o produto de todos os primos da terceira coluna.

2.5 Equações Diofantinas

As Equações Diofantinas são equações polinomiais com coeficientes inteiros e cujas soluções serão inteiros também, trata-se de uma aplicação do Máximo Divisor Comum. O nome dessas equações é uma homenagem ao matemático grego Diofanto de Alexandria, que viveu por volta do século III d.C.

Definição 2.47. *Uma equação diofantina linear de duas incógnitas x e y é uma equação do tipo $a \cdot x + b \cdot y = c$ com a, b e c inteiros. Dizemos que a equação tem solução em $\mathbb{Z}$ se existirem inteiros x_0 e y_0 tais que $a \cdot x_0 + b \cdot y_0 = c$, e o par ordenado (x_0, y_0) é então chamado de solução da equação.*

Teorema 2.48. *Sejam a e b inteiros e $d = mdc(a, b)$. Se $d \nmid c$ então a equação $a \cdot x + b \cdot y = c$ não possui solução inteira. Se $d \mid c$ ela possui infinitas soluções e se $x = x_0$ e $y = y_0$ é uma solução particular, então todas as soluções são dadas por*

$$x = x_0 + \left(\frac{b}{d}\right) \cdot k$$

$$y = y_0 - \left(\frac{a}{d}\right) \cdot k,$$

onde k é um inteiro.

Demonstração. Se $d \nmid c$, então a equação $a \cdot x + b \cdot y = c$ não possui solução pois, como $d \mid a$ e $d \mid b$, d deveria dividir c, o qual é uma combinação linear de a e b. Suponhamos, pois que $d \mid c$. Pela Proposição 2.14, existem inteiros n_0 e m_0 tais que

$$a \cdot n_0 + b \cdot m_0 = d \tag{2.24}$$

Como $d \mid c$, existe um inteiro k tal que $c = k \cdot d$. Se multiplicarmos ambos os membros da equação (2.24) por k, teremos $a \cdot (n_0 \cdot k) + b \cdot (m_0 \cdot k) = k \cdot d = c$. Isto nos diz que o par (x_0, y_0) com $x_0 = n_0 \cdot k$ e $y_0 = m_0 \cdot k$ é uma solução de $a \cdot x + b \cdot y = d$. É fácil a verificação de que os pares da forma

$$x = x_0 + \left(\frac{b}{d}\right) \cdot k$$

$$y = y_0 - \left(\frac{a}{d}\right) \cdot k$$

são soluções, uma vez que

$$\begin{aligned} a \cdot x + b \cdot y &= a \cdot \left(x_0 + \left(\frac{b}{d}\right) \cdot k\right) + b \cdot \left(y_0 - \left(\frac{a}{d}\right) \cdot k\right) \\ &= a \cdot x_0 + \frac{a \cdot b}{d} \cdot k + b \cdot y_0 - \frac{a \cdot b}{d} \cdot k \\ &= a \cdot x_0 + b \cdot y_0 = c. \end{aligned}$$

O que acabamos de mostrar é que, conhecida uma solução particular (x_0, y_0) podemos, a partir dela, gerar infinitas soluções. Agora, precisamos mostrar que toda solução da equação $a \cdot x + b \cdot y = c$ é da forma $x = x_0 + \left(\frac{b}{d}\right) \cdot k, \quad y = y_0 - \left(\frac{a}{d}\right) \cdot k$. Vamos supor que (x, y) seja uma solução, isto é, $a \cdot x + b \cdot y = c$. Mas, como $a \cdot x_0 + b \cdot y_0 = c$, obtemos subtraindo membro a membro, que

$$a \cdot x + b \cdot y - a \cdot x_0 - b \cdot y_0 = a \cdot (x - x_0) + b \cdot (y - y_0) = 0,$$

o que implica $a \cdot (x - x_0) = b \cdot (y_0 - y)$. Como $d = mdc(a, b)$, temos pelo Corolário 2.23,

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

Portanto, dividindo-se os dois membros da última igualdade por d, teremos

$$\frac{a}{d} \cdot (x - x_0) = \frac{b}{d} \cdot (y - y_0). \tag{2.25}$$

Logo, pelo Teorema 2.24, $\left(\frac{b}{d}\right) \mid (x - x_0)$ e portanto existe um inteiro k satisfazendo $x - x_0 = k \cdot \left(\frac{b}{d}\right)$, ou seja, $x = x_0 + \left(\frac{b}{d}\right) \cdot k$. Substituindo-se este valor de x na equação (2.25) temos $y = y_0 - \left(\frac{a}{d}\right) \cdot k$, o que conclui a demonstração. □

Exemplo 2.49. *Consideremos o problema de encontrar todas as soluções inteiras da equação* $43 \cdot x + 5 \cdot y = 250$. *Como* $mdc(43, 5) = 1$, *que obviamente divide 250, a equação tem solução. É importante lembrar que, se* (x_0, y_0) *é uma solução de* $43 \cdot x + 5 \cdot y = 1$, *então* $(250 \cdot x_0, 250 \cdot y_0)$ *é solução da equação* $43 \cdot x + 5 \cdot y = 250$. *Usaremos o Algoritmo de Euclides para achar uma solução de* $43 \cdot x + 5 \cdot y = 1$.

43	5	3	2	1
3	2	1	0	

Disso, segue que:

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 = 3 - (5 - 3 \cdot 1) \cdot 1 = 3 \cdot 2 + 5 \cdot (-1) \\ &= (43 - 5 \cdot 8) \cdot 2 + 5 \cdot (-1) \\ &= 43 \cdot 2 + 5 \cdot (-17). \end{aligned}$$

Portanto, uma solução de $43 \cdot x + 5 \cdot y = 1$ *é* $(2, -17)$. *Logo, uma solução de* $43 \cdot x + 5 \cdot y = 250$ *é* $(500, -4250)$. *De onde a solução geral da equação pode ser expressa por* $(500 + 5 \cdot k, -4250 - 43 \cdot k)$, $k \in \mathbb{Z}$.

2.6 Aritmética modular

O conceito de congruência foi introduzido por Karl Friedrich Gauss (1777) em sua obra *Disquisitiones arithmeticae* (1801), e foi de extrema importância para o

desenvolvimento da Teoria dos Números. Esse conceito é percebido no cotidiano através de situações cíclicas, por exemplo, as horas do dia que repetem a cada 24 horas, os dias de semana são os mesmos a cada sete dias.

Definição 2.50. *Sejam a e b inteiros quaisquer e m um inteiro maior que 1. Dizemos que a é congruente a b módulo m se $m \mid (a - b)$.*

Denotamos isto por $a \equiv b(\text{mod } m)$. Se $m \nmid (a-b)$ dizemos que a é incongruente a b módulo m e denotamos $a \not\equiv b(\text{mod } m)$.

Uma interpretação, não formal, da definição acima, nos diz que, pulando de m em m, todos os números inteiros são equivalentes. Ou ainda, dois inteiros cuja diferença é um múltiplo de m são equivalentes.

Exemplo 2.51. $61 \equiv 43(mod\ 9)$ *pois* $9 \mid (61 - 43)$. *E* $18 \not\equiv 4(mod\ 3)$, *pois 3 não divide* $18 - 4 = 14$.

Proposição 2.52. *Se a, b e m são inteiros, com $m > 1$, temos que $a \equiv b(mod\ m)$ se, e somente se, existir um inteiro k tal que $a = b + k \cdot m$.*

Demonstração. Se $a \equiv b(\text{mod } m)$, então $m \mid (a - b)$ o que implica na existência de um inteiro k tal que $a - b = k \cdot m$, ou seja, $a = b + k \cdot m$. A recíproca é trivial pois da existência de k satisfazendo $a = b + k \cdot m$, temos $k \cdot m = a - b$, ou seja, $m \mid (a - b)$, isto é, $a \equiv b(\text{mod } m)$. □

Ainda sobre o Algoritmo da Divisão, Teorema 2.8, temos o resultado abaixo que é semelhante a proposição demonstrada acima, entretanto nesse caso denotamos o inteiro b por r, evidenciando que trata-se do resto da divisão euclidiana de a por m.

Proposição 2.53. *Sejam a e m inteiros, com $m > 1$, e r um inteiro não negativo. Se r é o resto da divisão euclidiana de a por m, então $a \equiv r(mod\ m)$.*

Demonstração. Pelo Algoritmo da Divisão, existe um inteiro q tal que $a = m \cdot q + r$. Logo, $a - r = m \cdot q$, o que significa que $m \mid a - r$. Portanto, pela Definição 2.50, $a \equiv r(\text{mod } m)$. □

Proposição 2.54. *Se a, b, c e m são inteiros, $m > 1$, as seguintes sentenças são verdadeiras:*

(1) $a \equiv a(mod\ m)$;

(2) Se $a \equiv b(mod\ m)$, então $b \equiv a(mod\ m)$;

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

Demonstração. (1) Como $m \mid 0$, então $m \mid (a-a)$, o que implica $a \equiv a (\text{mod } m)$.

(2) Se $a \equiv b (\text{mod } m)$, então $a = b + k_1 \cdot m$ para algum inteiro k_1. Logo $b = a - k_1 \cdot m$, o que implica pela Proposição 2.52, $b \equiv a (\text{mod } m)$.

(3) Se $a \equiv b (\text{mod } m)$ e $b \equiv c (\text{mod } m)$, então existem k_1 e k_2 tais que $a - b = k_1 \cdot m$ e $b - c = k_2 \cdot m$. Somando-se, membro a membro, estas últimas equações, obtemos $a - c = (k_1 + k_2) \cdot m$, o que implica $a \equiv c (\text{mod } m)$. □

Observação 2.55. *A proposição acima mostra que a relação de congruência, definida no conjuntos dos números inteiros, é uma relação de equivalência, pois acabamos de provar que ela cumpre as propriedades* (1) *reflexiva,* (2) *simétrica e* (3) *transitiva. Para mais informações sobre relação de equivalência, o leitor pode consultar Silva (2018, p. 46).*

Proposição 2.56. *Seja m um número inteiro tal que $m > 1$.*

(a) Se a e b são inteiros tais que $a \equiv b (mod\ m)$, então $a - b \equiv 0 (mod\ m)$.

(b) Se a, b, c e d são inteiros tais que $a \equiv b (mod\ m)$ e $c \equiv d (mod\ m)$, então $a + c \equiv b + d (mod\ m)$.

(c) Se a, b, c e d são inteiros tais que $a \equiv b (mod\ m)$ e $c \equiv d (mod\ m)$, então $a - c \equiv b - d (mod\ m)$.

(d) Se a, b, c e d são inteiros tais que $a \equiv b (mod\ m)$ e $c \equiv d (mod\ m)$, então $a \cdot c \equiv b \cdot d (mod\ m)$.

(e) Se a e b são inteiros tais que $a \equiv b (mod\ m)$, então $a \cdot x \equiv b \cdot x (mod\ m)$, para todo inteiro x.

(f) Seja d um inteiro tal que $mdc(d, m) = 1$. Se a e b são inteiros tais que $a \cdot d \equiv b \cdot d (mod\ m)$, então $a \equiv b (mod\ m)$.

(g) Se a, b e d são inteiros tais que $a \cdot d \equiv b \cdot d (mod\ m \cdot d)$, então $a \equiv b (mod\ m)$.

(h) Se a e b são inteiros tais que $a \equiv b (mod\, m)$, então $a^x \equiv b^x (mod\, m)$ para todo natural x.

Demonstração. (a) Por hipótese temos que $m \mid a - b$ e precisamos verificar que m divide $(a - b) - 0$. Como $(a - b) - 0 = a - b$, temos o desejado.

(b) Por hipótese, temos que m divide $a - b$ e m divide $c - d$. Aplicando o item (e) da Proposição 2.3, com $x = y = 1$, concluímos que m divide $(a-b)+(c-d)$. Reagrupando as parcelas da última soma, obtemos que m divide $(a+c)-(b+d)$, logo $a+c \equiv b+d (\text{mod } m)$.

(c) Por hipótese, temos que existem inteiros k_1 e k_2 tais que $a-b = k_1 \cdot m$ e $c-d = k_2 \cdot m$ obtendo $(a-b)-(c-d) = (a-c)-(b-d) = (k_1-k_2)\cdot m$, o que implica em $a-c \equiv b-d (\text{mod } m)$.

(d) Das hipóteses, existem inteiros k_1 e k_2 tais que

$$a - b = m \cdot k_1 \tag{2.26}$$

e

$$c - d = m \cdot k_2. \tag{2.27}$$

Multiplicando-se os dois lados da igualdade (2.26) por c e os dois lados da igualdade (2.27) por b, obtemos

$$a \cdot c - b \cdot c = m \cdot k_1 \cdot c \tag{2.28}$$

e

$$b \cdot c - b \cdot d = m \cdot k_2 \cdot b. \tag{2.29}$$

Adicionando-se (2.28) e (2.29), obtemos

$$(a \cdot c - b \cdot c) + (b \cdot c - b \cdot d) = m \cdot k_1 \cdot c + m \cdot k_2 \cdot b,$$

o que nos dá

$$a \cdot c - b \cdot d = m \cdot (k_1 \cdot c + k_2 \cdot b).$$

Como k_1, b, k_2 e c são números inteiros, o número $k_3 = k_1 \cdot c + k_2 \cdot b$ é inteiro, de modo que m divide $a \cdot c - b \cdot d$, que é equivalente a afirmar que $a \cdot c \equiv b \cdot d (\text{mod } m)$.

(e) De $a \equiv b (\text{mod } m)$, existe um inteiro k_1 tal que $a - b = m \cdot k_1$. Multiplicando-se os dois lados dessa igualdade por um inteiro qualquer x e aplicando a propriedade distributiva da multiplicação em relação à adição, temos $a \cdot x - b \cdot x = m \cdot k_1 \cdot x$. Logo, m divide $a \cdot x - b \cdot x$, ou seja, $a \cdot x \equiv b \cdot x (\text{mod } m)$.

(f) Como $mdc(d, m) = 1$, d e m são primos entre si. Por outro lado, como $a \cdot d \equiv b \cdot d (\text{mod } m)$, temos que m divide $a \cdot d - b \cdot d = d \cdot (a - b)$. Aplicando o Teorema 2.24, vemos que m divide $a - b$, o que é equivalente a $a \equiv b (\text{mod } m)$.

(g) A hipótese implica que existe um inteiro k tal que $a \cdot d - b \cdot d = m \cdot d \cdot k$. Aplicando a Lei do Cancelamento a essa igualdade, temos $a - b = m \cdot k$. Portanto, $a \equiv b (\text{mod } m)$.

(h) Vamos provar usando Indução Finita. Para $x = 0$, resulta em $1 \equiv 1 (\text{mod } m)$, como m divide $0 = 1 - 1$, temos que $a^0 \equiv b^0 (\text{mod } m)$ é verdade. Vamos supor que $a^x \equiv b^x (\text{mod } m)$ seja verdade para um dado x natural. E vamos verificar se é válido para $a^{x+1} \equiv b^{x+1} (\text{mod } m)$, ou seja, queremos provar que m divide $a^{x+1} - b^{x+1}$. Temos que $a^{x+1} - b^{x+1} = a \cdot a^x - b \cdot a^x + b \cdot a^x - b \cdot b^x = (a-b) \cdot a^x + b \cdot (a^x - b^x)$. Pela hipótese inicial m divide $a - b$ e, pela hipótese de indução, m divide $a^x - b^x$, sendo assim, pelo item

(e) da Proposição 2.3, temos que m divide $(a-b)\cdot a^x + b\cdot(a^x - b^x)$, ou seja, m divide $a^{x+1} - b^{x+1}$. Logo, temos que $a^{x+1} \equiv b^{x+1}(\text{mod } m)$ é verdade. Portanto, pelo Princípio de Indução Finita, a propriedade é válida para todo n natural. □

Observação 2.57. *Casos particulares dos itens (b) e (c) da proposição acima surgem quando utilizamos a propriedade reflexiva da relação de congruência. Ou seja, $c \equiv c(mod\ m)$ para qualquer $c \in \mathbb{Z}$, então $a \equiv b(mod\ m)$, implica $a + c \equiv b + c(mod\ m)$, $a - c \equiv b - c(mod\ m)$ e $a \cdot c \equiv b \cdot c(mod\ m)$.*

Observação 2.58. *A Lei do cancelamento com relação à adição vale para as congruências. Ou seja, dados a, b, c, $m \in \mathbb{Z}$, com $m > 1$, tem-se que $a + c \equiv b + c(mod\ m)$ se, e somente se, $a \equiv b(mod\ m)$. Para demonstrar isso, usamos a própria definição de congruência e a propriedade reflexiva, conforme citado na observação acima. Os itens (f) e (g), cada um a seu modo, nos dizem que a Lei do Cancelamento com relação à multiplicação vale para as congruências. Entretanto, conforme exemplo abaixo, isso nem sempre é possível.*

Exemplo 2.59. *Como $6 \cdot 9 - 6 \cdot 5 = 24$ e $8 \mid 24$, temos que $6 \cdot 9 \equiv 6 \cdot 5(mod\ 8)$, e, no entanto, $9 \not\equiv 5(mod\ 8)$.*

Teorema 2.60. *Se a, b, c e m são inteiros e $a \cdot c \equiv b \cdot c(mod\ m)$, então $a \equiv b(mod\ \frac{m}{d})$ onde $d = mdc(c, m)$.*

Demonstração. Por definição, de $a\cdot c \equiv b\cdot c(\text{mod } m)$, temos que $a\cdot c - b\cdot c = c\cdot(a-b) = k\cdot m$. Dividindo os dois membros da equação por d, teremos $(\frac{c}{d})\cdot(a-b) = k\cdot(\frac{m}{d})$. Logo, $(\frac{m}{d}) \mid (\frac{c}{d})\cdot(a-b)$ e, como $mdc(\frac{m}{d}, \frac{c}{d}) = 1$, pelo Teorema 2.24, $(\frac{m}{d}) \mid (a-b)$ o que implica $a \equiv b(\text{mod } \frac{m}{d})$. □

Definição 2.61. *Sejam a, r e m números inteiros, com $m > 1$. Dizemos que r é um resíduo de a módulo m se $a \equiv r(mod\ m)$.*

Definição 2.62. *Seja $m \in \mathbb{Z}$ tal que $m > 1$. Dizemos que o conjunto de números inteiros $\{r_1, r_2, \ldots, r_m\}$ é um sistema completo de resíduos módulo m se*

(1) $r_i \not\equiv r_j(mod\ m)$ para $i \neq j$;

(2) para todo inteiro n existe um r_i tal que $n \equiv r_i(mod\ m)$.

Exemplo 2.63. *$\{0, 1, 2, \ldots, m-1\}$ é um sistema completo de resíduos módulo m.*

Exemplo 2.64. *Os conjuntos $\{0, 1, 2, 3, 4\}$ e $\{5, 16, 17, 28, 29\}$ são sistemas completos de resíduos módulo 5.*

Proposição 2.65. *Se k inteiros $r_1, r_2, \ldots, r_k$ formam um sistema completo de resíduos módulo m então $k = m$.*

Demonstração. Primeiramente demonstramos que os inteiros $t_0, t_1, \ldots, t_{m-1}$, como $t_i = i$ formam, de fato, um sistema completo de resíduos módulo m. Pelo Teorema 2.8 sabemos que, para cada n, existe um único par de inteiros q e s tal que $n = m \cdot q + s$, $0 \leq s < m$. Logo $n \equiv s (\text{mod } m)$, sendo s um dos t_i. Como $|t_i - t_j| \leq m-1$, temos que $t_i \not\equiv t_j (\text{mod } m)$ para $i \neq j$. Portanto, o conjunto $t_0, t_1, \ldots, t_{m-1}$ é um sistema completo de resíduos módulo m. Disto concluímos que cada r_i é congruente a exatamente um dos t_i, o que garante que $k \leq m$. Como o conjunto $\{r_1, r_2, \ldots, r_k\}$ forma, por hipótese, um sistema completo de resíduos módulo m, cada t_i é congruente a exatamente um dos r_i e portanto $m \leq k$. Desta forma $k = m$. □

Proposição 2.66. *Seja m um inteiro maior que 1. Se $\{r_1, r_2, \ldots, r_m\}$ é um sistema completo de resíduos módulo m, a e b são inteiros tais que $mdc(a, m) = 1$, então $\{a \cdot r_1 + b, a \cdot r_2 + b, \ldots, a \cdot r_m + b\}$ é também um sistema completo de resíduos módulo m.*

Demonstração. Considerando o resultado da proposição anterior, será suficiente mostrar que quaisquer dois inteiros do conjunto $\{a \cdot r_1 + b, a \cdot r_2 + b, \ldots, a \cdot r_m + b\}$ são incongruentes módulo m. Para isto vamos supor que $a \cdot r_i + b \equiv a \cdot r_j + b (\text{mod } m)$ para $i \neq j$. Usando a Lei do Cancelamento, temos $a \cdot r_i \equiv a \cdot r_j (\text{mod } m)$ e, como $mdc(a, m) = 1$, pelo item (f) da Proposição 2.56, temos $r_i \equiv r_j (\text{mod } m)$, o que contradiz a hipótese de o conjunto $\{r_1, r_2, \ldots, r_m\}$ ser um sistema completo de resíduos módulo m. □

Resumindo, todo conjunto de números inteiros cujos restos pela divisão por m são números $0, 1, \ldots, m-1$, sem repetições e em qualquer ordem, é um sistema completo de resíduos módulo m.

O conjunto quociente de $\mathbb{Z}$ pela relação de congruência módulo m, também chamado conjunto dos inteiros módulo m, é denotado $\mathbb{Z}_m$. Ele é formado por subconjuntos de $\mathbb{Z}$, que são classes de equivalência da congruência módulo m. Seja $a \in \mathbb{Z}$, a classe de equivalência de a é formada pelos $x \in \mathbb{Z}$ que satisfazem $x - a$ é múltiplo de m, isto é $x - a = k \cdot m$, para algum $k \in \mathbb{Z}$. Pela Proposição 2.52, podemos descrever a classe de a na forma:

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

Em particular, $\overline{0}$ é o conjunto dos múltiplos de m.

E ainda pela Proposição 2.53, se $x \in \mathbb{Z}$, então podemos dividi-lo por m, obtendo q e r inteiros tais que

$$x = m \cdot q + r \quad \text{e} \quad 0 \leq r \leq m - 1$$

Logo $x - r = m \cdot q$ é um múltiplo de m. Portanto, $x \equiv r (\text{mod } m)$. Ou seja, um número inteiro qualquer é congruente módulo m a um inteiro que está entre 0

e $m-1$. Nesse caso, concluímos que o conjunto quociente $\mathbb{Z}_m$ é formado pelas classes de equivalência $\overline{0},\ \overline{1}, \ldots,\ \overline{m-1}$. Além disso, duas destas classes não podem ser iguais, a única maneira de dois números entre 0 e $m-1$ serem congruentes módulo m é se forem iguais.

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

Quando uma classe de $\mathbb{Z}_m$ estiver representada na forma $\overline{a}$ com $0 \leq a \leq m-1$, diremos que está na forma reduzida.

Exemplo 2.67. *Consideremos o caso em que $m = 5$. Vamos descrever as classes de equivalência módulo 5 dos números 0 a 4.*

$$\overline{0} = \{x \in \mathbb{Z} |\ x \equiv 0 (mod\ 5)\} = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$$

$$\overline{1} = \{x \in \mathbb{Z} |\ x \equiv 1 (mod\ 5)\} = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\}$$

$$\overline{2} = \{x \in \mathbb{Z} |\ x \equiv 2 (mod\ 5)\} = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}$$

$$\overline{3} = \{x \in \mathbb{Z} |\ x \equiv 3 (mod\ 5)\} = \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\}$$

$$\overline{4} = \{x \in \mathbb{Z} |\ x \equiv 4 (mod\ 5)\} = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}.$$

E também, o conjunto quociente de $\mathbb{Z}$ pela relação de congruência módulo 5 é

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

Exemplo 2.68. *Qual é a classe de equivalência módulo 5 dos números -1, -36 e 2393? Fazendo a divisão euclidiana de -1, -36 e 2393 por 5, temos $-36 = (-8) \cdot 5 + 4$, $-1 = (-1) \cdot 5 + 4$ e $2393 = 478 \cdot 5 + 3$. Usando a Proposição 2.53, o resto da divisão euclidiana de -1 e -36 por 5 é 4, e de 2393 por 5 é 3. Logo, $\overline{-1} = \overline{-36} = \overline{4}$ e $\overline{2393} = \overline{3}$.*

Através dos exemplos acima, é possível observar que qualquer número inteiro estará em uma das classes de equivalência de $\overline{0}$ a $\overline{4}$ módulo 5, ou seja, a união dessas classes é igual ao conjunto dos números inteiros. E também, são uma partição de $\mathbb{Z}$, pois duas classes distintas não possuem elementos em comum.

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} \cup \overline{4}.$$

Outra observação interessante é que quaisquer dois elementos de uma mesma classe são congruentes módulo 5, e se tomarmos quaisquer dois elementos em classes distintas, estes não são congruentes módulo 5.

Proposição 2.69. *Sejam a, b e $m \in \mathbb{Z}$, com $m > 1$, $a \equiv b (mod\ m)$ se, e somente se, a e b possuem o mesmo resto na divisão euclidiana por m.*

Demonstração. Por hipótese, $a-b = m\cdot q$, para algum inteiro q. Logo, $a = b+m\cdot q$. Sejam q_1 e r o quociente e o resto da divisão euclidiana de a por m, $a = m\cdot q_1+r \quad (0 \leq r < m)$. Das duas últimas igualdades segue que $b + m \cdot q = m \cdot q_1 + r$ e, então:

$$b = m \cdot (q_1 - q) + r \quad (0 \leq r < m).$$

Portanto, r é o resto da divisão de b por m. Reciprocamente, por hipótese, a e b dão o mesmo resto na divisão euclidiana por m:

$$a = m \cdot q_1 + r \quad \text{e} \quad b = m \cdot q_2 + r \quad (0 \leq r < m).$$

Subtraindo-se membro a membro essas igualdades:

$$a - b = m \cdot (q_1 - q_2).$$

De onde, $a \equiv b(\text{mod } m)$. □

2.7 Equações de congruências lineares

Chamamos de equação de congruência linear toda equação da forma $a \cdot x \equiv b(\text{mod } m)$, onde a, b, $m \in \mathbb{Z}$ e $m > 1$ e x é uma incógnita que deve assumir valores inteiros.

Seja x_0 uma solução particular da equação de congruência linear $a \cdot x \equiv b(\text{mod } m)$, ou seja, $a \cdot x_0 \equiv b(\text{mod } m)$, suponhamos que x_1 seja um inteiro tal que $x_1 \equiv x_0(\text{mod } m)$. Então x_1 também é uma solução de $a \cdot x \equiv b(\text{mod } m)$, pois

$$x_1 \equiv x_0(\text{mod } m) \Leftrightarrow a \cdot x_1 \equiv a \cdot x_0(\text{mod } m) \Leftrightarrow a \cdot x_1 \equiv b(\text{mod } m).$$

Portanto, se um elemento de uma classe de congruência módulo m é solução de $a \cdot x \equiv b(\text{mod } m)$, então todo elemento da referida classe também é solução.

Exemplo 2.70. *As equações* $8 \cdot x \equiv 2(mod\ 30)$ *e* $35 \cdot x - 1 \equiv 54(mod\ 15)$ *são exemplos de equações de congruências lineares.*

Para resolver essas equações, é necessário simplificá-las através dos seguintes resultados: Proposição 2.53, Proposição 2.54 e Proposição 2.56 .

Teorema 2.71. *Sejam a e b inteiros e m um inteiro maior que 1. A equação $a \cdot x \equiv b(mod\ m)$ tem solução se, e somente se, $mdc(a, m)$ divide b.*

Demonstração. Seja $x_0 \in \mathbb{Z}$ que satisfaz $a \cdot x \equiv b(\text{mod } m)$, então temos que m divide $a\cdot x_0 - b$. O que significa que existe $y_0 \in \mathbb{Z}$ tal que $a\cdot x_0 - b = m\cdot y_0$, ou seja, $a\cdot x_0 - m\cdot y_0 = b$.

Logo, resolver a equação de congruência linear $a \cdot x \equiv b(\text{mod } m)$ trata-se de resolver uma equação diofantina linear. Pelo Teorema 2.48, essa equação tem solução se, e somente se, $mdc(a, -m) = mdc(a, m)$ divide b. □

Teorema 2.72. *Sejam a e b e m inteiros tais que $m > 1$ e $mdc(a, m) = d$. No caso em que $d \nmid b$ a congruência $a \cdot x \equiv b(mod\ m)$ não possui nenhuma solução e quando $d \mid b$, possui exatamente d soluções incongruentes módulo m.*

Demonstração. Pela Proposição 2.52, $x \in \mathbb{Z}$ é solução de $a \cdot x \equiv b(\text{mod } m)$ se, e somente se, existe $y \in \mathbb{Z}$ tal que $a \cdot x = b + m \cdot y$, ou, o que é equivalente,

$$a \cdot x - m \cdot y = b. \tag{2.30}$$

Do Teorema 2.48, a equação (2.30) não possui nenhuma solução caso $d \nmid b$, e que se $d \mid b$ ela possui infinitas soluções dadas por $x = x_0 - (\frac{m}{d}) \cdot k$ e $y = y_0 - (\frac{a}{d}) \cdot k$, onde (x_0, y_0) é uma solução particular de (2.30). Logo a congruência $a \cdot x \equiv b(\text{mod } m)$ possui infinitas soluções dadas por $x = x_0 - (\frac{m}{d}) \cdot k$. Queremos saber o número de soluções incongruentes, então vamos tentar descobrir sob que condições $x_1 = x_0 - (\frac{m}{d}) \cdot k_1$ e $x_2 = x_0 - (\frac{m}{d}) \cdot k_2$ são congruentes módulo m. Se x_1 e x_2 são congruentes então $x_0 - (\frac{m}{d}) \cdot k_1 \equiv x_0 - (\frac{m}{d}) \cdot k_2(\text{mod } m)$. Isto implica $(\frac{m}{d}) \cdot k_1 \equiv (\frac{m}{d}) \cdot k_2(\text{mod } m)$, e como $(\frac{m}{d}) \mid m$, do Lema 2.15 temos $mdc(\frac{m}{d}, m) = \frac{m}{d}$, o que nos permite o cancelamento de $\frac{m}{d}$, resultando, pelo Teorema 2.60 $k_1 \equiv k_2(\text{mod } d)$. Podemos observar que m foi substituído por $d = \frac{m}{\frac{m}{d}}$, o que mostra que soluções incongruentes serão obtidas ao tomarmos $x = x_0 - (\frac{m}{d}) \cdot k$, onde k percorre um sistema completo de resíduos módulo d, o que conclui a demonstração. □

Definição 2.73. *Sejam $a \in \mathbb{Z}$ e m um inteiro maior que 1. Uma solução de $a \cdot x \equiv 1(mod\ m)$ é chamado de inverso de a módulo m.*

Proposição 2.74. *Seja m um inteiro maior que 1. O número inteiro a possui inverso módulo m se, e somente se, $mdc(a, m) = 1$.*

Demonstração. Se $a \in \mathbb{Z}$, suponhamos que a tem inverso x módulo m, então, pela Definição 2.73, $a \cdot x \equiv 1(\text{mod } m)$, ou seja, $m \mid (a \cdot x - 1)$. Logo, existe $k \in \mathbb{Z}$, tal que $a \cdot x + k \cdot m = 1$. Seja $d = mdc(a, m)$, temos que $d \mid a$ e $d \mid m$, então $d \mid (a \cdot x + k \cdot m)$, o que implica $d \mid 1$, logo $d = 1$. Portanto a tem inverso módulo m, então $mdc(a, m) = 1$. Se $mdc(a, m) = 1$, então pelas divisões sucessivas existem k_1 e k_2 tais que $a \cdot k_1 + m \cdot k_2 = 1$. Logo, $a \cdot k_1 - 1 = -m \cdot k_2$ é múltiplo m, ou seja, $a \cdot k_1 \equiv 1(\text{mod } m)$. Portanto, pela Definição 2.73, a tem inverso módulo m. □

Observação 2.75. *Para determinar os inversos na aritmética modular, é necessário resolver a equação de congruência linear $a \cdot x \equiv 1(mod\ m)$, o que nos leva a resolver a equação diofantina $a \cdot x - m \cdot k = 1$, com $k \in \mathbb{Z}$. Em um sistema completo de resíduos*

módulo p, sendo p um número primo, todo elemento do conjunto $\{1, 2, \ldots, p-1\}$ *admite inverso módulo p.*

Exemplo 2.76. *Como* $2 \cdot 5 \equiv 1(mod\ 9)$*, 2 é o inverso de 5 módulo 9 e vice-versa.*

Proposição 2.77. *Seja p um número primo. O inteiro positivo a é o seu próprio inverso módulo p se, e somente se,* $a \equiv 1(mod\ p)$ *ou* $a \equiv -1(mod\ p)$*.*

Demonstração. Pela Definição 2.73, se a é o seu próprio inverso módulo p, então $a^2 \equiv 1(\text{mod } p)$, o que significa que $p \mid (a^2 - 1) = (a-1) \cdot (a+1)$. Mas, pelo Lema 2.27, se $p \mid (a-1) \cdot (a+1)$, sendo p primo, $p \mid (a-1)$ ou $p \mid (a+1)$, o que implica $a \equiv 1(\text{mod } p)$ ou $a \equiv -1(\text{mod } p)$.

Reciprocamente, se $a \equiv 1(\text{mod } p)$ ou $a \equiv -1(\text{mod } p)$, então $p \mid (a-1)$ ou $p \mid (a+1)$. Portanto, $p \mid (a-1) \cdot (a+1) = (a^2 - 1)$, o que significa $a^2 \equiv 1(\text{mod } p)$ e, pela definição, a é seu próprio inverso módulo p. □

2.8 Teoremas de Fermat, Euler e Wilson

Nesta seção, demonstraremos três importantes teoremas em Teoria dos Números e com aplicabilidade no método RSA. Conforme Boyer (2012, p. 310), o Pequeno Teorema de Fermat foi uma conjetura de Fermat, sendo Euler o primeiro a publicar uma demonstração dela. E, a partir disso, Euler demonstrou uma afirmação um pouco mais geral, que trata-se do Teorema de Euler. E enfim, o Teorema de Wilson que auxilia na caracterização de números primos.

Teorema 2.78. *(Pequeno Teorema de Fermat) Seja p primo. Se* $p \nmid a$ *então* $a^{p-1} \equiv 1(mod\ p)$*.*

Demonstração. Sabemos que o conjunto formado pelos p números $0, 1, 2, \ldots, p-1$ constitui um sistema completo de resíduos módulo p. Isto significa que qualquer conjunto contendo no máximo p elementos incongruentes módulo p pode ser colocado em correspondência biunívoca com um subconjunto de $\{0, 1, 2, \ldots, p-1\}$. Vamos agora considerar os números $a, 2 \cdot a, 3 \cdot a, \ldots, (p-1) \cdot a$. Como $mdc(a, p) = 1$, nenhum destes números $i \cdot a$, $1 \leq i \leq p-1$ é divisível por p, ou seja, nenhum é congruente a zero módulo p. Quaisquer dois deles são incongruentes módulo p, pois $a \cdot j \equiv a \cdot k(\text{mod } p)$ implica $j \equiv k(\text{mod } p)$ e isto só possível se $j = k$, uma vez que ambos j e k são positivos e menores que p e não divisíveis por p. Temos, portanto, um conjunto de $p-1$ elementos incongruentes módulo p e não divisíveis por p. Logo, cada um deles é congruente a exatamente um dentre os

elementos $0, 1, 2, \ldots, p-1$. Se multiplicarmos estas congruências, membro a membro, teremos:

$$a \cdot (2 \cdot a) \cdot (3 \cdot a) \ldots (p-1) \cdot a \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) (\text{mod } p)$$

ou seja, $a^{p-1} \cdot (p-1)! \equiv (p-1)! (\text{mod } p)$. Mas como, $mdc((p-1)!, p) = 1$, podemos cancelar o fator $(p-1)!$ em ambos os lados, obtendo

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

o que conclui a demonstração. □

Corolário 2.79. *Se p é um primo e a é um inteiro positivo, então $a^p \equiv a (mod\ p)$.*

Demonstração. Temos que analisar dois casos, se $p \mid a$ e se $p \nmid a$. Se $p \mid a$, então $p \mid (a \cdot (a^{p-1} - 1))$ e, portanto $a^p \equiv a (\text{mod } p)$. Se $p \nmid a$, pelo Pequeno Teorema de Fermat $p \mid (a^{p-1} - 1)$ e, portanto, $p \mid (a^p - a)$. Logo, em ambos os casos, $a^p \equiv a (\text{mod } p)$. □

Definição 2.80. *Se m é um inteiro positivo, a função ϕ de Euler, denotada por $\phi(m)$, é definida como sendo o número de inteiros positivos menores do que ou iguais a m que são coprimos com m.*

Definição 2.81. *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 coprimo com m, e se $i \neq j$, então $r_i \not\equiv r_j (mod\ m)$.*

Exemplo 2.82. *O conjunto $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ é um sistema completo de resíduos módulo 9, portanto $\{1, 2, 4, 5, 7, 8\}$ é sistema reduzido de resíduos módulo 9, ou seja, $\phi(9) = 6$. A fim de obter um sistema reduzido de resíduos de um sistema completo módulo m, basta retirar os elementos do sistema completo que não são coprimos com m.*

Observação 2.83. *É possível observar que $\phi(m) \leq m - 1$ para $m \geq 2$. Também para $m \geq 2$, temos que $\phi(m) = m - 1$ se, e somente se, m é um número primo. Realmente, m é primo se, e somente se, $\{1, 2, \ldots, m-1\}$ é um sistema reduzido de resíduos módulo m, o que significa $\phi(m) = m - 1$.*

Teorema 2.84. *Sejam a um inteiro positivo tal que $mdc(a, m) = 1$. Se $r_1, r_2, \ldots, r_{\phi(m)}$ é um sistema reduzido de resíduos módulo m, então $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\phi(m)}$ é, também, um sistema reduzido de resíduos módulo m.*

Demonstração. Na sequência $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\phi(m)}$ temos $\phi(m)$ elementos, é necessário mostrar que todos eles são coprimos com m e, dois a dois, incongruentes módulo m. Como $mdc(a, m) = 1$ e $mdc(r_i, m) = 1$, pela Proposição 2.26, $mdc(a \cdot r_i, m) = 1$. Logo, nos resta mostrar que $a \cdot r_i \not\equiv a \cdot r_j (\text{mod } m)$ se $i \neq j$. Mas, como $mdc(a, m) = 1$, pelo item (f) da

Proposição 2.56, de $a \cdot r_i \equiv a \cdot r_j (\text{mod } m)$ temos $r_i \equiv r_j (\text{mod } m)$, o que implica $i = j$, uma vez que $r_1, r_2, \ldots, r_{\phi(m)}$ é um sistema reduzido de resíduos módulo m, o que conclui a demonstração. □

Proposição 2.85. *Sejam p um número primo e k um natural não nulo. Então $\phi(p^k) = p^k - p^{k-1}$.*

Demonstração. Inicialmente, note que $mdc(n, p^k) = 1$ se, e somente se, p não divide n. Agora, como existem exatamente p^{k-1} naturais entre 1 e p^k que são divisíveis por p, a saber, os números $p, 2 \cdot p, 3 \cdot p, \ldots, (p^{k-1}) \cdot p$, segue que o conjunto $\{1, 2, \ldots, p^k\}$ contém precisamente $p^k - p^{k-1}$ naturais que são coprimos com p^k, de modo que, pela definição da função ϕ, concluímos que $\phi(p^k) = p^k - p^{k-1}$. □

Exemplo 2.86. *Para $m = 8$, temos $\phi(8) = \phi(2^3) = 2^3 - 2^2 = 4$. Isso significa, que existem 4 naturais menores que 8 que são coprimos com 8, sendo eles: 1, 3, 5 e 7.*

Proposição 2.87. *A função ϕ de Euler satisfaz a seguinte propriedade $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$, sempre que m, $n \in \mathbb{N}^*$ e $mdc(m, n) = 1$.*

Demonstração. Consideremos m, $n \in \mathbb{N}^*$ coprimos. Primeiramente, é fácil ver que a proposição é válida para os casos onde $m = 1$ e $n = 1$. De fato,

$$\phi(m \cdot 1) = \phi(m) = \phi(m) \cdot 1 = \phi(m) \cdot \phi(1)$$

e

$$\phi(1 \cdot n) = \phi(n) = 1 \cdot \phi(n) = \phi(1) \cdot \phi(n).$$

Suponhamos $m > 1$ e $n > 1$. Para demonstrar esse caso, vamos dispor todos os naturais compreendidos entre 1 e $m \cdot n$ da seguinte maneira:

$$\begin{array}{ccccccc} 1 & 2 & \cdots & \text{t} & \cdots & n \\ n+1 & n+2 & \cdots & n+t & \cdots & 2 \cdot n \\ 2 \cdot n + 1 & 2 \cdot n + 2 & \cdots & 2 \cdot n + t & \cdots & 3 \cdot n \\ \vdots & \vdots & & \vdots & & \vdots \\ (m-1) \cdot n + 1 & (m-1) \cdot n + 2 & \cdots & (m-1) \cdot n + t & \cdots & m \cdot n \end{array}$$

Pelo Lema 2.16, $mdc(q \cdot n + t, n) = mdc(n, t)$, e os números naturais da t-ésima coluna são coprimos com n se, e somente se, t é um número coprimo com n. E como na primeira linha o número de naturais que são coprimos com n é igual $\phi(n)$, decorre que existem apenas $\phi(n)$ colunas formadas com naturais que são todos coprimos com n. Por outro lado, para cada $t \in \{1, 2, \ldots, n\}$, analisando cada coluna, consideremos a progressão aritmética (PA)

$$t, n + t, 2 \cdot n + t, \ldots, (m-1) \cdot n + t.$$

Inicialmente, observamos que nessa PA não há termos que deixem o mesmo resto na divisão euclidiana por m. Com efeito, se dois termos distintos $k_1 \cdot n + t$ e $k_2 \cdot n + t$ com k_1, $k_2 \in \{0, 1, \ldots, m-1\}$, deixassem o mesmo resto r na divisão por m, então teríamos, segundo o Algoritmo da Divisão, $k_1 \cdot n + t = q_1 \cdot m + r$ e $k_2 \cdot n + t = q_2 \cdot m + r$, q_1, $q_2 \in \mathbb{N}$, donde seria possível inferir que $(k_1 - k_2) \cdot n = (q_1 - q_2) \cdot m$ e, com isso, m seria divisor de $(k_1 - k_2) \cdot n$. Como $mdc(m, n) = 1$ e pelo Teorema 2.24, teríamos m como divisor $(k_1 - k_2)$, o que só seria possível, segundo a Definição 2.62 e Exemplo 2.63, se $k_1 = k_2$, uma vez que k_1, $k_2 \in \{0, 1, \ldots, m-1\}$, uma contradição. Como termos distintos da PA deixam restos distintos na divisão euclidiana por m e a PA tem exatamente m termos distintos, teremos também exatamente m restos distintos (que reunidos, formam exatamente o conjunto $\{0, 1, \ldots, m-1\}$). Além disso, como $mdc(k \cdot n + t, m) = mdc(m, r)$, onde r é o resto da divisão de $k \cdot n + t$ por m, temos que o números de termos da PA que são coprimos com m é igual ao número de restos obtidos na divisão de seus termos por m e que sejam coprimos com m, que, por sua vez, é igual a $\phi(m)$. Dessa forma, em cada uma da $\phi(n)$ colunas mencionadas anteriormente existem $\phi(m)$ naturais que são coprimos com m. Concluímos que o número total de naturais que são coprimos com n e m, ou seja, que são coprimos com o produto $m \cdot n$ é igual a $\phi(m) \cdot \phi(n)$. Isso significa que $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$. □

Proposição 2.88. *Se $n = p_1^{a_1} \cdot p_2^{a_2} \ldots p_t^{a_t}$ é a fatoração de n, onde $n > 1$, então*

$$\phi(n) = (p_1^{a_1} - p_1^{a_1 - 1}) \cdot (p_2^{a_2} - p_2^{a_2 - 1}) \ldots (p_t^{a^t} - p_t^{a_t - 1}).$$

Demonstração. Faremos a demonstração por indução sobre t, que trata-se do número de fatores primos distintos na fatoração-padrão de n. Para $t = 1$, n é uma potência de algum primo com expoente positivo. Logo, pela Proposição 2.85, a proposição que estamos demonstrando é verdadeira para $t = 1$. Então, suponhamos que a proposição é válida para $t = r$, onde $r \geq 1$. Vamos provar que a proposição é válida no caso em que $t = r + 1$. Nesse caso, $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r} \cdot p_{r+1}^{a_{r+1}}$ é a fatoração-padrão de n, então sabendo $mdc(p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}, p_{r+1}^{a_{r+1}}) = 1$ e que $\phi(n)$ satisfaz a propriedade exibida na Proposição 2.87, temos

$$\phi([p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}] \cdot p_{r+1}^{a_{r+1}}) = \phi(p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}) \cdot \phi(p_{r+1}^{a_{r+1}}),$$

e utilizando a Proposição 2.85,

$$\phi([p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}] \cdot p_{r+1}^{a_{r+1}}) = \phi(p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}) \cdot (p_{r+1}^{a_{r+1}} - p_{r+1}^{a_{r+1}-1}). \tag{2.31}$$

Pela hipótese de indução, é válido que

$$\phi(p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}) = (p_1^{a_1} - p_1^{a_1 - 1}) \cdots (p_r^{a_r} - p_r^{a_r - 1}). \tag{2.32}$$

Juntando (2.31) e (2.32), obtemos

$$\phi(p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r} \cdot p_{r+1}^{a_{r+1}}) = (p_1^{a_1} - p_1^{a_1 - 1}) \cdots (p_r^{a_r} - p_r^{a_r - 1}) \cdot (p_{r+1}^{a_{r+1}} - p_{r+1}^{a_{r+1}-1}),$$

logo a proposição é válida para $t = r + 1$.

Portanto, pelo Princípio da Indução Finita, concluímos que a proposição é válida para todo $t \geq 1$. □

Exemplo 2.89. *Calculemos* $\phi(5040)$. *Pela Proposição anterior, escrevendo* $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$, *temos*

$$\phi(5040) = (2^4 - 2^3) \cdot (3^2 - 3^1) \cdot (5^1 - 5^0) \cdot (7^1 - 7^0) = 1152.$$

Teorema 2.90. *(Euler) Sejam* m, $a \in \mathbb{Z}$ *com* $m > 1$ *e* $mdc(a, m) = 1$, *então*

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

Demonstração. O Teorema 2.84 mostra que os elementos $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\phi(m)}$ constituem 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. Isto significa que $a \cdot r_i$ é congruente a exatamente um dos r_j, $1 \leq j \leq \phi(m)$, e portanto o produto dos $a \cdot r_i$ deve ser congruente ao produto dos r_j módulo m, isto é,

$$a \cdot r_1 \cdot a \cdot r_2 \cdots a \cdot r_{\phi(m)} \equiv r_1 \cdot r_2 \cdots r_{\phi(m)} (\text{mod } m),$$

ou seja,

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

Como

$$mdc\left(\prod_{i=1}^{\phi(m)} r_i, m\right) = 1,$$

pelo item (f) da Proposição 2.56, podemos cancelar

$$\prod_{i=1}^{\phi(m)} r_i$$

em ambos os lados para obter $a^{\phi(m)} \equiv 1 (\text{mod } m)$. □

Como para p primo, $\phi(p) = p - 1$, o Teorema de Euler é uma generalização do Pequeno Teorema de Fermat.

Apesar de sua aplicação não ser prática, devido a dificuldade do cálculo de $(p-1)!$, o próximo teorema trata-se de um teste de primalidade.

Teorema 2.91. *(Teorema de Wilson) O número inteiro* $p > 1$ *é primo se, e somente se,* $(p-1)! \equiv -1 (mod\ p)$.

Demonstração. Primeiramente, vamos mostrar que se $(p-1)! \equiv -1(\text{mod } p)$ então p é primo. Suponhamos que p fosse composto, isso implicaria em p ter um divisor d com $1 < d < p$. Além disso, como $d \leq p-1$, segue-se que d é um dos fatores de $(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1)$, ou seja, d é divisor de $(p-1)!$. Mas, por hipótese, $(p-1)! \equiv -1(\text{mod } p)$, isto é, pela definição de congruência, p é divisor de $(p-1)!+1$, então d também é divisor de $(p-1)!+1$. Como d é divisor de $(p-1)!$, isso somente seria possível se d fosse divisor de 1, o que não é o caso, pois $d > 1$. Logo, p é primo.

Agora, vamos supor que p seja primo e mostrar que vale a congruência $(p-1)! \equiv -1(\text{mod } p)$. O resultado vale para $p = 2$ e $p = 3$, pois $(2-1)! \equiv -1(\text{mod } 2)$ e $(3-1)! \equiv -1(\text{mod } 3)$. Portanto, podemos supor que $p \geq 5$. Consideremos a congruência linear

$$a \cdot x \equiv 1(\text{mod } p), \tag{2.33}$$

onde a é qualquer um dos elementos do conjunto $\{1, 2, 3, \ldots, p-1\}$. Como $mdc(a, p) = 1$, pelos Teoremas 2.71 e 2.72, a equação (2.33) admite uma única solução p, isto é, existe um único inteiro b, com $1 \leq b \leq p-1$, tal que

$$a \cdot b \equiv 1(\text{mod } p). \tag{2.34}$$

Note que da Definição 2.73, a equação (2.34) nos diz que a e b são inversos módulo p. Como p é primo, a Proposição 2.77 nos dá que $a = b$ se, e somente se, $a = 1$ ou $a = p-1$. Agora, para os números $2, 3, 4, \ldots, p-2$, podemos agrupá-los em $\frac{p-3}{2}$ pares (a, b) satisfazendo $a \cdot b \equiv 1(\text{mod } p)$ (hipótese $p \geq 5$). Multiplicando todas essas $\frac{p-3}{2}$ congruências, obtemos

$$2 \cdot 3 \cdot 4 \cdot 5 \cdots (p-2) \equiv 1(\text{mod} p) \tag{2.35}$$

e, multiplicando (2.35) por $p-1$, ficará

$$2 \cdot 3 \cdot 4 \cdot 5 \cdots (p-2) \cdot (p-1) \equiv p-1(\text{mod} p).$$

Como $p - 1 \equiv -1(\text{mod } p)$, por transitividade,

$$(p-1)! \equiv -1(\text{mod } p).$$

□

Exemplo 2.92. *Mostre que 19 é primo usando o Teorema de Wilson.*

Precisamos mostrar que $(19-1)! \equiv -1(mod\ 19)$*, ou seja,* $18! \equiv -1(mod\ 19)$*. Para isso,*

$$2 \cdot 10 \equiv \quad 1(mod\ 19)$$
$$3 \cdot 13 \equiv \quad 1(mod\ 19)$$

$$\begin{aligned} 4 \cdot 5 &\equiv 1 (mod\ 19) \\ 6 \cdot 16 &\equiv 1 (mod\ 19) \\ 7 \cdot 11 &\equiv 1 (mod\ 19) \\ 8 \cdot 12 &\equiv 1 (mod\ 19) \\ 9 \cdot 17 &\equiv 1 (mod\ 19) \\ 14 \cdot 15 &\equiv 1 (mod\ 19). \end{aligned}$$

Multiplicando as congruências acima, obtemos

$$(2 \cdot 10) \cdot (3 \cdot 13) \cdot (4 \cdot 5) \cdot (6 \cdot 16) \cdot (7 \cdot 11) \cdot (8 \cdot 12) \cdot (9 \cdot 17) \cdot (14 \cdot 15) \equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 (mod\ 19),$$

ou ainda,

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \cdot 14 \cdot 15 \cdot 16 \cdot 17 \equiv 1 (mod\ 19).$$

Multiplicando a última congruência por 18,

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \cdot 14 \cdot 15 \cdot 16 \cdot 17 \cdot 18 \equiv 18 (mod\ 19),$$

logo

$$18! \equiv 18 (mod\ 19).$$

Mas, como $18 \equiv -1 (mod\ 19)$*, pela propriedade transitiva*

$$18! \equiv -1 (mod\ 19).$$

Portanto, pelo Teorema de Wilson, 19 é um número primo.

A seguir algumas aplicações dos Teoremas de Fermat e de Euler.

Exemplo 2.93. *Vamos calcular o resto da divisão de* 2^{100000} *por 17. Queremos determinar* $0 \leq r \leq 16$*, de modo que* $2^{100000} \equiv r (mod\ 17)$*. Como 17 é um número primo e* $17 \nmid 2$*, pelo Pequeno Teorema de Fermat,* $2^{16} \equiv 1 (mod\ 17)$*. Mas* $100000 = 16 \cdot 6250$ *e, portanto,*

$$2^{100000} \equiv 2^{16 \cdot 6250} \equiv (2^{16})^{6250} \equiv 1^{6250} \equiv 1 (mod\ 17).$$

Logo, o resto da divisão por 17 de 2^{100000} *é 1.*

Exemplo 2.94. *Vamos obter o resto da divisão de* 8^{747} *por 45. Queremos determinar* $0 \leq r \leq 44$*, de modo que* $8^{747} \equiv r (mod\ 45)$*. Como* $mdc(8, 45) = 1$ *e* $\phi(45) = \phi(3^2 \cdot 5) = \phi(3^2) \cdot \phi(5) = (3^2 - 3^1) \cdot (5^1 - 5^0) = 24$*, pelo Teorema de Euler,* $8^{24} \equiv 1 (mod\ 45)$*. Dividindo 747 por 24, obtemos quociente 31 e resto 3, ou seja,* $747 = 24 \cdot 31 + 3$*. Assim, usando as propriedades da congruência (Proposição 2.56), temos*

$$8^{747} \equiv 8^{24 \cdot 31 + 3} \equiv (8^{24})^{31} \cdot 8^3 \equiv 1^{31} . 8^3 \equiv 17 (mod\ 45).$$

Logo, o resto da divisão é 17.

Exemplo 2.95. *Vamos obter a solução da equação de congruência linear* $2 \cdot x \equiv 13(mod\ 17)$. *Como 17 é primo e* $17 \nmid 2$, *temos* $2^{16} \equiv 1(mod\ 17)$. *Multiplicando ambos os lados da equação* $2 \cdot x \equiv 13(mod\ 17)$ *por* 2^{15}, *obtemos* $x \equiv 2^{15} \cdot 13(mod\ 17)$. *Para obter* x *satisfazendo* $0 \leq x \leq 16$, *aplicamos as propriedades de congruências. De* $2^4 \equiv 16 \equiv -1(mod\ 17)$, *obtemos* $2^8 \equiv 1(mod\ 17)$, $2^{12} \equiv -1(mod\ 17)$ *e* $2^{15} = 2^{12} \cdot 2^3 \equiv -1 \cdot 8 \equiv 16 \cdot 8 \equiv 128 \equiv 9(mod\ 17)$. *Portanto,* $x \equiv 9 \cdot 13 \equiv 117 \equiv 15(mod\ 17)$.

Capítulo 3

Criptografia RSA

O método de criptografia RSA que estudaremos nesse capítulo garante, conforme Carneiro (2017, p. 97), "a transmissão de informações confidenciais através de redes inseguras e ainda a autenticação do usuário extremamente necessária em transações bancárias". Em outras palavras, ele tornou viável a comunicação através da Internet e, possibilitou o desenvolvimento da assinatura digital.

O RSA é um método de criptografia de chave pública bastante utilizado, devido a segurança que ele fornece. Esse fato, conforme já escrevemos nesse trabalho, reside na inexistência de uma forma rápida para fatorar números muito grandes.

Neste capítulo, mediante os conteúdos matemáticos do capítulo anterior, faremos a descrição e fundamentação do método de Criptografia RSA e desenvolveremos um exemplo. Para isso, serão usados os livros "Números Inteiros e Criptografia RSA", do Severino Collier Coutinho e "Criptografia e Teoria dos Números", do Framilson José Ferreira Carneiro.

3.1 Codificação e Decodificação

A primeira etapa para conseguirmos aplicar o método de criptografia RSA trata-se de uma pré-codificação, que consiste na substituição das letras da mensagem por números, o que transforma a mensagem em uma sequência numérica. A substituição é realizada usando a seguinte tabela:

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

Os espaços entre as palavras serão substituídos pelo número 36.

Observamos que a escolha desses números para substituir as letras em vez de 1, 2, 3, ..., e assim sucessivamente, é para evitar ambiguidades. Por exemplo, ao correspondermos A e B aos números 1 e 2, respectivamente, no decorrer do texto, o número 12 resultaria na dúvida, é A e B ou é L?

Posteriormente, determinamos os parâmetros do método de criptografia RSA, escolhendo dois números primos p e q. O par (n, e) é a chave de codificação do sistema RSA, sendo $n = p \cdot q$ e e um número inteiro, tal que e é inversível módulo $\phi(n)$. Como vimos no capítulo anterior, a função ϕ é conceituada pela Definição 2.80, e os cálculos de $\phi(n)$ podem ser realizados usando a Proposição 2.88, isto é, $\phi(n) = (p_1^{a_1} - p_1^{a_1-1}) \cdot (p_2^{a_2} - p_2^{a_2-1}) = (p^1 - p^0) \cdot (q^1 - q^0) = (p-1) \cdot (q-1)$. Já o número e para ser inversível módulo $\phi(n)$ precisa seguir o disposto na Proposição 2.74, ou seja, $mdc(e, \phi(n)) = 1$.

Para finalizar a pré-codificação, a sequência numérica será dividida em blocos, sendo cada bloco denotado por b. A divisão em blocos seguirá regras, os blocos não podem iniciar com o número 0 e deverão ser menores que n, para evitar problemas na decodificação; e para maior segurança, não corresponder a palavras ou letras, o que torna impossível a análise de frequência.

O bloco b codificado será $C(b) = a$, que é igual ao resto da divisão de b^e por n, ou ainda,

$$b^e \equiv a (\text{mod } n), \text{ com } 0 < a < n. \tag{3.1}$$

Cada bloco b passará pela etapa de codificação separadamente. A mensagem codificada é uma sequência blocos codificados $(C(b_1), C(b_2), \ldots, C(b_n))$. Vale salientar que os blocos codificados devem ser mantidos separados, para não tornar impossível a decodificação da mensagem.

A chave de decodificação do sistema RSA é o par (n, d), onde d é o inverso de e módulo $\phi(n)$. Assim como acontece com e, o $mdc(d, \phi(n)) = 1$. É possível obter d pelo método das divisões sucessivas, resolvendo a equação diofantina (Exemplo 2.49) que resulta da equação de congruência linear $e \cdot d \equiv 1 (\text{m}od\ \phi(n))$ (Definição 2.73).

A decodificação trata-se de encontrar o bloco da mensagem original. O bloco da mensagem decodificado será $D(a) = l$, que é igual ao resto da divisão de a^d por n, ou seja,

$$a^d \equiv l (\text{mod } n) \text{ com } 0 < l < n. \tag{3.2}$$

Para calcularmos as congruências (3.1) e (3.2), é possível aplicar os Teoremas de Fermat e de Euler e também a Proposição 2.56.

3.2 Por que o método de Criptografia RSA funciona e é seguro?

O método funciona se, decodificando um bloco codificado, conseguimos obter o bloco correspondente da mensagem original. Considerando as notações adotadas anteriormente, temos um sistema de Criptografia RSA de parâmetros p e q, $n = p \cdot q$, a chave de codificação (n, e) e a chave de decodificação (n, d), e queremos mostrar que se b é um inteiro e $1 \leq b \leq n-1$, então $D(C(b)) \equiv b(\text{mod } n)$. Com a orientação de dividirmos a mensagem original em blocos menores do que n, temos b e $D(C(b))$ estão entre 1 e $n-1$, ou seja, só podem ser congruentes módulo n se são iguais. Sendo assim, precisamos provar apenas que $D(C(b)) \equiv b(\text{mod } n)$. De (3.1) e (3.2), contamos com $C(b) \equiv b^e \equiv a(\text{mod } n)$ e $D(a) \equiv a^d \equiv l(\text{mod } n)$, o que resulta em

$$D(C(b)) \equiv (b^e)^d \equiv b^{e \cdot d}(\text{mod } n). \tag{3.3}$$

Dessa forma, e retomando o fato que $n = p \cdot q$, onde p e q são números primos distintos, calcularemos, separadamente,

$$b^{e \cdot d} \equiv b(\text{mod } p) \tag{3.4}$$

e

$$b^{e \cdot d} \equiv b(\text{mod } q). \tag{3.5}$$

Sabemos que d é o inverso de e módulo $\phi(n)$, logo, pela Definição 2.73, $e \cdot d \equiv 1(\text{mod } \phi(n))$, o que corresponde a $e \cdot d = 1 + k \cdot \phi(n)$ pela Proposição 2.52. Usando a Proposição 2.88,

$$e \cdot d = 1 + k \cdot (p-1) \cdot (q-1), \text{ para algum inteiro } k. \tag{3.6}$$

Substituindo (3.6) em (3.4) e (3.5),

$$b^{e \cdot d} \equiv b^{1+k \cdot (p-1) \cdot (q-1)} \equiv b \cdot b^{k \cdot (p-1) \cdot (q-1)}(\text{mod } p). \tag{3.7}$$

e

$$b^{e \cdot d} \equiv b^{1+k \cdot (p-1) \cdot (q-1)} \equiv b \cdot b^{k \cdot (p-1) \cdot (q-1)}(\text{mod } q). \tag{3.8}$$

Primeiramente, mostraremos que $b^{e \cdot d} \equiv b(\text{mod } p)$. Supondo que $p \mid b$, logo $b = 0 + k \cdot p$, para algum k inteiro, o que resulta em, pela Proposição 2.52, $b \equiv 0(\text{mod } p)$, e também $b^{e \cdot d} \equiv 0(\text{mod } p)$. Logo,

$$b^{e \cdot d} \equiv b(\text{mod } p). \tag{3.9}$$

Agora, supondo que $p \nmid b$, pelo Pequeno Teorema de Fermat,

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

Assim, dos itens (h) e (e) da Proposição 2.56, obtemos, respectivamente,

$$(b^{(p-1)})^{k\cdot(q-1)} \equiv 1^{k\cdot(q-1)} \equiv 1(\text{mod } p)$$

e

$$(b^{(p-1)})^{k\cdot(q-1)} \cdot b \equiv 1 \cdot b \equiv b(\text{mod } p) \tag{3.10}$$

De, (3.7) e (3.10), $b^{e\cdot d} \equiv b(\text{mod } p)$. Portanto, $b^{e\cdot d} \equiv b(\text{mod } p)$ para qualquer b inteiro.

Analogamente, $b^{e\cdot d} \equiv b(\text{mod } q)$ para qualquer b inteiro. Se $q \mid b$, implica que $b = 0 + k \cdot q$, para algum k inteiro. Logo, $b \equiv 0(\text{mod } q)$, e também $b^{e\cdot d} \equiv 0(\text{mod } q)$. Portanto, $b^{e\cdot d} \equiv b(\text{mod } q)$. Agora, como q é primo e se $q \nmid b$, pelo Pequeno Teorema de Fermat, temos $b^{q-1} \equiv 1(\text{mod } q)$, resultando em

$$\begin{aligned} (b^{(q-1)})^{k\cdot(p-1)} &\equiv 1^{k\cdot(p-1)} \equiv 1(\text{mod } q) \\ (b^{(p-1)})^{k\cdot(q-1)} \cdot b &\equiv 1 \cdot b \equiv b(\text{mod } p). \end{aligned}$$

Portanto, $b^{e\cdot d} \equiv b(\text{mod } q)$ para qualquer b inteiro.

Acabamos de mostrar as congruências $b^{e\cdot d} \equiv b(\text{mod } p)$ e $b^{e\cdot d} \equiv b(\text{mod } q)$ para qualquer b inteiro. A Definição 2.50 de congruência nos permite dizer que p e q dividem $b^{e\cdot d} - b$. Sendo assim, e como $mdc(p, q) = 1$, segue da Proposição 2.25 que $p \cdot q$ divide $b^{e\cdot d} - b$ ou n divide $b^{e\cdot d} - b$, pois $n = p \cdot q$. Portanto, podemos concluir que $b^{e\cdot d} \equiv b(\text{mod } n)$. Isto encerra a demonstração de que o método RSA funciona.

Como vimos anteriormente, a criptografia RSA é um método de chave pública, considerando os parâmetros do sistema adotados anteriormente, sendo eles os números primos p e q, e $n = p \cdot q$. A chave de codificação ou chave pública (n, e) é acessível a qualquer usuário, já a chave de decodificação (n, d) é privada. Por isso, o método RSA só será seguro se for difícil de calcular d, quando conhecemos apenas n e e.

Para calcular d aplicamos o método das divisões sucessivas a $\phi(n)$ e e. No entanto, para calcular $\phi(n)$ é necessário fatorar n para obter p e q. Se n for um número grande, fatorá-lo torna-se muito difícil por não existirem algoritmos rápidos para fatoração.

Então, acredita-se que quebrar o código RSA é equivalente a fatorar n. Por isso é importante a escolha de primos suficientemente grandes. Mas, além de p e q grandes, $|p - q|$ precisa ser grande também, caso contrário, será fácil fatorar n usando a fatoração pelo método de Fermat.

Em 2010, de acordo com o site do Instituto de Matemática Pura e Aplicada (IMPA), pesquisadores conseguiram fatorar um número de 232 dígitos (768 bits) em um desafio da RSA usando uma rede de computadores. Depois disso, são usadas chaves de 1024 bits, 2048 bits e 4096 bits, sempre com mais de 309 dígitos.

Atualmente, também de acordo com o site do IMPA, o maior número primo conhecido é o $51^{\underline{o}}$ primo de Mersenne, $2^{82.589.933-1}$. Ele foi descoberto por Patrick Laroche, em 07 de dezembro de 2018, através do projeto de pesquisa mundial Great Internet Mersenne Prime Search (GIMPS). O projeto GIMPS foi criado em 1966, ele possibilita que os participantes façam o download de um software especial para encontrar números primos cada vez maiores. Isso traz perspectivas boas para segurança do método RSA no futuro, mas também, tudo depende do não surgimento de um algoritmo de fatoração capaz de decompor rapidamente números muito grande.

3.3 Exemplo

Para ilustrar o método de criptografia RSA descrito acima, faremos um exemplo, codificando a mensagem **"PIERRE DE FERMAT"**.

Primeiramente, faremos a etapa de pré-codificação usando a tabela da seção 3.1, o que nos dá a seguinte sequência numérica:

2518142727143613143615142722102 9

Os parâmetros escolhidos são $p = 5$ e $q = 17$, então temos $n = p \cdot q = 5 \cdot 17 = 85$ e $\phi(n) = (p-1) \cdot (q-1) = 4 \cdot 16 = 64$. O número 3 é inversível módulo $\phi(85) = 64$, então tomaremos $e = 3$. Lembrando que os blocos devem ser menores que $n = 85$, obtemos os seguintes blocos da sequência numérica acima:

2-51-81-42-72-71-43-61-31-43-61-51-42-72-2-10-2-9

Seja $(85, 3)$ a chave de codificação e $C(b) \equiv b^e (\text{mod } n)$ a fórmula, iniciemos a codificação dos blocos:

1. $b_1 = 2$:

Como $2^3 = 8$ e $8 \equiv 8 (\text{mod } \ 85)$. Logo $C(2) = 8$.

2. $b_2 = 51$:

Como $51^3 = 132651$ e $132651 \equiv 51 (\text{mod } \ 85)$. Logo $C(51) = 51$.

3. $b_3 = 81$:

Como $81 \equiv -4 (\text{mod } 85)$, então $81^3 \equiv (-4)^3 \equiv -64 \equiv 21 (\text{mod } 85)$. Logo $C(81) = 21$.

4. $b_4 = 42$:

Como $42^3 = 74088$ e $42^3 \equiv 53 (\text{mod } 85)$. Logo $C(42) = 53$.

5. $b_5 = 72$:

Como $72^3 = 373248$ e $72^3 \equiv 13 (\text{mod } 85)$. Logo $C(72) = 13$.

6. $b_6 = 71$:

Como $71^3 = 357911$ e $71^3 \equiv 61 (\text{mod } 85)$. Logo $C(71) = 61$.

7. $b_7 = 43$

Como $43^3 = 79507$ e $43^3 \equiv 32 (\text{mod } 85)$. Logo $C(43) = 32$.

8. $b_8 = 61$

Como $61^3 = 226981$ e $61^3 \equiv 31 (\text{mod } 85)$. Logo $C(61) = 31$.

9. $b_9 = 31$

Como $31^3 = 29791$ e $31^3 \equiv 41 (\text{mod } 85)$. Logo $C(31) = 41$.

10. $b_{10} = 43$

Como $43^3 = 79507$ e $43^3 \equiv 32 (\text{mod } 85)$. Logo $C(43) = 32$.

11. $b_{11} = 61$

Como $61^3 = 226981$ e $61^3 \equiv 31 (\text{mod } 85)$. Logo $C(61) = 31$.

12. $b_{12} = 51$:

Como $51^3 = 132651$ e $132651 \equiv 51 (\text{mod } 85)$. Logo $C(51) = 51$.

13. $b_{13} = 42$:

Como $42^3 = 74088$ e $42^3 \equiv 53 (\text{mod } 85)$. Logo $C(42) = 53$.

14. $b_{14} = 72$:

Como $72^3 = 373248$ e $72^3 \equiv 13 (\text{mod } 85)$. Logo $C(72) = 13$.

15. $b_{15} = 2$:

Como $2^3 = 8$ e $8 \equiv 8 (\text{mod } 85)$. Logo $C(2) = 8$.

16. $b_{16} = 10$:

Como $10^3 = 10^2 \cdot 10$, $10 \equiv 10(\text{mod } 85)$ e $10^2 \equiv 15(\text{mod } 85)$, então $10^3 \equiv 15 \cdot 10 \equiv 65(\text{mod } 85)$. Logo $C(10) = 65$.

17. $b_{17} = 2$:

Como $2^3 = 8$ e $8 \equiv 8(\text{mod } 85)$. Logo $C(2) = 8$.

18. $b_{18} = 9$:

Como $9^3 = 9^2 \cdot 9 = 81 \cdot 9$ e $81 \equiv (-4)(\text{mod } 85)$, então $9^3 \equiv (-4) \cdot 9 \equiv -36 \equiv 49(\text{mod } 85)$. Logo $C(9) = 49$.

Portanto, a mensagem codificada é

8-51-21-53-13-61-32-31-41-32-31-51-53-13-8-65-8-49

Agora, o objetivo é decodificar, então será necessário a chave de decodificação $(85, d)$, mas ainda não conhecemos o d. O que sabemos é que d é o inverso de e módulo $\phi(n)$, logo $3 \cdot d \equiv 1(\text{mod } 64)$, o que implica, $64 \cdot k + 3 \cdot (-d) = 1$. Aplicando o método das divisões sucessivas de 64 por 3, temos

64	3	1
1	0	

Disso, segue que $1 = 64 + 3 \cdot (-21)$. Logo, o inverso de 3 módulo 64 é -21, mas precisamos de d positivo, pois usaremos como expoente de potências, então $d = 64 - 21 = 43$ que é o menor inteiro positivo congruente a -21 módulo 64. Agora, já possuímos a chave de decodificação (85, 43) e a fórmula $D(a) \equiv a^d(\text{mod } n)$, então podemos ilustrar o processo de decodificação dos blocos:

1. $a_1 = 8$:

Como $8^3 = 512$, $512 \equiv 2(\text{mod } 85)$ e $43 = 3 \cdot 14 + 1$, temos

$$\begin{aligned} 8^3 &\equiv 2(\text{mod } 85) \\ (8^3)^{14} &\equiv 2^{14} \equiv 16384 \equiv 64(\text{mod } 85) \\ 8^{42} \cdot 8 &\equiv 64 \cdot 8(\text{mod } 85) \\ 8^{43} &\equiv 2(\text{mod } 85). \end{aligned}$$

Logo $D(8) = 2$.

2. $a_2 = 51$:

Como $51^3 = 132651$, $132651 \equiv 51(\text{mod } 85)$ e $43 = 3 \cdot 14 + 1$, temos

$$51^3 \equiv 51(\text{mod } 85)$$

$$\begin{aligned}(51^3)^{14} &\equiv 51^{14} \equiv 51^3 \cdot 51^3 \cdot 51^3 \cdot 51^3 \cdot 51^2 \equiv 51 \cdot 51 \cdot 51 \cdot 51 \cdot 51^2 (\text{mod } 85)\\ 51^{42} &\equiv 51^3 \cdot 51^3 \equiv 51 \cdot 51 (\text{mod } 85)\\ 51^{42} \cdot 51 &\equiv 51 \cdot 51 \cdot 51 \equiv 51^3 \equiv 51 (\text{mod } 85)\\ 51^{43} &\equiv 51 (\text{mod } 85).\end{aligned}$$

Logo $D(51) = 51$.

3. $a_3 = 21$:

Como $21^4 = 194481$, $194481 \equiv 1 (\text{mod } 85)$ e $43 = 4 \cdot 10 + 3$, temos

$$\begin{aligned}21^4 &\equiv 1 (\text{mod } 85)\\ (21^4)^{10} &\equiv 1^{10} \equiv 1 (\text{mod } 85)\\ 21^{40} &\equiv 1 (\text{mod } 85)\\ 21^{40} \cdot 21^3 &\equiv 1 \cdot 21^3 \equiv 9261 \equiv 81 (\text{mod } 85)\\ 21^{43} &\equiv 81 (\text{mod } 85).\end{aligned}$$

Logo $D(21) = 81$.

4. $a_4 = 53$:

Como $53^4 = 7890481$, $7890481 \equiv 16 (\text{mod } 85)$, $16^2 = 256 \equiv 1 (\text{mod } 85)$ e $43 = 4 \cdot 10 + 3$, temos

$$\begin{aligned}53^4 &\equiv 16 (\text{mod } 85)\\ (53^4)^{10} &\equiv 16^{10} \equiv (16^2)^5 \equiv 1^5 \equiv 1 (\text{mod } 85)\\ 53^{40} &\equiv 1 (\text{mod } 85)\\ 53^{40} \cdot 53^3 &\equiv 1 \cdot 53^3 \equiv 148877 \equiv 42 (\text{mod } 85)\\ 53^{43} &\equiv 42 (\text{mod } 85).\end{aligned}$$

Logo $D(53) = 42$.

5. $a_5 = 13$:

Como $13^2 = 169$, $169 \equiv -1 (\text{mod } 85)$ e $43 = 2 \cdot 21 + 1$, temos

$$\begin{aligned}13^2 &\equiv -1 (\text{mod } 85)\\ (13^2)^{21} &\equiv (-1)^{21} \equiv -1 (\text{mod } 85)\\ 13^{42} &\equiv -1 (\text{mod } 85)\\ 13^{42} \cdot 13 &\equiv -1 \cdot 13 \equiv -13 \equiv 72 (\text{mod } 85)\\ 13^{43} &\equiv 72 (\text{mod } 85).\end{aligned}$$

Logo $D(13) = 72$.

6. $a_6 = 61$:

Como $61^4 = 13845841$, $13845841 \equiv 21 (\text{mod } 85)$, $21^4 \equiv 1 (\text{mod } 85)$ e $43 = 4 \cdot 10 + 3$, temos

$$\begin{aligned} 61^4 &\equiv 21 (\text{mod } 85) \\ (61^4)^{10} &\equiv (21)^{10} \equiv (21^4)^2 \cdot 21^2 \equiv 1^2 \cdot 441 \equiv 16 (\text{mod } 85) \\ 61^{40} &\equiv 16 (\text{mod } 85) \\ 61^{40} \cdot 61^3 &\equiv 16 \cdot 226981 \equiv 16 \cdot 31 \equiv 496 \equiv 71 (\text{mod } 85) \\ 61^{43} &\equiv 71 (\text{mod } 85). \end{aligned}$$

Logo $D(61) = 71$.

7. $a_7 = 32$:

Como $32^2 = 1024$, $1024 \equiv 4 (\text{mod } 85)$, $43 = 2 \cdot 20 + 3$, temos

$$\begin{aligned} 32^2 &\equiv 4 (\text{mod } 85) \\ (32^2)^{20} &\equiv 4^{20} \equiv 2^{40} \equiv (2^8)^5 \equiv 1^5 \equiv 1 (\text{mod } 85) \\ 32^{40} \cdot 32^3 &\equiv 1 \cdot 32^2 \cdot 32 \equiv 4 \cdot 32 \equiv 128 \equiv 43 (\text{mod } 85) \\ 32^{43} &\equiv 43 (\text{mod } 85). \end{aligned}$$

Logo $D(32) = 43$.

8. $a_8 = 31$:

Como $31^4 = 923521$, $923521 \equiv 81 \equiv -4 (\text{mod } 85)$, $43 = 4 \cdot 10 + 3$, temos

$$\begin{aligned} 31^4 &\equiv -4 (\text{mod } 85) \\ (31^4)^{10} &\equiv (-4)^{10} \equiv 2^{20} \equiv (2^8)^2 \cdot 2^4 \equiv 1^2 \cdot 16 \equiv 16 (\text{mod } 85) \\ 31^{40} \cdot 31^3 &\equiv 16 \cdot 29791 \equiv 16 \cdot 41 \equiv 61 (\text{mod } 85) \\ 31^{43} &\equiv 61 (\text{mod } 85). \end{aligned}$$

Logo $D(31) = 61$.

9. $a_9 = 41$:

Como $41^4 = 2825761$, $2825761 \equiv 21 (\text{mod } 85)$, $21^4 \equiv 1 (\text{mod } 85)$ e $43 = 4 \cdot 10 + 3$, temos

$$\begin{aligned} 41^4 &\equiv 21 (\text{mod } 85) \\ (41^4)^{10} &\equiv (21)^{10} \equiv (21^4)^2 \cdot 21^2 \equiv (1)^2 \cdot 441 \equiv 1 \cdot 16 \equiv 16 (\text{mod } 85) \\ 41^{40} \cdot 41^3 &\equiv 16 \cdot 68921 \equiv 16 \cdot 71 \equiv 1136 \equiv 31 (\text{mod } 85) \\ 41^{43} &\equiv 31 (\text{mod } 85). \end{aligned}$$

Logo $D(41) = 31$.

10. $a_{10} = 32$:

Como $32^2 = 1024$, $1024 \equiv 4 (\text{mod } 85)$, $43 = 2 \cdot 20 + 3$, temos

$$\begin{aligned} 32^2 &\equiv 4 (\text{mod } 85) \\ (32^2)^{20} &\equiv 4^{20} \equiv 2^{40} \equiv (2^8)^5 \equiv 1^5 \equiv 1 (\text{mod } 85) \\ 32^{40} \cdot 32^3 &\equiv 1 \cdot 32^2 \cdot 32 \equiv 4 \cdot 32 \equiv 128 \equiv 43 (\text{mod } 85) \\ 32^{43} &\equiv 43 (\text{mod } 85). \end{aligned}$$

Logo $D(32) = 43$.

11. $a_{11} = 31$:

Como $31^4 = 923521$, $923521 \equiv 81 \equiv -4 (\text{mod } 85)$, $43 = 4 \cdot 10 + 3$, temos

$$\begin{aligned} 31^4 &\equiv -4 (\text{mod } 85) \\ (31^4)^{10} &\equiv (-4)^{10} \equiv 2^{20} \equiv (2^8)^2 \cdot 2^4 \equiv 1^2 \cdot 16 \equiv 16 (\text{mod } 85) \\ 31^{40} \cdot 31^3 &\equiv 16 \cdot 29791 \equiv 16 \cdot 41 \equiv 61 (\text{mod } 85) \\ 31^{43} &\equiv 61 (\text{mod } 85). \end{aligned}$$

Logo $D(31) = 61$.

12. $a_{12} = 51$:

Como $51^3 = 132651$, $132651 \equiv 51 (\text{mod } 85)$ e $43 = 3 \cdot 14 + 1$, temos

$$\begin{aligned} 51^3 &\equiv 51 (\text{mod } 85) \\ (51^3)^{14} &\equiv 51^{14} \equiv 51^3 \cdot 51^3 \cdot 51^3 \cdot 51^3 \cdot 51^2 \equiv 51 \cdot 51 \cdot 51 \cdot 51 \cdot 51^2 (\text{mod } 85) \\ 51^{42} &\equiv 51^3 \cdot 51^3 \equiv 51 \cdot 51 (\text{mod } 85) \\ 51^{42} \cdot 51 &\equiv 51 \cdot 51 \cdot 51 \equiv 51^3 \equiv 51 (\text{mod } 85) \\ 51^{43} &\equiv 51 (\text{mod } 85). \end{aligned}$$

Logo $D(51) = 51$.

13. $a_{13} = 53$:

Como $53^4 = 7890481$, $7890481 \equiv 16 (\text{mod } 85)$, $16^2 = 256 \equiv 1 (\text{mod } 85)$ e $43 = 4 \cdot 10 + 3$, temos

$$\begin{aligned} 53^4 &\equiv 16 (\text{mod } 85) \\ (53^4)^{10} &\equiv 16^{10} \equiv (16^2)^5 \equiv 1^5 \equiv 1 (\text{mod } 85) \\ 53^{40} &\equiv 1 (\text{mod } 85) \end{aligned}$$

$$\begin{aligned} 53^{40} \cdot 53^3 &\equiv 1 \cdot 53^3 \equiv 148877 \equiv 42 (\text{mod } 85) \\ 53^{43} &\equiv 42 (\text{mod } 85). \end{aligned}$$

Logo $D(53) = 42$.

14. $a_{14} = 13$:

Como $13^2 = 169$, $169 \equiv -1 (\text{mod } 85)$ e $43 = 2 \cdot 21 + 1$, temos

$$\begin{aligned} 13^2 &\equiv -1 (\text{mod } 85) \\ (13^2)^{21} &\equiv (-1)^{21} \equiv -1 (\text{mod } 85) \\ 13^{42} &\equiv -1 (\text{mod } 85) \\ 13^{42} \cdot 13 &\equiv -1 \cdot 13 \equiv -13 \equiv 72 (\text{mod } 85) \\ 13^{43} &\equiv 72 (\text{mod } 85). \end{aligned}$$

Logo $D(13) = 72$.

15. $a_{15} = 8$:

Como $8^3 = 512$, $512 \equiv 2 (\text{mod } 85)$ e $43 = 3 \cdot 14 + 1$, temos

$$\begin{aligned} 8^3 &\equiv 2 (\text{mod } 85) \\ (8^3)^{14} &\equiv 2^{14} \equiv 16384 \equiv 64 (\text{mod } 85) \\ 8^{42} \cdot 8 &\equiv 64 \cdot 8 (\text{mod } 85) \\ 8^{43} &\equiv 2 (\text{mod } 85). \end{aligned}$$

Logo $D(8) = 2$.

16. $a_{16} = 65$:

Como $65^3 = 274625$, $274625 \equiv 75 \equiv -10 (\text{mod } 85)$, $10^2 \equiv 100 \equiv 15 (\text{mod } 85)$, $15^5 \equiv 759375 \equiv 70 (\text{mod } 85)$ e $43 = 3 \cdot 14 + 1$, temos

$$\begin{aligned} 65^3 &\equiv -10 (\text{mod } 85) \\ (65^3)^{14} &\equiv (-10)^{14} \equiv (10^2)^7 \equiv 15^7 \equiv 15^5 \cdot 15^2 \equiv 70 \cdot 225 \equiv 70 \cdot 55 \equiv 3850 \equiv 25 (\text{mod } 85) \\ 65^{42} \cdot 65 &\equiv 25 \cdot 65 \equiv 1625 \equiv 10 (\text{mod } 85) \\ 65^{43} &\equiv 10 (\text{mod } 85). \end{aligned}$$

Logo $D(65) = 10$.

17. $a_{17} = 8$:

Como $8^3 = 512$, $512 \equiv 2 (\text{mod } 85)$ e $43 = 3 \cdot 14 + 1$, temos

$$8^3 \equiv 2 (\text{mod } 85)$$

$$\begin{aligned}(8^3)^{14} &\equiv 2^{14} \equiv 16384 \equiv 64(\text{mod } 85)\\ 8^{42}\cdot 8 &\equiv 64\cdot 8(\text{mod } 85)\\ 8^{43} &\equiv 2(\text{mod } 85).\end{aligned}$$

Logo $D(8) = 2$.

18. $a_{18} = 49$:

Como $49^2 = 2401$, $2401 \equiv 21(\text{mod } 85)$, $21^4 \equiv 1(\text{mod } 85)$ e $43 = 2\cdot 21 + 1$, temos

$$\begin{aligned}49^2 &\equiv 21(\text{mod } 85)\\ (49^2)^{21} &\equiv 21^{21} \equiv (21^4)^5\cdot 21 \equiv 1^5\cdot 21 \equiv 21(\text{mod } 85)\\ 49^{42}\cdot 49 &\equiv 21\cdot 49 \equiv 1029 \equiv 9(\text{mod } 85)\\ 49^{43} &\equiv 9(\text{mod } 85).\end{aligned}$$

Logo $D(49) = 9$.

Logo, a sequência decodificada será

2-51-81-42-72-71-43-61-31-43-61-51-42-72-2-10-2-9,

reescrevendo a sequência temos

25-18-14-27-27-14-36-13-14-36-15-14-27-22-10-29.

Agora, já podemos fazer a conversão para letras usando a tabela da seção 3.1:

P-I-E-R-R-E–D-E–F-E-R-M-A-T.

Portanto, a mensagem é PIERRE DE FERMAT, assim concluindo a decodificação e o nosso exemplo do método.

Observação 3.1. *Para tomarmos $e = 3$ e não encontrarmos problemas na obtenção de d na decodificação, é preciso escolhermos p e q ambos congruentes a 5 módulo 6, pois isso garante que sempre teremos 3 inversível módulo $\phi(n)$ e será fácil obter o valor do número d. Por exemplo, sejam $p = 5$ e $q = 7$, então $n = p\cdot q = 5\cdot 7 = 35$ e $\phi(n) = (p-1)\cdot(q-1) = 4\cdot 6 = 24$. Tomando $e = 3$ que é divisor de 24, não existe o inverso de 3 módulo 24 ($3\cdot d \not\equiv 1(mod\ 24)$).*

Capítulo 4

Sequências didáticas

A Base Nacional Comum Curricular (2017, p. 16 - 17) elenca um rol de medidas para assegurar as aprendizagens essenciais definidas para cada etapa da Educação Básica, dentre as quais estão:

- Contextualizar os conteúdos dos componentes curriculares, identificando estratégias para apresentá-los, representá-los, exemplificá-los, conectá-los e torná-los significativos, com base na realidade do lugar e do tempo nos quais as aprendizagens estão situadas;
- Conceber e pôr em prática situações e procedimentos para motivar e engajar os alunos nas aprendizagens;

Diante disso, neste capítulo apresentaremos atividades que envolvem conteúdos matemáticos e criptografia. O objetivo é fornecer ideias aos professores para tornar dinâmica as aulas de matemática, e até mesmo lúdicas, com formação de grupos, participação em jogos e com o uso de materiais manipuláveis. Assim, a criptografia possibilitará ao professor trazer mais sentido e significado aos conteúdos matemáticos para os alunos.

4.1 Atividade 1 - Cifra de substituição e porcentagem

Objetivos da atividade: Coletar, organizar e registrar dados; Representar um número na forma fracionária e decimal; Calcular porcentagens.

Conteúdos relacionados: Estatística, Número decimal, Número Fracionário e Porcentagem.

A atividade destina-se ao 6º ano do Ensino Fundamental.

Duração estimada: 6 aulas.

Materiais: Quadro, giz, lápis, borracha, caderno, papel, régua e tesoura.

Descrição da atividade:

O professor fará uma breve introdução sobre Criptografia, falando sobre seu significado, onde era utilizada a escrita secreta antigamente e na atualidade, citando alguns métodos. E então cada aluno, com o auxílio do professor, construirá o instrumento de criptografia abaixo, que trata-se de duas réguas que possuem o alfabeto em vez de números, sendo uma delas deslizante, o que possibilita o deslocamento do alfabeto, conforme a chave para cifrar.

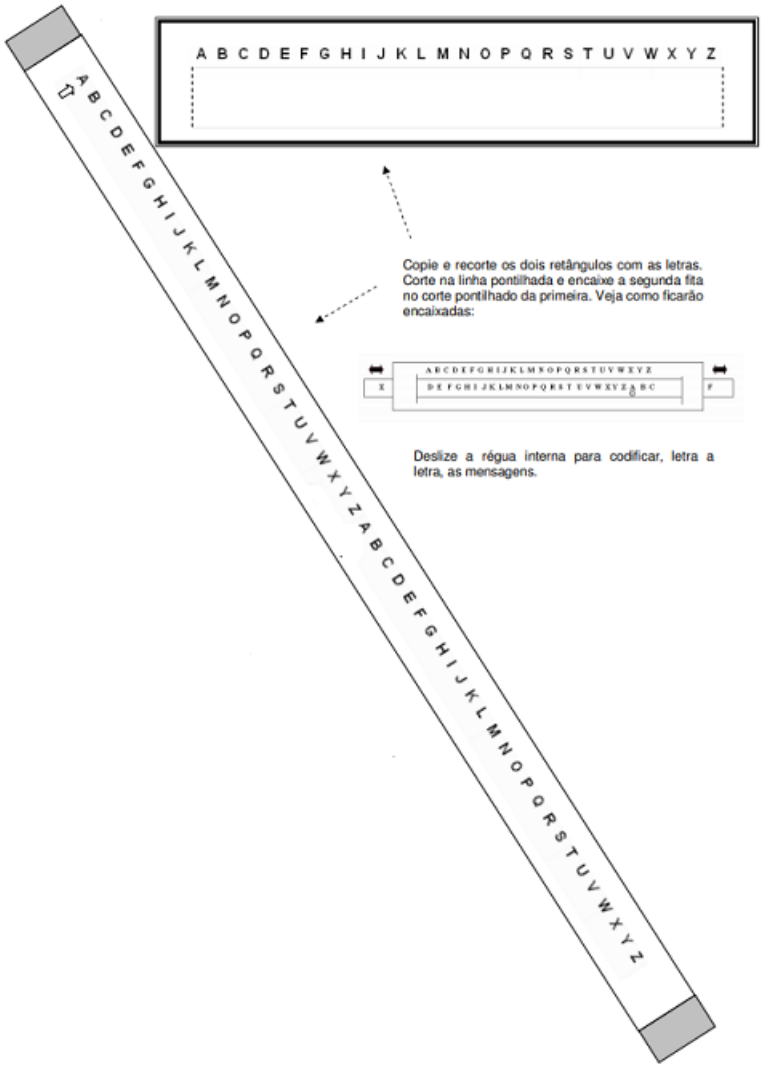


Figura 4.1: Régua de Cifra de substituição

Fonte: *http : //www.mat.ufpb.br/bienalsbm/arquivos/Oficinas/PedroMalagutti − TemasInterdisciplinares/Aprendendo_Criptologia_de_Forma_Divertida_Final.pdf*

O professor pode iniciar com a Cifra de César para codificar a palavra "MATEMÁTICA", sendo a chave o número 3, ou seja, o alfabeto será deslocado três casas, obtendo o seguinte alfabeto cifrado:

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

Mensagem original	M	A	T	E	M	Á	T	I	C	A
Mensagem codificada	p	d	w	h	p	d	w	l	f	d

Na sequência, poderá estimular os alunos a codificarem outras palavras, inclusive alterando a chave, ou seja, usando outros deslocamentos no alfabeto, também mencionando que o alfabeto pode ser substituído por números ou outros símbolos, ou o alfabeto cifrado pode ser embaralhado de diversas formas.

Depois dessa interação dos alunos, o professor explicará que a cifra de substituição é muito frágil, pois há muitos anos atrás, os criptoanalistas descobriram a análise de frequência das letras no texto, técnica capaz de quebrar essa cifra, tornando-a muito insegura. A análise de frequência é possível pois a frequência média das letras nos textos da língua portuguesa, e até mesmo de outros idiomas, é quase constante, conforme Tabela 1.4.

Neste momento da aula, o professor pode apresentar um texto codificado, e solicitar aos alunos que contem a quantidade de letras do texto, depois a quantidade de cada uma das letras do alfabeto, e então preencher a coluna "Frequência" da Tabela 4.1. A atividade pode ser realizada em grupo, mas cada aluno com sua tabela, o texto poderá ser dividido entre os alunos do grupo, e no final, eles podem unir as informações. A seguir, vamos apresentar uma sugestão de texto codificado, que possui no total 350 letras:

> "Glwlh xlmsvxvn l evosl qltl wz evosz. L qltl wz evosz v gzl evosl jfv mrmtfvn hv ovnyiz wv jfzmwl xlnvxlf z qltz- ol xln hvfh znrtlh wl xlovtrl. Xlrhz wz rmuzmxrz. Vmgivgzmgl, kziz lh xfirlhlh, l qltl wz evosz ulr fnz lgrnz lkligfmrwzwv kziz izxrlxrmzi v gvmgzi wvhvmeloevi fnz vhgizgvtrz kziz tzmszi. Zh xirzmxzh jfv kvmhzizn ml qltl kvixvyvizn jfv hfv hl hv tzmsz jfzmwl l zwevihzirl qltz nzo, nzh, kli lfgil ozwl, v klhhrevo mfmxz kviwvi."

Na sequência, o professor solicitará aos alunos o preenchimento das outras colunas da Tabela 4.1, onde os alunos representarão a frequência na forma fracionária, sabendo que o total de letras do texto é 350; e então farão os cálculos para representar na forma decimal e, posteriormente, calcularão a porcentagem:

Letra	Frequência	Fração	Decimal	Porcentagem(%)
A	0	$\frac{0}{350}$	0,000	0%
B	0	$\frac{0}{350}$	0,000	0%
C	0	$\frac{0}{350}$	0,000	0%
D	0	$\frac{0}{350}$	0,000	0%
E	9	$\frac{9}{350}$	0,026	2,6%
F	14	$\frac{14}{350} = \frac{1}{25}$	0,04	4%
G	12	$\frac{12}{350} = \frac{6}{175}$	0,034	3,4%
H	20	$\frac{20}{350} = \frac{2}{35}$	0,057	5,7%
I	23	$\frac{23}{350}$	0,066	6,6%
J	5	$\frac{5}{350} = \frac{1}{70}$	0,014	1,4%
K	9	$\frac{9}{350}$	0,026	2,6%
L	49	$\frac{49}{350} = \frac{7}{50}$	0,14	14%
M	20	$\frac{20}{350} = \frac{2}{35}$	0,057	5,7%
N	13	$\frac{13}{350}$	0,037	3,7%
O	12	$\frac{12}{350} = \frac{6}{175}$	0,034	3,4%
P	0	$\frac{0}{350}$	0,000	0%
Q	6	$\frac{6}{350} = \frac{3}{175}$	0,017	1,7%
R	16	$\frac{16}{350} = \frac{8}{175}$	0,046	4,6%
S	8	$\frac{8}{350} = \frac{4}{175}$	0,023	2,3%
T	12	$\frac{12}{350} = \frac{6}{175}$	0,034	3,4%
U	2	$\frac{2}{350} = \frac{1}{175}$	0,006	0,6%
V	38	$\frac{38}{350} = \frac{19}{175}$	0,109	10,9%
W	1	$\frac{15}{350} = \frac{3}{70}$	0,043	4,3%
X	15	$\frac{15}{350} = \frac{3}{70}$	0,043	4,3%
Y	2	$\frac{2}{350} = \frac{1}{175}$	0,006	0,6%
Z	50	$\frac{50}{350} = \frac{1}{7}$	0,143	14,3%

Tabela 4.1: Contando a frequência relativa

Prosseguindo, o professor solicitará que os alunos comparem os dados das Tabelas 1.4 e 4.1. Uma sugestão, é que a comparação ocorra através de gráficos. A frequência das letras na língua portuguesa, segue a ordem: A, E, O, S, R, I, N, ...; no texto codificado a frequência das letras segue a ordem: Z, L, V, I, H, M, R, ... A partir disso, é possível levantar algumas conjecturas, por exemplo, "o A foi substituído pelo Z", "o E foi substituído pelo L", ou ainda, "o E foi substituído pelo V", pois apesar de a letra V não ser a segunda letra mais frequente do texto codificado, isso pode acontecer, as frequências poderão variar.

Alfabeto original	Porcentagem(%)	Alfabeto cifrado	Porcentagem(%)
A	14,63%	A	0%
B	1,04%	B	0%
C	3,88%	C	0%
D	4,99%	D	0%
E	12,57%	E	2,6%
F	1,02%	F	4%
G	1,30%	G	3,4%
H	1,28%	H	5,7%
I	6,18%	I	6,6%
J	0,40%	J	1,4%
K	0,02%	K	2,6%
L	2,78%	L	14%
M	4,74%	M	5,7%
N	5,05%	N	3,7%
O	10,73%	O	3,4%
P	2,52%	P	0%
Q	1,20%	Q	1,7%
R	6,53%	R	4,6%
S	7,81%	S	2,3%
T	4,34%	T	3,4%
U	4,63%	U	0,6%
V	1,67%	V	10,9%
W	0,01%	W	4,3%
X	0,21%	X	4,3%
Y	0,01%	Y	0,6%
Z	0,47%	Z	14,3%

Para decodificar o texto, os alunos poderão observar características da língua portuguesa, como palavras de duas ou três letras, os dígrafos, o que facilitará a decodificação. Para verificação, o texto codificado acima é o seguinte:

> "Todos conhecem o velho jogo da velha. O jogo da velha é tão velho que ninguém se lembra de quando começou a jogá-lo com seus amigos do colégio. Coisa da infância. Entretanto, para os curiosos, o jogo da velha foi uma ótima oportunidade para raciocinar e tentar desenvolver uma estratégia para ganhar. As crianças que pensaram no jogo perceberam que só se ganha quando o adversário joga mal, mas, por outro lado, é possível nunca perder (Wagner, 2015, p. 42)."

Outra sugestão, é a formulação de questões sobre a Tabela 4.1, por exemplo:

1. Qual o tipo de letra mais frequente no texto, vogal ou consoante? Das vogais qual a de maior e a de menor frequência? A soma da frequência das vogais é maior ou menor que a soma das frequências das consoantes?

2. Que porcentagem das letras no texto codificado eram letra T?

3. Aproximadamente, quantos Ts você esperaria em um texto de 100 letras?

4. Escreva as letras do texto codificado em ordem, da mais comum para menos comum.

(Essa atividade foi adaptada das referências "Aprendendo Criptologia de Forma Divertida" (p. 22 - 23 - 24 - 25 - 27), BEISSINGER e PLESS (2006, p. 24 - 25 - 26) e REIS (2020, p. 74).)

4.2 Atividade 2 - Abordar o cálculo de potências com expoentes inteiros através da Criptografia RSA

Objetivos da atividade: Identificar os múltiplos de um número; Reconhecer números primos em um determinado conjunto de números; Realizar cálculos envolvendo as operações de adição, subtração, multiplicação e divisões; Efetuar cálculos com potências de expoentes inteiros.

Conteúdos relacionados: Múltiplos de um número; números primos; operações de adição, subtração, multiplicação e divisão; e potenciação.

A atividade destina-se ao 8º ano do Ensino Fundamental.

Duração estimada: 4 aulas.

Materiais: Quadro, lápis, papel, borracha, cartões numerados de 1 a 100, fita adesiva, Crivos de Eratóstenes de 0 a 150 impressos em folha sulfite (o número depende da quantidades de alunos), caderno e calculadora.

Descrição da atividade:

Essa atividade é composta por várias etapas menores. Na primeira etapa, usaremos o Crivo de Eratóstenes para identificar os números primos existentes entre 1 e 100. Os alunos formarão duplas. Os cartões numerados de 1 a 100 serão colados com fita adesiva no quadro em ordem crescente, formando uma tabela de 10 linhas e 10 colunas. O professor apresenta o Crivo de Eratóstenes aos alunos e remove o número 1, na sequência, os alunos executarão as seguintes tarefas no Crivos de Eratóstenes que receberão impresso em folha sulfite:

1. Pinte todo o quadrado que contém o número 1 de preto.
2. Circule o número 2 e risque todos os seus múltiplos.
3. Circule o número 3 e risque todos os seus múltiplos.
4. Circule o número 5 e risque todos os seus múltiplos.
5. Continue esse processo até que não haja mais números a serem riscados ou circulados.

Concomitantemente, duplas serão sorteadas para que removam do quadro os cartões que possuem múltiplos de 2, múltiplos de 3, e assim sucessivamente.

Ao final, os alunos perceberão que restaram (ou que foram circulados) os números 2,3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 e 97, estes são todos os números primos entre 1 e 100.

Para complementar a atividade do Crivo de Eratóstenes e aulixar na compreensão, o professor poderá propor as seguintes questões:

1. Existe algum número primo que é par? Se sim, quantos primos são pares? Por que isso acontece?
2. Podemos concluir que os números que são múltiplos 2, 3, 5, 7, e dos demais números primos, não podem ser números primos. Porque isso acontece? Qual é a relação existente entre um número ser múltiplo de outro, e os seus divisores?
3. Encontre os números primos de 0 a 150. (TAREFA DE CASA)

(A atividade acima foi adaptada das referências SILVA (2019, p. 85) e do site Laboratório Sustentável de Matemática.)

Na segunda etapa, o professor fará uma breve explanação aos alunos sobre a história da criptografia, contando sobre a evolução dos algoritmos. E então abordará a cifra de substituição, substituindo as letras por números, fazendo uso da tabela abaixo:

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

Cifrando a palavra **PRIMO**, os alunos obterão a mensagem codificada **25-27-18-22-24** ou **2527182224**.

O professor argumentará a respeito da segurança das cifras. A partir disso introduzirá a criptografia RSA, os alunos deverão criptografar a palavra PRIMO, ou ainda, **2527182224**. No entanto, o processo apresentado no Capítulo 3 será simplificado, em vez de a chave pública n ser igual ao produto de dois números primos, será utilizado apenas um número primo, e não será mencionado o conceito de congruência. Dessa forma, a chave será $n = p$ e $\phi(n) = p - 1$.

No exemplo apresentado aos alunos, será adotado $n = 23$ e $e = 3$ como chave pública. Como a palavra PRIMO, já foi transformada em uma sequência numérica **2527182224**, é necessário dividi-la em blocos menores que $n = 23$, ou seja, **2 - 5 - 2 - 7 - 18 - 22 - 2 - 4**.

Seja b um bloco, o bloco b codificado é igual ao resto da divisão de b^e por n. Ou seja, para o bloco $b = 2$, temos $2^3 = 8$, dividindo-o por 23, temos $8 = 0 \cdot 23 + 8$.

Denotando por $C(b)$ o bloco codificado, então $C(2) = 8$. Repetindo os processos para os outros blocos obtemos:

C(2)=8; C(5)=10; C(2)=8; C(7)=21; C(18)=13; C(22)=22; C(2)=8; C(4)=18.

Logo, a mensagem codificada é **8 - 10 - 8 - 21 - 13 - 22 - 8 - 18**.

O professor poderá codificar os primeiros blocos, e solicitar aos alunos que codifiquem os próximos, e também que codifiquem outras palavras repetindo o processo.

A última etapa da atividade é o processo de decodificação, o que implica na determinação do valor de d. O professor explicará que d é igual ao número que multiplicado por e deixa resto 1 na divisão por $\phi(23) = 23 - 1 = 22$. Nesse caso, $d = 15$, pois $15 \cdot 3 = 45 = 2 \cdot 22 + 1$. Portanto a chave privada é (23, 15).

Seja a um bloco codificado, o bloco a decodificado é igual ao resto da divisão de a^d por n. Ou seja, para o bloco $a = 8$, temos 8^{15} dividindo-o por 23, o resto é 2. Como em alguns casos a potência é muito grande, o aluno poderá usar a calculadora. Nesse momento, o professor poderá levantar a questão sobre a escolha de números grandes como chave pública, assegurando a segurança da criptografia RSA, pois para alguns números, até mesmo computadores extremamente potentes não são capazes de obter a chave privada para assim decodificar a mensagem secreta.

(Essa atividade foi adaptada das referências SILVA (2019, p. 77 - 78 - 79) e OKUMURA (2014, p. 26 - 27).)

4.3 Atividade 3 - Abordar o cálculo de matriz inversa através de criptografia

Objetivos da atividade: Efetuar a operação de multiplicação entre matrizes; Obter a matriz inversa de uma matriz 2×2.

Conteúdos relacionados: Matrizes; Multiplicação de matrizes; Matriz inversa.

A atividade destina-se ao 2º ano do Ensino Médio.

Duração estimada: 3 aulas.

Materiais: Quadro, giz, lápis, borracha, caderno e papel.

Descrição da atividade:

O professor pode iniciar com uma introdução sobre a história da criptografia, e então explicar aos alunos que farão uma atividade usando criptografia e solicitar que os alunos formem duplas, sendo um aluno o remetente e o outro destinatário.

Na primeira etapa, os alunos remetentes receberão a chave do professor, que trata-se de uma matriz quadrada de ordem 2, invertível, cujos elementos são todos inteiros, que é chamada de matriz codificadora. Seja A a matriz codificadora de ordem 2 e invertível, ou seja, existe uma matriz B de mesma ordem tal que

$$A \cdot B = B \cdot A = I,$$

onde I é a matriz identidade de ordem 2. A matriz B será a matriz decodificadora. Como sugestão, temos:

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

O professor solicitará aos alunos remetentes que codifiquem a palavra "NÚMERO PRIMO". Para isso, farão a substituição, conforme tabela abaixo, das letras das palavras por números.

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

O espaço entre as palavras será o número 0. Caso seja necessário outro símbolo, o remetente e o destinatário deverão combinar previamente.

Após a substituição, obterão a seguinte sequência numérica:

14 - 21 - 13 - 5 - 18 - 15 - 0 - 16 - 18 - 9 - 13 - 15.

Continuando o processo, os alunos remetentes deverão separar a sequência acima, em grupos de dois números consecutivos, ou seja,

14 21 - 13 5 - 18 15 - 0 16 - 18 9 - 13 15,

que formarão as seguintes matrizes coluna 2×1:

$$\begin{bmatrix} 14 \\ 21 \end{bmatrix}, \begin{bmatrix} 13 \\ 5 \end{bmatrix}, \begin{bmatrix} 18 \\ 15 \end{bmatrix}, \begin{bmatrix} 0 \\ 16 \end{bmatrix}, \begin{bmatrix} 18 \\ 9 \end{bmatrix}, \begin{bmatrix} 13 \\ 15 \end{bmatrix}$$

No caso da mensagem possuir um número ímpar de elementos, completamos a mensagem com o número 0, que corresponde ao espaço entre as palavras.

Para codificar, eles deverão multiplicar à esquerda pela matriz A cada uma das matrizes coluna acima, ou seja,

$$\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 14 \\ 21 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 13 \\ 5 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 18 \\ 15 \end{bmatrix},$$

$$\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 16 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 18 \\ 9 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 13 \\ 15 \end{bmatrix},$$

o que resulta em,

$$\begin{bmatrix} 49 \\ 35 \end{bmatrix}, \begin{bmatrix} 31 \\ 18 \end{bmatrix}, \begin{bmatrix} 51 \\ 33 \end{bmatrix}, \begin{bmatrix} 16 \\ 16 \end{bmatrix}, \begin{bmatrix} 45 \\ 27 \end{bmatrix}, \begin{bmatrix} 41 \\ 28 \end{bmatrix}.$$

Logo, a mensagem codificada e transmitida ao destinatário será,

49 - 35 - 31 - 18 - 51 - 33 - 16 - 16 - 45 - 27 - 41 - 28.

O professor pode chamar atenção dos alunos em relação ao fato de a mensagem codificada quase não possuir repetições, o que dificulta a análise de frequência.

Quando os alunos destinatários receberem a mensagem codificada, eles precisarão calcular a matriz B inversa de A, que decodificará a mensagem. Nesse caso, temos

$$B = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}.$$

E então, calcular os seguintes produtos entre a matriz B e as matrizes codificadas:

$$\begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 49 \\ 35 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 31 \\ 18 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 51 \\ 33 \end{bmatrix},$$

$$\begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 16 \\ 16 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 45 \\ 27 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 41 \\ 28 \end{bmatrix},$$

o que resulta em,

$$\begin{bmatrix} 14 \\ 21 \end{bmatrix}, \begin{bmatrix} 13 \\ 5 \end{bmatrix}, \begin{bmatrix} 18 \\ 15 \end{bmatrix}, \begin{bmatrix} 0 \\ 16 \end{bmatrix}, \begin{bmatrix} 18 \\ 9 \end{bmatrix}, \begin{bmatrix} 13 \\ 15 \end{bmatrix}.$$

Ou ainda,

14 - 21 - 13 - 5 - 18 - 15 - 0 - 16 - 18 - 9 - 13 - 15,

o que corresponde a seguinte mensagem, conforme a tabela do início da atividade,

NÚMERO PRIMO.

O professor pode propor que o remente passe a ocupar a função de destinatário e vice-versa. E também, que criem suas próprias mensagens e escolham suas matrizes codificadoras.

(Essa atividade foi adaptada da referência EDWARDS e PENNEY (1998, p. 61 - 62 - 63 - 64)).

Referências

ANTUNES, C. M. **Métodos de Fatoração de Números Inteiros**. Dissertação (Mestrado)- Universidade Federal do Rio Grande do Sul, Programa de Pós-Graduação em Matemática Aplicada, Porto Alegre, 2002.

BEISSINGER , J; PLESS, V. **The Cryptoclub Workbook: Using Mathematics to Make and Break Secret Codes**. Wellesley: A K Peters/CRC Press, 2006.

BOYER, C. B; MERZBACH, U. C. **História da matemática**, 3 ed. - São Paulo: Blucher, 2012.

CARNEIRO, F. J. F. **Criptografia e Teoria do Números**. Rio de Janeiro: Editora Ciência Moderna Ltda., 2017.

COUTINHO, S. **Números Inteiros e Criptografia RSA**. 2 ed. Rio de Janeiro: IMPA, 2005.

DOMINGUES, H. H.; IEZZI, G. **Álgebra Moderna**. 4 ed. reformulada. São Paulo: Atual, 2003.

EDWARDS, C. H. J., PENNEY, D. E. **Introdução à Álgebra Linear**. Tradução: João Paulo Cursino dos Santos, José Antônio e Souza, Zaira Geriballo de Arruda Botelho. Rio de Janeiro: Prentice- Hall do Brasil Ltda, 1998.

FIARRESGA, V. M. C. **Criptografia e Matemática**. Dissertação (Mestrado)- Universidade de Lisboa, 2010.

HEFEZ, A. **Exercícios resolvidos de Aritmética**. 1ª ed. Rio de Janeiro: SBM, 2016.

HOWARD, A.; RORRES, C. **Álgebra linear com aplicações**; trad. Claus Ivo Doering. 8ª ed. Porto Alegre: Bookman, 2001.

OKUMURA, M. K. **Números primos e criptografia RSA**. Dissertação (Mestrado em Matemática) - Instituto de Ciências Matemáticas e de Computação – Universidade de São Paulo. São Carlo, 2014.

REIS, M. S. dos. **Criptografia: um estudo histórico e aplicado a matemática do ensino básico**. Dissertação (Mestrado Profissionalizante em Matemática) - Unidade de Dourados - Universidade Estadual de Mato Grosso do Sul. Dourados, 2020.

SANTOS, J. P. O. **Introdução à Teoria do Números**. 3ª ed. Rio de Janeiro: IMPA, 2020.

SILVA, J. C.; GOMES, O. R. **Estruturas Algébricas para Licenciatura: Elementos de Aritmética Superior**. V. 2. São Paulo: Blucher, 2018.

SILVA, V. B. da. **Números Primos e Criptografia: do Conceito ao Sistema RSA**. Dissertação (Mestrado em Matemática) - Universidade Federal do Tocantins. Arraias, 2019.

SINGH, S. **O livro dos códigos**. 5ª ed. Rio de Janeiro: Record, 2005.

STALLINGS, W. **Criptografia e segurança de redes: princípios e práticas**. 6. ed. São Paulo: Pearson, 2015.

TKOTZ, V. **Criptografia - Segredos Embalados para Viagem**. [S.l.: s.n.], 2005.

WAGNER, E. O jogo da velha em 3D. **RPM - Revista do Professor de Matemática**, Rio de Janeiro, nº 87, p. 42, 2º quadrimestre de 2015.

Base Nacional Comum Curricular. Disponível em: $\langle http://basenacionalcomum.mec.gov.br/\rangle$. Acessado em: 08 de ago. de 2021.

Aprendendo Criptologia de Forma Divertida. Disponível em: $\langle http://www.mat.ufpb.br/bienalsbm/arquivos/Oficinas/PedroMalagutti-Temas\ Interdisciplinares/Aprendendo\_Criptologia\_de\_Forma\_Divertida\_Final.pdf\rangle$. Acessado em: 08 de ago. de 2021.

Descoberto número primo com quase 25 milhões de dígitos. **IMPA: Instituto de Matemática Pura e Aplicada**, 2019. Disponível em: $\langle https://impa.br/noticias/descoberto-numero-primo-com-quase-25-milhoes-de-digitos/\rangle$. Acessado em: 05 de jul. de 2021.

Leve o Crivo de Eratóstenes para ensinar números primos na sua turma de sexto ano! Atividade disponível para download!! Por prof. Daniel Lucas. **Laboratório Sustentável de Matemática**, 2018. Disponível em: $\langle https://www.laboratoriosustentaveldematematica.com/2018/08/o-crivo-de-erastostenes-na-sua-turma-de-6-ano.html\rangle$. Acessado em: 01 de ago. de 2021.

Por que a descoberta do maior número primo importa?. **IMPA:**

Instituto de Matemática Pura e Aplicada, 2019. Disponível em: $\langle https://impa.br/noticias/por-que-a-descoberta-do-maior-numero-primo-importa/\rangle$. Acessado em: 16 de jul. de 2021.