Alex Almeida Rosa

Uso da Criptografia RSA no Ensino de Matemática

Vitória

2023

Alex Almeida Rosa

Uso da Criptografia RSA no Ensino de Matemática

Dissertação de mestrado apresentada ao PROFMAT como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

Orientador: Prof. Dr. Alcebíades Dal Col Júnior

Vitória

2023

Ficha catalográfica disponibilizada pelo Sistema Integrado de Bibliotecas - SIBI/UFES e elaborada pelo autor

---

Rosa, Alex Almeida, 1979-
R788u Uso da criptografia RSA no ensino de matemática / Alex Almeida Rosa. - 2023.
115 f. : il.

Orientador: Alcebíades Dal Col Júnior.
Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Federal do Espírito Santo, Centro de Ciências Exatas.

1. Criptografia. 2. Números primos. 3. Teoria dos números. I. Dal Col Júnior, Alcebíades. II. Universidade Federal do Espírito Santo. Centro de Ciências Exatas. III. Título.

CDU: 51

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

Centro de Ciências Exatas

Programa de Pós-Graduação em Matemática em Rede Nacional – PROFMAT

“Uso da Criptografia RSA no Ensino de Matemática”

Alex Almeida Rosa

Defesa de Dissertação de Mestrado Profissional submetida ao Programa de Pós-Graduação em Matemática em Rede Nacional da Universidade Federal do Espírito Santo como requisito parcial para a obtenção do título de Mestre em Matemática.

Aprovada em 24/08/2023 por:

_____

Prof.(a) Dr.(a) Alcebíades Dal Col Júnior
Orientador(a) – UFES

_____

Prof.(a) Dr.(a) Alancardek Pereira Araújo
Membro Interno – UFES

_____

Prof.(a) Dr.(a) Fidelis Zanetti de Castro
Membro Externo – IFES

Documento assinado eletronicamente nos moldes do art. 10 da MP 2200/01 e Lei 14063/20
[Hash SHA256] a640076778cedaa53fcdd7cfe28a717374abc8a50ea425fa7604c5b24cbdc133

Datas e horários baseados em Brasília, Brasil
Sincronizado com o NTP.br e Observatório Nacional (ON) em 25/08/2023 às 09:28:35

Folha de Assinaturas Alex Almeida Rosa

Data e Hora de Criação: 25/08/2023 às 08:20:30

Documentos que originaram esse envelope:
- Folha de Assinaturas Alex Almeida Rosa.pdf (Arquivo PDF) - 1 página(s)

Hashs únicas referente à esse envelope de documentos

[SHA256]: a640076778cedaa53fcdd7cfe28a717374abc8a50ea425fa7604c5b24cbdc133
[SHA512]: c346578a3729dd4c832ca2e21682eb9607a3e59b436428846c9796cea5559f1c197928fc6f89cf7a7c5c0ae0e3c8510dddd7900660ed6e3eb29ebdae8024e0d0

Lista de assinaturas solicitadas e associadas à esse envelope

ASSINADO - Alancardek Pereira Araújo (alancardek.araujo@ufes.br)
Data/Hora: 25/08/2023 - 09:28:35, IP: 177.97.119.245, Geolocalização: [-20.291750, -40.298641]
[SHA256]: 44396a6cd755cc5360ca6b5a68bafd65eda8a453284d42afc6b2776076b88cbe

Alancardek Pereira Araujo

ASSINADO - Alcebíades Dal Col Júnior (alcebiades.col@ufes.br)
Data/Hora: 25/08/2023 - 08:42:40, IP: 179.66.165.178, Geolocalização: [-20.344101, -40.389373]
[SHA256]: 9f3e0e89e4608879642f4a3ace7e0f506cdec1ae97ba27996171854a097da2dd

ASSINADO - Fidelis Zanetti de Castro (fidelis.castro@gmail.com)
Data/Hora: 25/08/2023 - 08:26:21, IP: 191.30.49.97, Geolocalização: [-20.191690, -40.266115]
[SHA256]: 718aeb7596ca5a25375f8610ff54b22223a336de91633e654646af4bd4fde446

Histórico de eventos registrados neste envelope

25/08/2023 09:28:35 - Envelope finalizado por alancardek.araujo@ufes.br, IP 177.97.119.245
25/08/2023 09:28:35 - Assinatura realizada por alancardek.araujo@ufes.br, IP 177.97.119.245
25/08/2023 09:28:22 - Envelope visualizado por alancardek.araujo@ufes.br, IP 177.97.119.245
25/08/2023 08:42:40 - Assinatura realizada por alcebiades.col@ufes.br, IP 179.66.165.178
25/08/2023 08:41:58 - Envelope visualizado por alcebiades.col@ufes.br, IP 179.66.165.178
25/08/2023 08:26:21 - Assinatura realizada por fidelis.castro@gmail.com, IP 191.30.49.97
25/08/2023 08:26:13 - Envelope visualizado por fidelis.castro@gmail.com, IP 191.30.49.97
25/08/2023 08:21:51 - Envelope registrado na Blockchain por ivan.barbosa@ufes.br, IP 200.137.65.107
25/08/2023 08:21:50 - Envelope encaminhado para assinaturas por ivan.barbosa@ufes.br, IP 200.137.65.107
25/08/2023 08:20:30 - Envelope criado por ivan.barbosa@ufes.br, IP 200.137.65.107

Documento em conformidade com o padrão de assinatura digital ICP-Brasil e validado de acordo com o Instituto Nacional de Tecnologia da Informação

Os registros de assinatura presentes nesse documento pertencem única e exclusivamente a esse envelope.
Documento final gerado e certificado por **Universidade Federal do Espírito Santo**

Alex Almeida Rosa

Uso da Criptografia RSA no Ensino de Matemática

Dissertação de mestrado apresentada ao PROFMAT como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática

Trabalho aprovado. Vitória, 24 de agosto de 2023

Prof. Dr. Alcebíades Dal Col Júnior
Universidade Federal do Espírito Santo
Orientador

Prof. Dr. Alancardek Pereira Araújo
Universidade Federal do Espírito Santo
Membro Interno

Prof. Dr. Fidelis Zanetti de Castro
Instituto Federal de Educação, Ciência e Tecnologia do Espírito Santo (IFES)
Membro Externo

Vitória
2023

Dedico à minha esposa Fernanda e aos meus filhos Beatriz e Arthur, que sempre me incentivaram a prosseguir.

Agradecimentos

A Deus, pela vida, saúde e força que me dá todos os dias.

A todos professores do PROFMAT-UFES, pela dedicação e excelência do trabalho que desempenham. Em especial, agradeço ao professor Alancardek Pereira Araújo, que foi quem primeiro me estimulou e incentivou na produção deste trabalho.

À minha esposa Fernanda e meus filhos Beatriz e Arthur, pela compreensão e paciência, que sempre tiveram no decorrer do curso.

Aos coordenadores do Mestrado no período de 2021 a 2023: Florêncio Ferreira Guimarães Filho, Moacir Rosado Filho, e Fábio Júlio Valentim, pela presteza quanto a todas as solicitações a eles feitas nesse período.

Aos colegas de turma, em especial à Gilcélia, Welington, Rose e Moacir, pela parceria, aprendizado e companheirismo.

Ao meu orientador, Professor Alcebíades Dal Col Júnior, ao qual não tenho nem palavras para agradecer pelos ensinamentos, prontidão e por ceder o seu tempo para me auxiliar.

"Arte da guerra nos ensina a contar não com a probabilidade de o inimigo não chegar, mas com nossa própria prontidão para recebê-lo; não com a chance de não ser atacado, mas, sim, com o fato de tornar nossa posição inatacável"

(A arte da guerra, Sun tzu)

Resumo

Vivemos na era da tecnologia, onde a informação é transmitida quase que instantaneamente pelos meios de comunicação. Mensagens são enviadas aos milhões todas as horas. O objetivo deste trabalho é demonstrar como a matemática é importante nesse processo, principalmente no que tange à segurança da informação. Exploraremos a importância dos conceitos matemáticos fundamentais para o entendimento da Criptografia RSA, como Números Primos e Aritmética Modular. Temas como a Criptografia RSA, que envolvem atualidade e tecnologia, chamam a atenção do estudante que durante as aulas tradicionais geralmente não associa a teoria e a prática. Por este motivo, este trabalho tem como proposta final a realização de uma Sequência Didática que associa teoria à prática por meio de softwares e aplicativos gratuitos e de fácil acesso.

Palavras-chave: Criptografia. Criptografia RSA. Números Primos. Aritmática Modular. Aplicativos.

Abstract

We live in the age of technology, where information is passed on almost instantly by the means of communication. Messages are forwarded by the millions every hour. The objective of this work is to demonstrate how mathematics is important in this process, especially with regard to information security. We will explore the importance of fundamental mathematical concepts for understanding RSA Cryptography, which is the main theme of this work, such as Prime Numbers and Modular Arithmetic. Topics such as RSA Cryptography, which involve current affairs and technology,call the attention of students who during traditional classes generally do not combine theory and practice. For this reason, this work has as its final proposal the realization of a Didactic Sequence that associates theory with practice through free and easily accessible software and applications.

Keywords: Cryptography. RSA encryption. Prime numbers. Modular arithmetic. Apps.

Lista de ilustrações

Lista de tabelas

Sumário

1 Introdução

A história nos conta vários episódios em que a criptografia foi usada para transmitir mensagens secretas. Apresentaremos neste capítulo algumas das soluções que a humanidade criou para transmitir tais mensagens, desde tempos remotos, até tempos atuais.

1.1 Criptografia na Antiguidade

Com o surgimento da escrita, surgiu também a necessidade de se enviar mensagens que só poderiam ser compreendidas entre quem as envia e quem as recebe, por motivos sentimentais, religiosos, políticos e principalmente de guerra. Em consequência, surge também a necessidade de se interceptar essas mensagens e tentar descobrir seu conteúdo. Nasce então o terreno para o desenvolvimento da criptografia como a ciência destinada a produzir técnicas de se transmitir mensagens de forma secreta, e a Criptoanálise, para produzir técnicas para decifrar as mensagens criptografadas.

De acordo com COSTA E FIGUEIREDO (COSTA; FIGUEIREDO, 2010), os primeiros indícios do uso da criptografia, surgem cerca de 2000 anos antes de Cristo. Os egípcios usavam técnicas de criptografia na sua escrita hieroglífica, restrita aos sacerdotes e nobres, que não podia ser compreendida pelo povo, que tinha um outro tipo de escrita, a demótica, que era uma escrita mais simples. Neste mesmo período, a Babilônia, também produzia algo semelhante com sua escrita Cuneiforme.

Como uma espécie de protótipo da criptografia, surge a esteganografia que era a técnica de ocultar uma mensagem, sem contudo mudar seu texto original. Esta técnica pode ser bem vulnerável em caso de interceptação da mensagem por terceiros, onde a mensagem será de imediato conhecida, não sendo considerada ainda um sistema de criptografia. Veja um exemplo histórico de utilização desta técnica:

> Heródoto conta a história de um grego que precisava transmitir uma mensagem secretamente. Ele então raspa o cabelo do mensageiro, tatua a mensagem na cabeça raspada e espera que o cabelo cresça novamente. Ao chegar ao destinatário, o mensageiro raspa a cabeça, revelando a mensagem. (COSTA; FIGUEIREDO, 2010, p. 11)

Apesar de parecer arcaica, a esteganografia tem sido usada historicamente em várias épocas. Eis alguns exemplos:

- *Marcação de caractere:* São selecionadas letras de um texto, com lápis em grafite passado por cima. As marcas só são visíveis se usadas contra uma fonte de luz.

- *Microfilmagem:* Redução de uma página de um texto ou imagem, ao tamanho de um ponto, que era ampliado posteriormente pelo receptor.
- *Fitas corretivas de máquina de escrever:* Usadas entre as linhas já digitadas. Só era possível ler a escrita com a fita corretiva contra uma fonte de luz.

Para criptografar uma mensagem é necessário modificar a mensagem antes do envio, ato este, chamado encriptar ou cifrar a mensagem. Para isso é preciso um algoritmo e uma chave que somente emissor e receptor podem saber. No caso de uma interceptação da mensagem, o interceptador precisa além da mensagem, conhecer o algoritmo e a chave.

Por outro lado, o objetivo de se atacar um sistema de criptografia, além de recuperar o texto claro (original) a partir do texto cifrado, é obter as chaves que foram usadas. O interceptador geralmente usa duas técnicas para o ataque:

Criptoanálise - Neste tipo de ataque, utiliza-se da natureza do algoritmo, buscando características e estatísticas do texto cifrado que são comuns a textos claros.

Ataque de força bruta - O objetivo deste tipo de ataque é analisar e testar todas as chaves possíveis dentro de um texto cifrado. Para que este ataque obtenha sucesso, em média, é necessário que pelo menos metade das chaves tenham sido testadas.

Segundo STALLINGS (STALLINGS, 2006), quando um destes ataques obtém sucesso, todas as futuras mensagens criptografadas com essa chave ficam comprometidas. Um atacante, também deve ficar atento, se o custo envolvido no processo de quebrar a cifra compensa o valor da informação a ser obtida e se o tempo necessário neste processo supera a vida útil da informação obtida.

1.1.1 Técnicas de substituição e de transposição

Em um período de muitas guerras na Grécia e em Roma, (400-40 a.C) duas técnicas fundamentais de criptografia surgiram: a transposição e a substituição, também conhecidas por Técnicas de Encriptação Clássicas.

Técnicas de substituição

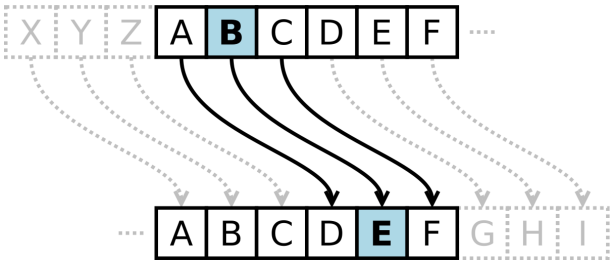
As técnicas de substituição são aquelas em que as letras de um texto claro (original) são substituídas por outras letras, símbolos ou números, de acordo com STALLINGS (STALLINGS, 2006, p. 25). Veremos a seguir, a técnica de substituição mais famosa da antiguidade, a Cifra de César.

Cifra de César

A cifra mais antiga de substituição a que se tem informação, foi utiliza pelo imperador romano Júlio César. A ideia desta cifra é trocar cada letra do alfabeto por outra que fica

três posições a frente. A Figura 1 ilustra a cifra de César com deslocamento de três letras. Mas, qualquer cifra com deslocamento em um número fixo de posições, pode ser chamada de cifra de César.

Figura 1 – Cifra de César



Fonte: Disponível em: <https://cryptoid.com.br/criptografia-identificacao-digital-id-biometria/a-historia-da-criptografia/>. Acesso em: 28 de ago. de 2023.

Exemplo 1.1.1. *Exemplo de mensagem encriptada com a cifra de César com deslocamento de 3 posições:*

Texto Claro: *INFORMANTE OCULTO*

Texto Cifrado: *LQIRUPDQWH RFXOWR*

Vamos atribuir agora um valor numérico a cada letra, conforme a Tabela 1:

Tabela 1 – Atribuição numérica das letras do alfabeto

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Fonte: Produção do próprio autor(2023).

Observada a atribuição numérica apresentada pela Tabela 1, o algoritmo para a cifra de César pode ser dado por:

$$C \equiv (k+d) \pmod{26} \Rightarrow C - d \equiv (k+d) - d = k \pmod{26} \tag{1.1}$$

onde C é cada letra do texto cifrado, k é cada letra do texto claro e d é um deslocamento tal que $1 \leqslant d \leqslant 25$. O algoritmo para decriptar é dado por:

$$k \equiv (C - d) \pmod{26} \tag{1.2}$$

Observação: A terminologia $x \pmod{26}$, refere-se ao resto da divisão do número inteiro x por 26, que será apresentada com mais detalhes no Capítulo 2, na seção Congruências.

No caso de um interceptador ter acesso ao texto cifrado, e conhecer que a cifra utilizada é a cifra de César, basta que ele realize um ataque de força bruta, testando as 25 chaves possíveis. Neste caso, o interceptador estaria realizando um ataque de força bruta.

Exemplo 1.1.2. *Vamos utilizar o texto cifrado no Exemplo 1.1.1 e aplicar a técnica de força bruta, retrocedendo uma letra a cada chave testada:*

Texto cifrado	*LQIRUPDQWH RFXOWR*
Chave 1	*KPHQTOCPVG QEWNVQ (não faz sentido)*
Chave 2	*JOGPSNBOUF PDVMUP (não faz sentido)*
Chave 3	*INFORMANTE OCULTO (faz sentido)*

Observe que no Exemplo 1.1.2 foram usadas apenas 3 chaves para encontrar o texto claro. As outras chaves também podem gerar algum texto com sentido, por isso é fundamental que as outras também sejam analisadas.

Está claro que a Cifra de César está longe de ser segura, porém foi muito útil num período da história onde eram poucas as pessoas que sabiam ler. Posteriormente, veremos como esta cifra pode ser aprimorada, de modo que fique mais segura, sendo mais difícil um ataque por força bruta.

Técnicas de transposição

As técnicas de transposição são aquelas em que se usam permutações, ou seja, o ato de trocar (transpor) a posição das letras de um texto claro. A mais famosa técnica de transposição usada na antiguidade é chamada de Scytale espartano ou Bastão de Licurgo.

A técnica do Scytale ou Bastão de Licurgo

O Bastão de Licurgo era uma técnica de cifrar textos muito utilizadas por soldados da cidade Estado Grega de Esparta. Guerras eram frequentes entre Esparta e Atenas por volta do século V a.C.

> A cidade-estado grega de Esparta, por volta do século V a.C., era uma sociedade na qual a democracia não era uma prática. A retórica e a cultura, tão bem cultuadas na vizinha cidade-estado de Atenas, passavam longe das preocupações de Esparta. Dominados por uma rígida cultura da guerra, os espartanos tinham grande preocupação com a segurança das comunicações militares. Isto impulsionou várias formas de codificar mensagens, sendo o "Scytale espartano" ou "Bastão de Licurgo" o exemplo mais notável desta época. A técnica do Scytale foi descrita por Plutarco, ensaísta e biógrafo grego, em 90 d.C., no livro "Vidas de Homens Ilustres". Era um bastão de madeira ao redor do qual se enrolava-se firmemente, em forma de espiral, uma tira, de couro ou papiro, longa e estreita. (COSTA; FIGUEIREDO, 2010, p. 44)

No livro, "Vidas de Homens Ilustres", Plutarco, falando sobre Lisandro, general espartano, escreve:

> "... os éforos ficaram indignados e, quando encontraram Tórax, um dos Amigos e companheiros de Lisandro, com dinheiro em sua posse privada, o mataram , e enviaram um rolo de despacho para Lisandro, ordenando-lhe o retorno. Quando os éforos[1] enviam um almirante ou um general para uma missão, eles fazem duas peças de madeira, com exatamente o mesmo comprimento e diâmetro, de modo que cada uma corresponda à outra em suas dimensões. Ficam com uma das peças e dão a outra ao seu enviado. Eles denominam estas peças de madeira de "scytalae". Depois, sempre que quiserem enviar alguma mensagem secreta e importante, fazem um rolo de pergaminho, longo e estreito, como se fosse uma tira de couro, e a enrolam ao redor do "scytalae", não deixando nenhum espaço vazio, mas sim cobrindo toda a superfície com o pergaminho. Após fazer isto, eles escrevem o que querem sobre o pergaminho, enquanto ainda está enrolado ao redor do "scytalae"; e, quando eles escreveram sua mensagem, eles retiram o pergaminho e o enviam, sem a peça de madeira, para o comandante. Ele, quando o tiver recebido, não pode entender o significado, - uma vez que as letras não têm conexão, mas estão desarranjadas, - a não ser que ele pegue seu "scytalae" e enrole ao seu redor a tira de pergaminho de modo que, quando seu curso espiralado for restaurado perfeitamente, e o que segue é ligado ao que precede, ele lê ao redor do bastão e, desse modo, descobre a continuidade da mensagem. E o pergaminho, assim como o bastão, é chamado de "scytalae", assim como a coisa medida possui o mesmo nome da medida." (PERRIN, 1916, p. 285)

A Figura 2, ilustra o Scytale:

Figura 2 – Scytale

Fonte: Disponível em:<https://cryptoid.com.br/wp-content/uploads/2015/07/scytale.png>. Acesso em: 03 de set. de 2023.

Como descrito acima, uma tira de tecido ou couro, era enrolada em um bastão que tinha largura e comprimento pré-definido. A pessoa que enviava a mensagem, escrevia na horizontal, ou seja na direção do comprimento do bastão. Após esse processo, a tira era desenrolada, e usada como um cinto para quem levaria a mensagem. Quando a mensagem chegava ao destinatário, o mesmo, munido de seu bastão idêntico ao do remetente, enrolava a tira, tendo assim acesso à mensagem.

[1] Os éforos eram os oficiais da antiga Esparta. Cinco éforos eram eleitos anualmente. Eles atuavam no papel de fiscais da vida pública, inclusive da atuação dos reis.

É possível ver uma mensagem, se fizermos sua transposição para uma tabela.

Exemplo 1.1.3. *Suponha que queiramos enviar a mensagem: "PREPARE O EXÉRCITO, O ATAQUE SERÁ AMANHÃ", pela técnica de cifragem Scytale.*
Desprezando-se os espaços, vírgula e os caracteres especiais, teremos a mensagem clara desta forma: "PREPAREOEXERCITOOATAQUESERAAMANHA", composta por 33 *caracteres. Vamos dividir o tamanho da mensagem, ou seja,* 33 *caracteres, pelo número de colunas, que será nossa chave. Adotemos como chave* 7 *colunas (comprimento do bastão). Desse modo, teremos* 5 *linhas, pois a divisão de* 33 *por* 7 *não é exata, ou seja,* $33 = 4 \cdot 7 + 5$ *(largura do bastão).*

Tabela 2 – Cifragem pela técnica Scytale.
Sentido da escrita do texto claro $\longrightarrow$

P	R	E	P	A	R	E
O	E	X	E	R	C	I
T	O	O	A	T	A	Q
U	E	S	E	R	A	A
M	A	N	H	A		

Fonte: Produção do próprio autor (2023).

Tabela 3 – Cifragem pela técnica Scytale.
Sentido da codificação $\downarrow$

P	R	E	P	A	R	E
O	E	X	E	R	C	I
T	O	O	A	T	A	Q
U	E	S	E	R	A	A
M	A	N	H	A		

Fonte: Produção do próprio autor (2023).

Logo pela Tabela 3, o texto cifrado seria:

"POTUMREOEAEXOSNPEAEHARTRARCAAEIQA".

1.2 Criptografia na Idade Média

O período de quase 1000 anos (476 - 1453) que compreende a Idade Média, foi um período de poucos registros do uso de criptografia. Segundo COSTA E FIGUEIREDO (COSTA; FIGUEIREDO, 2010), uma das principais causas era a perseguição religiosa, que considerava que escritas secretas e mensagens indecifráveis teriam ligações com as forças do Mal. Dentre esses registros, os códigos mais utilizados eram as Cifras Monoalfabéticas

as quais correspondiam cada letra do alfabeto a um símbolo distinto que poderiam ser letras ou símbolos.

As Tabelas 4 e 5 mostram duas possíveis cifras monoalfabéticas, onde a cada letra minúscula, faz-se corresponder uma letra maiúscula, um símbolo ou um sinal. O texto claro será dado por letras minúsculas e a cifragem por seus correspondentes na tabela.

Tabela 4 – Exemplo de Cifra Monoalfabética I

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

Fonte: Produção do próprio autor (2023).

Tabela 5 – Exemplo de Cifra Monoalfabética II

a	b	c	d	e	f	g	h	i	j	k	l	m
P	R	K	O	X	U	+	L	#	M	H	:	<
n	o	p	q	r	s	t	u	v	w	x	y	z
>	E	$	Z	B	A	J	?	Y	-	C	!	L

Fonte: Produção do próprio autor (2023).

Exemplo 1.2.1. *De acordo com as Tabelas 4 e 5 podemos cifrar a palavra "caminho", das seguintes formas:*
Cifra 1 : OMALXVG
Cifra 2 : KP<#>LE

Para que a transmissão de mensagens usando esse processo tenha sucesso, é necessário que o emissor e o receptor da mensagem, tenham a chave. Observe que ao criar essas cifras aleatórias, com cada símbolo representando uma letra, fica muito difícil de se decorar a chave, o que muitas vezes torna necessário escrever essa cifra em algum lugar. Desta maneira, se um interceptador tiver acesso à chave, poderá acessar a mensagem clara facilmente.

A criptografia por Cifras Monoalfabéticas, com o passar do tempo, tornou-se facilmente "quebrável", com o desenvolvimento da Criptoanálise, que utilizava, frequentemente o método da Força Bruta, e o método da palavra Provável. De acordo com COSTA e FIGUEIREDO (COSTA; FIGUEIREDO, 2010), por volta do ano 750, os árabes contribuem com a criptoanálise, desenvolvendo o método da Análise de Frequências, que explora a frequência com que símbolos aparecem em um texto. Com esse processo, criaram-se então as bases científicas da criptoanálise, criando também, um clima desafiador, entre os criadores de cifras e os decifradores.

1.3 Criptografia na Idade Moderna

Cifras Homófonas

A partir de 1450, data aproximada do início da idade moderna, a Europa, ciente de que as cifras Monoalfabéticas mostravam-se muito vulneráveis frente ao ataque por meio do método da Análise de frequências, incentivou os criptólogos a aperfeiçoar seus métodos. Novos tempos pediam novas técnicas e como resultado dessa busca desenfreada por fugir da Análise de Frequências, desenvolveram-se então as Cifras de substituição Homófonas. Essas cifras atribuíam a cada letra do alfabeto mais que um símbolo. Como o método de Análise de Frequências se baseava no fato de que em um texto longo, as vogais tem mais probabilidade de aparecer, ou seja, aparecem com maior frequência que as consoantes, a cifra Homófona atribuía às vogais, mais símbolos que às consoantes, dificultando assim a Análise de Frequências.

Exemplo 1.3.1. *Exemplo de Cifra Homófona que utiliza* 26 *letras maiúsculas,* 26 *letras minúsculas e* 10 *algarismos.*

Tabela 6 – Exemplo de Alfabeto para cifragem Homófona

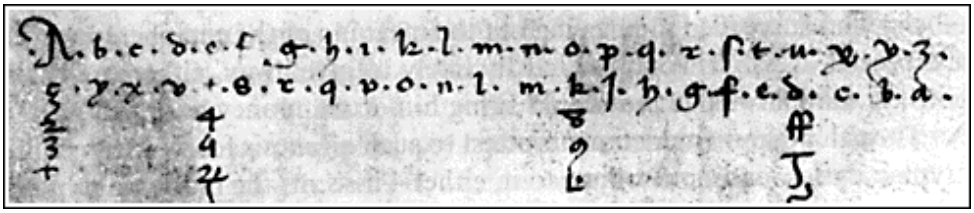
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
5	R	s	O	8	U	p	L	n	o	H	x	Z	g	Y	D	e	F	i	l	4	J	N	C	V	K
T	Q	j	1	P	r	a	v	0			G	B	y	6	z		2	9	f	7	m				
w		A	E	q				k			W	I		h			t								
3				u				d			b			S			M								
c														X											

Fonte: Produção do próprio autor (2023).

De acordo com o alfabeto de cifragem homófona, representado na Tabela 6, a mensagem: "se preparem, acampamento inimigo adiante" poderia ser cifrada assim:
"iP D2qzTFuI 5jwZq3IPyfS ngdB0aY c1kTylq".
Geralmente, para dificultar ainda mais uma possível decifragem, as letras eram agrupadas em grupos de 5 letras. A mensagem então era enviada assim:
"iPD2q zTFuI 5jwZq 3IPyf SngdB 0aYc1 kTylq".
Observe que a mensagem poderia ser cifrada de várias maneiras diferentes.

Um dos pioneiros, na utilização das cifras homófonas foi o italiano Simeone de Crema. Ele criou em 1401 a chamada Cifra de Crema, onde substituía as vogais por letras, por algarismos e por caracteres especiais.

Figura 3 – Cifra de Crema



Fonte: Disponível em:<http://home.hiwaay.net/~paul/cryptology/history.html>. Acesso em: 03 de set. de 2023.

Por volta do século XVI, a Espanha que dominava grande parte do mundo com seu império, necessitava de uma cifra eficaz para suas comunicações em meio as frentes de batalha. Durante o reinado de Felipe II, a Espanha tinha uma cifra com mais de 500 caracteres, com um diferencial de que possuia símbolos para representar dígrafos e palavras menores com frequência maior de uso. Apesar da Cifra ser difícil de ser quebrada, o rei Felipe não contava com a força do método do matemático François Viète, criptólogo do rei da França Henrique IV, que utilizou com excelência a Análise de Frequências, considerando que a cifra era uma variação da cifra Monoalfabética. O rei da Espanha indignado, acusou Viète de pacto com o demônio perante o Papa, que desconsiderou tal acusação.

Um fato histórico, sobre Cifras monoalfabéticas está descrito no texto abaixo:

> Uma das situações mais trágicas da época ocorre com a quebra de um código monoalfabético que provocou a condenação da Rainha Maria da Escócia pela rainha Elisabeth I da Inglaterra. Maria era prisioneira de Elizabeth e, de seu cárcere, trocava correspondência cifrada com um grupo de católicos que tramavam a morte da rainha e a libertação de Maria para assumir o trono inglês. A correspondência de Maria foi interceptada e decifrada por Thomas Phelipes, secretário de cifras do Reino. Maria foi decapitada em 1538. (COSTA; FIGUEIREDO, 2010, p. 57)

Cifras Polialfabéticas

As cifras Homófonas também se mostraram em desvantagem frente a Criptoanálise. Como opção à cifra Homófona, o italiano Leon Battista Alberti, criou, em 1470, a que foi considerada a primeira Cifra Polialfabética. Foi ele quem introduziu o processo de mecanização da cifragem, criando um disco para cifrar as mensagens. A Figura 4 ilustra o disco:

Figura 4 – Disco de Alberti

Fonte: Disponível em: <https://en.wikipedia.org/wiki/File:Alberti_cipher_disk.JPG>. Acesso em: 03 de set. de 2023.

O disco se subdividia em dois discos, um externo fixo e outro interno e móvel. No disco externo, temos o alfabeto plano com as letras da mensagem original. Já no disco interno temos o alfabeto cifrado. Uma descrição mais precisa do disco é dada abaixo:

> O disco de Alberti , é composto por dois anéis concêntricos, um externo e um interno. O anel externo é fixo, com 24 casas contendo 20 letras latinas maiúsculas (incluindo o Z, com U=V e excluindo H J K W Y) e os números 1,2, 3, e 4 para o texto claro. O anel interno é móvel, com as 24 letras latinas minúsculas para o texto cifrado. As 20 letras maiúsculas estão em ordem alfabética e as 24 minúsculas estão desordenadas. Letras minúsculas fora de ordem é uma norma fundamental pois, caso estivessem em ordem, a cifra seria apenas uma generalização do Código de César. (TKOTZ, 2005, p. 194)

Existem alguns métodos de utilização do disco. Um destes métodos consiste em escolher como chave uma letra, que usaremos aqui, para exemplificar, a letra p. O processo de cifragem acontece acrescentando-se letras maiúsculas na mensagem que será cifrada. Assim que for encontrada uma letra maiúscula, a chave deve ser movida até essa letra. A cifragem das demais letras ocorre pela correspondência entre os dois discos. O processo se repete se outra letra maiúscula for encontrada, até que se acabe a mensagem.

Exemplo 1.3.2. *Suponha que vamos enviar a mensagem "general sob suspeita". Retirando se os espaços e observando que a letra p corresponde à letra E (Figura 4), a mensagem deve começar com esta letra e ficará assim: "Egeneralsobsuspeita". Vamos agora adicionar outras letras maiúsculas ao texto, que para este exemplo ficará assim "EgeneralMsobTsuspeita".*

1. *Quando* $p \longrightarrow E$

Tabela 7 – Iteração 1

D. fixo	A	B	C	D	E	F	G	I	L	M	N	O	P	Q	R	S	T	V	X	Z	1	2	3	4
D. móvel	g	k	l	n	p	r	t	v	z	&	x	y	s	o	m	q	i	h	f	d	b	a	c	e

Fonte: Produção do próprio autor (2023).

Assim, a parte do texto claro, referente à 1^a *iteração, ou seja, "EgeneralM" ficará cifrada da seguinte maneira: "EtpxpmgzM".*

2. *Quando* $p \longrightarrow M$

Tabela 8 – Iteração 2

D. fixo	A	B	C	D	E	F	G	I	L	M	N	O	P	Q	R	S	T	V	X	Z	1	2	3	4
D. móvel	d	b	a	c	e	g	k	l	n	p	r	t	v	z	&	x	y	s	o	m	q	i	h	f

Fonte: Produção do próprio autor (2023).

Desse modo, a parte do texto claro, até a 2^a *iteração, ou seja, "EgeneralMsobT"ficará cifrada da seguinte maneira: "EtpxpmgzMxtbT".*

3. *Quando* $p \longrightarrow T$

Tabela 9 – Iteração 3

D. fixo	A	B	C	D	E	F	G	I	L	M	N	O	P	Q	R	S	T	V	X	Z	1	2	3	4
D. móvel	s	o	m	q	i	h	f	d	b	a	c	e	g	k	l	n	p	r	t	v	z	&	x	y

Fonte: Produção do próprio autor (2023).

Finalmente, após esta iteração, todo o texto claro, ou seja, "EgeneralMsobTsuspeita", será cifrado da seguinte maneira: "EtpxpmgzMxtbTnrngidp".

Mesmo com a inovação apresentada por Alberti em sua cifra, ela não resistiu à Análise de frequências. Muitas outras cifras polialfabéticas foram desenvolvidas logo após, mas a mais popular de todas foi a Cifra de Vigenère, atribuída a Blaise de Vigenère, nascido em 1523, que ficou conhecida como a "Cifra Indecifrável", por quase 300 anos, de acordo com COSTA e FIGUEIREDO (COSTA; FIGUEIREDO, 2010). A cifra, consistia em 26 cifras Monoalfabéticas de César, com deslocamentos de 0 a 25. A chave é composta por uma palavra que pode ser repetida quantas vezes forem necessárias, até completar o comprimento total do texto claro. Cada cifra é indicada, por uma das letras desta chave, que será a letra do texto cifrado que substitui a letra do texto claro.

Figura 5 – Tabela de Vigenère

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

Fonte: Disponível em: <https://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-Base.html>. Acesso em: 03 de set. de 2023.

Exemplo 1.3.3. *Suponha que a mensagem "morte ao general" deva ser cifrada com a Cifra de Vigenère e que a palavra chave seja: honra.*
Passando tudo para letras maiúsculas e retirando espaços e pontuação, teremos:
Chave: *HONRAHONRAHONR*
Texto Claro: *MORTEAOGENERAL*

Observe a Figura 6 que mostra a intersecção das letras H e M na tabela de Vienère, que corresponde à letra T que será a letra correspondente cifrada.

Figura 6 – Exemplo de Utilização da Tabela de Vigenère

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

Fonte: Disponível em:<https://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-Base.html>. Acesso em: 03 de set. de 2023.

Fazendo este processo para as demais letras do texto claro teremos:

Chave: *HONRAHONRAHONR*
Texto Claro: *MORTEAOGENERAL*
Texto Cifrado: *TCEKEHCTVNLFNC*

A força desta cifra está no fato de que existem muitas letras de texto cifrado, para cada letra do texto claro, o que dificultava uma Análise de Frequências. Mas, como dissemos anteriormente, essa cifra foi quebrada por volta de 1850 e deixou de ser considerada a Cifra indecifrável. Era o fim do período relativo à idade Moderna e a busca era por uma cifra realmente confiável e que realmente pudesse estabelecer uma comunicação secreta, face a um novo mundo em que o avanço dos processos mecânicos era iminente. Não há de se dizer que também já se iniciava a comunicação via telégrafo, e a necessidade de um código que realmente pudesse trazer segurança e proteção à informação era imediata.

1.4 Criptografia na Idade Contemporânea

A história recente, foi marcada por duas grandes Guerras Mundiais, nas quais os países envolvidos contavam não só com a comunicação via telégrafo, como com a comunicação via rádio, que oferecia comunicação rápida e livre, porém sem a segurança de que a transmissão ficaria realmente secreta. Neste contexto, necessitavam de cifras para as mensagens mais secretas.

A cifra mais usada na Primeira Guerra Mundial, foi a cifra alemã ADFGVX. De acordo com TKOTZ (TKOTZ, 2005), após intensas ofensivas militares da Alemanha, quando estava já prestes a invadir Paris, o criptoanalista das forças aliadas, Georges Pavin conseguiu após muito esforço e noites sem dormir decifrar o algoritmo ADFGVX e daí em diante conseguiu prever todos os ataques da Alemanha, que teve que recuar. O sistema ADFGVX consistia em uma tabela 6x6 onde são colocadas as 26 letras do alfabeto e 10 algarismos (0 a 9). Este método era realizado em duas etapas, uma de substituição e outra de transposição. A Tabela 10 mostra um exemplo de cifra ADFGVX.

Tabela 10 – Exemplo de Cifra ADFGVX

	A	D	F	G	V	X
A	5	M	J	F	9	L
D	A	R	G	4	2	P
F	S	D	0	I	Z	6
G	W	C	B	N	T	X
V	H	1	V	E	Y	7
X	Q	K	8	U	3	O

Fonte: Produção do próprio autor (2023).

Exemplo 1.4.1. *Vejamos como codificar o texto "BOMBARDEIO ÀS 9:00 AM", com a Cifra ADFGVX da Tabela 10 e como chave a palavra "PRIVADO".*

- *1ª Etapa: Cada letra do texto claro será substituída pelas letras da linha e da coluna Respectivamente, em que está inserida. Por exemplo, a letra B será substituída pelas letras "GF" nesta sequência. Fazendo o mesmo para as demais letras, vamos obter:*

Texto Claro	B	O	M	B	A	R	D	E	I	O	A	S	9	0	0	A	M
Texto Cifrado	GF	XX	AD	GF	DA	DD	FD	VG	FG	XX	DA	FA	AV	FF	FF	DA	AD

Fonte: Produção do próprio autor (2023).

O texto cifrado da 1ª etapa será:

"GFXXADGFDADDFDVGFGXXDAFAAVFFFFDAAD"

- *2ª Etapa: A segunda Etapa é uma transposição de colunas, tendo como base a palavra chave. De posse do texto cifrado da 1ª Etapa e da palavra chave, montaremos uma tabela em que a primeira linha contém a palavra chave. A segunda linha a numeração correspondente à ordem alfabética das letras da palavra chave. Por fim, a cifragem é feita de cima para baixo seguindo a ordem alfabética das colunas:*

Tabela 11 – Segunda Etapa da Cifra ADFGVX

P	R	I	V	A	D	O
5	6	3	7	1	2	4
G	F	X	X	A	D	G
F	D	A	D	D	F	D
V	G	F	G	X	X	D
A	F	A	A	V	F	F
F	F	D	A	A	D	

Fonte: Produção do próprio autor (2023).

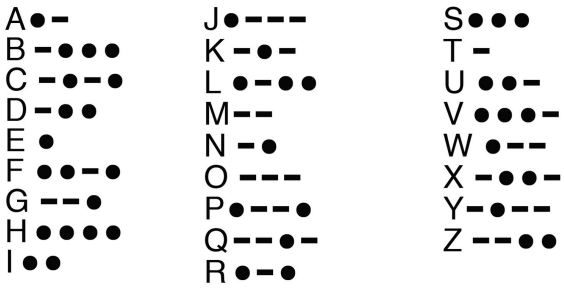
O texto cifrado final será:

"ADXVA DFXFD XAFAD GDDF GFVAF FDGFF XDGAA"

O uso exclusivo das letras A,D,F,G,V,X é esclarecido no texto abaixo:

> O motivo da escolha de letras para identificar as linhas e as colunas da grade está no Código Morse usado nas transmissões telegráficas. Os pontos e traços das letras ADFGVX dificilmente são confundidos, tanto na transmissão quanto na recepção, o que diminui em muito os erros de comunicação. (TKOTZ, 2005, p. 235)

Figura 7 – Código Morse



Fonte: Disponível em: <https://www.infoescola.com/wp-content/uploads/2013/02/codigo-morse.jpg>. Acesso em: 03 de set. de 2023.

A Figura 7 mostra a tabela do Código Morse, onde o ponto representa um sinal curto (pulso elétrico curto) e o traço representa um sinal longo (pulso elétrico longo).

Em se falando de criptografia, a Segunda Guerra Mundial foi marcada pela utilização de uma máquina de cifras chamada de *Enigma*. Inicialmente, esta máquina foi construída pelo engenheiro Alemão Arthur Scherbius com propósito simplesmente comercial, para troca segura de informação entre homens de negócios. Mais tarde, o Governo Alemão se interessa pelo uso militar da máquina e faz um redesenho para utilizá-la na Guerra, começando a utilizá-la por volta de 1930.

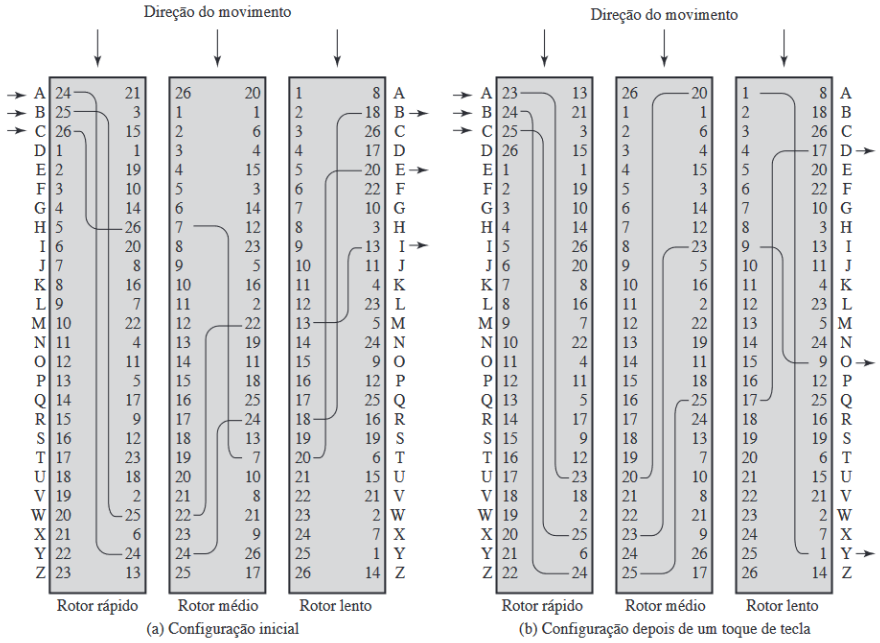
A Enigma pertencia a um sistema de encriptação denominado Máquinas de Rotor. O princípio da Máquina de três rotores com fiação representada por contatos numerados (como a Enigma) é descrito abaixo:

> A máquina consiste em um conjunto de cilindros rotativos independentes, através dos quais pulsos elétricos podem fluir. Cada cilindro tem 26 pinos de entrada e 26 pinos de saída, com fiação interna que conecta cada pino de entrada a um único pino de saída. (STALLINGS, 2006, p. 38)

Na Figura 8, STALLINGS (STALLINGS, 2006) mostra o princípio básico da maquina de rotor.

Nas Figuras 9 e 10, temos a representação de um sistema com 3 rotores. A parte esquerda da figura apresenta uma posição para a entrada do usuário. Suponha que ele pressione a tecla A (texto claro), um sinal elétrico é aplicado ao primeiro pino, e o processo é direcionado pelos três rotores, até a saída no terceiro rotor, com a letra B. O rotor mais próximo à entrada gira uma posição a cada toque. A segunda parte da figura, apresenta o sistema após um único toque. Depois que o primeiro rotor completa uma rotação, o segundo rotor gira uma posição e, de mesma maneira, quando o segundo rotor completa uma rotação, o terceiro rotor gira uma posição. Como consequência, tem-se $26^3 = 17.576$ alfabetos diferentes de substituição.

Figura 8 – Máquina de três rotores com fiação representada por contatos numerados



Fonte: (STALLINGS, 2006, p. 38)

Figura 9 – Enigma

Fonte: Disponível em:<https://miro.medium.com/v2/resize:fit:875/0*P0hQ53NL7V7ZDWi7.jpg>. Acesso em: 03 de set. de 2023.

Figura 10 – Painel de plugs da Enigma

Fonte: Disponível em: <https://miro.medium.com/v2/resize:fit:875/0*78zglqA95dwVpb8d.jpg>. Acesso em: 03 de set. de 2023.

Ficavam à disposição para serem usados na Enigma cinco rotores, dos quais três eram usados por vez na máquina. Além dos rotores, a máquina possuía um painel de plugs na parte frontal que permitia que as letras fossem trocadas, gerando assim um reforço imenso na codificação.

> Para permitir que as conexões do teclado com o primeiro rotor fossem modificadas, Scherbius criou um pequeno painel de ligações parecido com as mesas de telefonia antigas. Por meio de cabos com dois plugues nas pontas, o operador pode alterar a entrada de seis pares de letras. (TKOTZ, 2005, p. 249)

A Tabela 12, extraída e adaptada de TKOTZ (TKOTZ, 2005), nos mostra o cálculo de segurança do método praticado na Enigma:

Tabela 12 – Cálculo do possível número de Cifras da Enigma

	Cálculo	Valor
Posições dos três rotores	26^3	17.576
Sequência dos três rotores	3!	6
Escolha de três entre os 5 rotores	$C_3^5 = \frac{5!}{3!(5-3)!}$	10
Seis pares de letras entre 26 letras	$\frac{n!}{(n-2m)!m!2^m} = \frac{26!}{14!6!2^6}$	100.391.791.500
Total	$17.576 \times 6 \times 10 \times 100.391.791.500$	105.869.167.644.240.000

Fonte: Produção do próprio autor (2023).

> A Enigma mais antiga possuía um conjunto de três rotores com 26 contatos. Após digitar uma tecla do teclado, o primeiro rotar girava uma posição. Quando o primeiro rotor tivesse dado uma volta completa, o segundo rotar girava uma posição. Da mesma forma, quando o segundo rotor tivesse dado uma volta completa, o terceiro era deslocado em uma posição. Isto significa que o número de combinações possíveis era 26 x 26 x 26, ou seja, 17.576. Desta forma, a máquina podia fornecer criptogramas bem mais seguros, obtidos por meio de uma substituição polialfabética baseada em 17.576 alfabetos cifrantes diferentes. (TKOTZ, 2005, p. 248)

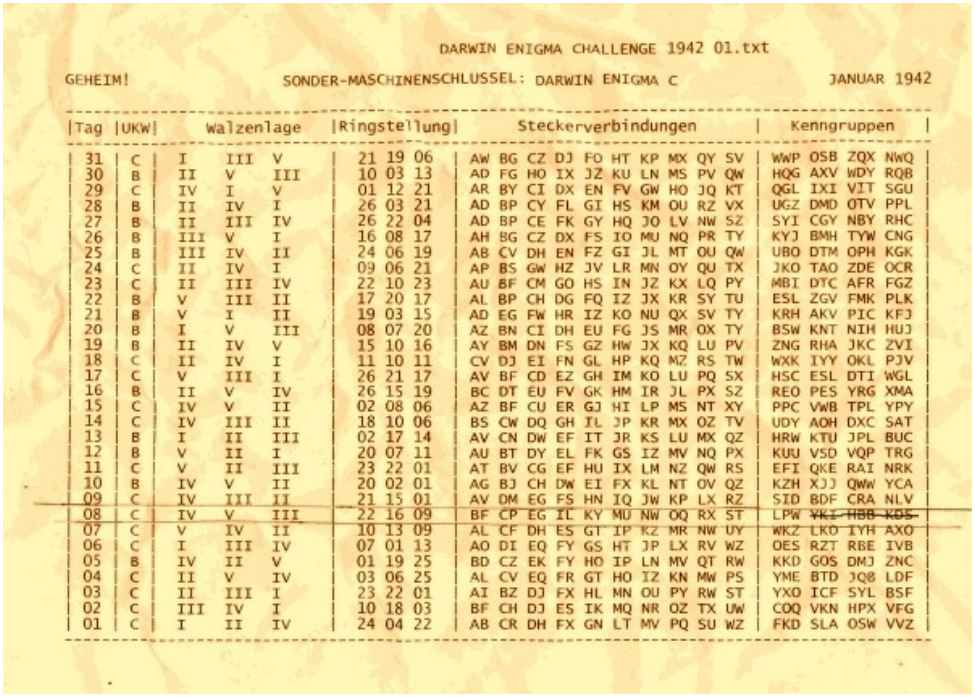
Ainda de acordo com TKOTZ (TKOTZ, 2005), a posição dos três rotores poderia ser alterada, gerando sequências diferentes nos três rotores. Por exemplo, identificando os rotores como 1, 2 e 3, teríamos as sequências $123, 131, 213, 231, 312$ ou $321 = 6 = 3!$, ou seja, seis posições possíveis para os rotores, o que aumentaria seis vezes o conjunto de chaves. O número de combinações possíveis para a troca de seis pares de letras num alfabeto de 26 letras é um número significativo $\frac{26!}{14!6!2^6} = 100.391.791.500$. Acrescentando a isso, a escolha de três entre os cinco rotores disponíveis, a segurança da enigma ainda aumentava consideravelmente: $C_3^5 = \frac{5!}{3!(5-3)!} = 10$, ou seja, 10 vezes.

As mais de 105 quatrilhões de posições iniciais possíveis, apresentadas pela Tabela 12, para a enigma, já era motivo de sobra, para qualquer criptógrafo desistir de enfrentar a enigma.

Além da infinidade de possíveis cifras, os operadores da Enigma possuíam uma espécie de livro contendo tabelas diferentes para cada dia do Mês (Figura 11). Essa tabela mostrava quais dos cinco rotores usar naquele dia, qual sua posição e também qual o posicionamento dos plugs. Desta maneira os criptoanalistas só tinham 24 horas para

decifrar alguma mensagem. Ao final do mês o livro era trocado para garantir a eficiência do processo.

Figura 11 – Modelo de tabela usada para codificação da Enigma



DARWIN ENIGMA CHALLENGE 1942 01.txt

GEHEIM! SONDER-MASCHINENSCHLUSSEL: DARWIN ENIGMA C JANUAR 1942

Tag	UKW	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
31	C	I III V	21 19 06	AW BG CZ DJ FO HT KP MX QY SV	WWP OSB ZQX NWQ
30	B	II V III	10 03 13	AD FG HO IX JZ KU LN MS PV QW	HQG AXV WDY RQB
29	C	IV I V	01 12 21	AR BY CI DX EN FV GW HO JQ KT	QGL IXI VIT SGU
28	B	II IV I	26 03 21	AD BP CY FL GI HS KM OU RZ VX	UGZ DMD OTV PPL
27	B	II III IV	26 22 04	AD BP CE FK GY HQ JO LV NW SZ	SYI CGY NBY RHC
26	B	III V I	16 08 17	AH BG CZ DX FS IO MU NQ PR TY	KYJ BMH TYW CNG
25	B	III IV II	24 06 19	AB CV DH EN FZ GI JL MT OU QW	UBO DTM OPH KGK
24	C	II IV I	09 06 21	AP BS GW HZ JV LR MN OY QU TX	JKO TAO ZDE OCR
23	C	II III IV	22 10 23	AU BF CM GO HS IN JZ KX LQ PY	MBI DTC AFR FGZ
22	B	V III II	17 20 17	AL BP CH DG FQ IZ JX KR SY TU	ESL ZGV FMK PLK
21	B	V I II	19 03 15	AD EG FW HR IZ KO NU QX SV TY	KRH AKV PIC KFJ
20	B	I V III	08 07 20	AZ BN CI DH EU FG JS MR OX TY	BSW KNT NIH HUJ
19	B	II IV V	15 10 16	AY BM DN FS GZ HW JX KQ LU PV	ZNG RHA JKC ZVI
18	C	II IV I	11 10 11	CV DJ EI FN GL HP KQ MZ RS TW	WXK IYY OKL PJV
17	C	V III I	26 21 17	AV BF CD EZ GH IM KO LU PQ SX	HSC ESL DTI WGL
16	B	II V IV	26 15 19	BC DT EU FV GK HM IR JL PX SZ	REO PES YRG XMA
15	C	IV V II	02 08 06	AZ BF CU ER GJ HI LP MS NT XY	PPC VWB TPL YPY
14	C	IV III II	18 10 06	BS CW DQ GH IL JP KR MX OZ TV	UDY AOH DXC SAT
13	B	I II III	02 17 14	AV CN DW EF IT JR KS LU MX QZ	HRW KTU JPL BUC
12	B	V II I	20 07 11	AU BT DY EL FK GS IZ MV NQ PX	KUU VSD VQP TRG
11	C	V II III	23 22 01	AT BV CG EF HU IX LM NZ QW RS	EFI QKE RAI NRK
10	B	IV V II	20 02 01	AG BJ CH DW EI FX KL NT OV QZ	KZH XJJ QWW YCA
09	C	IV III II	21 15 01	AV DM EG FS HN IQ JW KP LX RZ	SID BDF CRA NLV
08	C	IV V III	22 16 09	BF CP EG IL KY MU NW OQ RX ST	LPW ~~YKI HBB KDS~~
07	C	V IV II	10 13 09	AL CF DH ES GT IP KZ MR NW UY	WKZ LKO IYH AXO
06	C	I III IV	07 01 13	AO DI EQ FY GS HT JP LX RV WZ	OES RZT RBE IVB
05	B	IV II V	01 19 25	BD CZ EK FY HO IP LN MV QT RW	KKD GOS DMJ ZNC
04	C	II V IV	03 06 25	AL CV EQ FR GT HO IZ KN MW PS	YME BTD JQ8 LDF
03	C	II III I	23 22 01	AI BZ DJ FX HL MN OU PY RW ST	YXO ICF SYL BSF
02	C	III IV I	10 18 03	BF CH DJ ES IK MQ NR OZ TX UW	COQ VKN HPX VFG
01	C	I II IV	24 04 22	AB CR DH FX GN LT MV PQ SU WZ	FKD SLA OSW VVZ

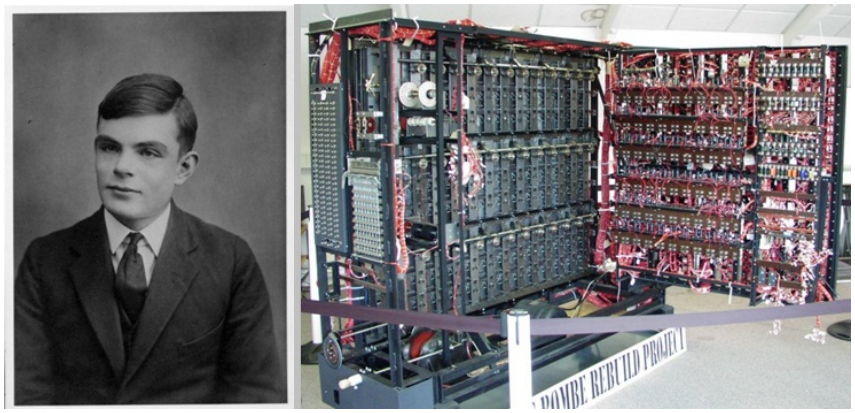
Fonte: Disponível em: <https://i.blogs.es/96242c/enigma1/1366_2000.jpg>. Acesso em: 03 de set. de 2023.

Segundo TKOTZ (TKOTZ, 2005), para encriptar uma mensagem, um oficial passava o texto para um operador da máquina, que digitava o texto, e um segundo soldado anotava todas as letras que apareciam no painel luminoso que correspondia ao texto cifrado. Este soldado então passava este texto cifrado, para um operador de rádio que convertia esta mensagem em Código Morse. O receptor por sua vez anotava as letras correspondentes ao Código Morse e as digitava na Enigma obtendo assim o texto claro.

Muitas equipes lideradas por matemáticos e criptoanalistas iniciaram os trabalhos de quebra das cifras da Enigma. Muitos obtiveram alguns êxitos, baseados em interceptações de textos cifrados ou com auxílio de espiões, mas a equipe que mais se destacou, foi a equipe inglesa liderada pelo brilhante matemático Alan Turing (Figura 12), entusiasmado, pela construção de uma máquina que realizasse milhares de cálculos rapidamente. Por volta de 1940, conseguiram construir essa máquina, que foi chamada de The Bombe. Mais tarde, essa máquina, seria o protótipo do computador moderno. Perseverando com suais ideias, conseguiram quebrar o código da Enigma, e tal feito, conseguiu encurtar a guerra em aproximadamente 2 anos, salvando milhares de vidas.

O filme de 2014 chamado “O jogo da imitação”, é baseado na história real de Alan Turing e narra a corrida contra o tempo de Alan Turing e sua equipe para decifrar os códigos nazistas da máquina Enigma.

Figura 12 – Alan Turing e a máquina The Bombe



Fonte: Disponível em: <https://oempregoeseucom.files.wordpress.com/2020/06/alan-turing.jpg>. Acesso em: 03 de set. de 2023.

Atualmente, as cifras são desenvolvidas e executadas com suporte de tecnologia computacional e são comumente denominadas de Algoritmos. Esses algoritmos, devido ao uso constante de chaves, são categorizados como simétricos ou assimétricos. O uso de um algoritmo de Criptografia, seja simétrico ou assimétrico, não desmerece o uso de outro, uma vez que cada um tem utilização mais indicada para determinada ação.

No Capítulo 3, falaremos sobre estes algoritmos, e daremos ênfase ao algoritmo assimétrico RSA, que é o objeto de estudo deste trabalho. Os outros algoritmos, até por sua importância na atualidade, merecem um trabalho dedicado a eles.

Os livros, artigos, vídeos ou trabalhos a seguir contribuíram ou serviram de base para a produção deste capítulo. Embora não sejam citados , não poderíamos deixar de mencioná-los: (SAUTOY, 2007; HEFEZ, 2012; COSTA; FIGUEIREDO, 2010; PERRIN, 1916)

2 Conceitos Matemáticos Fundamentais

Nesta seção, serão apresentados alguns conceitos matemáticos fundamentais para o entendimento da criptografia RSA.

2.1 Divisibilidade

Dados dois números a e b inteiros, com b diferente de zero, dizemos que b divide a, se $a = k \cdot b$ para algum k inteiro. Desse modo, b divide a, se na divisão o resto for zero. Usaremos a notação $b|a$ para representar que b divide a, ou seja, b é um divisor de a.

Exemplo 2.1.1. *Alguns exemplos de um número b que é divisor de um número a.*

$$17|425, -9|72, 19|0$$

Vejamos agora algumas propriedades da divisibilidade de inteiros. Sejam dados números a, b e $c \in \mathbb{Z}$, temos:

1. $a|1 \Rightarrow a = \pm 1$.
   Demonstração: Seja $a \in \mathbb{Z}$, temos que $1 = 1 \cdot 1$ ou $1 = (-1) \cdot (-1)$. Portanto, $a = \pm 1$.

2. Se $b|a$ e $a|b \Rightarrow b = \pm a$.
   Demonstração: Sejam a e $b \in \mathbb{Z}$, tais que $a = x \cdot b$ para algum $x \in \mathbb{Z}$ e $b = y \cdot a$ Para algum $y \in \mathbb{Z}$. Logo, $b = y \cdot x \cdot b \Rightarrow b - x \cdot y \cdot b = 0 \Rightarrow b \cdot (1 - x \cdot y) = 0 \Rightarrow b = 0$ ou $1 - x \cdot y = 0 \Rightarrow x \cdot y = 1 \Rightarrow$ Se $x = 1$ então $y = 1$. Se $x = (-1)$, então $y = (-1)$. Daí segue que $b = 1 \cdot a$ ou $b = (-1) \cdot a \Rightarrow b = \pm a$.

3. $1|a$.
   Demonstração: De fato, como $a \in \mathbb{Z}$, temos que : $a = a \cdot 1$.

4. $a|a$.
   Demonstração: De fato, como $a \in \mathbb{Z}$, temos que: $a = 1 \cdot a$.

5. Se $a \neq 0$, então $a|0$.
   De fato, como $a \in \mathbb{Z}$, temos que: $0 = 0 \cdot a$.

6. Se $b|a$ e $a|c$, então $b|c$.
   Demonstração: Sejam a , b e $c \in \mathbb{Z}$, de maneira que: $a = x \cdot b$, para algum $x \in \mathbb{Z}$ e $c = y \cdot a$, para algum $y \in \mathbb{Z}$, então, $c = y \cdot x \cdot b \Rightarrow c = (x \cdot y) \cdot b \Rightarrow c = k \cdot b$, para algum $k \in \mathbb{Z}$. Portanto $b|c$.

7. Para quaisquer x e $y \in \mathbb{Z}$, temos que se $b|a$ e $b|c$, então $b|(x \cdot a + y \cdot c)$.
   Demonstração: Sejam a, b e $c \in \mathbb{Z}$. Observe que : Se $b|a \Rightarrow a = m \cdot b$, para algum $m \in \mathbb{Z}$ e se $b|c \Rightarrow c = n \cdot b$, para algum $n \in \mathbb{Z}$ então, para qualquer $x \in \mathbb{Z}$ e para qualquer $y \in \mathbb{Z}$, temos que: $x \cdot a + y \cdot c = x \cdot m \cdot b + y \cdot n \cdot b = b \cdot (m \cdot x + n \cdot y) = b \cdot k$ para algum $k \in \mathbb{Z}$. Portanto, $b|(x \cdot a + y \cdot c)$.

8. Se $b|a \Rightarrow b \cdot c|a \cdot c$.
   Demonstração: Sejam a, b e $c \in \mathbb{Z}$. Se $b|a$ então, para algum $k \in \mathbb{Z}$, temos que $a = k \cdot b \Rightarrow a \cdot c = k \cdot b \cdot c = k \cdot (b \cdot c) \Rightarrow b \cdot c|a \cdot c$.

9. Se $b|(a \pm c) \Rightarrow b|a \iff b|c$.
   Demonstração: Sejam $a, b \in \mathbb{Z}$. Primeiro vamos considerar que $b|(a + c)$, então $a + c = x \cdot b$ para algum $x \in \mathbb{Z}$. Agora, se $b|a \Rightarrow a = y \cdot b$, para algum $y \in \mathbb{Z}$. Substituindo a na primeira equação teremos: $y \cdot b + c = x \cdot b \Rightarrow c = x \cdot b - y \cdot b \Rightarrow c = (x - y) \cdot b \Rightarrow c = k \cdot b$, para algum $k \in \mathbb{Z}$. Portanto, $b|c$. A prova da implicação $b|c \Rightarrow b|a$ é feita analogamente. Para o caso em que $b|(a - c)$, temos que $a - c = m \cdot b$, para algum $m \in \mathbb{Z}$. Agora, se $b|a \Rightarrow a = n \cdot b$, para algum $n \in \mathbb{Z}$. Substituindo a na primeira equação teremos: $n \cdot b - c = m \cdot b \Rightarrow c = n \cdot b - m \cdot b \Rightarrow c = (n - m) \cdot b \Rightarrow c = q \cdot b$, para algum $q \in \mathbb{Z}$. Portanto $b|c$.

10. Para esta propriedade assumamos também que $d \in \mathbb{Z}$. Se $b|a$ e $d|c$ então $b \cdot d|a \cdot c$.
    Demonstração: Sejam $a, b, c, d \in \mathbb{Z}$ tais que se $b|a$ então $a = x \cdot b$, para algum $x \in \mathbb{Z}$ e se $d|c$ então $c = y \cdot d$, para algum $y \in \mathbb{Z}$. Das equações acima temos que $a \cdot c = x \cdot b \cdot y \cdot d \Rightarrow a \cdot c = (x \cdot y) \cdot (b \cdot d) = k \cdot (b \cdot d)$, para algum $k \in \mathbb{Z}$. Portanto, $b \cdot d|a \cdot c$.

11. Sejam a e $b \in \mathbb{N}$ então, se $b|a \Rightarrow b \leq a$.
    Demonstração: Sejam a e $b \in \mathbb{N}$, tais que se $b|a$ então $a = k \cdot b$, para algum $k \in \mathbb{Z}$. Como a e $b \in \mathbb{N}$ temos que ambos são maiores que zero, $a, b > 0$, o que implica que $c > 0$. Daí temos que $c \geq 1 \Rightarrow c \cdot b \geq 1 \cdot b \Rightarrow c \cdot b \geq b \Rightarrow a \geq b$, ou seja, $b \leq a$.

2.2 Divisão Euclidiana

Teorema 2.2.1. *Sejam $a, b \in \mathbb{Z}$ e $a \neq 0$. Existem $q, r \in \mathbb{Z}$ únicos, de modo que:*

$$b = a \cdot q + r, \qquad com \quad 0 \leqslant r < |a|$$

Os números q e r do teorema acima, são denominados quociente e resto da divisão do número b pelo número a, respectivamente. Quando o resto desta divisão é zero, temos que a divide b, ou seja $a|b$.

Exemplo 2.2.2. *Exemplos de divisão com os seus quocientes e restos.*

- *Dividindo* 23 *por* 7*, obtemos quociente* $q = 3$ *e resto* $r = 2$*. Podemos escrever que* $23 = 7 \cdot 3 + 2$*.*
- *Dividindo* 45 *por* 9*, obtemos quociente* $q = 5$ *e resto* $r = 0$*. Neste caso,* $9|45$*. Podemos escrever que* $45 = 9 \cdot 5 + 0$*, ou apenas* $45 = 9 \cdot 5$*.*
- *Dividindo* -14 *por* 5*, obtemos quociente* $q = -3$ *e resto* $r = 1$*. Podemos escrever que* $-14 = -3 \cdot 5 + 1$*.*

O conjunto dos números inteiros, se divide em duas classes, a dos números pares e dos números ímpares. O caráter de um um número inteiro ser par ou ímpar é chamado de paridade do número.

Dado um número $n \in \mathbb{Z}$, este número atende a uma das seguintes possibilidades:

1. n é divisível por 2, ou seja, o resto da divisão de n por 2 é zero. Neste caso, existe $q \in \mathbb{N}$, tal que $n = 2 \cdot q$
2. n não é divisível por 2, ou seja, existe um resto na divisão de n por 2. Neste caso, $q \in \mathbb{N}$ tal que $n = 2 \cdot q + 1$.

Generalizando, escolhido ou fixado um um número $m \in \mathbb{N}$, com $m \geqslant 2$, podemos escrever este número n de maneira única como $n = m \cdot q + r$, onde $q, r \in \mathbb{Z}$ e $0 \leqslant r < m$. Exemplificando:

- Escolhido ou fixado $m = 3$, todo número n pode ser escrito de uma, e somente uma, das formas: $3 \cdot q$, $3 \cdot q + 1$, $3 \cdot q + 2$.
- Escolhido ou fixado $m = 4$, todo número pode ser escrito de uma, e somente uma, das formas: $4 \cdot q$, $4 \cdot q + 1$, $4 \cdot q + 2$, $4 \cdot q + 3$.

2.3 Máximo Divisor Comum (MDC)

Sejam os números a e $b \in \mathbb{Z}$ que não sejam ambos nulos. Se $d|a$ e $d|b$, com $d \in \mathbb{Z}$, dizemos que d é um divisor comum de a e b.

O maior inteiro d, natural, que divide tanto a quanto b é chamado de Máximo Divisor Comum de a e b, e será representado por $mdc(a, b)$ ou simplesmente (a, b). Formalmente, o número natural d será considerado Máximo Divisor Comum de a e b, se possuir as seguintes propriedades:

1. $d|a$ e $d|b$.

2. Qualquer divisor comum de a e b, também é um divisor de d. Ex.: $c|a$ e $c|b \Rightarrow c|d$.

Como consequência da segunda propriedade, se d é o máximo divisor comum de a e b, e c é um dos divisores comuns de a e b, temos que $|c| \leqslant d$ e ainda que $c \leqslant |c| \leqslant d$. Isso nos mostra que de fato, o máximo divisor comum de a e b é o maior entre os divisores comuns destes números.

A unicidade do $mdc(a, b)$ pode ser demonstrada da seguinte maneira: suponha, que tenhamos dois máximos divisores comuns c e d entre os dois números a e b supracitados. Isso implica que $c \leqslant d$ e $d \leqslant c \Rightarrow c = d$. Portanto o $mdc(a, b)$ é único.

Daqui em diante, denotaremos o mdc entre um par de números inteiros a e b, quando ele existir, por (a, b). O mdc de um par de números não depende de sua ordem, ou seja, $(a, b) = (b, a)$. Em geral , temos que

$$(a, b) = (|a|, |b|) \Rightarrow (a, b) = (-a, b) = (a, -b) = (-a, -b).$$

Como todo número inteiro diferente de zero divide zero, temos que $(a, 0) = |a|$. Ainda, de imediato, é possível verificar que: $(a, 1) = 1$ e $(a, a) = |a|$. Se $(a, b) = 1$, dizemos que a e b são relativamente primos. O Lema de Euclides é usado para provar a existência do mdc de um par de números inteiros não-negativos:

Proposição 2.3.1. *Lema de Euclides*
Dados a, b *e* $n \in \mathbb{Z}$*, se existir* $(a, b - na)$*, então existe* $(a, b) = (a, b - na)$

Exemplo 2.3.2. *Usando o Lema de Euclides para calcular* $(534, 192)$.
$(534, 192) = (192, 534) = (192, 534 - 2 \cdot 192) = (192, 534 - 384) = (192, 150) = (150, 192) = (150, 192 - 1 \cdot 150) = (150, 192 - 150) = (150, 42) = (42, 150) = (42, 150 - 3 \cdot 42) = (42, 150 - 126) = (42, 24) = (24, 42) = (24, 42 - 1 \cdot 24) = (24, 42 - 24) = (24, 18) = (18, 24) = (18, 24 - 1 \cdot 18) = (18, 24 - 18) = (18, 6) = (6, 18) = (6, 18 - 3 \cdot 6) = (6, 18 - 18) = (6, 0) = 6.$
Portanto, $(534, 192) = 6$.

O Algoritmo de Euclides

O algoritmo que vamos descrever, atribuído a Euclides de Alexandria, em sua obra: Os Elementos, persiste por mais de 2 mil anos, como um método altamente eficaz e funcional, para a determinação do mdc entre dois números inteiros.

Sejam $a, b \in \mathbb{N}$, com $a \leqslant b$. Sabemos que se $a = 1 \Rightarrow (a, b) = 1 = a$, se $a = b, (a, b) = (a, a) = a$ e que se $a|b$, então $(a, b) = a$. Suponha, agora que $a \neq 1$ e $a \neq b$, temos então, que $1 < a < b$. suponha também que $a \nmid b$. portanto, usando a divisão Euclidiana, temos que:

$$b = a \cdot q_1 + r_1 \qquad com \quad 0 < r_1 < a \tag{2.1}$$

A divisão Euclidiana acima nos fornece r_1 que deve obedecer a uma das seguintes possibilidades:

1. r_1 divide a, ou seja $r_1 \mid a$.
   Observe que pela divisão euclidiana, temos que $b = a \cdot q_1 + r_1 \Rightarrow r_1 = b - a \cdot q_1$.
   Usando o Lema de Euclides e a substituição de r_1 temos:

$$r_1 = (a, r_1) = (a, b - a \cdot q_1) = (a, b) \tag{2.2}$$

   Desse modo, $(a, b) = r_1$. Temos o fim do algoritmo. Senão:

2. r_1 não divide a, ou seja $r_1 \nmid a$.
   Neste caso prosseguimos com o algoritmo, dividindo agora, a por r_1.

$$a = r_1 \cdot q_2 + r_2 \qquad com \quad 0 < r_2 < r_1 \tag{2.3}$$

   logo, para o caso em que $r_1 \nmid a$, temos também as seguintes possibilidades:

   a) r_2 divide r_1, ou seja, $r_2 \mid r_1$.
      Observe, novamente, que pela divisão euclidiana, $a = r_1 \cdot q_2 + r_2 \Rightarrow r_2 = a - r_1 \cdot q_2$.
      Usando o lema de Euclides e a substituição de r_2 e de r_1, feita no item anterior, temos:

$$r_2 = (r_1, r_2) = (r_1, a - r_1 \cdot q_2) = (r_1, a) = (b - a \cdot q_1, a) = (a, b - a \cdot q_1) = (a, b). \tag{2.4}$$

      Desse modo, $(a, b) = r_2$. Temos o fim do algoritmo. Senão:

   b) r_2 não divide r_1, ou seja, $r_2 \nmid r_1$.
      Neste caso prosseguimos com o algoritmo, dividindo agora r_1 por r_2.

$$r_1 = r_2 \cdot q_3 + r_3 \qquad com \quad 0 < r_3 < r_2 \tag{2.5}$$

De modo geral, este procedimento ocorre, até que se encontre um resto, tal que este resto divida o resto da etapa anterior, ou seja até que encontremos um $n \in \mathbb{N}$ tal que $r_n \mid r_{n-1}$.

O algoritmo é prático e pode ser representado pelo diagrama como faremos a seguir. Iniciaremos com a divisão $b = a \cdot q + r_1$, veja a Tabela 13.

Tabela 13 – Algoritmo de Euclides - Etapa 1

	q_1	
b	a	
r_1		

Fonte: Produção do próprio autor (2023).

Caso necessário, ou seja, quando $r_1 \nmid a$, prosseguiremos com a divisão $a = r_1 \cdot q_2 + r_2$.

Tabela 14 – Algoritmo de Euclides - Etapa 2

	q_1	q_2	
b	a	r_1	
r_1	r_2		

Fonte: Produção do próprio autor (2023).

Caso necessário, ou seja, $r_2 \nmid r_1$, prosseguimos com as divisões sucessivas, até que encontremos $n \in \mathbb{N}$, tal que $r_n \mid r_{n-1}$.

Tabela 15 – Algoritmo de Euclides - Etapa n

	q_1	q_2	q_3	$\dots$	q_{n-1}	q_n	q_{n+1}
b	a	r_1	r_2	$\dots$	r_{n-2}	r_{n-1}	$r_n = (a, b)$
r_1	r_2	r_3	r_4	$\dots$	r_n		

Fonte: Produção do próprio autor (2023).

Exemplo 2.3.3. *Vamos usar agora o algoritmo de Euclides, para calcular* $(534, 192)$*:*

Tabela 16 – Exemplo de cálculo de *mdc*

	2	1	3	1	1	3
534	192	150	42	24	18	$6 = (534, 192)$
150	42	24	18	6	0	

Fonte: Produção do próprio autor (2023).

Analisando os restos obtidos pelo algoritmo no Exemplo 2.3.3, podemos ver que:
$6 = 24 - 1 \cdot 18$
$18 = 42 - 1 \cdot 24$
$24 = 150 - 3 \cdot 42$
$42 = 192 - 1 \cdot 150$
$150 = 534 - 2 \cdot 192$
Substituindo os valores encontrados, obtemos que: $(534, 192) = 6 = 24 - 1 \cdot 18 = 24 - 1 \cdot (42 - 1 \cdot 24) = 24 - 42 + 24 = 2 \cdot 24 - 42 = 2 \cdot (150 - 3 \cdot 42) - 42 = 2 \cdot 150 - 6 \cdot 42 - 42 = 2 \cdot 150 - 7 \cdot 42 = 2 \cdot 150 - 7 \cdot (192 - 1 \cdot 150) = 2 \cdot 150 - 7 \cdot 192 + 7 \cdot 150 = 9 \cdot 150 - 7 \cdot 192 = 9 \cdot (534 - 2 \cdot 192) - 7 \cdot 192 = 9 \cdot 534 - 18 \cdot 192 - 7 \cdot 192 = 9 \cdot 534 - 25 \cdot 192$

Além de simplesmente calcular o *mdc* entre dois inteiros, o Algoritmo de Euclides também é uma excelente ferramenta para escrever esse *mdc* como uma soma de múltiplos dos números a e b. De acordo com o Exemplo 2.3.3, e da análise de seus restos, feita acima, podemos escrever $(534, 192) = 6 = 9 \cdot 534 + (-25) \cdot 192$. Esta técnica de escrever $(a, b) = m \cdot a + n \cdot b$, com $m, n \in \mathbb{Z}$, é chamada de Algoritmo de Euclides Estendido.

Quando o único divisor comum e positivo entre dois números $a, b \in \mathbb{Z}$ é o número 1, ou seja, $(a, b) = 1$, estes números são chamados primos entre si, ou coprimos. Veja a seguinte proposição:

Proposição 2.3.4. *Dados $a, b \in \mathbb{Z}$, serão primos entre si, ou coprimos, se, e somente se, existirem $m, n \in \mathbb{Z}$, tais que $m \cdot a + n \cdot b = 1$.*

Demonstração. A demonstração desta Proposição pode ser encontrada em (HEFEZ, 2012, cap. 6, p. 4) □

2.4 Mínimo Múltiplo Comum (MMC)

Sejam $a, b \in \mathbb{Z}$. Se um número inteiro é múltiplo simultaneamente de a e de b, dizemos que ele é um múltiplo comum de a e b. É fácil observar que ab e 0 são múltiplos comuns de a e b.

Ao menor dos números naturais que são múltiplos comuns de a e b, ambos não nulos, chamaremos de Mínimo Múltiplo Comum de a e b, e denotaremos por $mmc[a, b]$, ou simplesmente $[a, b]$. Se o número natural m é um mínimo múltiplo comum de a e b então deve ter as propriedades simultaneamente:

(i) m é múltiplo comum de a e b.

(ii) Se $c \in \mathbb{Z}$ é um múltiplo comum de a e b então $m \mid c$.

A Unicidade do mmc pode ser demonstrada deste modo: Sejam m_1 e m_2 dois mínimos múltiplos comuns de a e b. Então pela propriedade (ii) acima, temos que $m_1 \mid m_2$ e $m_2 \mid m_1$. Isso nos mostra que $m_1 = m_2$, pois $m_1, m_2 \in \mathbb{N}$, e que se o mínimo múltiplo comum existir ele é único.

Exemplo 2.4.1. *Veja este exemplo:*
O número 24 é um múltiplo comum de 4 e 6, porém não é o $mmc[4, 6]$. O número 12 é o $mmc[4, 6]$, pois 12 é o menor dos múltiplos comuns de 4 e 6 e $12 \mid 24$.

Temos também que $[-a, b] = [a, -b] = [-a, -b] = [a, b]$.

Proposição 2.4.2. *Dados $a, b \in \mathbb{Z}$, então existe $[a, b]$ e temos que:*

$$[a, b](a, b) = |ab|$$

Corolário 2.4.3. *Dados $a, b \in \mathbb{Z}$, tal que $(a, b) = 1$, tem-se que;*

$$[a, b] = |ab|.$$

Exemplo 2.4.4. *Observe exemplos referentes à Proposição 2.4.2 e ao Corolário 2.4.3, respectivamente:*

1. *Seja* $a = 8$ *e* $b = 12$*, então,* $[8, 12](8, 12) = 24 \cdot 4 = 96 = |96| = |ab|$.
2. *Seja* $a = 8$ *e* $b = 11$*, então,* $[8, 11] = 8 \cdot 11 = 88 = |88| = |ab|$*. Note que* $(8, 11) = 1$*, ou seja, são relativamente primos ou primos entre si.*

Proposição 2.4.5. *Dados* $a_1, \ldots, a_{n-1}, a_n \in \mathbb{Z}$*, existe* $[a_1, \ldots, a_{n-1}, a_n]$ *e* $[a_1, \ldots, a_{n-1}, a_n] = [a_1, \ldots, [a_{n-1}, a_n]]$.

Demonstração. A demonstração desta Proposição pode ser encontrada em (HEFEZ, 2012, cap. 7. p. 4) □

Exemplo 2.4.6. *Vamos calcular o mínimo múltiplo comum* $[8, 12, 15, 16]$*. Pela Proposição 2.4.5, temos que* $[8, 12, 15, 16] = [8, 12, [15, 16]]$*. Observe que* $(15, 16) = 1$*, então pelo Corolário 2.4.3,* $[15, 16] = 15 \cdot 16 = 240$*. Logo,* $[8, 12, 15, 16] = [8, 12, 240] = [8, [12, 240]]$*. Temos que* $[12, 240] = 240$*. Logo,* $[8, [12, 240]] = [8, 240] = 240$.

2.5 Equações Diofantinas Lineares

Equações diofantinas lineares são equações do tipo:

$$aX + bY = c,$$

com $a, b, c \in \mathbb{Z}$. O nome "Diofantinas" vem em homenagem ao matemático helenístico Diofanto de Alexandria, que estudou tais equações e foi um dos primeiros a utilizar símbolos na álgebra. Observe que algumas destas equações possuem muitas soluções, como é o caso da equação:

$$3X + 6Y = 24,$$

que tem como exemplo de soluções inteiras:

$$3 \cdot 4 + 6 \cdot 2 = 24$$

$$3 \cdot 6 + 6 \cdot 1 = 24$$

$$3 \cdot (-2) + 6 \cdot 5 = 24.$$

Porém, existem equações que não possuem solução, como a equação:

$$4X + 6Y = 35.$$

Note que $4X + 6Y$ é par para quaisquer valores de X e Y inteiros e, portanto, nunca resultará em 35.

Teorema 2.5.1. *Critério de existência de soluções em equações diofantinas.*
Sejam $a, b, c \in \mathbb{Z}$, temos que a equação $aX + bY = c$, admite solução se, e somente se, $(a, b) \mid c$.

Proposição 2.5.2. *Se x_0, y_0 é uma solução da equação $aX + bY = c$, com $(a, b) = 1$ então:*

$$x = x_0 + tb$$

$$y = y_0 - ta,$$

com $t \in \mathbb{Z}$, são as soluções da equação.

Demonstração. Seja x, y uma solução qualquer da equação $aX + bY = c$, então,
$ax + by = ax_0 + by_0 = c \Rightarrow ax - ax_0 = by_0 - by \Rightarrow a(x - x_0) = b(y_0 - y)$.
Como $(a, b) = 1$, temos que $b|(x - x_0) \Rightarrow x - x_0 = tb \Rightarrow x = x_0 + tb$, com $t \in \mathbb{Z}$.
Analogamente, temos que $a|(y_0 - y) \Rightarrow y_0 - y = ta \Rightarrow -y = -y_0 + ta \Rightarrow y = yo - ta$, com $t \in \mathbb{Z}$.

□

Exemplo 2.5.3. *Vamos resolver a equação $22X + 12Y = 14$. Como $(22, 12) = 2 \mid 14$, a equação tem solução. Dividindo os membros da equação por 2 temos: $11X + 6Y = 7$. Usando o algoritmo de Euclides temos:*

Tabela 17 – Calculando $(11, 6)$

	1	1	5
11	6	5	1
5	1	0	

Fonte: Produção do próprio autor (2023).

Pela Tabela 17, temos:
$1 = 6 - 1 \cdot 5$
$5 = 11 - 1 \cdot 6$.
Substituindo os valores encontrados, temos que $(11, 6) = 1 = 6 - 1 \cdot 5 = 6 - 1 \cdot (11 - 1 \cdot 6) = 6 - 1 \cdot 11 + 1 \cdot 6 = -1 \cdot 11 + 2 \cdot 6 \Rightarrow 1 = -1 \cdot 11 + 2 \cdot 6 \Rightarrow 7 = 11 \cdot (-7) + 6 \cdot 14$. *Portanto, $x_0 = -7$ e $y_0 = 14$ é uma solução particular da equação. Considerando que $(11, 6) = 1$, as demais soluções são:*

$$x = -7 + 6t, \quad y = 14 - 11t,$$

com $t \in \mathbb{Z}$.

Não raro, precisamos resolver equações diofantinas do tipo $aX + bY = c$ em $\mathbb{N} \cup \{0\}$ em que $a, b, c \in \mathbb{N}$. Dependeremos de algumas definições e proposições para essas resoluções.

Proposição 2.5.4. *Todo número natural c pode ser escrito de maneira única como $c = na + mb$, com $a, b \in \mathbb{N}$, com $0 \leqslant n < b$ e $n, m \in \mathbb{Z}$.*

Demonstração. A demonstração da Proposição pode ser encontrada em (HEFEZ, 2012, cap.8, p. 5) □

Definiremos o conjunto $S(a, b) = \{xa + yb; x, y \in \mathbb{N} \cup \{0\}\}$.

Definiremos também que o conjunto das lacunas de $S(a, b)$ como sendo o conjunto $\ell(a, b) = \mathbb{N} - S(a, b)$. Temos que:

$$\ell(a, b) = \{na - mb; n, m, na - mb \in \mathbb{N}, n < b\}.$$

O conjunto finito $\ell(a, b)$ tem um maior elemento dado por $\max \ell(a, b) = (b - 1) \cdot a - b$.

Teorema 2.5.5. *A equação $aX + bY = c$, com $(a, b) = 1$ tem solução em $\mathbb{N} \cup \{0\}$ se, e somente se $c \notin \ell(a, b) = \{na - mb; n, m, na - mb \in \mathbb{N}, n < b\}$.*

Demonstração. A demonstração deste Teorema pode ser encontrada em (HEFEZ, 2012, cap.8, p.6) □

Exemplo 2.5.6. *Determinar para quais valores de c, a equação $9X + 5Y = c$ tem solução em $\mathbb{N} \cup \{0\}$. Vamos determinar o conjunto de lacunas de $S(9, 5)$ que será dado por $\ell(9, 5) = \{9n - 5m; n, m, 9n - 5m \in \mathbb{N}, n < 5\}$.*
Temos que o maior elemento do conjunto de lacunas é dado por: $\max \ell(9, 5) = (5-1)\cdot 9-5 = 4 \cdot 9 - 5 = 36 - 5 = 31$.
Calculando as lacunas, encontramos:
$9 \cdot 1 - 5 \cdot 1 = 9 - 5 = 4$
$9 \cdot 1 - 5 \cdot 2 = -1$ *(não serve, pois* $(-1) \notin \mathbb{N}$*).*
$9 \cdot 2 - 5 \cdot 1 = 18 - 5 = 13$
$9 \cdot 2 - 5 \cdot 2 = 18 - 10 = 8$
$9 \cdot 2 - 5 \cdot 3 = 18 - 15 = 3$
$9 \cdot 2 - 5 \cdot 4 = 18 - 20 = -2$ *(não serve, pois* $(-2) \notin \mathbb{N}$*)*
$9 \cdot 3 - 5 \cdot 1 = 27 - 5 = 22$
$9 \cdot 3 - 5 \cdot 2 = 27 - 10 = 17$
$9 \cdot 3 - 5 \cdot 3 = 27 - 15 = 12$
$9 \cdot 3 - 5 \cdot 4 = 27 - 20 = 7$
$9 \cdot 3 - 5 \cdot 5 = 27 - 25 = 2$
$9 \cdot 3 - 5 \cdot 6 = 27 - 30 = -3$ *(não serve, pois* $(-3) \notin \mathbb{N}$*)*
$9 \cdot 4 - 5 \cdot 1 = 36 - 5 = 31$ *(maior elemento)*
$9 \cdot 4 - 5 \cdot 2 = 36 - 10 = 26$
$9 \cdot 4 - 5 \cdot 3 = 36 - 15 = 21$

$9 \cdot 4 - 5 \cdot 4 = 36 - 20 = 16$
$9 \cdot 4 - 5 \cdot 5 = 36 - 25 = 11$
$9 \cdot 4 - 5 \cdot 6 = 36 - 30 = 6$
$9 \cdot 4 - 5 \cdot 7 = 36 - 35 = 1$
$9 \cdot 4 - 5 \cdot 8 = 36 - 40 = -4$ *(não serve, pois* $(-4) \notin \mathbb{N}$*)*
O conjunto de lacunas de $S(9,5)$ *é o conjunto* $\ell(9,5) = \{1,2,3,4,6,7,8,11,12,13,16,17,21,22,26,31\}$. *Logo* $9X + 5Y = c$ *admitirá solução se, e somente se,* $c \notin \ell(9,5)$.

Exemplo 2.5.7. *Resolver a equação* $9X + 5Y = 24$ *em* $\mathbb{N} \cup \{0\}$. *Como pelo Exemplo 2.5.6,* $24 \notin \ell(9,5)$ *, o Teorema 2.5.5 garante que a equação possui soluções. Usando o algoritmo de Euclides (veja a Tabela 18), temos:*

Tabela 18 – Calculando $(9,5)$

	1	1	4
9	5	4	1
4	1	0	

Fonte: Produção do próprio autor (2023).

$1 = 5 - 1 \cdot 4$
$4 = 9 - 1 \cdot 5.$
Substituindo os valores encontrados, temos que $(9,5) = 1 = 5 - 1 \cdot 4 = 5 - 1 \cdot (9 - 1 \cdot 5) = 5 - 1 \cdot 9 + 1 \cdot 5 = -1 \cdot 9 + 2 \cdot 5 \Rightarrow 1 = -1 \cdot 9 + 2 \cdot 5 \Rightarrow 24 = 9 \cdot (-24) + 5 \cdot 48$. Portanto, $x_0 = -24$ e $y_0 = 48$ é uma solução da equação. Como $(9,5) = 1$, demais são dadas por:

$$x = -24 + 5t, \quad y = 48 - 9t,$$

com $t \in \mathbb{Z}$.
Como queremos soluções em $\mathbb{N} \cup \{0\}$, teremos:
$-24 + 5t \geqslant 0 \Rightarrow 5t \geqslant 24 \Rightarrow t \geqslant \frac{24}{5} \Rightarrow t \geqslant 4,8.$
$48 - 9t \geqslant 0 \Rightarrow -9t \geqslant -48 \Rightarrow 9t \leqslant 48 \Rightarrow t \leqslant \frac{48}{9} \Rightarrow t \leqslant 5,34.$
Portanto, $4,8 \leqslant t \leqslant 5,34 \Rightarrow t = 5$.
Portanto, a equação terá solução única para $\mathbb{N} \cup \{0\}$, quando $t = 5$. A solução será:

$$x = -24 + 5 \cdot 5 = -24 + 25 = 1$$

$$y = 48 - 9 \cdot 5 = 48 - 45 = 3.$$

2.6 Números Primos

2.6.1 Natureza dos Números Primos

O estudo dos números primos é essencial para a compreensão da Teoria dos Números. Desde milênios, os números primos instigam a curiosidade e a admiração dos amantes da Matemática. Inúmeros livros e textos foram escritos sobre o assunto. De acordo com SAUTOY (SAUTOY, 2007), estes números, pela sua própria natureza, estão para a Aritmética, assim como os átomos estão para química e física. São números que não podem ser divididos (a não ser por um e por eles mesmos), nem representados pelo produto de outros números menores. Estes números representam um presente da natureza por sua importância para a Matemática, bem como, por sua capacidade de gerar todos os outros números. São como blocos de construção dos demais números.

A Definição 2.6.1, a seguir é uma consequência do Teorema Fundamental da Aritmética:

Definição 2.6.1. *Um número Natural $p > 1$ é um número primo se, e somente se, seus únicos divisores positivos forem 1 e ele mesmo. Todo número Natural n> 1 pode ser escrito na forma: $n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_t^{a_t}$, ou seja, decomposto em fatores primos.*

Apesar da Definição 2.6.1 ser clara sobre a natureza dos números primos, temos definição alternativa que a complementa e justifica a não primalidade do número 1:

Definição 2.6.2. *Um número primo tem exatamente dois divisores.*

Por consequência desta definição temos que:

- 1 não é primo, pois 1 só possui um divisor natural, no caso ele mesmo.
- 2 é o primeiro número primo e o único número primo par.
- Nenhum número negativo pode ser primo.

Definição 2.6.3. *Um número que não é primo e é maior que 1 é chamado de Número Composto.*

Como não são primos, estes números possuirão divisor ou divisores naturais, além de 1 e eles próprios. Por consequência, temos que 0 e 1 não são números compostos. Isso implica que 0 e 1 não são nem primos, nem compostos.

Exemplo 2.6.4. *Exemplos de números Primos e números Compostos:*
$2, 3, 5, 7, 11, 13, 17, 19$ *e* 23 *são números primos;*
$4, 6, 8, 10, 12, 14, 16, 18, 20$ *e* 22 *são números compostos.*

Teorema 2.6.5. *Teorema Fundamental da Aritmética*
Todo número Natural n, tal que $n > 1$, é primo ou se escreve de forma exclusiva, como um produto de números primos.

Demonstração. A demonstração deste teorema pode ser encontrado em (ARAUJO, 2009, p.36) □

De acordo com o Teorema 2.6.5 , qualquer número Natural $n > 1$ pode ser escrito da forma:

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_{t-1}^{a_{t-1}} \cdot p_t^{a_t}, \tag{2.6}$$

com $p_1, p_2, p_3, \ldots, p_{t-1}, p_t$ primos, $p_1 < p_2 < p_3 < \ldots < p_{t-1} < p_t$, e a_i é um número natural.

Exemplo 2.6.6. *Exemplo de números fatorados:*
$29 = 29$
$123 = 3 \cdot 41$
$2400 = 2^5 \cdot 3 \cdot 5^2$
$3388 = 2^2 \cdot 7 \cdot 11^2$

É possível determinar o número de divisores positivos de um número natural. A seguir veremos como calcular esse número.

Lema 2.6.7. *Seja n um número natural, com $n > 1$, cuja decomposição como produto de potências de primos é $n = p_1^{n_1} \cdot p_2^{n_2} \cdot p_3^{n_3} \ldots p_r^{n_r}$. Então, um número natural d é divisor de n se, e somente se, $d = p_1^{d_1} \cdot p_2^{d_2} \cdot p_3^{d_3} \ldots p_r^{d_r}$, com $0 \leq d_i \leq n_i$, para $i = 1, 2, 3, \ldots, r$.*

Observe que os extremos da variação $0 \leq d_i \leq n_i$, para cada $i = 1, 2, \ldots, r$, nos fornecem os divisores extremos de n:

- Se cada d_i for 0, obtemos o menor divisor: d = 1;
- Se cada d_i for o respectivo n_i, obtemos o maior divisor: $d = n$.

Seja n um número natural tal que $n = p_1^{n_1} \cdot p_2^{n_2} \cdot p_3^{n_3} \cdots p_r^{n_r}$, com $p_1, p_2, p_3, \ldots, p_r$ primos e $p_1 < p_2 < p_3 < \cdots < p_r$, e n_i é um número natural, para $i = 1, 2, 3, \ldots, r$. Seja também $\tau(n)$ o número dos divisores naturais de n. Então:

$$\tau(n) = (n_1 + 1) \cdot (n_2 + 1) \cdot (n_3 + 1) \cdots (n_r + 1) \tag{2.7}$$

Demonstração. Dado um número natural n como nas hipóteses, o Lema 2.6.7 garante que um número natural d é divisor de n se, e somente se, $d = p_1^{d_1} \cdot p_2^{d_2} \cdot p_3^{d_3} \cdots p_r^{d_r}$, com $0 \leq d_i \leq n_i$, para $i = 1, 2, 3, \ldots, r$. Para obtermos $\tau(n)$, vamos contar, quantos números naturais tem

essa forma. Utilizando-se do Principio Fundamental da Contagem, a quantidade de números d, é dada pelo produto das possibilidades de escolhermos, simultaneamente, um valor para cada d_i, $i = 1, 2, \ldots, r$. Mas, para cada i, $i = 1, 2, \ldots, r$, a própria definição de $d_i (0 \leq d_i \leq n_i)$ nos mostra as possibilidades de escolha: entre 0 e n_i, temos $(n_i + 1)$ números. Deste modo, temos: $\tau(n) = (n_1 + 1) \cdot (n_2 + 1) \cdot (n_3 + 1) \cdots (n_r + 1)$ □

Observando a demonstração acima, vemos que para determinar o número de divisores de um número natural, basta somar 1 unidade ao expoente de cada fator primo e multiplicar os resultados.

Exemplo 2.6.8. *Vamos encontrar os divisores positivos de 80.*
Temos que

$$80 = 2^4 \cdot 5$$

Podemos ver que os divisores de 80 são da forma $2^x \cdot 5^y$, *com* $0 \leq x \leq 4$, $0 \leq y \leq 1$, *e assim temos:*
$d_1 = 2^0 \cdot 5^0 = 1$
$d_2 = 2^1 \cdot 5^0 = 2$
$d_3 = 2^2 \cdot 5^0 = 4$
$d_4 = 2^3 \cdot 5^0 = 8$
$d_5 = 2^4 \cdot 5^0 = 16$
$d_6 = 2^0 \cdot 5^1 = 5$
$d_7 = 2^1 \cdot 5^1 = 10$
$d_8 = 2^2 \cdot 5^1 = 20$
$d_9 = 2^3 \cdot 5^1 = 40$
$d_{10} = 2^4 \cdot 5^1 = 80$.
Logo os divisores positivos de 80 *são:* $\{1, 2, 4, 5, 8, 10, 16, 20, 40, 80\}$.

Exemplo 2.6.9. *Exemplo do cálculo do número de divisores do número 180, usando a Equação* (2.7).

$$180 = 2^2 \cdot 3^2 \cdot 5$$

A Equação (2.7) *nos fornece* $\tau = (2+1) \cdot (2+1) \cdot (1+1) = 3 \cdot 3 \cdot 2 = 18$ *divisores naturais. Portanto, o número* 180 *tem* 18 *divisores naturais que são:*

$$\{1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90, 180\}.$$

Podemos determinar o Máximo Divisor Comum entre dois inteiros positivos, se eles forem representados em sua forma fatorada, como um produto de números primos.

Teorema 2.6.10. *Sejam* $a, b \in \mathbb{Z}$. *Se* $a = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_t^{a_t}$ *e* $b = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdot \ldots \cdot p_t^{b_t}$. *Colocando* $\alpha_i = min(a_i, b_i)$, *temos que* $(a, b) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_t^{\alpha_t}$.

Exemplo 2.6.11. *Pelo Teorema 2.6.10 podemos calcular* $(180, 72)$ *da seguinte maneira:*
$180 = 2^2 \cdot 3^2 \cdot 5$
$72 = 2^3 \cdot 3^2$
$(180, 72) = 2^2 \cdot 3^2 \cdot 5^0 = 4 \cdot 9 \cdot 1 = 36.$

2.6.2 Distribuição dos Números Primos

Muitas são as perguntas que vem à mente quando o assunto são os números primos. Uma destas perguntas foi respondida por Euclides aproximadamente no ano $300 A.C$: 'Quantos são os números primos?'. Eis a resposta, dada por meio do Teorema:

Teorema 2.6.12. *Há uma infinidade de números primos.*

Demonstração. Suponha que o número de primos seja finito. Considere P o conjunto de todos os números primos, ou seja, $P = \{p_1, p_2, p_3, p_4, \ldots, p_t\}$. Consideremos o número Natural n, dado por $n = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot \ldots \cdot p_t \Rightarrow n + 1 = (p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot \ldots \cdot p_t) + 1$, temos que $n + 1$ não será divisível por nenhum dos primos $p_1, p_2, p_3, p_4, \ldots, p_t$. Pelo Teorema 2.6.5, temos então duas possibilidades:

1. $n + 1$ é primo.
   Neste caso, temos um novo primo que $\notin P$. Absurdo!

2. $n + 1$ é produto de primos.
   Neste caso, esses primos que compõem $n, \notin P$. Absurdo!
   Portanto, existem infinitos números primos.

□

Outro fato que nos chama atenção quanto aos números primos é sua distribuição irregular dentro dos números naturais. Não existe um padrão ou fórmula que descreva com exatidão a distância entre dois primos consecutivos. Um matemático grego, que foi o diretor de uma grande biblioteca da Grécia em Alexandria, chamado Eratóstenes, que viveu aproximadamente 2 séculos antes de Cristo, desenvolveu um método que ficou conhecido como Crivo de Eratóstenes que permite determinar todos os números primos até onde se quiser, porém não é muito eficaz para valores muito grandes.

Inicialmente, Eratóstenes produzia uma tabela, ou lista, com os todos os números de 1 a 1000. Logo após separava o número 2 que era o primeiro primo e retirava da lista todos os múltiplos de 2, no caso, números pares que por serem divisíveis por 2 não eram primos. Em seguida, passava para o próximo número que não foi retirado da lista, no caso o número 3, separava ele e retirava da lista todos os seus múltiplos, que por serem divisíveis por 3 não seriam primos. E foi em frente, separava o primeiro número primo que não foi

retirado da lista e retirava da lista todos os seus múltiplos, que por consequência eram divisíveis por 5 e portanto não eram primos. Então, a cada novo primo que encontrava, criava um crivo, para eliminar os números que não eram primos. Ao fim de sua lista só resistiram aos crivos os números primos.

Teorema 2.6.13. *Seja n um número natural, de modo que $n > 1$. Se n não for divisível por nenhum número primo p tal que $p^2 \leqslant n$, então n é um número primo.*

Demonstração. Vamos supor que n não seja divisível por nenhum primo p tal que $p^2 \leqslant n$ e que também n não seja primo. Seja p_1 o menor número primo que divida n, isso é possível pois por hipótese n não é primo. Se $p_1 \mid n \Rightarrow n = p_1 \cdot k$, com $p_1 \leqslant k \Rightarrow p_1^2 \leqslant p_1 \cdot k \Rightarrow p_1^2 \leqslant n$. Portanto n é divisível por p_1. Absurdo! □

Exemplo 2.6.14. *Veja a Tabela 19, com os números compostos de 2 a 150.*

Tabela 19 – Crivo de Eratóstenes com números de 2 a 150.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~
131	~~132~~	~~133~~	~~134~~	~~135~~	~~136~~	137	~~138~~	139	~~140~~
~~141~~	~~142~~	~~143~~	~~144~~	~~145~~	~~146~~	~~147~~	~~148~~	149	~~150~~

Fonte: Produção do próprio autor (2023).

Pelo Teorema 2.6.13, podemos notar, que na Tabela 19, precisamos eliminar apenas os múltiplos dos primos até o primo 11, pois o próximo primo é o 13, cujo quadrado é 169, que ultrapassa 150. Este teorema, nos fornece um teste chamado Teste da Primalidade, onde para verificar se um dado número n é primo, é suficiente verificar que esse número não seja divisível por nenhum primo p, tal que $p^2 \leqslant n \Rightarrow p \leqslant \sqrt{n}$.

Temos ainda que todo número primo p tal que $p > 3$ é da forma $6k - 1$ ou $6k + 1$.

Demonstração. Pelo algoritmo da divisão, temos que todo número natural n quando dividido por 6, é da forma $6k, 6k + 1, 6k + 2, 6k + 3, 6k + 4$ ou $6k + 5$. Temos os casos:

1. Se $n = 6k$, então n é múltiplo de 6 e, portanto, não pode ser primo.
2. Se $n = 6k + 1$, então n pode ser primo.
3. Se $n = 6k + 2$, então $n = 2 \cdot (3k + 1)$. Logo, n é par e, portanto, não pode ser primo.
4. Se $n = 6k + 3$, então $n = 3 \cdot (2k + 1)$. Logo, n é múltiplo de 3 e, portanto, não pode ser primo.
5. Se $n = 6k + 4$, então $n = 2 \cdot (3k + 2)$. Logo, n é par e, portanto, não pode ser primo.
6. Se $n = 6k+5$, então $n = 6k+6-1 \Rightarrow n = 6 \cdot 6(k+1)-1$. Logo, n é do tipo $6k_1 - 1$, com $k_1 = k + 1$, e, portanto, pode ser primo.

Portanto, se n é primo, então ele deve ser do tipo $6k + 1$ ou $6k - 1$. □

Observando ainda a Tabela 19, vemos que existem muitos pares de primos consecutivos, da forma p, $p + 2$. Os Pares de primos desta forma, são chamados de Números Gêmeos.

Exemplo 2.6.15. *São exemplos de Números Gêmeos:*
$(3, 5), (5, 7), (11, 13), (17, 19), (41, 43), (59, 61), (71, 73), (101, 103), (107, 109), (137, 139)$.

Conjectura-se que existam infinitos pares de Números Gêmeos. Foi Euclides de Alexandria quem primeiro fez essa conjectura e ela está em aberto até os dias atuais.

Em contrapartida à proximidade dos primos que são Gêmeos, pode-se provar que existem desertos de números primos, ou seja a distância entre um primo e outro é enorme.

Exemplo 2.6.16. *Existe um deserto de primos de 1000 números*
A frase acima é correspondente a dizer que existem 1000 números compostos consecutivos. De fato, considere o número $1001!$ *que pode ser representado pelo produto* $2 \cdot 3 \cdot 4 \cdot 5 \ldots 1001$.
Temos que:
$2 \cdot 3 \cdot 4 \cdot 5 \ldots 1001 + 2$ *é um número par, portanto divisível por* 2
$2 \cdot 3 \cdot 4 \cdot 5 \ldots 1001 + 3$ *é um número divisível por* 3.
$2 \cdot 3 \cdot 4 \cdot 5 \ldots 1001 + 4$ *é um número divisível por* 4.
$2 \cdot 3 \cdot 4 \cdot 5 \ldots 1001 + 5$ *é um número divisível por* 5,
$\vdots \qquad \vdots \qquad \vdots$
$2 \cdot 3 \cdot 4 \cdot 5 \ldots 1001 + 1001$ *é um número divisível por* 1001.
Portanto, temos aqui um deserto de 1000 *números sem nenhum primo.*

Dado um número primo p, não existe um padrão para determinar qual será o próximo número primo. Com relação à densidade deles em meio aos números naturais, em alguns lugares há uma grande quantidade deles e em outros lugares existe uma grande ausência. Pode-se realizar um estudo relativo à frequência dos primos com o auxílio da probabilidade.

Observe a Tabela 20 com a quantidade de números primos até certo número natural dado (dados obtidos no site Khan Academy (ACADEMY, acesso em 08 de junho de 2023)):

Tabela 20 – Quantidade e frequência de primos até certo número Natural.

Número Natural	Quantidade de primos	Frequência
10	4	$\frac{4}{10} = 0,25 = 25\%$
100	25	$\frac{25}{100} = 0,25 = 25\%$
1.000	168	$\frac{168}{1000} = 0168 = 16,8\%$
10.000	1.229	$\frac{1.229}{10.000} = 0,1229 = 12,29\%$
100.000	9.592	$\frac{9.592}{100.000} = 0,09592 \approx 9,59\%$
1.000.000	78.498	$\frac{78.498}{1.000.000} \approx 0,07849 \approx 7,84\%$
10.000.000	664.579	$\frac{664.579}{10.000.000} \approx 0,06645 \approx 6,64\%$
100.000.000	5.761.455	$\frac{5.761.455}{100.000.000} \approx 0,05761 \approx 5,76\%$

Fonte: Produção do próprio autor (2023).

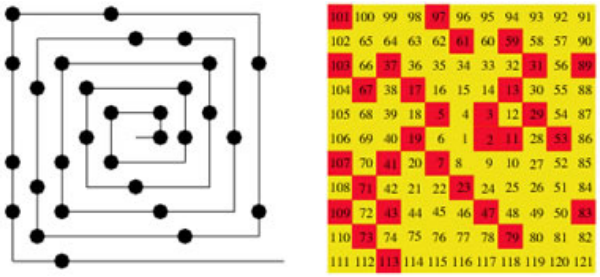
A Tabela 20 nos leva a conjecturar que à medida que aumentamos a quantidade de números naturais, a densidade de primos diminui.

Vamos denotar por $\pi : \mathbb{N} \to \mathbb{N}$ a função tal que $\pi(x)$ é a quantidade de números primos menores ou iguais a um número natural x. Deste modo, considerando o conjunto $\{1, 2, \ldots, x\}$, temos que a probabilidade de que um dos elementos desse conjunto seja um número primo, será dada por $P = \frac{\pi(x)}{x}$.

Exemplo 2.6.17. *Veja exemplos, onde dado um número natural x, determinamos a quantidade de números primos menores ou iguais a x, onde $\#$ representa o número de elementos de um conjunto:*
$\pi(1) = \#\{\} = 0$ *, Pois não existem números primos menores ou iguais a* 1.
$\pi(2) = \#\{2\} = 1$, *Pois só existe o número primo* 2, *que é menor ou igual a* 2.
$\pi(3) = \#\{2, 3\} = 2$
$\pi(10) = \#\{2, 3, 5, 7\} = 4$.
$\pi(150) = \#\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149\} = 35$. *Veja os números que resistiram aos crivos de Eratóstenes na Tabela 19.*

Se construíssemos um gráfico da densidade dos números primos em função dos números naturais, poderíamos ver que quanto mais essa busca avança nos naturais, mais vemos a densidade cair. Esse padrão parece moldar-se quase que fielmente à Espiral Logarítmica, onde, no centro da espiral temos uma densidade maior, uma maior concentração, e em pontos mais afastados do centro essa concentração diminui. Na natureza encontramos padrões semelhantes, como em tempestades, galáxias, flores e animais. Veja a Figura 13 que representa a Espiral de números primos formada até o número natural 121.

Figura 13 – Espiral de números primos até 121

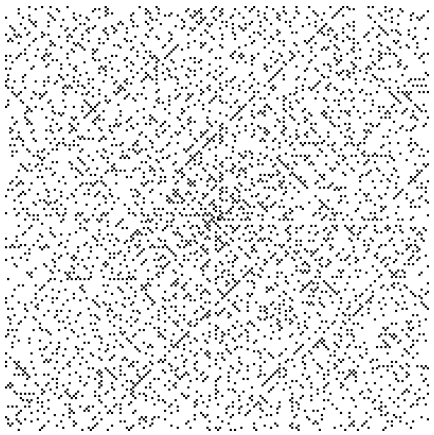


Fonte: Disponível em: <https://www.somatematica.com.br/curiosidades/c104.php>. Acesso em: 03 de set. de 2023.

Esta espiral foi descoberta pelo matemático Stanisław Marcin Ulam em 1963 e mais tarde, em 1964 escrita em um artigo por Stein, M. L.; Ulam, S. M.; e Wells, M. B.. Ela ficou conhecida como espiral de Ulam. Segundo STEIN, ULAM e WELLS (STEIN M. L.; ULAM; WELLS, 1964), o método consiste em numerarmos pontos num plano, de modo que forme uma única sequência e no sentido anti-horário, começando por $(0,0)$ que corresponde ao número 1, ou seja, $(0,0) \Rightarrow 1$, $(1,0) \Rightarrow 2$, $(1,1) \Rightarrow 3, (0,1) \Rightarrow 4$, $(-1,1) \Rightarrow 5$, $(-1,0) \Rightarrow 6$, $(-1,-1) \Rightarrow 7$, $(0,-1) \Rightarrow 8$, $(1,-1) \Rightarrow 9$, $(2,-1) \Rightarrow 10$, $(2,0) \Rightarrow 11$, $(2,1) \Rightarrow 12$, $(2,2) \Rightarrow 13$, e assim sucessivamente até quantos pontos quisermos numerar no plano. Ao marcar os primos em seu plano, Ulam ficou admirado ao notar que os primos apareciam em filas diagonais.

A Figura 14 mostra uma Espiral de Ulam de 40.000 números onde os números primos são representados de preto. O padrão dos primos tenderem a se dispor em diagonais parece repetir-se indistintamente. Observa-se também com um olhar atento que algumas diagonais possuem uma quantidade maior de primos. Um estudo mais aprofundado da Espiral de Ulam pode ser obtida em STEIN, ULAM e WELLS (STEIN M. L.; ULAM; WELLS, 1964) e em livros específicos sobre a disposição dos Números Primos.

Figura 14 – Espiral de Ulam $200X200$



Fonte: Disponível em: <https://upload.wikimedia.org/wikipedia/commons/6/69/Ulam_1.png>. Acesso em: 07 de set. de 2023.

Analisando tabelas de distribuição de primos bem extensas, matemáticos como Legendre e Gauss, concluíram já em sua época, que a densidade dada por $\frac{\pi(x)}{x}$, para um x suficientemente grande, se aproxima e assemelha à já conhecida função $y = \frac{1}{\ln x}$, HEFEZ (HEFEZ, 2012). Esta função nos fornece agora, uma estimativa com bastante precisão da densidade de números primos até um número natural n. A estimativa é cada vez mais precisa à medida que tomamos n cada vez maior.

Exemplo 2.6.18. *Veja alguns exemplos desta estimativa da densidade de números primos até um número Natural n, na qual encontramos a porcentagem de números primos até este número Natural.*

- $\frac{1}{\ln(10.000)} \approx 10,85\%$
- $\frac{1}{\ln(100.000)} \approx 8,68\%$
- $\frac{1}{\ln(1.000.000)} \approx 7,23\%$
- $\frac{1}{\ln(10.000.000)} \approx 6,20\%$
- $\frac{1}{\ln(100.000.000)} \approx 5,42\%$
- $\frac{1}{\ln(10.000.000.000)} \approx 4,34\%$
- $\frac{1}{\ln(100.000.000.000)} \approx 3,94\%$
- $\frac{1}{\ln(100.000.000.000.000)} \approx 3,10\%$

Comparando a Tabela 20 e o Exemplo 2.6.18, podemos notar que à medida que n cresce, a estimativa obtida pela função $y = \frac{1}{\ln x}$, com $x \in \mathbb{N}$ fica mais precisa. Perceba que através desta estimativa para a densidade de primos, podemos também estimar a quantidade de números primos menores que um número Natural x:

$$\frac{\pi(x)}{x} \approx \frac{1}{\ln x} \Rightarrow \pi(x) \approx \frac{x}{\ln x} \tag{2.8}$$

Exemplo 2.6.19. *Veja a estimativa da quantidade de números primos até um número Natural x, nestes exemplos:*

- $\pi(10.000.000) \approx \frac{10.000.000}{\ln(10.000.000)} \approx 620.420$
- $\pi(100.000.000) \approx \frac{100.000.000}{\ln(100.000.000)} \approx 5.428.681$
- $\pi(10.000.000.000) \approx \frac{10.000.000.000}{\ln(10.000.000.000)} \approx 434.294.481$
- $\pi(100.000.000.000) \approx \frac{100.000.000.000}{\ln(100.000.000.000)} \approx 3.948.131.653$
- $\pi(100.000.000.000.000) \approx \frac{100.000.000.000.000}{\ln(100.000.000.000.000)} \approx 3.102.103.442.166$

Esta estimativa torna-se cada vez mais precisa à medida que x torna-se suficientemente grande. No último item do Exemplo 2.6.19 temos uma uma estimativa de aproximadamente 3,1 trilhões de primos até o natural 100 trilhões, enquanto a quantidade real está na casa dos 3,2 trilhões. Essa precisão é de 99,9968%. A maneira como os primos estão distribuídos ainda é um mistério a ser desvendado, assim como alguns problemas em aberto a eles associados. como exemplos temos:

- A conjectura de Goldbach, que diz que todo número natural par e maior ou igual a 4, pode ser escrito como a soma de dois números primos.
- A conjectura dos primos gêmeos, da qual já comentamos neste texto.
- Conjectura-se que a sequência de Fibonacci possua infinitos números primos.
- A Hipótese de Riemann: Essa hipótese diz que a distribuição dos números primos não é aleatória, mas que segue uma padronização que pode ser descrita pela chamada função Zeta de Riemann. Se provada, ela ajudará a desvendar muitos dos mistérios relacionados aos números primos.

Existem hoje programas de computador baseados em grande parte no crivo de Eratóstenes, bem eficazes na busca por números primos bem grandes, bem como procedimentos

para verificar se um dado número é primo ou não. Encontrando dois desses números primos grandes e multiplicando os dois, obtemos um número composto muito maior, que dependendo do tamanho desses primos, mesmo os "melhores" computadores de hoje poderiam levar alguns milhões de anos para fatorar. Essa dificuldade na fatoração de desses números é explorada pelos modernos sistemas de criptografia e são usados hoje para codificar mensagens, com fins comerciais, políticas, sociais, militares, dentre outras. Números primos muito grandes, são um importante recurso para a criptografia.

2.7 Pequeno Teorema de Fermat e Função Totiente de Euler

2.7.1 Pequeno Teorema de Fermat

Há aproximadamente 375 anos, Pierre de Fermat anunciava a um amigo matemático, por meio de uma carta, que havia descoberto um pequeno teorema, mas que era capaz de verificar a primalidade de um número. Esse teorema pode ser pequeno no nome, mas é notável em importância. Veremos agora um lema que será necessário para provarmos o Pequeno Teorema de Fermat:

Lema 2.7.1. *Lema*
Se p é um número primo, então, todos os números $\binom{p}{i}$, com $0 < i < p$, são divisíveis por p.

Demonstração. A demonstração deste Lema pode ser encontrada em (HEFEZ, 2012, cap.13, p.2) □

Teorema 2.7.2. *Pequeno Teorema de Fermat*
Se p é um número primo, então, para todo número inteiro a, tem-se que p divide $a^p - a$.

Demonstração. Provemos por indução sobre a.

(i) Para $a = 0$, temos que $a^p - a = 0$, portanto válido, pois $p \mid 0$.
Para $a = 1$, temos que $a^p - a = 0$, portanto também válido.

(ii) Suponha que $p \mid (a^p - a)$. Vamos provar que $p \mid (a+1)^p - (a+1)$. Temos que $(a+1)^p - (a+1) = \binom{p}{0}a^p + \binom{p}{1}a^{p-1}\cdot 1 + \binom{p}{2}a^{p-2}\cdot 1 + \ldots + \binom{p}{p-1}a\cdot 1^{p-1} + \binom{p}{p}1^p - a - 1 = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \ldots + \binom{p}{p-1}a + 1 - a - 1 = a^p - a + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \ldots + \binom{p}{p-1}a$.
Pela hipótese de indução, temos que $p \mid a^p - a$ e pelo Lema 2.7.1 sabemos que $p \mid \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \ldots + \binom{p}{p-1}a$. Logo $p \mid a^p - a + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \ldots + \binom{p}{p-1}a$.
Portanto, $p \mid a^p - a \ \ \forall \ a \in \mathbb{Z}$.

□

Exemplo 2.7.3. *Mostre que* $42 \mid a^7 - a$ *para todo número inteiro* a.
Observe que $42 = 2 \cdot 3 \cdot 7$. *Temos que:*

(i) a^7 *e* a *têm a mesma paridade, portanto,* $a^7 - a$ *é par e logo,* $2 \mid a^7 - a$.

(ii) $a^7 - a = a \cdot (a^6 - 1) = a \cdot (a^3 - 1) \cdot (a^3 + 1) = a \cdot (a-1) \cdot (a^2 + a + 1) \cdot (a+1) \cdot (a^2 - a + 1) = (a-1) \cdot a \cdot (a+1) \cdot (a^2 + a + 1) \cdot (a^2 - a + 1)$. *Como,* $3 \mid (a-1) \cdot a \cdot (a+1)$ *que é o produto de três inteiros consecutivos, temos que* $3 \mid (a-1) \cdot a \cdot (a+1) \cdot (a^2 + a + 1) \cdot (a^2 - a + 1)$. *Logo,* $3 \mid a^7 - a$.

(iii) Pelo Pequeno Teorema de Fermat, $7 \mid a^7 - a$.

Portanto, $2 \cdot 3 \cdot 7 = 42 \mid a^7 - a$.

Como consequência do Pequeno Teorema de Fermat, o corolário seguinte é imediato:

Corolário 2.7.4. *Corolário do Pequeno Teorema de Fermat*
Seja p *um número primo e* a *um número inteiro, tal que* $p \nmid a$, *então,* $p \mid a^{p-1} - 1$.

Demonstração. De fato, pois $a^p - a = a \cdot (a^{p-1} - 1)$. Temos que $p \mid a^p - a \Rightarrow p \mid a \cdot (a^{p-1} - 1)$ e como $p \nmid a$, resta que $p \mid a^{p-1} - 1$. □

Exemplo 2.7.5. *Veja alguns exemplos de aplicação do Corolário 2.7.4 que também é chamado de Pequeno Teorema de Fermat:*

- $13 \mid 2^{12} - 1$. *De fato, pois* $2^{12} - 1 = 4096 - 1 = 4095$ *e* 4095 *dividido por* 13 *é igual a* 315. *Observe que* $13 \nmid 2$.
- $19 \mid 8^{18} - 1$. *De fato, pois* $8^{18} - 1 = 18.014.398.509.481.984 - 1 = 18.014.398.509.481.983$ *e* 18.014.398.509.481.983 *dividido por* 19 *é igual a* 948.126.237.341.157. *Observe que* $19 \nmid 8$.
- $5 \mid 12^4 - 1$. *De fato, pois* $12^4 - 1 = 20.736 - 1 = 20.735$ *e* 20.735 *dividido por* 5 *é igual a* 4.147. *Observe que* $5 \nmid 12$.

2.7.2 Função Totiente de Euler

Um elemento importante na teoria dos números, é a chamada de Função Totiente de Euler $\varphi = \mathbb{N} \longrightarrow \mathbb{N}$, que designaremos por $\varphi(n)$, e que corresponde à quantidade de números naturais menores que n e primos relativos com n. Convenciona-se que $\varphi(1) = 1$.

Teorema 2.7.6. *Se* p *é um número primo, então* $\varphi(p) = p - 1$.

Demonstração. De fato, se p é primo, então, todo número natural menor que p é um primo relativo a p. □

Exemplo 2.7.7. *Determine* $\varphi(25)$, $\varphi(41)$ *e* $\varphi(72)$.

- $\varphi(25) = 20$, *pois existem* 20 *números naturais menores que* 25, *que são primos relativos a 25 que são:* $\{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$.
- $\varphi(41) = 40$, *pois* 41 *é primo.*
- $\varphi(72) = 24$, *pois existem* 24 *números naturais menores que* 25, *que são primos relativos a* 72 *que são:* $\{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 65, 67, 71\}$.

O Exemplo 2.7.7 nos mostra os primos relativos aos números compostos 25 e 72 menores que eles, mas não como encontrar a quantidade de primos sem precisar descrevê-los. Veremos adiante como calcular $\varphi(n)$ em geral.

Proposição 2.7.8. *Sejam* m *e* n *números naturais, com* $(m, n) = 1$, *então* $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

Teorema 2.7.9. *Sejam* p *e* q *números primos, tal que* $(p, q) = 1$ *e seja* $n = p \cdot q$ *então,* $\varphi(n) = \varphi(p) \cdot \varphi(q)$.

Demonstração. Seja o conjunto dos números naturais menores que n dado por:
$\{1, \ldots, pq - 1\}$ dentro desse conjunto existem os seguintes conjuntos que são os conjuntos dos números Naturais que não são primos relativos de n, dados por $\{p, 2p, \ldots, (q-1) \cdot p\}$ e $\{q, 2q, \ldots, (p-1) \cdot q)$. Portanto, $\varphi(n) = (pq - 1) - [(q - 1) + (p - 1)] = pq - (p + q) + 1 = (p - 1) \cdot (q - 1) \Rightarrow \varphi(n) = \varphi(p) \cdot \varphi(q)$ □

Exemplo 2.7.10. *Análise do cálculo de* $\varphi(21)$
Observe que $21 = 3 \cdot 7$. *Considere* $p = 3$ *e* $q = 7$. *Então, pelo Teorema 2.7.9, temos* $\varphi(21) = \varphi(3) \cdot \varphi(7) = 2 \cdot 6 = 12$.
Veja que os naturais menores que 21, *são dados por:*
$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20\}$.
Os naturais que não são primos relativos com 21 *são:* $\{7, 14\}$ *e* $\{3, 6, 9, 12, 15, 18\}$. *Note ainda que* $18 = (7 - 1) \cdot 3 = (q - 1) \cdot p$ *e que* $14 = (3 - 1) \cdot 7 = (p - 1) \cdot q$. *Por fim, os* 20 *elementos do primeiro conjunto, subtraídos dos* $2 = (3 - 1) = (p - 1)$ *elementos do segundo conjunto e dos* $6 = (7 - 1) = (q - 1)$ *elementos do terceiro conjunto, resulta em* 12 *elementos.*

Lema 2.7.11. *Se p é um número primo e r um número natural, então, $\varphi(p^r) = p^r - p^{r-1}$.*

Demonstração. Precisamos encontrar o número de primos relativos com p^r e que são menores que ele. Considere o conjunto dos números naturais menores ou iguais a p^r: $\{1, \ldots, p^r\}$, cujo número de elementos é p^r. Vamos retirar desse conjunto os números naturais menores que p^r e que não são primos relativos com p^r, ou seja, os múltiplos de p: $\{p, 2p, \ldots, p^{r-1} \cdot p\}$ cujo número de elementos é p^{r-1}.

Assim, temos que $\varphi(p^r) = p^r - p^{r-1}$. □

O Lema 2.7.11 pode ser rescrito como $\varphi(p^r) = p^r \cdot \left(1 - \frac{1}{p}\right)$.

O teorema a seguir, nos fornece $\varphi(n)$ para todo $n \in \mathbb{N}$.

Teorema 2.7.12. *Seja $n = p_1^{r_1} \ldots {p_n}^{r_n}$, com n >1, então,*
$\varphi(n) = p_1^{r_1} \ldots {p_n}^{r_n} \left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_n}\right)$.

O Teorema 2.7.12 pode ser reescrito da seguinte maneira:
$\varphi(n) = p_1^{r_1 - 1} \ldots p_n^{r_n - 1}(p_1 - 1) \ldots (p_n - 1) \Rightarrow$
$\varphi(p_1^{r_1} \ldots {p_n}^{r_n}) = p_1^{r_1 - 1} \ldots p_n^{r_n - 1}(p_1 - 1) \ldots (p_n - 1)$

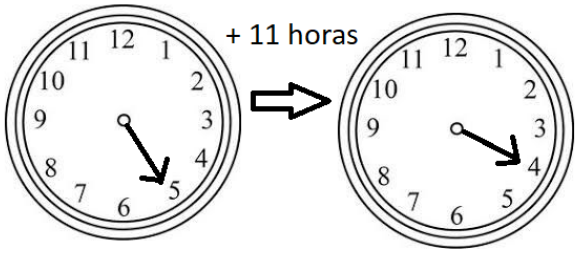
Exemplo 2.7.13. *Determine $\varphi(72)$.*
Temos que $\varphi(72) = \varphi(2^3 \cdot 3^2) = 2^2 \cdot 3^1 \cdot (2-1) \cdot (3-1) = 4 \cdot 3 \cdot 1 \cdot 2 = 24$.

2.8 Congruências

Euler foi o primeiro matemático a abordar o tema Congruência, aproximadamente em 1750. Posteriormente, Gauss modernizou o conceito, por volta de 1801, em seu livro Disquisitiones Arithmeticae. A aritmética modular é uma aritmética para números inteiros, onde esses números retrocedem, quando alcançam um certo número que chamaremos de módulo. Um exemplo simples do uso dessa aritmética está quando observamos um relógio de 12 horas. Se agora são 5 horas, daqui a 11 horas serão 4 horas. Se fossemos apenas somar as horas, teríamos $5 + 11 = 16$ horas, porém como as horas retrocedem no relógio quando atingem 12 horas, teremos apenas 4 horas. Temos que esta aritmética utilizada neste exemplo, pode ser chamada de aritmética módulo 12 e por conseguinte, dizemos que 16 é congruente a 4 módulo 12. Isto significa que 16 horas em um relógio de 24 horas é correspondente a 4 horas em um relógio de 12 horas. A aritmética modular também é conhecida como Aritmética do Relógio.

Veja a imagem representativa do exemplo dado acima.

Figura 15 – A figura mostra que 16 horas é congruente a 4 horas módulo 12 horas



Fonte: Produção do próprio autor (2023).

Definição 2.8.1. *Seja a um número inteiro e n um número natural não nulo. Definimos $a \pmod n$ como resto da divisão euclidiana de a por n, onde n é chamado módulo. Temos então que todo número a pode ser escrito da seguinte maneira:*

$$a = q \cdot n + r, \quad 0 \leqslant r < n \Rightarrow a = q \cdot n + (a \pmod n) \tag{2.9}$$

Em outras palavras, $r = a \pmod n$.

Exemplo 2.8.2. *Veja exemplos de aplicação da Definição 2.8.1:*

- $15 \pmod 8 = 7$, *pois* $15 = 1 \cdot 8 + 7$.
- $-15 \pmod 8 = 1$, *pois* $-15 = (-2) \cdot 8 + 1$

Proposição 2.8.3. *Dodos dois números inteiros a e b, dizemos que eles são congruentes módulo n, se tivermos $a \pmod n = b \pmod n$. Escreveremos essa relação de congruência como:*

$$a \equiv b \pmod n.$$

Exemplo 2.8.4. *Veja exemplos de congruências:*

- $25 \equiv 4 \pmod 7$, *pois* 25 *e* 4 *deixam mesmo resto na divisão por* 7.
- $18 \equiv -2 \pmod 5$ *pois* 18 *e* -2 *deixam mesmo resto na divisão por* 5.
- $25 \equiv 11 \pmod 2$ *pois* 25 *e* 11 *deixam mesmo resto na divisão por* 2.
- $72 \equiv 0 \pmod 6$ *pois* 72 *e* 0 *deixam mesmo resto na divisão por* 6.

Se $a \equiv 0 \pmod n$, então $n \mid a$. Observando o quarto item do Exemplo 2.8.4, podemos afirmar que $6 \mid 72$.

Propriedades: Para todo $n \in \mathbb{N}$, e todos a, b e $c \in \mathbb{Z}$, temos que:

1. $a \equiv a \pmod{n}$. (Reflexividade)
2. $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$. (Simetria)
3. $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$. (Transitividade)

Proposição 2.8.5. *Dados a e $b \in \mathbb{Z}$ e $n \in \mathbb{N}$ com $n > 1$, temos que $a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b)$.*

Demonstração. (i) $\Rightarrow$ Se $a \equiv b \pmod{n}$, então, $a = k \cdot n + b$ para algum $k \in \mathbb{Z}$. Desse modo, $(a - b) = k \cdot n$ e portanto, $n \mid (a - b)$.

(ii) $\Leftarrow$ Temos que se $n \mid (a - b)$ então $a - b = k \cdot n$ para algum $k \in \mathbb{Z}$. Logo, $a = k \cdot n + b$. Pela Definição 2.8.1, $b \equiv a \pmod{n}$.

□

Exemplo 2.8.6. *Veja os exemplos:*

- $27 \equiv 2 \pmod{5}$, *pois* $5 \mid (27 - 2) = 25$.
- $-17 \equiv 3 \pmod{4}$, *pois* $4 \mid (-17 - 3) = -20$.
- $24 \equiv 10 \pmod{7}$, *pois* $7 \mid (24 - 10) = 14$.

A relação de congruência, tem compatibilidade com as operações de adição, multiplicação e potenciação. Sejam a, b, c e $d \in \mathbb{Z}$, n e $k \in \mathbb{N}$, com $n > 1$, seguem as seguintes propriedades:

1. $a \pmod{n} + b \pmod{n} = (a + b) \pmod{n}$.
2. $a \pmod{n} - b \pmod{n} = (a - b) \pmod{n}$.
3. $a \pmod{n} \cdot b \pmod{n} = (a \cdot b) \pmod{n}$.
4. Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então $(a + c) \equiv (b + d) \pmod{n}$
5. Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então $(a \cdot c) \equiv (b \cdot d) \pmod{n}$
6. Se $a \equiv b \pmod{n}$, então $a^k \equiv b^k \pmod{n}$.

Exemplo 2.8.7. *Eis alguns exemplos destas propriedades:*
Para os itens 1,2 e 3 considere $17 \pmod{9} = 8$ *e* $23 \pmod{9} = 5$. *Para os itens restantes, considere* $17 \equiv 8 \pmod{9}$ *e* $23 \equiv 5 \pmod{9}$.

1. $[(17 \pmod 9) + (23 \pmod 9) \pmod 9] = [8 + 5 \pmod{19}] = 13 \pmod 9 = 4$.
   Usando a propriedade acima: $(17 + 23) \pmod 9 = 40 \pmod 9 = 4$.

2. $[(17 \pmod 9) - (23 \pmod 9) \pmod 9] = [8 - 5 \pmod 9] = 3 \pmod 9 = 3$.
   Usando a propriedade acima: $(17 - 23) \pmod 9 = -6 \pmod 9 = 3$.

3. $[(17 \pmod 9) \cdot (23 \pmod 9) \pmod 9] = [8 \cdot 5 \pmod 9] = 40 \pmod 9 = 4$.
   Usando a propriedade acima: $(17 \cdot 23) \pmod 9 = 391 \pmod 9 = 4$.

4. *Seja* $17 \equiv 8 \pmod 9$ *e* $23 \equiv 5 \pmod 9$. *Temos que* $(17 + 23) \pmod 9 = 40 \pmod 9 = 4$ *e* $(8 + 5) \pmod 9 = 13 \pmod 9 = 4$.
   Usando a propriedade acima: $(17 + 23) \equiv (8 + 5) \pmod 9 \Rightarrow 40 \equiv 13 \pmod 9$.

5. *Seja* $17 \equiv 8 \pmod 9$ *e* $23 \equiv 5 \pmod 9$. *Temos que* $(17 \cdot 23) \pmod 9 = 391 \pmod 9 = 4$ *e* $(8 \cdot 5) \pmod 9 = 40 \pmod 9 = 4$.
   Usando a propriedade acima: $(17 \cdot 23) \equiv (8 \cdot 5) \pmod 9 \Rightarrow 391 \equiv 40 \pmod 9$.

6. *Seja* $17 \equiv 8 \pmod 9$. *Temos que* $17^2 \pmod 9 = 289 \pmod 9 = 1$ *e* $8^2 \pmod 9 = 64 \pmod 9 = 1$.
   Usando a propriedade acima: $17^2 \equiv 8^2 \pmod 9 \Rightarrow 289 \equiv 64 \pmod 9$.

As regras da adição, subtração e multiplicação da aritmética tradicional também são utilizadas na aritmética modular. Observe as Tabelas 21 e 22 que nos dão alguns exemplos da adição e multiplicação módulo 9.

Tabela 21 – Adição módulo 9.

+	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

Fonte: Produção do próprio autor (2023).

Cada número inteiro possui um inverso aditivo módulo n na aritmética modular.

O inverso aditivo de um número inteiro x módulo n com $n \in \mathbb{N}$ é o número inteiro y tal que que $(x + y) \pmod n = 0$. A Tabela 21 nos mostra exemplos de inversos aditivos de um inteiro módulo 9. Para encontrar o inverso aditivo de um número em uma determinada coluna, é só percorrer as linhas correspondentes até encontrar 0. O valor correspondente ao primeiro número da coluna é o inverso aditivo.

Tabela 22 – Multiplicação módulo 9.

x	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

Fonte: Produção do próprio autor (2023).

Na aritmética modular, nem todo número inteiro possui um inverso multiplicativo módulo n. O inverso multiplicativo de um número inteiro x módulo n com $n \in \mathbb{N}$ é o número inteiro y tal que que $(x \cdot y) \pmod{n} = 1$. A Tabela 22 nos mostra exemplos de inversos multiplicativos de um inteiro módulo 9. Para encontrar o inverso multiplicativo de um número em uma determinada coluna, é só percorrer as linhas correspondentes até encontrar 1. O valor correspondente ao primeiro número da coluna é o inverso multiplicativo. Pode-se ver pela tabela que existem números inteiros módulo 9 que não possuem inverso multiplicativo como o caso do número 3 e do número 6.

Mais algumas propriedades da aritmética modular

Seja Z_n o conjunto de todos os inteiros não negativos e menores que n. Desse modo, $Z_n = \{0, 1, 2, 3, \ldots, (n-1)\}$ é chamado de Conjunto de Resíduos Módulo n ou Classe de Resíduos Módulo n, onde cada inteiro em Z_n representa uma classe de resíduos módulo n. Podemos denotar essas classes de resíduos módulo n por $[0], [1], [2], \ldots, [n-1]$, onde cada resíduo r é dado por: $[r] = \{a \mid a \text{ é um inteiro}, a \equiv r \pmod{n}\}$.

Exemplo 2.8.8. *As classes de resíduo módulo 9 são:*

- $[0] = \{\ldots, -36, -27, -18, -9, 0, 9, 18, 27, 36, \ldots\}$
- $[1] = \{\ldots, -35, -26, -17, -8, 1, 10, 19, 28, 37, \ldots\}$
- $[2] = \{\ldots, -34, -25, -16, -7, 2, 11, 20, 29, 38, \ldots\}$
- $[3] = \{\ldots, -33, -24, -15, -6, 3, 12, 21, 30, 39, \ldots\}$
- $[4] = \{\ldots, -32, -23, -14, -5, 4, 13, 22, 31, 40, \ldots\}$
- $[5] = \{\ldots, -31, -22, -13, -4, 5, 14, 23, 32, 41, \ldots\}$
- $[6] = \{\ldots, -30, -21, -12, -3, 6, 15, 24, 33, 42, \ldots\}$

- $[7] = \{\ldots, -29, -20, -11, -2, 7, 16, 25, 34, 43, \ldots\}$
- $[8] = \{\ldots, -28, -19, -10, -1, 8, 17, 26, 35, 44, \ldots\}$

Proposição 2.8.9. *Sejam a, b e $c \in \mathbb{Z}$ e $n \in \mathbb{N}$, temos que se $(a+b) \equiv (a+c) \pmod{n}$ então $b \equiv c \pmod{n}$.*

Essa congruência é compatível com a existência do inverso aditivo. Basta adicionar o inverso aditivo de a que chamaremos de $-a$ aos dois lados da congruência e teremos:

$$[(-a)+a+b] \equiv [(-a)+a+c] \pmod{n} \Rightarrow [0+b] \equiv [0+c] \pmod{n} \Rightarrow b \equiv c \pmod{n}$$

Proposição 2.8.10. *Sejam a, b e $c \in \mathbb{Z}$ e $n \in \mathbb{N}$, temos que se $(a \cdot b) \equiv (a \cdot c) \pmod{n}$ então $b \equiv c \pmod{n}$ se a e n forem primos relativos.*

Se a e n forem primos relativos, essa congruência é compatível com a existência do inverso multiplicativo. Basta multiplicar pelo inverso multiplicativo de a, que chamaremos a^{-1}, aos dois lados da congruência e teremos:

$$(a^{-1} \cdot a \cdot b) \equiv (a^{-1} \cdot a \cdot c) \pmod{n} \Rightarrow (1 \cdot b) \equiv (1 \cdot c) \pmod{n} \Rightarrow b \equiv c \pmod{n}$$

Exemplo 2.8.11. *Veja exemplos referentes às Proposições 2.8.9 e 2.8.10, respectivamente:*

1. $(6 + 35) \equiv (6 + 8) \pmod{9}$
   $35 \equiv 8 \pmod{9}$.
2. - $(7 \cdot 12) \equiv (7 \cdot 3) \pmod{9} \Rightarrow 84 \equiv 21 \pmod{9}$.
     Observe que $12 \equiv 3 \pmod{9}$ *e que* 7 *e* 9 *são primos relativos.*
   - $(6 \cdot 7) \equiv (6 \cdot 4) \pmod{9} \Rightarrow 42 \equiv 24 \pmod{9}$, *porém* $7 \not\equiv 4 \pmod{9}$.
     Observe que 6 *e* 9 *não são primos relativos.*

2.8.1 Algoritmo de Euclides Revisitado

Teorema 2.8.12. *Sejam a e b números inteiros com $0 \leqslant b \leqslant a$ temos que:*

$$(a, b) = (b, a \pmod{b}) \tag{2.10}$$

Demonstração. (i) $\Rightarrow$ Seja $d = (a, b)$ então $d \mid a$ e $d \mid b$. Temos que $a = k \cdot b + r$, para algum $k, r \in \mathbb{Z}$. Desse modo, temos que

$$a = k \cdot b + r \Rightarrow a \pmod{b} = r.$$

Segue então que $a \pmod{b} = a - k \cdot b$. Temos que $d \mid b$ e portanto, $d \mid k \cdot b$. Como sabemos também que $d \mid a$, temos que $d \mid (a - k \cdot b)$ então, $d \mid a \pmod{b}$.

(ii) $\Leftarrow$ Se $d = (b, a \pmod b)$, então $d \mid b$ e $d \mid a \pmod b$, logo $d \mid k \cdot b$ e

$$d \mid (k \cdot b + a \pmod b),$$

para algum $k \in \mathbb{Z}$. Portanto, $d \mid a$.

□

Pelo Teorema 2.8.12, podemos afirmar que o conjunto dos divisores de a e b é o mesmo conjunto dos divisores de b e $a \pmod b$.

Exemplo 2.8.13. *Exemplos de cálculo de $mdc(a, b)$ usando o algorítimo de Euclides na versão revisitada.*

- $(35, 14) = (14, (35 \pmod{14})) = (14, 7) = (7, (14 \pmod 7)) = (7, 0) = 7$.
- $(72, 28) = (28, (72 \pmod{28})) = (28, 16) = (16, (28 \pmod{16})) = (16, 12) = (12, (16 \pmod{12})) = (12, 4) = (4, (12 \pmod 4)) = (4, 0) = 4$.

2.8.2 Pequeno Teorema De Fermat com a notação de Congruência

Seja p um número primo e a um número inteiro, então:

$$a^p \equiv a \pmod p \tag{2.11}$$

Temos também que se $(a, p) = 1$, então:

$$a^{p-1} \equiv 1 \pmod p. \tag{2.12}$$

Exemplo 2.8.14. *Prove que $(a + b)^p \equiv a^p + b^p \pmod p$, para p primo e $a, b \in \mathbb{Z}$.*

Demonstração. Pelo Pequeno Teorema de Fermat temos que $(a + b)^p \equiv a + b \pmod p$. Observe também que pelo mesmo teorema temos:
$a^p \equiv a \pmod p$
$b^p \equiv b \pmod p$
$a^p + b^p \equiv a + b \pmod p \Rightarrow a + b \equiv a^p + b^p \pmod p \Rightarrow (a + b)^p \equiv a^p + b^p \pmod p$ □

Analogamente, ao Exemplo 2.8.14, pode-se provar que: $(a - b)^p \equiv a^p - b^p \pmod p$.

Exemplo 2.8.15. *Vamos calcular o resto da divisão de 15^{20} por 7.*
Como $(15, 7) = 1$, então, pelo Pequeno Teorema de Fermat, temos que $15^6 \equiv 1 \pmod 7 \Rightarrow (15^6)^3 \equiv 1^3 \pmod 7 \Rightarrow 15^{18} \equiv 1 \pmod 7 \Rightarrow 15^{18} \cdot 15^2 \equiv 1 \cdot 15^2 \pmod 7 \Rightarrow 15^{20} \equiv 15^2 \pmod 7 \Rightarrow 15^{20} \equiv 225 \pmod 7 \Rightarrow 15^{20} \equiv 1 \pmod 7$, pois $225 = 32 \cdot 7 + 1$.
Logo, o resto da divisão de 15^{20} por 7 é 1.

Exemplo 2.8.16. *Qual será o resto da divisão de* 237^{28} *por* 13*?*
Observe que $237 = 18 \cdot 13 + 3 \Rightarrow 237 \equiv 3 \pmod{13} \Rightarrow 237^{28} \equiv 3^{28} \pmod{13}$*. Usaremos este artifício em vários exemplos exemplos daqui para frente. Temos que* $3^{28} \equiv (3^2)^{14} \equiv 9^{14} \equiv (9^2)^7 \equiv 81^7 \equiv 3^7 \equiv (3^2)^3 \cdot 3 \equiv 9^3 \cdot 3 \equiv 729 \cdot 3 \equiv 1 \cdot 3 \equiv 3 \pmod{13}$.
Logo $237^{28} \equiv 3 \pmod{13}$ *e portanto, o resto da divisão de* 237^{28} *por 13 é 3.*
Outra maneira de responder a esta pergunta é usando o Pequeno Teorema de Fermat. Como $(237, 13) = 1$*, pelo Pequeno Teorema de Fermat, temos que* $237^{12} \equiv 1 \pmod{13} \Rightarrow (237^{12})^2 \equiv 1^2 \pmod{13}) \Rightarrow 237^{24} \equiv 1 \pmod{13} \Rightarrow 237^{24} \cdot 237^4 \equiv 1 \cdot 237^4 \pmod{13} \Rightarrow 237^{28} \equiv 237^4 \pmod{13})$*. Já vimos acima que* $237 \equiv 3 \pmod{13}$*. Logo,* $237^{28} \equiv 3^4 \pmod{13} \Rightarrow 237^{28} \equiv 81 \pmod{13} \Rightarrow 237^{28} \equiv 3 \pmod{13}$ *e portanto, 3 é resto da divisão de* 237^{28} *por* 13*.*

Proposição 2.8.17. *Sejam* $a, b \in \mathbb{Z}$ *e* $m_1, \ldots, m_n \in \mathbb{Z}$ *e maiores que* 1*, então:*

$$a \equiv b \pmod{m_i}, \forall i = 1, \ldots, n \Leftrightarrow a \equiv b \pmod{[m_1, \ldots, m_r]}$$

Exemplo 2.8.18. *Vamos encontrar o menor múltiplo positivo de* 11 *que deixa resto* 1 *quando dividido por* $3, 4, 5$ *e* 6*?*
Para responder a esta pergunta, devemos encontrar o menor valor de X*, tal que :*
$11X \equiv 1 \pmod{3}$
$11X \equiv 1 \pmod{4}$
$11X \equiv 1 \pmod{5}$
$11X \equiv 1 \pmod{6}$.
Pela Proposição 2.8.17, teremos então:

$$11X \equiv 1 \pmod{[3, 4, 5, 6]} \Rightarrow 11X \equiv 1 \pmod{60}$$

Resolver essa congruência é equivalente a resolver a equação diofantina $11X - 60Y = 1$*. Como* $(11, 60) = 1$ *e* $1 \mid 1$*, a equação tem solução. Usando o algoritmo de Euclides teremos:*

Tabela 23 – Calculando $(60, 11)$

	5	2	5
60	11	5	1
5	1	0	

Fonte: Produção do próprio autor (2023).

Pela Tabela 23 temos:
$1 = 11 - 2 \cdot 5$
$5 = 60 - 5 \cdot 11$.

Substituindo os valores encontrados, temos que $(60, 11) = 1 = 11-2\cdot 5 = 11-2\cdot(60-5\cdot 11) = 11 - 2\cdot 60 + 10\cdot 11 = 11\cdot 11 - 2\cdot 60 \Rightarrow 1 = 11\cdot 11 - 2\cdot 60$. *Portanto, para a equação* $11X + 60(-Y) = 1$, *temos que* $x_0 = 11$ *e* $y_0 = 2$ *é uma solução da equação. As demais soluções são dadas por (Proposição 2.5.2):*

$$x = 11 + 60t, \quad y = 2 + 11t,$$

com $t \in \mathbb{Z}$.
Portanto o menor valor positivo para X, *ocorre quando* $t = 0$, *ou seja,* $X = 11+60\cdot 0 = 11$. *Logo o menor múltiplo positivo de* 11 *que deixa resto* 1 *quando dividido por* $3, 4, 5$ *e* 6 *é* $11 \cdot 11 = 121$.

2.8.3 Teorema de Euler

O Teorema de Euler, também conhecido como Teorema de Euler-Fermat, é um importante teorema não só para a Teoria dos Números, mas por suas aplicações práticas como em criptografia de chave pública.

Teorema 2.8.19. *Teorema de Euler*
Sejam $a, n \in \mathbb{Z}$, *com* $n > 1$ *e* a *e* n *relativamente primos, ou seja,* $(a, n) = 1$, *tem-se que:*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Onde $\varphi(n)$ *é a função Totiente de Euler.*

Podemos afirmar que se n for um número primo, é imediato o teorema, pois prevalece o Pequeno Teorema de Fermat:

$$a^{\varphi(n)} \equiv 1 \pmod{n} \Rightarrow a^{n-1} \equiv 1 \pmod{n}.$$

Assim como no Pequeno Teorema de Fermat, o Teorema de Euler possui uma outra forma, que não requer que $(a, n) = 1$. Ei-la:

$$a^{\varphi(n)+1} \equiv a \pmod{n}$$

Exemplo 2.8.20. *Exemplos de cálculos envolvendo o Teorema de Euler:*

- *Sejam* $a = 7$; $n = 10$, *então* $(7, 10) = 1$ *e* $\varphi(10) = \varphi(2\cdot 5) = (2-1)\cdot(5-1) = 4$. *Logo,* $a^{\varphi(n)} = 7^4 = 2401 \equiv 1 \pmod{10}$.
- *Sejam* $a = 5$; $n = 72$, *então* $(5, 72) = 1$ *e* $\varphi(72) = \varphi(2^3\cdot 3^2) = 2^2\cdot 3^1\cdot(2-1)\cdot(3-1) = 4\cdot 3\cdot 1\cdot 2 = 24$. *Logo,* $a^{\varphi(n)} = 5^{24} \equiv (5^2)^{12} \equiv 25^{12} \equiv 1^{12} \equiv 1 \pmod{12}$.

Exemplo 2.8.21. *Exemplos de cálculo do resto de uma divisão usando o Teorema de Euler:*

- *Vamos calcular o resto da divisão de* 5^{100} *por* 11.
  Temos que $(5, 11) = 1$ *e* $\varphi(11) = (11 - 1) = 10$. *Pelo teorema de Euler, temos que* $5^{10} \equiv 1 \pmod{11} \Rightarrow (5^{10})^{10} \equiv 1^{10} \pmod{11} \Rightarrow 5^{100} \equiv 1 \pmod{11}$. *Logo, o resto da divisão de* 5^{100} *por* 11 *é* 1.

- *Vamos calcular o resto da divisão de* 31^{200} *por* 28.
  Temos que $(28, 31) = 1$ *e* $\varphi(28) = (2^2 \cdot 7) = 2^1 \cdot (2 - 1) \cdot (7 - 1) = 2 \cdot 1 \cdot 6 = 12$. *Pelo teorema de Euler, temos que* $31^{12} \equiv 1 \pmod{28} \Rightarrow (31^{12})^{16} \equiv 1^{16} \pmod{28} \Rightarrow 31^{192} \equiv 1 \pmod{28} \Rightarrow 31^{192} \cdot 31^8 \equiv 1 \cdot 31^8 \pmod{28} \Rightarrow 31^{200} \equiv 3^8 \equiv (3^2)^4 \equiv 9^4 \equiv (9^2)^2 \equiv 81^2 \equiv (-3)^2 \equiv 9 \pmod{28}$. *Logo, o resto da divisão de* 31^{200} *por* 28 *é* 9.

Observe que no segundo item do Exemplo 2.8.21 usamos a congruência $81^2 \equiv (-3)^2 \pmod{28}$. Isso é possível pela Proposição 2.8.5, uma vez que $28 \mid (81 - (-3)) \Rightarrow 28 \mid 84$. Usaremos essa técnica diversas vezes adiante. A vantagem é que se não usássemos $(-3)^2$, teríamos que usar 25^2, o que seria um pouco mais trabalhoso.

2.8.4 Teorema de Wilson

Este teorema foi atribuído ao matemático inglês John Wilson por volta de 1770, porém provado por Lagrange. Este Teorema é bastante útil para verificar se um número é primo ou não. Para primos muito grandes, ele se torna trabalhoso e inviável computacionalmente.

Teorema 2.8.22. *Teorema do Wilson*
Se p *é um número primo e* k *um número inteiro, então* $(p - 1)! + 1 = k \cdot p$ *ou seja, na notação de congruência:*

$$(p - 1)! \equiv -1 \pmod{p}$$

Proposição 2.8.23. *Recíproca do Teorema do Wilson*
Seja $p \in \mathbb{Z}$ *e* $p > 1$. *Se* $(p - 1)! \equiv -1 \pmod{p}$, *então* p *é um número primo.*

Teorema 2.8.24. *Seja* $p \in \mathbb{Z}$ *e* $p > 1$, *então:*

$$(p - 1)! \equiv \begin{cases} -1 \pmod{p} & , \text{ se } p \text{ é primo.} \\ 0 \pmod{p} & , \text{ se } p \text{ é composto e } p \neq 4. \end{cases}.$$

Exemplo 2.8.25. *Veja os exemplos:*

- *Considere o número primo* 7. *Temos que* $(7-1)! = 6! = 720 \equiv 6 \equiv -1 \pmod 7$.
- *Considere o número composto* 6. *Temos* $(6-1)! = 5! = 120 \equiv 0 \pmod 6$.
- *Considere o número* 1231. *Queremos saber se este número é primo ou composto. Usando a recíproca do Teorema de Wilson (Teorema 2.8.23), e um computador, temos que:* $(1231-1)! = 1230! \approx 2,213840066385629709660640960642 3 \cdot 10^{3268} \equiv 1230 \equiv -1 \pmod{1231}$. *Logo,* 1231 *é um número primo.*
- *Considere o número* 2497. *Da mesma forma que no item anterior, vamos verificar se o número* 2497 *é primo ou composto. Temos que:* $(2497-1)! = 2496! \approx 4,17997896021998457659094104299 23 \cdot 10^{7397} \equiv 0 \pmod{2497}$. *Logo,* 2497 *é um número composto, a saber, ele é divisível por 11.*

Exemplo 2.8.26. *Prove para* p *primo e* $a \in \mathbb{N}$ *que* $a^p + (p-1)! \cdot a \equiv 0 \pmod p$.

Demonstração. Pelo Teorema de Wilson, temos que:
$(p-1)! \equiv -1 \pmod p \Rightarrow (p-1)! \cdot a \equiv -a \pmod p$.
Pelo Pequeno Teorema de Fermat, temos que: $a^p \equiv a \pmod p$.
Somando as duas congruências membro a membro, temos: $a^p + (p-1)! \cdot a \equiv 0 \pmod p$. □

2.9 Tópicos de Aritmética Modular

Falaremos nesta seção a respeito de dois importantes tópicos da Aritmética Modular: Congruências Lineares e Teorema Chinês dos Restos.

2.9.1 Congruências Lineares

Congruência Linear é uma congruência do tipo: $aX \equiv b \pmod n$, com, $a, b, n \in \mathbb{Z}$ e $n > 1$. Resolver uma congruência linear é determinar se existem números $x \in \mathbb{Z}$ de modo que $aX \equiv b \pmod n$.

Proposição 2.9.1. *A congruência* $aX \equiv b \pmod n$, *com* $a, b, n \in \mathbb{Z}$ *e* $n > 1$, *tem solução se, e somente se,* $(a, n) \mid b$.

Demonstração. $\Rightarrow$ Suponha que x seja uma solução de $aX \equiv b \pmod n$, então, $ax \equiv b \pmod n \Rightarrow ax - b \equiv 0 \pmod n \Rightarrow ax - b = ny$. Logo, a equação aX - nY = b possui solução. Pelo Teorema 2.5.1, temos que $(a, n) \mid b$.
$\Leftarrow$ Suponha agora que $(a, n) \mid b$. Logo, Pelo mesmo teorema citado acima, a equação $aX - nY = b$ possui solução. Admitindo x, y como solução, temos que $ax - ny = b \Rightarrow ax = b + ny \Rightarrow ax \equiv b \pmod n$. □

Teorema 2.9.2. *Seja a congruência* $aX \equiv b \pmod{n}$*, com* $a, b, n, d \in \mathbb{Z}$*,* $n > 1$ *e* $d = (a, n)$*. Se* x_0 *é uma solução desta congruência, então:*

$$x_0, \quad x_0 + \frac{n}{d}, \quad x_0 + 2 \cdot \frac{n}{d}, \quad \dots \quad , \quad (d-1) \cdot \frac{n}{d}$$

são soluções módulo n *da congruência.*

Exemplo 2.9.3. *Vamos resolver a congruência* $12X \equiv 6 \pmod{18}$.
Temos que $(12, 18) = 6 \mid 6$*. Temos que a congruência terá* 6 *soluções módulo* 18*. Facilmente podemos encontrar* $x_0 = 2$*, fazendo algumas tentativas. Logo, as soluções módulo* 18 *são:*

$$2, \quad 2 + \frac{18}{6}, \quad 2 + 2 \cdot \frac{18}{6}, \quad 2 + 3 \cdot \frac{18}{6}, \quad 2 + 4 \cdot \frac{18}{6}, \quad 2 + 5 \cdot \frac{18}{6}$$

$$2, \quad 2 + 3, \quad 2 + 6, \quad 2 + 9, \quad 2 + 12, \quad 2 + 15$$

$$2, 5, 8, 11, 14, 17$$

Corolário 2.9.4. *Seja a congruência* $aX \equiv b \pmod{n}$*, com* $a, b, n \in \mathbb{Z}$ *e* $n > 1$*. Se* $(a, n) = 1$*, então a congruência possui uma única solução módulo* n*.*

Pelo Corolário 2.9.4, a congruência $aX \equiv 1 \pmod{n}$ com $(a, n) = 1$ possui uma única solução módulo n. Chamaremos esta solução de Inverso multiplicativo de a módulo n. Esta solução é muito importante nos estudos de Criptografia R.S.A.

Exemplo 2.9.5. *Vamos resolver a congruência* $11X \equiv 5 \pmod{70}$*.*
Como $(11, 70) = 1$ *temos que a congruência terá uma única solução módulo* 70*. Temos ainda que* $70 = 2 \cdot 5 \cdot 7$ *e que,* $[2, 5, 7] = 70$*. Devemos então procurar o menor valor de* X*, tal que:*
$11X \equiv 5 \pmod{2} \Rightarrow 11X \equiv 1 \pmod{2}$
$11X \equiv 5 \pmod{5} \Rightarrow 11X \equiv 0 \pmod{5}$
$11X \equiv 5 \pmod{7}$
Por tentativa e erro, podemos ver que $x_0 = 45$ *é solução de todas as congruências acima. Finalizando, temos que* $x = 45 + 70t$ *com* $t \in \mathbb{Z}$ *são todas as soluções da congruência.*

Observe que resolver a congruência $11X \equiv 5 \pmod{70}$ *é equivalente a resolver a equação diofantina* $11X - 70Y = 5$*. Deixo a cargo do leitor a resolução da equação. Um exemplo semelhante é o Exemplo 2.8.18.*

Exemplo 2.9.6. *Vamos resolver agora a congruência* $7X \equiv 1 \pmod{72}$
Como $(7, 72) = 1$*, temos que a congruência terá uma única solução módulo* 72*. Como vimos acima, chamaremos esta solução de: "Inverso Multiplicativo de* 7 *módulo* 72*". Observe ainda que* $72 = 2^3 \cdot 3^2$ *e que* $[8, 9] = 72$*. Vamos resolver então o sistema de congruências:*
$7X \equiv 1 \pmod{8}$
$7X \equiv 1 \pmod{9}$.

Novamente, por tentativa e erro, temos que $x_0 = 31$ *é solução simultânea das duas congruências e portanto,* 31 *é o Inverso Multiplicativo de* 7 *módulo* 72*. As outras soluções são dadas por* $x = 31 + 72t$ *com* $t \in \mathbb{Z}$*.*

Observe que resolver a congruência $7X \equiv 1 \pmod{72}$ é equivalente a resolver a equação Diofantina $7X - 72Y = 1$. Vamos resolver essa equação Diofantina, por ser de particular interesse para esse trabalho, pois, posteriormente, a usaremos em alguns dos cálculos que faremos com criptografia RSA. Vamos então utilizar o algoritmo de Euclides:

Tabela 24 – Calculando $(72, 7)$

	10	3	2
72	7	2	1
2	1	0	

Fonte: Produção do próprio autor (2023).

Pela Tabela 24, temos:
$1 = 7 - 3 \cdot 2$
$2 = 72 - 10 \cdot 7$
Substituindo os valores encontrados, temos que $(72, 7) = 1 = 7 - 3 \cdot 2 = 7 - 3 \cdot (72 - 10 \cdot 7) = 7 - 3 \cdot 72 + 30 \cdot 7 = 31 \cdot 7 - 3 \cdot 72 \Rightarrow 1 = 31 \cdot 7 - 3 \cdot 72$. Portanto, para a equação $7X - 72Y = 1$, temos que $x_0 = 31$ e $y_0 = 3$ é uma solução da equação. As demais são dadas por (Proposição 2.5.2):

$$x = 31 + 72t, \quad y = 3 + 7t,$$

com $t \in \mathbb{Z}$.
Portanto, o menor valor positivo para X ocorre quando $t = 0$, ou seja, $x_0 = 31 + 72 \cdot 0 = 31$.

2.9.2 Teorema Chinês dos Restos

Um dos mais importantes resultados da teoria dos Números é chamado Teorema Chinês dos restos. De um modo geral, este teorema afirma que pode-se reestruturar números inteiros em dado intervalo partindo de seus resíduos módulo um conjunto de números relativamente primos aos pares. O texto abaixo, explica porque o Teorema que descreveremos é chamado de Teorema Chinês dos Restos:

> "...é conhecido como algoritmo chinês do resto, porque um dos primeiros lugares em que aparece é o livro Manual de aritmética do mestre Sun, escrito entre 287 d.C. e 473 d.C. Entretanto, o mesmo resultado é mencionado na Aritmética de Nicômaco de Gerasa, escrita por volta de 100 d.C.". (COUTINHO, 2015, p. 113)

No Manual, Sun descreve o seguinte problema: Qual é o menor número que deixa restos 2, 3 e 2 quando dividido, respectivamente, por 3, 5 e 7? Problema que ele mesmo respondeu como sendo o número 23.

Teorema 2.9.7. *Sejam $n_1, n_2, \ldots, n_r$ números tais que $(n_i, n_j) = 1, \forall i \neq j$, então o sistema de r congruências*
$X \equiv c_1 \pmod{n_1}$
$X \equiv c_2 \pmod{n_2}$
$\vdots$
$X \equiv c_r \pmod{n_r}$
possui solução única módulo $N = n_1 \cdot n_2 \ldots n_r$. Essa solução pode ser obtida por:

$$x = N_1 y_1 c_1 + N_2 y_2 c_2 + \ldots + N_r y_r c_r \tag{2.13}$$

onde $N_i = \frac{N}{n_i}$, y_i é a solução de $N_i Y \equiv 1 \pmod{n_i}$, $\quad i = 1, 2, \ldots, r$.
As outras soluções do sistema são dadas por:

$$x = N_1 y_1 c_1 + N_2 y_2 c_2 + \ldots + N_r y_r c_r + Nt, \quad t \in \mathbb{Z}. \tag{2.14}$$

Exemplo 2.9.8. ***Vamos determinar a solução geral do sistema de congruências:***
$X \equiv 1 \pmod{3}$
$X \equiv 2 \pmod{5}$
$X \equiv 3 \pmod{7}$
Como, $(3,5) = 1, (3,7) = 1, (5,7) = 1$, pelo Teorema Chinês dos Restos (Teorema 2.9.7), o sistema de congruências tem solução geral dada por:

$$x = N_1 y_1 c_1 + N_2 y_2 c_2 + N_3 y_3 c_3 + Nt, \quad t \in \mathbb{Z}$$

$N = 3 \cdot 5 \cdot 7 = 105$, $N_1 = \frac{105}{3} = 35 = 5 \cdot 7$, $N_2 = \frac{105}{5} = 21 = 3 \cdot 7$, $N_3 = \frac{105}{7} = 15 = 3 \cdot 5$, $c_1 = 1$, $c_2 = 2$, $c_3 = 3$, y_1 *é o inverso de* N_1 *módulo* 3, y_2 *é o inverso de* N_2 *módulo* 5 *e* y_3 *é o inverso de* N_3 *módulo* 7. *Temos então:*
$35y_1 \equiv 1 \pmod{3} \Rightarrow y_1 = 2$
$21y_2 \equiv 1 \pmod{5} \Rightarrow y_2 = 1$
$15y_3 \equiv 1 \pmod{7} \Rightarrow y_3 = 1$
Logo:

$$x = 35 \cdot 2 \cdot 1 + 21 \cdot 1 \cdot 2 + 15 \cdot 1 \cdot 3 + 105t$$

$$x = 70 + 42 + 45 + 105t$$

$$x = 157 + 105t$$

$$x = 52 + 105t, \quad t \in \mathbb{Z}.$$

Quantas soluções desse sistema pertencem ao intervalo $50 < X < 800$?
Temos que $50 < X < 800 \Leftrightarrow 50 < 52 + 105t < 800 \Leftrightarrow 50 - 52 < 105t < 800 - 52 \Leftrightarrow -2 < 105t < 748 \Leftrightarrow \frac{-2}{105} < t < \frac{748}{105} \Leftrightarrow -0,19 < t < 7,12 \Rightarrow 0 \leqslant t \leqslant 7$. *Logo existem 8 soluções neste intervalo:*
$52,\ 52+105\cdot 1,\ 52+105\cdot 2,\ 52+105\cdot 3,\ 52+105\cdot 4,\ 52+105\cdot 5,\ 52+105\cdot 6,\ 52+105\cdot 7$.
As soluções são: $52, 157, 262, 367, 472, 577, 682, 787$. *Ou seja, uma progressão aritmética de primeiro termo 52 e razão 105.*

Veja o problema e a solução do problema descrito pelo mestre Sun em seu manual de Aritmética:

> Suponha que temos um número desconhecido de objetos. Se forem contados em três, restam 2, se forem contados em cinco, restam 3 e se forem contados em sete, 2 são deixados. Quantos objetos existem? Resposta: 23. Regra: Se forem contados em três, restam 2: defina 140. Se forem contados em cinco, 3 restam: conjunto 63. Se forem contados em setes, restam 2: conjunto 30. Faça a soma destes [três números] para obter 233. Subtraia 210 deste total; isso dá a resposta (MARTZLOFF, 1997, p. 310).

Exemplo 2.9.9. *Vamos resolver o sistema de congruências:*
$4X \equiv 2 \pmod 3$
$8X \equiv 6 \pmod 7$
$7X \equiv 8 \pmod{11}$
Temos que:
$4X \equiv 2 \pmod 3 \Rightarrow X = 2$ *é solução* $\Rightarrow X \equiv 2 \pmod 3$
$8X \equiv 6 \pmod 7 \Rightarrow X = 6$ *é solução* $\Rightarrow X \equiv 6 \pmod 7$
$7X \equiv 8 \pmod{11} \Rightarrow X = 9$ *é solução* $\Rightarrow X \equiv 9 \pmod{11}$
Como, $(3,7) = (3,11) = (7,11) = 1$, *pelo Teorema Chinês dos Restos, o sistema de congruências tem solução dada por:*

$$x = N_1 y_1 c_1 + N_2 y_2 c_2 + N_3 y_3 c_3 + Nt, \quad t \in \mathbb{Z}$$

$N = 3\cdot 7\cdot 11 = 231$, $N_1 = \frac{231}{3} = 77 = 7\cdot 11$, $N_2 = \frac{231}{7} = 33 = 3\cdot 11$, $N_3 = \frac{231}{11} = 21 = 3\cdot 7$, $c_1 = 2$, $c_2 = 6$, $c_3 = 9$, y_1 *é o inverso de* N_1 *módulo* 3, y_2 *é o inverso de* N_2 *módulo* 7 *e* y_3 *é o inverso de* N_3 *módulo* 11. *Temos então:*
$77y_1 \equiv 1 \pmod 3 \Rightarrow y_1 = 2$
$33y_2 \equiv 1 \pmod 7 \Rightarrow y_2 = 3$
$21y_3 \equiv 1 \pmod{11} \Rightarrow y_3 = 10$
Logo:

$$x = 77\cdot 2\cdot 2 + 33\cdot 3\cdot 6 + 21\cdot 10\cdot 9 + 231t$$

$$x = 308 + 594 + 1890 + 231t$$

$$x = 2792 + 231t$$

Segue que 20 é solução única módulo 231. As outras soluções são dadas por: $20 + 231t$, $t \in \mathbb{Z}$.

2.9.2.1 Quando os módulos não são relativamente primos

Quando os módulos do sistema de congruências não são relativamente primos, usaremos de algumas estratégias para sua resolução. Analisemos o sistema de congruências:

$$\begin{aligned} X &\equiv 2 \pmod 4 \\ X &\equiv 4 \pmod 6 \end{aligned} \tag{2.15}$$

Na primeira congruência, transformando a congruência em uma equação, temos que $x = 2+4y$, para algum $y \in \mathbb{Z}$, substituindo na segunda congruência, temos: $2+4y \equiv 4 \pmod 6 \Rightarrow 4y \equiv 2 \pmod 6$. Observe que 4 e 6 tem o fator comum 2 e, portanto, 4 não é invertível módulo 6 ou vice-versa. Transformando a congruência $4y \equiv 2 \pmod 6$ em equação, teremos: $4y = 2 + 6k$ para algum $k \in \mathbb{Z} \Rightarrow 2y = 1 + 3k$. Revertendo a igualdade para congruência obtemos $2y \equiv 1 \pmod 3 \Rightarrow y \equiv 2 \pmod 3$. Então, podemos escrever que $y = 2 + 3t$ para algum $t \in \mathbb{Z}$. Substituindo y na equação $x = 2 + 4y$, obtemos: $x = 2 + 4 \cdot (2 + 3t) \Rightarrow x = 2 + 8 + 12t \Rightarrow x = 10 + 12t$ que é a solução do sistema.

Analisemos agora o sistema de congruências:

$$\begin{aligned} X &\equiv 2 \pmod 4 \\ X &\equiv 5 \pmod 6 \end{aligned} \tag{2.16}$$

A primeira congruência é a mesma do sistema (2.15), então, já sabemos que podemos usar $x = 2 + 4y$ para algum $y \in \mathbb{Z}$. Substituindo x na segunda congruência, obtemos: $2+4y \equiv 5 \pmod 6 \Rightarrow 4y \equiv 3 \pmod 6$. Já vimos que 4 e 6 tem o fator comum 2 e, portanto, 4 não é invertível módulo 6 ou vice-versa. Transformando a congruência $4y \equiv 3 \pmod 6$ em equação, teremos: $4y = 3 + 6z$ para algum $z \in \mathbb{Z} \Rightarrow 4x - 6z = 3 \Rightarrow 2(2x - 3z) = 3$. Absurdo, pois para $x, y \in \mathbb{Z}$, 3 não é múltiplo de 2. Desta forma, o sistema não tem solução.

Através dos sistemas (2.15) e (2.16), observamos que quando os módulos não são relativamente primos, o sistema dependerá dos coeficientes da congruência para ter solução.

Proposição 2.9.10. *Sejam* n_1, n_2 *números tais que* $(n_1, n_2) = d \neq 1$, *então o sistema de congruências*
$X \equiv c_1 \pmod{n_1}$
$X \equiv c_2 \pmod{n_2}$
Terá solução, se $d \mid c_2 - c_1$.

Observe que em (2.15), temos que $(4, 6) = 2 \mid 2 = (4 - 2)$, portanto, teve solução. Já em (2.16), $(4, 6) = 2 \nmid (5 - 2)$ e consequentemente não tem solução.

Algumas demonstrações neste capítulo foram omitidas por necessitaram de alguns pré-requisitos que não foram trabalhados neste texto. As demonstrações que não foram realizadas, ou para as quais foram sugeridas fontes de pesquisa, podem ser encontradas em (HEFEZ, 2012; STALLINGS, 2006; ARAUJO, 2009; OBMEP-IMPA, 2012) ou em outros livros que tratam sobre a Teoria dos Números.

3 Criptografia RSA

3.1 Primeiros conceitos sobre criptografia

- A palavra Criptografia vem do Grego KRYPTOS, “escondido”, de KRYPTEIN, “esconder” e GRÁPHEIN, que significa a palavra “escrita”. Então Criptografia significa Escrita Escondida, que só é legível por pessoas ou entidades com autorização.
- Texto claro: É o texto original.
- Texto cifrado: É o texto que não se pode ler, incompreensível.
- Cifrar: É o processo de converter um texto claro em um texto cifrado.
- Decifrar: É o processo de converter um texto cifrado em um texto claro.
- Chave: É o conjunto de dados que são utilizados no processo para cifrar e decifrar.
- Criptoanálise: É o processo de decodificar uma mensagem sem o conhecimento das chaves.

3.1.1 Criptografia e segurança da informação

Papel da criptografia na Segurança da informação

A criptografia tem cinco objetivos principais:

Confidencialidade: Deve-se proteger a privacidade de um indivíduo. Somente ele, (destinatário) pode retirar a mensagem clara, da mensagem cifrada.

Autenticação: Deve haver uma confiança na validação de uma transmissão de uma mensagem ou sobre sua origem. Para isso deve-se ser capaz de verificar se os usuários são de fato quem dizem ser.

Disponibilidade: Toda informação deve estar disponível. Não se pode deixar que uma informação armazenada em algum servidor fique indisponível. Deve-se assegurar acesso rápido à informação.

Integridade: O destinatário deve ser capaz de prevenir-se e proteger-se contra uma modificação e/ou destruição da informação.

Não-repúdio ou irretratabilidade: As ações de uma entidade devem ser atribuídas exclusivamente a ela, não podendo ser possível negá-las.

Figura 16 – Princípios

Fonte: Disponível em: <https://www.facebook.com/professorsylviorodrigues/photos/pcb.822141181468174/822137474801878/?type=3&theater>. Acesso em 10 de set. de 2023

3.1.2 Procedimentos Criptográficos

Os processos usados para cifrar e decifrar se utilizam de uma chave secreta e um algoritmo que pode ser público.

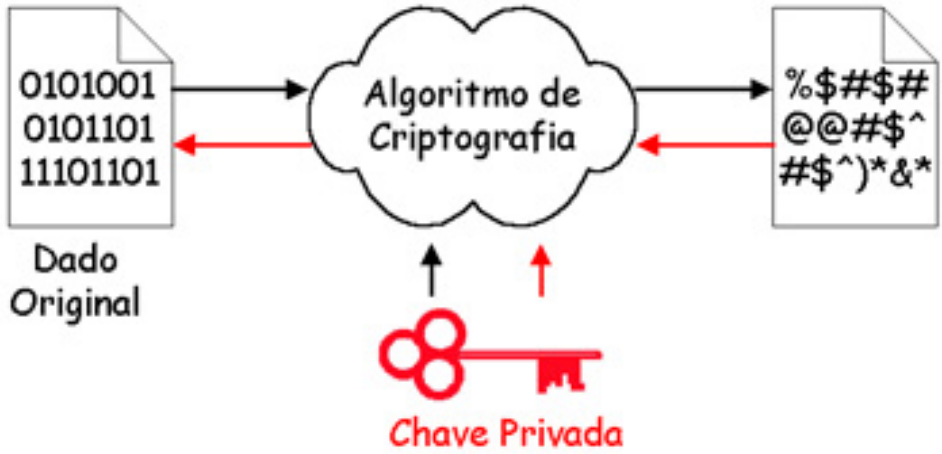
Figura 17 – Criptografia

Fonte: Disponívem em: <https://ufsm.br/r-791-2691>. Acesso em: 10 de set. de 2023

Criptografia simétrica

É aquela que utiliza um algoritmo de criptografia e uma única chave que é compartilhada entre o emissor e o destinatário. A partir desta chave pode-se cifrar ou decifrar uma mensagem.

Figura 18 – Criptografia simétrica



Fonte: Disponível em: <https://ufsm.br/r-791-2691>. Acesso em: 10 de set. de 2023.

Eis alguns dos algoritmos de criptografia simétrica mais utilizados: DES/3DES , AES (192, 256 ou 512 bits), Blowfish/Twofish (448 bits).

Criptografia Assimétrica

É a criptografia que utiliza um algoritmo e um par de chaves, uma pública e outra privada. A chave pública pode ser divulgada, enquanto a privada deve ser secreta.

Figura 19 – Criptografia assimétrica

Fonte: Disponível em: <https://ufsm.br/r-791-2691>. Acesso em: 10 de set. de 2023

Veja como funciona este sistema de criptografia :

1. São geradas as chaves públicas e privadas pelo servidor e cliente.
2. Servidor e cliente trocam as chaves públicas.
3. O cliente usa a chave pública do servidor para criptografar seus dados e posteriormente envia para o servidor.

4. Os dados são descriptografados pelo servidor, através de sua chave privada.

5. Novamente os dados que serão enviados para o cliente, são criptografados pelo servidor com a chave pública do cliente.

6. Enfim, o cliente descriptografa os dados usando sua chave privada.

Eis os algoritmos mais utilizados neste sistema de criptografia: RSA, El Gamal, DSA de curvas elípticas, etc

Dos requisitos para que um sistema criptográfico funcione:

Tenha reversibilidade - O algoritmo deve permitir que os dados criptografados possam ser descriptografados.

O receptor detenha a chave - Sem a chave, não é possível descriptografar os dados recebidos.

Não tenha ambiguidade - O algoritmo não pode admitir mais de um significado ou possibilidade.

Código ASCII

O ASCII (American Standart Code for Information Interchange) é um código proposto e adotado universalmente para representar caracteres (letras, números e símbolos) para a maioria dos sistemas digitais. Segundo CASAGRANDE (CASAGRANDE, 2005), os caracteres dos computadores atuais ocupam um byte, ou seja, 8 bits. Como cada bit (abreviação para digito binário - binary digit), é usado para representar sequências de 0 e 1, podem ocorrer em um byte, $2^8 = 256$ caracteres diferentes.

A tabela ASCII possui um grupo de caracteres de controle, que vão de 0 a 31, seguidos por caracteres imprimíveis, como números, letras maiúsculas e minúsculas e símbolos e sinais de pontuação, seguindo um padrão universal para computadores. O código ASCII será utilizado neste trabalho para a codificação e decodificação de dados. A seguir, confira a tabela ASCII, em sua forma resumida e adaptada (Tabela 25).

Tabela 25 – Tabela ASCII resumida e adaptada.

Carácter	Número	Carácter	Número	Carácter	Número	Carácter	Número
A	65	a	97	espaço	32	:	58
B	66	b	98	!	33	;	59
C	67	c	99	”	34	<	60
D	68	d	100	#	35	=	61
E	69	e	101	$	36	>	62
F	70	f	102	%	37	?	63
G	71	g	103	&	38	@	64
H	72	h	104	’	39	[	91
I	73	i	105	(	40	\	92
J	74	j	106	)	41	]	93
K	75	k	107	*	42	∧	94
L	76	l	108	+	43	_	95
M	77	m	109	,	44	‘	96
N	78	n	110	-	45	{	123
O	79	o	111	.	46	|	124
P	80	p	112	/	47	}	125
Q	81	q	113	0	48	∼	126
R	82	r	114	1	49	Ç	128
S	83	s	115	2	50	ç	135
T	84	t	116	3	51	ñ	164
U	85	u	117	4	52	Ñ	165
V	86	v	118	5	53	ª	166
W	87	w	119	6	54	≡	240
X	88	x	120	7	55	±	241
Y	89	y	121	8	56	÷	246
Z	90	z	122	9	57	°	248

Fonte: Produção do próprio autor (2023).

3.2 Criptografia RSA

Devido ao crescimento da internet, a segurança na transferência de dados, tornou-se essencial na busca por assegurar a integridade dos dados e assim uma comunicação segura entre duas partes. Após um artigo produzido por Bailey Whitfield Diffie e Martin Edward Hellman, entitulado “New Directions in Cryptography” (Novas Direções em Criptografia), publicado em 1976, que introduziu o conceito de troca de chaves pública e privada, muitos criptologistas foram desafiados a produzirem algoritmos que atendessem a sistemas de chaves públicas. Vários falharam neste desafio.

Uma das primeiras propostas aceitas e aprovadas foi desenvolvida em 1977 por Ronald Rivest, Adi Shamir, Leonard Adleman, publicada posteriormente em 1978. O algoritmo criado por eles ficou conhecido como RSA, sigla gerada pelas iniciais dos seus sobrenomes, e que tem sido até hoje, o mais aceito e implementado sistema de encriptação de chave pública.

O RSA é um tipo de algoritmo de criptografia assimétrica. Utiliza duas chaves, uma pública e uma privada. A chave pública é utilizada para criptografar, ou seja cifrar os dados que serão enviados, como senhas, logins ou números de cartão de crédito. A segunda, a privada, é utilizada para descriptografar, ou seja decifrar o texto que foi enviado cifrado, voltando ao texto original e somente ela consegue fazer este processo de decifragem. Este tipo de sistema de criptografia é diferente da criptografia simétrica, na qual apenas uma chave é utilizada, que neste caso, seria inviável, pois esta chave teria que ser enviada junto com a mensagem cifrada, podendo assim ser facilmente descoberta por um ataque e consequentemente os dados seriam revelados e usados para outros fins.

3.2.1 O Método RSA

Nesta seção, abordaremos o funcionamento do método RSA, suas etapas e processos até conseguirmos o objetivo que é a codificação e decodificação de uma informação. Faremos isso inicialmente, através de exemplos, a fim de facilitar a compreensão.

Quero enviar a mensagem : PAZ!

Observando a tabela ASCII vamos pré-codificar PAZ!

Temos os blocos b : $P = 80, A = 65, Z = 90, ! = 33$

80659033

Usaremos dois primos p e q que, didaticamente, serão primos pequenos:

$p = 5$ e $q = 19$

$n = p \cdot q = 95$ (chave de codificação)

$(p-1) \cdot (q-1) = 4 \cdot 18 = 72$

Escolheremos também um número d tal que $(72, d) = 1$. Para este exemplo, usaremos $d = 7$. A chave pública é dada por (n, d).

3.2.1.1 Algoritmo de Codificação

O Algoritmo de codificação é dado por:

$$b^d \equiv a \pmod{n} \tag{3.1}$$

Vamos elevar cada bloco ao número d e calcular qual é o resto da divisão deste número módulo n, obtendo assim o valor do número a.

Codificando o primeiro bloco:

$$80^7 \equiv a \pmod{95} \tag{3.2}$$

$$80^7 \equiv ((80)^2)^3 \cdot 80 \equiv ((-15)^2)^3 \cdot (-15) \equiv (225)^3 \cdot (-15) \equiv 35^3 \cdot (-15) \equiv 35^2 \cdot 35 \cdot (-15)$$
$$\equiv 1225 \cdot 35 \cdot (-15) \equiv 85 \cdot 35 \cdot (-15) \equiv (-10) \cdot 35 \cdot (-15) \equiv 150 \cdot 35$$
$$\equiv 55 \cdot 35 \equiv 1925 \equiv 25 \pmod{95}$$

Portanto,

$$80^7 \equiv 25 \pmod{95} \tag{3.3}$$

Codificando o segundo bloco:

$$65^7 \equiv a \pmod{95} \tag{3.4}$$

$$65^7 \equiv ((65)^2)^3 \cdot 65 \equiv ((-30)^2)^3 \cdot (-30) \equiv (900)^3 \cdot (-30) \equiv 45^3 \cdot (-30) \equiv 45^2 \cdot 45 \cdot (-30)$$
$$\equiv 2025 \cdot 45 \cdot (-30) \equiv 30 \cdot 45 \cdot (-30) \equiv 1350 \cdot (-30) \equiv 20 \cdot (-30)$$
$$\equiv -600 \equiv -30 \equiv 65 \pmod{95}$$

Portanto,

$$65^7 \equiv 65 \pmod{95} \tag{3.5}$$

Codificando o terceiro bloco:

$$90^7 \equiv a \pmod{95} \tag{3.6}$$

$$90^7 \equiv ((90)^2)^3 \cdot 90 \equiv ((-5)^2)^3 \cdot (-5) \equiv (25)^3 \cdot (-5) \equiv 25^2 \cdot 25 \cdot (-5) \equiv 625 \cdot 25 \cdot (-5)$$
$$\equiv 55 \cdot 25 \cdot (-5) \equiv (-40) \cdot 25 \cdot (-5) \equiv 200 \cdot 25 \equiv 10 \cdot 25$$
$$\equiv 250 \equiv 60 \pmod{95}$$

Portanto,

$$90^7 \equiv 60 \pmod{95} \tag{3.7}$$

Codificando o quarto bloco:

$$33^7 \equiv a \pmod{95} \tag{3.8}$$

$$33^7 \equiv ((33)^2)^3 \cdot 33 \equiv (1089)^3 \cdot 33 \equiv (44)^3 \cdot 33 \equiv 44^2 \cdot 44 \cdot 33 \equiv 1936 \cdot 44 \cdot 33$$
$$\equiv 36 \cdot 44 \cdot 33 \equiv 1584 \cdot 33 \equiv 64 \cdot 33 \equiv (-31) \cdot 33$$
$$\equiv -1023 \equiv -73 \equiv 22 \pmod{95}$$

Portanto,

$$33^7 \equiv 22 \pmod{95} \tag{3.9}$$

Desta forma, os blocos b: $80, 65, 90$ e 33 após a codificação foram transformados nos blocos a: $25, 65, 60$ e 22. Desse modo, a mesagem codificada é: 25656022.

3.2.1.2 Algoritmo de Decodificação

Lembre-se que $(p-1)\cdot(q-1) = 72$, ou seja, $4 \cdot 18 = 72$. A chave de decodificação é dada por (n, e), onde e é o inverso de $d \pmod{(p-1)\cdot(q-1)}$. Portanto,

$$d \cdot e \equiv 1 \pmod{(p-1)\cdot(q-1)} \tag{3.10}$$

daí, temos: $d \cdot e \equiv 1 \pmod{72} \Rightarrow 7 \cdot e \equiv 1 \pmod{72} \Rightarrow e = 31$

O algoritmo de decodificação é dado por:

$$a^e \equiv b \pmod{n} \tag{3.11}$$

Decodificando o primeiro bloco:

$$25^{31} \equiv b \pmod{95} \tag{3.12}$$

$$\begin{aligned} 25^{31} &\equiv ((25)^2)^{15} \cdot 25 \equiv 625^{15} \cdot 25 \equiv 55^{15} \cdot 25 \equiv (-40)^{15} \cdot 25 \equiv ((-40)^2)^7 \cdot (-40) \cdot 25 \\ &\equiv 1600^7 \cdot (-1000) \equiv 80^7 \cdot (-50) \equiv (-15)^7 \cdot (-50) \equiv ((-15)^2)^3 \cdot (-15) \cdot (-50) \\ &\equiv 225^3 \cdot (-15) \cdot (-50) \equiv 35^3 \cdot 750 \equiv 35^3 \cdot 85 \equiv 35^2 \cdot 35 \cdot 85 \equiv 1225 \cdot 35 \cdot (-10) \\ &\equiv 85 \cdot 35 \cdot (-10) \equiv (-10) \cdot (-10) \cdot 35 \equiv 100 \cdot 35 \equiv 5 \cdot 35 \equiv 175 \equiv 80 \pmod{95} \end{aligned}$$

Portanto,

$$25^{31} \equiv 80 \pmod{95} \tag{3.13}$$

Retornando ao bloco $b = 80$ que corresponde à letra P.

Decodificando o segundo bloco:

$$65^{31} \equiv b \pmod{95} \tag{3.14}$$

$$\begin{aligned} 65^{31} &\equiv ((65)^2)^{15} \cdot 65 \equiv ((-30)^2)^{15} \cdot (-30) \equiv 900^{15} \cdot (-30) \equiv 45^{15} \cdot (-30) \equiv (45^2)^7 \cdot 45 \cdot (-30) \\ &\equiv 2025^7 \cdot (-1350) \equiv 30^7 \cdot (-20) \equiv (30^2)^3 \cdot 30 \cdot (-20) \equiv 900^3 \cdot (-600) \equiv 45^3 \cdot (-30) \\ &\equiv 45^2 \cdot 45 \cdot (-30) \equiv 2025 \cdot 45 \cdot (-30) \equiv 30 \cdot 45 \cdot (-30) \equiv (-900) \cdot 45 \\ &\equiv (-45) \cdot 45 \equiv (-2025) \equiv (-30) \equiv 65 \pmod{95} \end{aligned}$$

Portanto,

$$65^{31} \equiv 65 \pmod{95} \tag{3.15}$$

Retornando ao bloco $b = 65$ que corresponde à letra A.

Decodificando o terceiro bloco:

$$60^{31} \equiv b \pmod{95} \tag{3.16}$$

$$\begin{aligned}60^{31} &\equiv ((60)^2)^{15}\cdot 60 \equiv ((-35)^2)^{15}\cdot(-35) \equiv 1225^{15}\cdot(-35) \equiv 85^{15}\cdot(-35) \equiv (-10)^{15}\cdot(-35)\\ &\equiv ((-10)^2)^7\cdot(-10)\cdot(-35) \equiv 100^7\cdot 350 \equiv 5^7\cdot 65 \equiv ((5)^2)^3\cdot 5\cdot 65 \equiv 25^3\cdot 5\cdot 65\\ &\equiv 25^2\cdot 25\cdot 5\cdot 65 \equiv 625\cdot 25\cdot 5\cdot 65 \equiv 55\cdot 25\cdot 5\cdot 65 \equiv (-40)\cdot 125\cdot(-30)\\ &\equiv (-40)\cdot(-30)\cdot 125 \equiv 1200\cdot 30 \equiv 60\cdot 30 \equiv 1800 \equiv 90 \pmod{95}\end{aligned}$$

Portanto,

$$60^{31} \equiv 90 \pmod{95} \tag{3.17}$$

Retornando ao bloco $b = 90$ que corresponde à letra Z.

Decodificando o quarto bloco:

$$22^{31} \equiv b \pmod{95} \tag{3.18}$$

$$\begin{aligned}22^{31} &\equiv ((22)^2)^{15}\cdot 22 \equiv 484^{15}\cdot 22 \equiv 9^{15}\cdot 22 \equiv ((9)^2)^7\cdot 9\cdot 22 \equiv 81^7\cdot 198\\ &\equiv (-14)^7\cdot 8 \equiv ((-14)^2)^3\cdot(-14)\cdot 8 \equiv 196^3\cdot(-112) \equiv 6^3\cdot(-17)\\ &\equiv 216\cdot(-17) \equiv 26\cdot(-17) \equiv -442 \equiv (-62) \equiv 33 \pmod{95}\end{aligned}$$

Portanto,

$$22^{31} \equiv 33 \pmod{95} \tag{3.19}$$

Retornando ao bloco $b = 33$ que corresponde ao simbolo !.

Após a decodificação, usando a tabela ASCII, encontramos a palavra enviada PAZ!.

3.3 Eficiência do Método RSA

Algo que garante a eficiência do método é a inexistência de uma ferramenta que consiga rapidamente fatorar números muito grandes. Se escolhermos os primos p e q muito grandes na casa de duzentos ou trezentos algarismos, temos que o número $n = p \cdot q$ será um número muito maior ainda. Surgem então, algumas considerações a serem feitas:

1. Se você não consegue fatorar o número n, você não vai conseguir descobrir os números p e q.
2. Se você não sabe os números p e q, você não sabe quem são os números $(p-1)$ e $(q-1)$, logo não saberá saberá o valor do produto $(p-1)\cdot(q-1)$ e, por consequência, não poderá calcular o número e, tal que $e \cdot d \equiv 1 \pmod{(p-1)\cdot(q-1)}$, que é o expoente utilizado na regra de decodificação.
3. Pelos itens anteriores, todos podem saber qual é o valor de n e qual é o valor de d, que são as chaves públicas.

3.4 Escolhas adequadas dos números d, p e q

3.4.1 A escolha do número d

Podem surgir alguns problemas quando da escolha do número d, devido à inexistência do inverso módulo $[(p-1)\cdot(q-1)]$. Cada usuário do método de criptografia RSA, pode usar um expoente d diferente para o algoritmo de codificação $b^d \equiv a \pmod{n}$. Então na prática, o que se faz é uniformizar esse número. Toma-se $d = 3$ fixo. Desta maneira, o algoritmo de codificação ficará assim: $b^3 \equiv a \pmod{n}$.

Para resolver o problema da inexistência do inverso módulo $[(p-1)\cdot(q-1)]$, devemos escolher os números p e q mais adequados à realidade de $d = 3$.

3.4.2 A escolha de p e q adequados

Devemos escolher p e q de modo que:

1. $p \equiv 5 \pmod{6} \Rightarrow p - 1 \equiv 4 \pmod{6}$
2. $q \equiv 5 \pmod{6} \Rightarrow q - 1 \equiv 4 \pmod{6}$

Desse modo, $(p-1)\cdot(q-1) \equiv 16 \equiv 4 \pmod{6} \Rightarrow (p-1)\cdot(q-1) \equiv 4 \pmod{6} \Rightarrow (p-1)\cdot(q-1) = 6k+4 \Rightarrow (p-1)\cdot(q-1) = 6k+3+1 = 3\cdot(2k+1)+1$.

Encontramos então uma nova congruência :

$$3\cdot(2k+1) \equiv -1 \pmod{6k+4} \tag{3.20}$$

Gostaríamos que do outro lado da congruência tivéssemos $1 \pmod{6k+4}$. Manipulando a congruência para que isto ocorra (multiplicando os dois membros da congruência por (-1)), obtemos $3\cdot(-2k-1) \equiv 1 \pmod{6k+4}$:

$$3\cdot(2k+1) \equiv -1 \pmod{6k+4} \Rightarrow 3\cdot(2k+1)\cdot(-1) \equiv -1\cdot(-1) \pmod{6k+4}$$

$$\Rightarrow 3\cdot(-2k-1) \equiv 1 \pmod{6k+4}$$

Afim de evitar valores negativos no primeiro membro da congruência, vamos substituir $(-2k-1)$ por um valor equivalente e congruente módulo $(6k+4)$. Para que isso ocorra, basta somar $(6k+4)$ a $(-2k-1)$, ou seja, $(-2k-1)+(6k+4) = (4k+3)$.

Desse modo, a congruência fica:

$$3\cdot(4k+3) \equiv 1 \pmod{6k+4} \tag{3.21}$$

Vale lembrar que $(6k+4) = (p-1)\cdot(q-1)$. Temos então um algoritmo que vai garantir que o inverso exista, e que calcula o valor desse inverso.

Tomando como exemplo os números:

- $p = 17 \equiv 5 \pmod 6$
- $q = 11 \equiv 5 \pmod 6$

Observando p e q acima, temos que $(p-1)\cdot(q-1) = 16\cdot 10 = 160 = 6k+4 \Rightarrow k = 26$. Substituindo $k = 26$ na congruência (3.21), teremos: $3 \cdot (4k + 3) \equiv 1 \pmod{6k + 4} \Rightarrow 3 \cdot (4 \cdot 26 + 3) \equiv 1 \pmod{6 \cdot 26 + 4} \Rightarrow 3 \cdot 107 \equiv 1 \pmod{160}$.

Observando a congruência $3 \cdot 107 \equiv 1 \pmod{160}$ e a congruência (3.10), encontramos o valor do inverso de $3 \pmod{160}$ que é igual a $e = 107$.

3.5 Por que o método RSA funciona?

Cada um dos blocos b de pré-codificação devem obedecer à restrição: $1 \leqslant b < n$. O algoritmo de codificação é dado por: $b^3 \equiv a \pmod n$. Desse modo, $0 \leqslant a < n$ em que a é a codificação do bloco b. Consideremos agora que o algoritmo de decodificação seja dado por: $a^e \equiv f \pmod n$, onde f é a decodificação do bloco a e $0 \leqslant f < n$. Esse método de codificação e decodificação só servirá se $f = b$, caso contrário o método não funcionará.

Temos que $f \equiv a^e \equiv (b^3)^e \pmod n \Rightarrow f \equiv b^{3\cdot e} \pmod n$. Sabemos que a chave de decodificação é obtida por:

$3 \cdot e \equiv 1 \pmod{(p-1)\cdot(q-1)}$, e desse modo,

$3 \cdot e = k \cdot [(p-1)\cdot(q-1)] + 1 \Rightarrow b^{3\cdot e} = b^{k\cdot[(p-1)\cdot(q-1)]+1} = b \cdot b^{k\cdot[(p-1)\cdot(q-1)]}$

Queremos provar que $b^{3\cdot e} \equiv b \pmod p$.

Vamos dividir a prova em dois casos:

- 1º caso : Se $(p, b) \neq 1$

  Neste caso, $b = k \cdot p \Rightarrow b \equiv 0 \pmod p \Rightarrow b^{3\cdot e} \equiv 0 \pmod p \Rightarrow b^{3\cdot e} \equiv b \pmod p$

- 2º caso: Se $(p, b) = 1$

  Neste caso, $b^{3\cdot e} = b \cdot b^{k\cdot[(p-1)\cdot(q-1)]} \Rightarrow b^{3\cdot e} = b \cdot [(b)^{p-1}]^{k\cdot(q-1)}$.

  Como $(p, b) = 1$, pelo Pequeno Teorema de Fermat, temos que $b^{p-1} \equiv 1 \pmod p$, logo, $b^{3\cdot e} = b \cdot [(b)^{p-1}]^{k\cdot(q-1)} \Rightarrow b^{3\cdot e} \equiv b \cdot 1 \equiv b \pmod p$.

  Portanto, $b^{3\cdot e} \equiv b \pmod p$.

Nos dois casos mostramos que $b^{3\cdot e} \equiv b \pmod p$.

Analogamente, podemos provar que $b^{3 \cdot e} \equiv b \pmod{q}$ e assim temos que:

$$\begin{cases} b^{3 \cdot e} \equiv b \pmod{p} \\ b^{3 \cdot e} \equiv b \pmod{q} \end{cases} \Rightarrow b^{3 \cdot e} \equiv b \pmod{p \cdot q}$$

$$\Rightarrow b^{3 \cdot e} \equiv b \pmod{n}$$

Como $b^{3 \cdot e} \equiv f \pmod{n}$, concluímos que $f \equiv b \pmod{n}$. Provamos que $f \equiv b \pmod{n}$, mas isso não garante que $f = b$, porém inicialmente, tínhamos as restrições: $1 \leqslant b < n$ e $0 \leqslant f < n$. Temos então que a congruência $f \equiv b \pmod{n}$ implica na igualdade $f = b$, como queríamos demonstrar.

Apesar de toda a segurança atribuída ao RSA, de acordo com ROUSSEAU; SAINT-AUBIN (ROUSSEAU; SAINT-AUBIN, 2015), em 1978, a estimativa era que levariam 74 anos para se fatorar um número com 100 dígitos e $3,8 \cdot 10^9$ anos para se fatorar um número com 200 dígitos. Porém, já em 2005, chaves com 200 dígitos já eram consideradas quebráveis. Nos anos 2000 já se recomendavam chaves de 309 dígitos para fins comerciais. Algoritmos poderosos têm sido produzidos, na tentativa de fatorar inteiros grandes. Um exemplo é o Algoritmo de Shor, chamado assim em homenagem ao matemático Peter Shor, e sobre ele é relatado abaixo:

> A introdução do algoritmo de fatoração em tempo polinomial de Shor em 1997 teve muitas repercussões. Entretanto, esse algoritmo requer um computador quântico, e mesmo que não sejam mais algo de ficção científica, também não são algo da realidade. (ROUSSEAU; SAINT-AUBIN, 2015, p. 260)

Enquanto os computadores quânticos não forem uma realidade palpável, o RSA continuará com seu reinado, sendo considerado muito seguro, porém deverá evoluir para que não perca esse posto.

4 Proposta Pedagógica

Como proposta pedagógica, utilizamos a disciplina Eletiva, que é um dos Componentes Integradores da parte diversificada do Currículo, para desenvolver e aplicar um Minicurso sobre Aritmética Modular e uma Sequência Didática sobre Criptografia, na Escola de Ensino Médio Theodomiro Ribeiro Coelho, com endereço: Rua São José, 533 Novo Horizonte, Cariacica - ES.

> A Eletiva é um Componente Integrador de livre escolha do estudante. A escola oferecerá um cardápio de Eletivas e o estudante poderá escolher uma eletiva diferente a cada trimestre, sempre considerando seus interesses, aptidões e Projeto de Vida. As Eletivas oportunizam aos estudantes a experimentação e diversificação do currículo, ampliando, aprofundando e enriquecendo o repertório de conhecimento, expandindo, dessa forma, suas capacidades de ler o mundo de maneira crítica e propositiva e, mais ainda, de sua própria atuação como estudante, como protagonista e como agente de transformação da sociedade. (SEDU-ES, 2021, Disponível em: <https://novoensinomedio.sedu.es.gov.br/itinerario-formativo>. Acesso em: 05 de jul. de 2023)

Por meio deste trabalho, no que tange à aplicação do Minicurso e da Sequência Didática, valorizam-se as propostas da Base Nacional Comum Curricular (BNCC) quanto ao Projeto de Vida do Estudante, pois os alunos desta Eletiva, optaram por ela de acordo com o seu projeto de vida. Trabalha-se também com temas integradores contemporâneos que são relevantes para a compreensão do mundo atual dentro do tópico Trabalho, Ciência e Tecnologia.

O Projeto de vida, outro componente integrador da parte diversificada do currículo é aqui definido:

> O Projeto de Vida é um Componente Integrador que tem como foco o autoconhecimento e a reflexão sobre a atuação do jovem no mundo, na família e na comunidade. Tem o objetivo de desenvolver a capacidade do estudante de dar sentido à sua existência, tomar decisões, planejar o futuro e agir no presente com autonomia e responsabilidade. Nas aulas de Projeto de Vida, o estudante terá, também, a oportunidade de fazer escolhas profissionais, embora este não seja o foco do componente. (SEDU-ES, 2021, Disponível em: <https://novoensinomedio.sedu.es.gov.br/itinerario-formativo>. Acesso em 05 de jul. de 2023)

4.1 Recursos computacionais

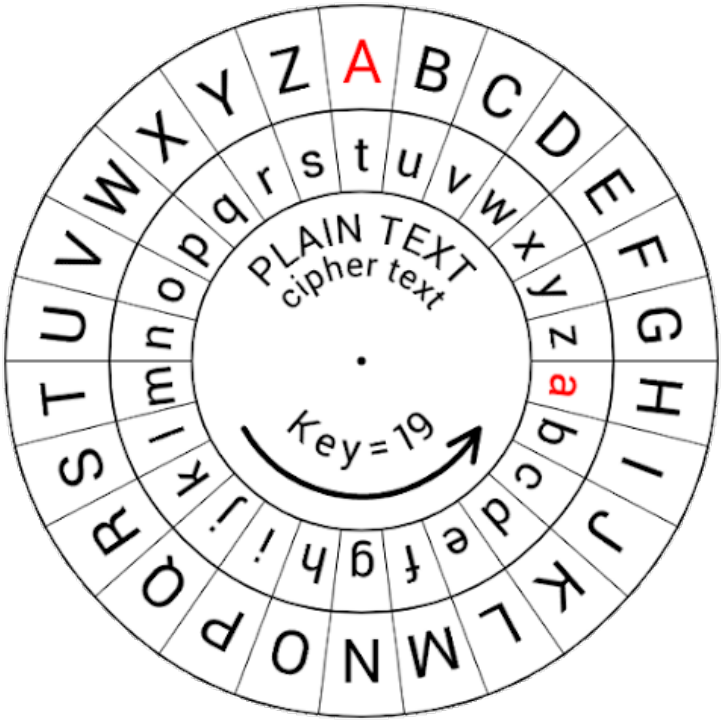
A BNCC estimula o desenvolvimento de competências e habilidades, relacionadas ao uso consciente e responsável de tecnologias digitais, tais como recursos computacionais, de forma direcionada ou transversal, como meio ou suporte para promover a aprendizagem e/ou promover o interesse dos alunos. A competência geral 5 da BNCC destaca:

> "Compreender, utilizar e criar tecnologias digitais de informação e comunicação de forma crítica, significativa, reflexiva e ética nas diversas práticas sociais (incluindo as escolares) para se comunicar, acessar e disseminar informações, produzir conhecimentos, resolver problemas e exercer protagonismo e autoria na vida pessoal e coletiva." (BRASIL, 2018, p. 9)

Foram utilizados recursos como aplicativos e programas, cada um com uma finalidade específica, podendo também em alguns momentos, serem usados em conjunto. Mostraremos aqui estes aplicativos e exploraremos suas funcionalidades na seção 3 deste capítulo. Todos os aplicativos e programas que serão aqui apresentados, são gratuitos, de fácil acesso através da internet e de plataformas de download.

A Figura 20 mostra a interface do aplicativo "Caesar Cipher Disk", que usamos para cifrar e decifrar textos, utilizando o método da cifra de César (Capítulo 1, seção 1).

Figura 20 – Interface do Aplicativo Caesar Cipher Disk



Fonte: Disponível em: <https://play.google.com/store/apps/details?id=com.nb974.caesarcipherwheel&hl=pt>. acesso em: 10 de set. de 2023.

A Figura 21 mostra a interface do aplicativo "Números Primos", que usamos para gerar e validar números primos, bem como identificar a posição de determinado número primo. Por exemplo: O número 91 é um número primo?

Figura 21 – Interface do Aplicativo Números Primos

Fonte: Disponível em: <https://play.google.com/store/apps/details?id=br.com.mxczpiscioneri.prime&hl=pt&gl=US>. Acesso em 10 de set. de 2023.

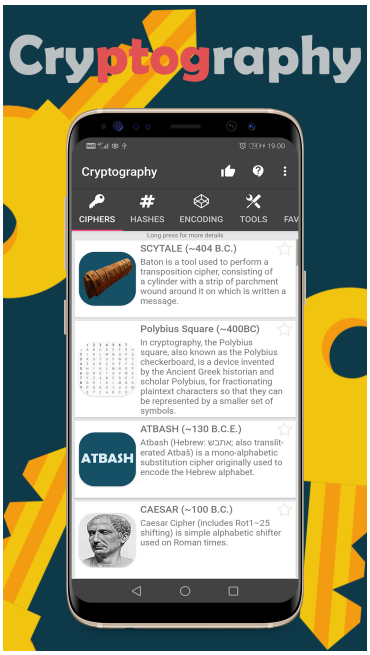
A Figura 22 mostra a interface do aplicativo "Verso-RSA" , que utilizamos para efetuar diversos cálculos matemáticos fundamentais de aritmética modular. Utilizamos também como suporte e conferência de cálculos, e para cifrar e decifrar por Criptografia RSA.

Figura 22 – Interface do Aplicativo Verso RSA

Fonte: Disponível em: <https://play.google.com/store/apps/details?id=professorhelvesio.verso_rsa_app>. Acesso em 10 de set. de 2023.

A Figura 23 mostra a interface do aplicativo "Cryptography". Este aplicativo possui várias aplicações de Métodos criptográficos diferentes, relatando um pouco da história por trás deles. Aplicativo muito interessante, e o utilizamos para cifrar textos por alguns métodos apresentados neste trabalho.

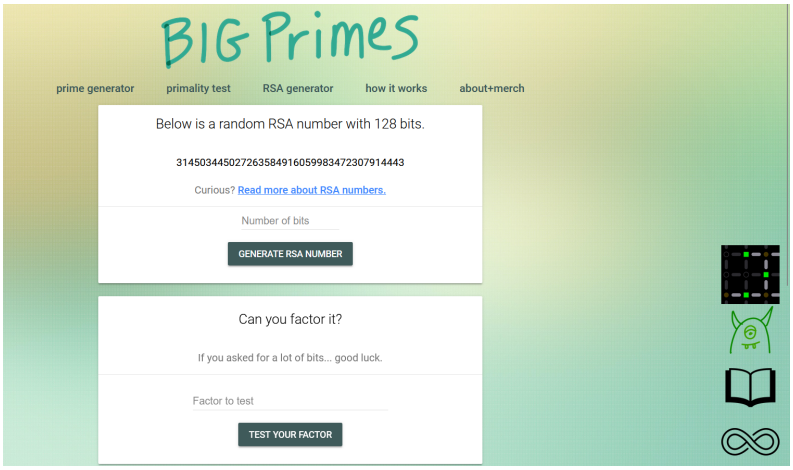
Figura 23 – Interface do Aplicativo Cryptography



Fonte: Disponível em: <https://play.google.com/store/apps/details?id=com.nitramite.cryptography&hl=pt_BR&gl=US>. Acesso em: 10 de set. de 2023.

A Figura 24 mostra a interface do programa "Big Primes", que gera grandes números primos. O programa também possui um jogo com números primos que utilizamos em nossa Sequência Didática.

Figura 24 – Interface do Programa Big Primes



Fonte: Disponível em|: <https://bigprimes.org/RSA-challenge>. Acesso em: 10 de set. de 2023.

4.2 Minicurso

No primeiro trimestre de 2023, a disciplina eletiva foi destinada para a realização de um minicurso sobre os conceitos matemáticos fundamentais para o entendimento da criptografia RSA. A eletiva "Minicurso de Aritmética Modular ", contava com duas aulas nas segundas-feiras, totalizando 11 segundas-feiras. Para tanto, o próprio texto deste trabalho serviu de manual e guia para o desenvolvimento das aulas por parte do professor.

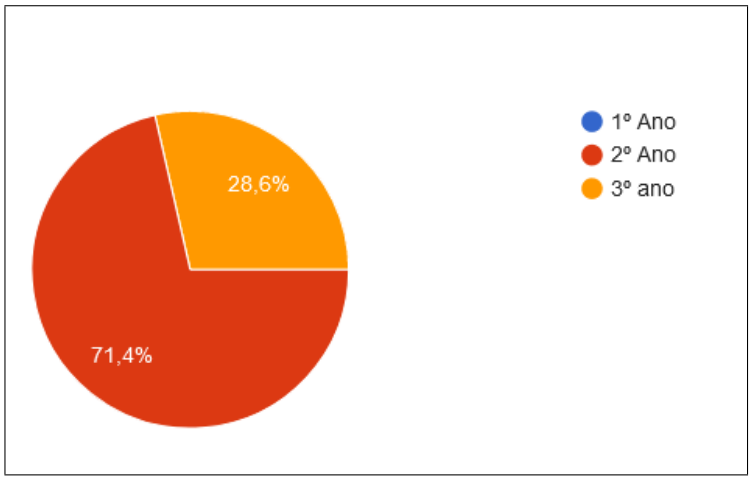
Objetivos do Minicurso:

- Preparar os alunos com conceitos necessários para o entendimento e aprendizagem de criptografia RSA.
- Utilizar os conceitos aprendidos como preparação para a Olimpíada Brasileira de Matemática das Escolas Públicas - OBMEP, tendo em vista o perfil dos participantes e que alguns deles possuem Menção Honrosa na OBMEP de 2022.
- Desenvolver e aprofundar interesse pela Matemática nos estudantes.

Ao iniciar o período da eletiva, foi disponibilizado aos alunos um formulário, via Google Formulários, com a finalidade de analisar seus conhecimentos prévios , confirmar se seu Projeto de Vida está conectado com matemática ou tecnologia, sendo este quesito desejável, porém não obrigatório ou eliminatório quanto à participação na Eletiva. O perfil dos 14 alunos que compuseram a Eletiva, analisado através do formulário foi:

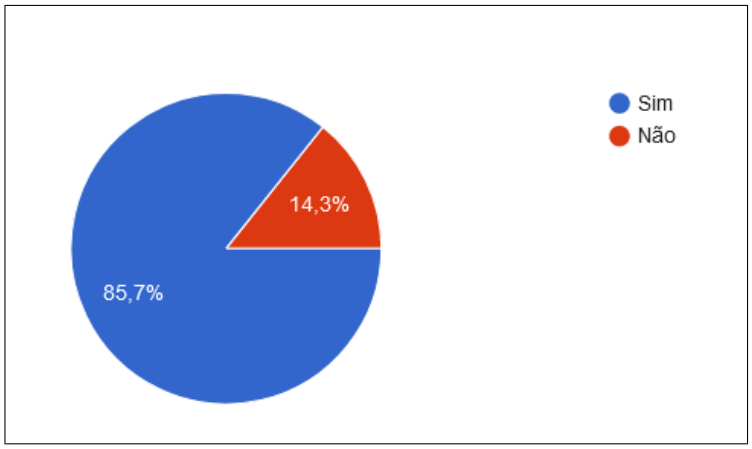
- Ano do ensino médio que está cursando:

Figura 25 – Porcentagem quanto ao ano do Ensino Médio



Fonte: Produção do próprio autor (2023)

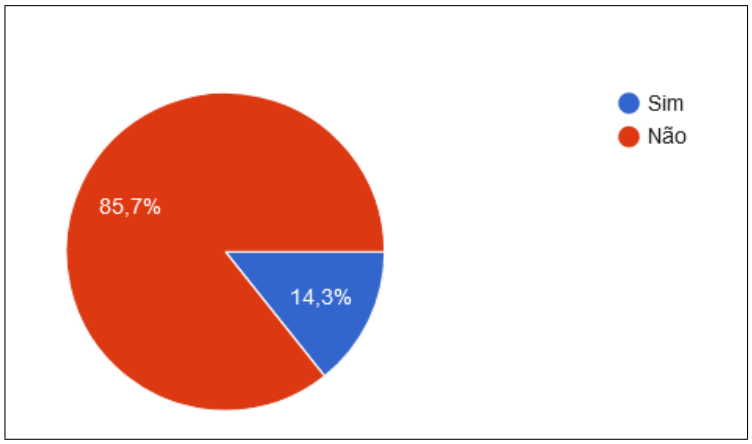
Figura 26 – Porcentagem quanto ao Projeto de Vida



Fonte: Produção do próprio autor (2023)

- No seu Projeto de vida, você se identifica com alguma carreira que esteja ligada à matemática ou áreas correlacionadas?
- Você já estudou algo sobre Criptografia?

Figura 27 – Porcentagem quanto ao estudo sobre Criptografia



Fonte: Produção do próprio autor (2023)

De posse destes dados e outros coletados por meio do formulário, foi possível traçar o perfil dos estudantes e fazer o planejamento das aulas. O conteúdo do Capítulo 2 deste trabalho foi dividido entre as 22 aulas (11 segundas-feiras) dando-se ênfase a Divisibilidade, Números Primos, Pequeno Teorema de Fermat, Congruências e Aritmética modular. A metodologia utilizada foi a de resolução de problemas e exercícios envolvendo os tópicos apresentados acima.

Afim de avaliar o aprendizado, foram selecionados exercícios e problemas retirados do Portal da OBMEP, disponível em <https://portaldaobmep.impa.br/index.php/modulo/ver?modulo=63&tipo=4>, acesso em 19/05/23.

1. Encontre o resto de $100 \cdot 103 \cdot 104$ na divisão por 7.

2. Observe os restos das potências de 2 na divisão por 3:

Figura 28 – Restos das potências de 2 na divisão por 3

	2^0	2^1	2^2	2^3
Resto	1	2	1	2
	2^4	2^5	2^6	2^7
Resto	1	2	1	2

Fonte: Produção do próprio autor (2023).

   (a) Seguindo o padrão da tabela, qual deve ser o resto de 2^{2016} na divisão por 3?
   (b) Verifique que $2^{2k} \equiv 1 \pmod 3$ e que $2^{2k+1} \equiv 2 \pmod 3$ para todo k inteiro não negativo.

3. Encontre os restos da divisão de 224 por:
   a) 5 b) 7 c) 11 d) 17.

4. Qual o resto na divisão de $2^{70} + 3^{70}$ por 13?

5. Qual o resto de 3^{200} por 100?

6. Determine o resto de $2^{20} - 1$ na divisão por 41.

4.3 Sequência Didática

O segundo trimestre da disciplina Eletiva foi destinado à realização de uma Sequência Didática sobre Criptografia, dando ênfase à Criptografia RSA. O trimestre contou com 12 segundas-feiras totalizando 24 aulas. A estratégia de uma sequência didática consiste na elaboração e desenvolvimento de atividades, seguindo uma lógica estrutural em forma de sequência de compartilhamento de informação e progressão do conhecimento. Neste sentido, a elaboração desta Sequência leva em consideração os conhecimentos adquiridos no Minicurso que foi referido na Seção 4.2 deste capítulo.

Tema da Sequência Didática:
Ensino de Alguns Métodos Criptográficos e Criptografia RSA no Ensino Médio.

Objetivos

- Introduzir os princípios de criptografia, bem como sua importância na proteção de informações.
- Estudar alguns dos métodos de criptografia mais usados na história.
- Compreender os princípios da criptografia RSA e como esse algoritmo moderno protege suas informações.
- Aprender a cifrar e decifrar textos e informações em RSA, com e sem o auxílio de recursos computacionais.
- Desenvolver competências e habilidades relacionadas com o uso de recursos computacionais na resolução de problemas.
- Ajudar a promover a consciência sobre a segurança do uso de dados pela internet.

Conteúdos

Cifra de César, Cifra de Vigenère, Cifra Alemã ADFGVX, Máquina Enigma, Algoritmo RSA.

Habilidades e Competências da BNCC a serem desenvolvidas

- (EM13MAT315) Investigar e registrar, por meio de um fluxograma, quando possível, um algoritmo que resolve um problema. (BRASIL, 2018, p.537)
- Competência Específica 2 - Matemática - Propor ou participar de ações para investigar desafios do mundo contemporâneo e tomar decisões éticas e socialmente responsáveis, com base na análise de problemas sociais, como os voltados a situações de saúde, sustentabilidade, das implicações da tecnologia no mundo do trabalho, entre outros, mobilizando e articulando conceitos, procedimentos e linguagens próprios da Matemática. (BRASIL, 2018, p. 534)
- Competência Geral 5 - Matemática - Investigar e estabelecer conjecturas a respeito de diferentes conceitos e propriedades matemáticas, empregando estratégias e recursos, como observação de padrões, experimentações e diferentes tecnologias, identificando a necessidade, ou não, de uma demonstração cada vez mais formal na validação das referidas conjecturas. (BRASIL, 2018, p. 9)

Tempo de execução

15 aulas.

Materiais Necessários

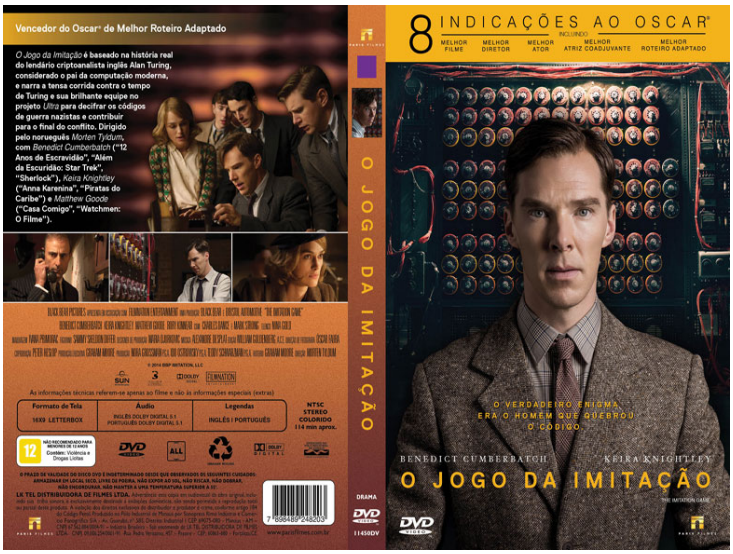
Computador e/ou celular, projetor, folhas de papel A_4, internet.

1ª Parte

Duração: 3 aulas.

Exibição e análise do filme: O Jogo da Imitação

Figura 29 – Imagem de capa do filme: O jogo da Imitação



Fonte: Disponível em: <https://edisciplinas.usp.br/mod/folder/view.php?id=2856138>. Acesso em: 10 de set. de 2023.

O filme é baseado na história real do criptoanalista inglês Alan Turing e narra a corrida contra o tempo de Alan Turing e sua equipe para decifrar os códigos nazistas da máquina Enigma.

Desenvolvimento

Após a exibição do filme, uma mesa redonda foi feita com os estudantes para a análise do filme. Foram dadas sugestões para análise como:

- A importância da criptografia e da criptoanálise para a guerra.
- Os benefícios e os malefícios do uso da tecnologia.
- Implicações éticas e de responsabilidades no uso de tecnologias, principalmente nos dias de hoje, com o avanço da Inteligência Artificial (IA).

Avaliação

A avaliação se deu através da participação dos alunos na mesa redonda.

2ª Parte

Duração: 2 aulas

Uso do aplicativo Caesar Cipher Disk para decifragem de mensagens, conhecida a chave. O aplicativo Caesar Cipher Disk tem como princípio, a cifra de César estudada no Capítulo 1, Seção 3. Ele dispões de 2 discos onde se fixa o disco interior e se desloca o disco maior quantas letras se deseja que seja a chave. Deve-se explicar o método e o funcionamento do aplicativo aos estudantes.

Desenvolvimento:

1º Passo: De posse do aplicativo Caesar Cipher Disk instalado via computador da escola ou celular dos estudantes, foi entregue a mensagem codificada em blocos de 5 letras: "ijxht gwnrt xtxjl wjit" , pedindo sua decodificação. Após 10 minutos, verificou-se quem conseguiu decifrar a mensagem sem a chave. Após esse tempo foi liberada a chave, que nesse caso será 5 (deslocamento de 5 letras). A Figura 30 mostra o deslocamento executado:

Figura 30 – Exemplo de utilização do aplicativo Caesar Cipher Disk com chave 5

Fonte: Produção do próprio autor (2023)

A mensagem decodificada será: "DESCOBRIMOS O SEGREDO".

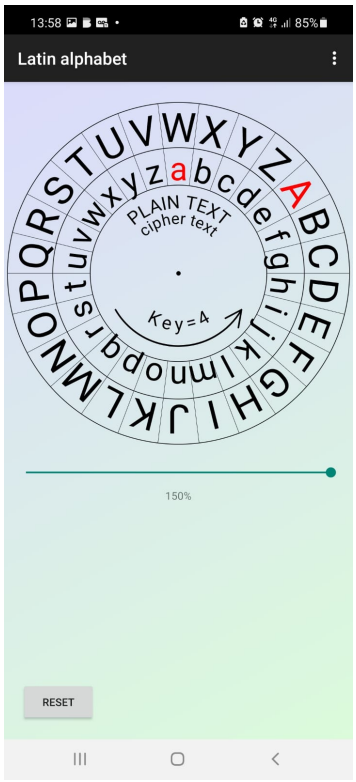
2º Passo: Os estudantes foram separados em duplas, de modo que cada integrante da dupla estivesse sentado distante. A tarefa consiste em que cada aluno deve combinar uma chave com sua dupla e enviar uma pequena mensagem através de um envelope contendo remetente e destinatário. Deve-se verificar após a atividade, se a cifragem e a decifragem da mensagem está correta.

3º Passo: Observa-se que a Cifra de César não é muito confiável nos dias atuais. Para tornar a decifragem um pouco mais difícil, é possível tomarmos múltiplas chaves. Para exemplificar, vamos tomar três chaves. A chave 3 para a 1ª letra, para a 4ª letra, para a 7ª letra e assim sucessivamente. De mesmo modo, usaremos a chave 4 para a 2ª letra, para a 5ª letra, para a 8ª letra e assim sucessivamente. E usaremos a chave 5 para a 3ª letra, para a 6ª letra, para a 9ª letra e assim sucessivamente. Foi pedido então, que cifrassem a mensagem: "PROVA SURPRESA" com essas chaves. As chaves estão representadas pelas Figuras 31, 32 e 33 :

Figura 31 – Chave 3 - Caesar Cipher Disk

Fonte: Produção do próprio autor (2023)

Figura 32 – Chave 4 - Caesar Cipher Disk



Fonte: Produção do próprio autor(2023)

Figura 33 – Chave 5 - Caesar Cipher Disk

Fonte: Produção do próprio autor (2023)

Após dar o tempo para que realizem a tarefa, foi mostrada a mensagem cifrada para que verifiquem se acertaram. A mensagem cifrada foi: “svtye xxvuu ixd ”. Repetimos agora o Passo 2 e pedimos que os alunos combinem as chaves com sua dupla enviem mensagens cifradas pela cifra de César com múltiplas chaves.

Avaliação

A avaliação se deu através da participação dos alunos e na produção de mensagens cifradas e decifradas.

3ª parte

Duração: 2 aulas

A Cifra de Vigenère - Utilização do aplicativo Cryptography

A cifra Vigenère, foi por mais de 300 anos considerada indecifrável. Ela foi apresentada no Capítulo 1, Seção 3 deste trabalho, e podemos usá-lo então como base para mostrar como funciona este método criptográfico. Fizemos uso também do aplicativo Cryptography para fins de conferência das Cifras.

Desenvolvimento:

1º Passo: Foi entregue uma Tabela de Vigenère impressa aos alunos e explicado como funciona a codificação de mensagens através da intersecção entre as letras do texto claro e da chave. Usamos a Tabela 34 utilizada no Capítulo 1, Seção 3, para demonstração, onde usamos o texto claro: “MORTE AO GENERAL” e a palavra chave “HONRA” e obtivemos como texto cifrado “TCEKEHCTVNLFNC”.

Figura 34 – Exemplo de Utilização da Tabela de Vigenère

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

Fonte: Disponível em: <https://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-Base.html>. Acesso em: 10 de set. de 2023.

2º passo: Nesse momento, foi pedido que os alunos cifrem o texto "MORTE AO GENERAL" com a palavra chave "HONRA" usando apenas a tabela impressa. Após a tentativa de cifragem, utilizamos o aplicativo Cryptography para conferência do resultado. A Figura 35 mostra a interface do aplicativo com o texto claro e a chave desejados e o texto cifrado;

Figura 35 – Exemplo de utilização do aplicativo Cryptography

Fonte: Produção do próprio autor (2023).

3º Passo: Deixar que os estudantes se divirtam enviando mensagens codificadas pela Cifra de Vigenère para os colegas.

Avaliação: A avaliação se deu através da participação dos alunos e na produção de mensagens cifradas e decifradas.

4ª parte

Duração: 2 aulas

A cifra Alemã ADFGVX

Por se tratar de uma cifra utilizada pela Alemanha Nazista durante um dos períodos mais sombrios da História, é interessante que haja um diálogo interdisciplinar com as disciplinas de História e Geografia a fim de que haja um entendimento mais completo desse episódio da idade contemporânea.

1º Passo: Convidamos o professor de História e o Professor de Geografia de sua escola para palestrarem sobre o tema, relatando acontecimentos, crises internacionais geradas, conflitos territoriais, etc.

2º Passo: Após a palestra, apresentamos aos estudantes a cifra ADFGVX, sua utilização e a metodologia criptográfica utilizada. A cifra ADFGVX foi apresentada neste trabalho no Capítulo 1, Seção 4, e pode servir de subsídio e guia para esta etapa.

A ideia desta atividade é que cada aluno crie a sua própria cifra ADFGVX. Para começar vamos entregar uma tabela 7×7 em folha impressa, com as letras ADFGVX na primeira linha e na primeira coluna preservando o primeiro quadrículo em branco. A Tabela 26 ilustra o modo como a atividade deve ser entregue.

Tabela 26 – Modelo para construção de Cifra ADFGVX

	A	D	F	G	V	X
A						
D						
F						
G						
V						
X						

Fonte: Produção do próprio autor (2023).

Foi pedido agora que completem aleatoriamente a tabela com as 26 letras do alfabeto e com 10 algarismos sem repetir letras ou algarismos. Para exemplificar perante os estudantes podemos dispor a tabela preenchida que usamos anteriormente, no Capítulo 1, Seção 3, frisando que a tabela deles deve ser diferente. Por comodidade, a tabela citada é repetida neste capítulo na Tabela 27.

Tabela 27 – Exemplo de Cifra ADFGVX

	A	D	F	G	V	X
A	5	M	J	F	9	L
D	A	R	G	4	2	P
F	S	D	0	I	Z	6
G	W	C	B	N	T	X
V	H	1	V	E	Y	7
X	Q	K	8	U	3	O

Fonte: Produção do próprio autor(2023).

Após cada estudante concluir sua tabela, vamos unificar a mensagem a ser cifrada. Vamos cifrar o texto: “ENCONTRO ÀS 10:30 PM”. A palavra chave também deverá ser a mesma para todos. Usaremos a chave: “ENIGMA”.

Dando sequência ao método, dividimos sua cifragem em duas etapas e para exemplificar, faremos a cifragem de acordo com nossa tabela e o aluno segue fazendo o mesmo com a tabela dele:

1ª etapa: Cada letra do texto claro deve ser substituída respectivamente pelas letras da 1ª linha e da 1ª coluna em que está inserida. Por exemplo, na tabela do professor, a letra E será substituída pelas letras "VG", nesta ordem. Fazendo a cifragem da 1ª etapa de todo o texto claro, para demonstração, obteremos:

Texto Claro	E	N	C	O	N	T	R	O	A	S	1	O	3	0	P	M
Texto Cifrado	VG	GG	GD	XX	GG	GV	DD	XX	DA	FA	VD	FF	XV	FF	DX	AD

Fonte: Produção do próprio autor.

O texto Cifrado na 1ª etapa será dado por:

"VGGGGDXXGGGVDDXXDAFAVDFFXVFFDXAD"

2ª etapa: A segunda Etapa é uma transposição de colunas, tendo como base a palavra chave. De posse da palavra chave e do texto cifrado na 1ª Etapa, montaremos uma tabela em que a primeira linha contêm a palavra chave. A segunda linha a numeração correspondente à ordem alfabética das letras da palavra chave. Por fim, a cifragem é feita de cima para baixo seguindo a ordem alfabética das colunas:

Tabela 28 – Segunda Etapa da Cifra ADFGVX

E	N	I	G	M	A
2	5	4	3	6	1
V	G	G	G	G	D
X	X	G	G	G	V
D	D	X	X	D	A
F	A	V	D	F	F
X	V	F	F	D	X
A	D				

Fonte: Produção do próprio autor.

O texto cifrado final será:

"DVAFXVXDFXAGGXDFGGXVFGXDAVDGGDFD"

E como era costume separar a cifra em Blocos de 5 caracteres:

"DVAFX VXDFX AGGXD FGGXV FGXDA VDGGD FD"

3º Passo: Neste momento, após o professor compartilhar sua tabela e sua cifragem final, alguns alunos, de acordo com seu interesse, podem também socializar as tabelas no quadro e sua cifragem final.

Avaliação: A avaliação se deu através da participação dos alunos e na produção das tabelas individuais e das correspondentes cifragens do texto solicitado.

5ª parte

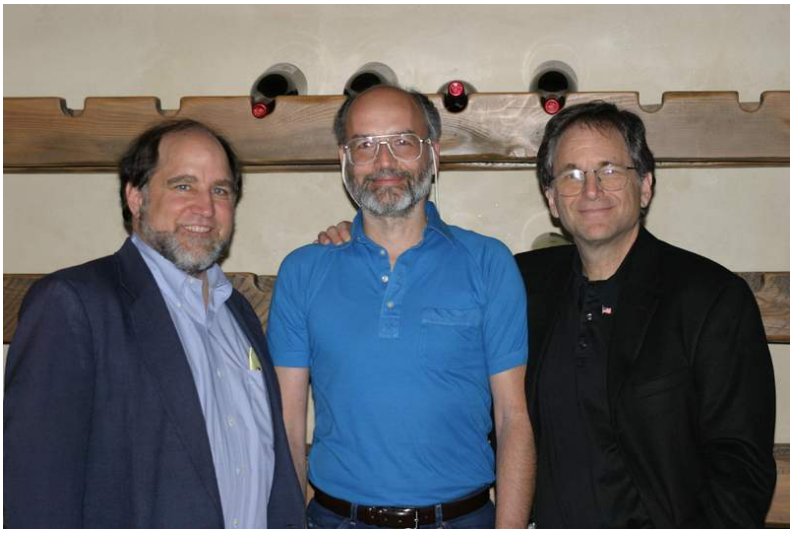
Duração: 2 aulas

Criptografia RSA e Algoritmo de Codificação

A Criptografia RSA é um tipo de algoritmo de criptografia assimétrica que utiliza duas chaves, uma pública e uma privada. Todo o Capítulo 3 deste trabalho foi destinado a ela e de uma forma mais geral, podemos dizer que o Capítulo 2 também o foi, pois se trata de uma preparação conceitual para o entendimento da mesma. A chave pública é utilizada para criptografar, ou seja cifrar os dados que serão enviados, como senhas, logins, números de cartão de crédito etc. A segunda, a privada, é utilizada para descriptografar, ou seja decifrar o texto que foi enviado cifrado, voltando ao texto original e somente com ela é possível fazer este processo de decifragem. Portanto, podemos perceber que a criptografia RSA é mais utilizada para proteger outras chaves, como já mencionamos. É natural que processos onde esses dados sejam requisitados sejam feitos, na grande maioria, via Internet e, portanto, a segurança na transferência e integridade dos dados é um fator fundamental. Para suprir essa necessidade, foi desenvolvida em 1977, a Criptografia RSA, por Ronald Rivest, Adi Shamir, Leonard Adleman, e publicada posteriormente em 1978. O esquema criado por eles ficou conhecido como RSA sigla gerada pelas iniciais dos nomes e que tem reinado como o mais aceito e implementado sistema de encriptação de chave pública.

Neste sistema de criptografia, o algoritmo para criptografar, o algoritmo para descriptografar e a chave pública podem ser de conhecimento de qualquer pessoa. Somente a chave privada é mantida em segredo. O código ASCII será utilizado neste trabalho para a codificação e decodificação de dados. A Figura 36 mostra os pioneiros da Criptografia RSA e a Tabela 29 mostra a tabela ASCII resumida e adaptada:

Figura 36 – Ronald Rivest, Adi Shamir e Leonard Adleman



Fonte: Disponível em: <https://www.wired.com/images_blogs/photos/uncategorized/2007/11/19/rsa_security_founders.jpg>. Acesso em: 10 de set. de 2023.

Tabela 29 – Tabela ASCII resumida e adaptada.

Carácter	Número	Carácter	Número	Carácter	Número	Carácter	Número
A	65	a	97	espaço	32	:	58
B	66	b	98	!	33	;	59
C	67	c	99	”	34	<	60
D	68	d	100	#	35	=	61
E	69	e	101	$	36	>	62
F	70	f	102	%	37	?	63
G	71	g	103	&	38	@	64
H	72	h	104	’	39	[	91
I	73	i	105	(	40	\	92
J	74	j	106	)	41	]	93
K	75	k	107	*	42	∧	94
L	76	l	108	+	43	_	95
M	77	m	109	,	44	‘	96
N	78	n	110	-	45	{	123
O	79	o	111	.	46	|	124
P	80	p	112	/	47	}	125
Q	81	q	113	0	48	∼	126
R	82	r	114	1	49	Ç	128
S	83	s	115	2	50	ç	135
T	84	t	116	3	51	ñ	164
U	85	u	117	4	52	Ñ	165
V	86	v	118	5	53	ª	166
W	87	w	119	6	54	≡	240
X	88	x	120	7	55	±	241
Y	89	y	121	8	56	÷	246
Z	90	z	122	9	57	°	248

Fonte: Produção do próprio autor (2023).

Desenvolvimento:

1º Passo: Apresentar aos estudantes o algoritmo de codificação:

$$b^d \equiv a \pmod{n} \tag{4.1}$$

Para o uso do algoritmo é necessário escolher dois números primos. Para efeito de entendimento, devemos usar dois primos pequenos, porém deixar claro que na prática, são usados primos muitos grandes, na casa de 200 a 300 dígitos. Elementos necessários:

- **Dois primos:** Como sugestão usar $p = 5$ e $q = 19$
- **Cálculo de n:** $n = p \cdot q = 5 \cdot 19 = 95$
- **Cálculo de** $\varphi(n)$ **:** $(p-1) \cdot (q-1) = 4 \cdot 18 = 72$
- **Escolha do número d:** Escolher um número d tal que $(72, d) = 1$. Usaremos $d = 7$.
- **Chave Pública:** A chave pública será dada pelo par (n, d).

2º Passo: Para exemplificar, cifrar com os alunos a palavra "SOL". Observando a tabela ASCII, vamos pré-codificar SOL. Temos os blocos b que são: $S = 83, O = 79, L = 76$. Logo, teremos 837976. Usando o algoritmo de codificação e as informações do Passo 1, teremos:

Codificando o primeiro bloco:

$$83^7 \equiv a \pmod{95} \tag{4.2}$$

$$83^7 \equiv ((83)^2)^3 \cdot 83 \equiv ((-12)^2)^3 \cdot (-12) \equiv 144^3 \cdot (-12) \equiv (49)^2 \cdot 49 \cdot (-12) \equiv 2401 \cdot (-588)$$
$$\equiv 26 \cdot (-18) \equiv -468 \equiv 7 \pmod{95}$$

Portanto, $83^7 \equiv 7 \pmod{95}$.

Codificando o segundo bloco:

$$79^7 \equiv a \pmod{95} \tag{4.3}$$

$$79^7 \equiv ((79)^2)^3 \cdot 79 \equiv ((-16)^2)^3 \cdot (-16) \equiv 256^3 \cdot (-16) \equiv 66^3 \cdot (-16) \equiv 66^2 \cdot 66 \cdot (-16) \equiv$$
$$(-29)^2 \cdot (-29) \cdot (-16) \equiv 841 \cdot 464 \equiv 81 \cdot 84 \equiv (-14) \cdot (-11) \equiv 154 \equiv 59 \pmod{95}$$

Portanto, $79^7 \equiv 59 \pmod{95}$

Codificando o terceiro bloco

$$76^7 \equiv a \pmod{95} \tag{4.4}$$

$$76^7 \equiv ((76)^2)^3 \cdot 76 \equiv ((-19)^2)^3 \cdot (-19) \equiv 361^3 \cdot (-19) \equiv 76^3 \cdot (-19) \equiv (-19)^3 \cdot (-19)$$
$$\equiv (-19)^2 \cdot (-19) \cdot (-19) \equiv 361 \cdot 361 \equiv (-19) \cdot (-19) \equiv 361 \equiv 76 \pmod{95}$$

Portanto, $76^7 \equiv 76 \pmod{95}$

O texto codificado será representado pela Tabela 30:

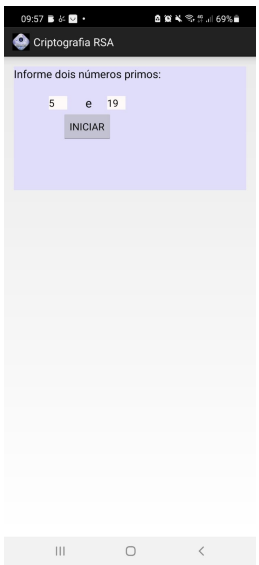
Tabela 30 – Codificação da palavra SOL

Caractere do Texto Claro	Numeração na Tabela ASCII	Código RSA	Texto Codificado	Binário Correspondente
S	83	7	BEL	00000111
O	79	59	;	00111011
L	76	76	L	01001100

Fonte: Produção do próprio autor (2023).

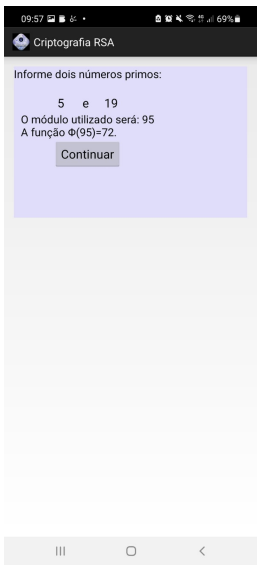
3º Passo: Apresentar o Aplicativo Verso RSA, destacando suas funcionalidades, uma vez que este é um dos aplicativos mais completos no que diz respeito à aritmética modular e criptografia RSA que encontramos, além de seu uso ser muito intuitivo. Usamos o aplicativo para conferir os cálculos propostos no 2º Passo. As Figuras 37, 38, 39, 40, 41 e 42 demonstram passo a passo o processo de conferência dos resultados:

Figura 37 – 1º Passo no Verso RSA



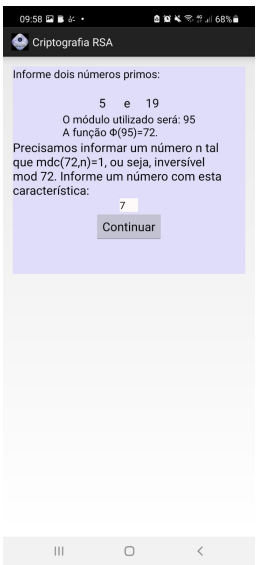
Fonte: Produção do próprio autor (2023).

Figura 38 – 2º Passo no Verso RSA



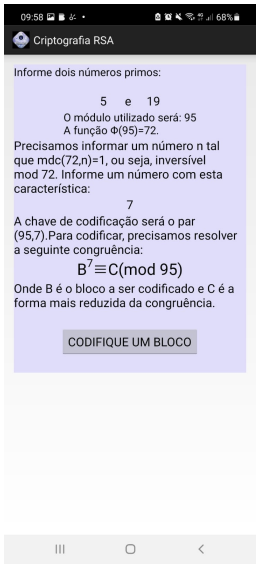
Fonte: Produção do próprio autor (2023).

Figura 39 – 3º Passo no Verso RSA



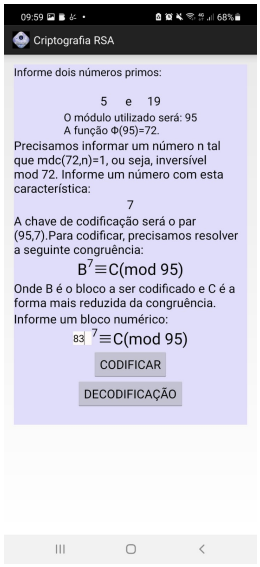
Fonte: Produção do próprio autor (2023).

Figura 40 – 4º Passo no Verso RSA



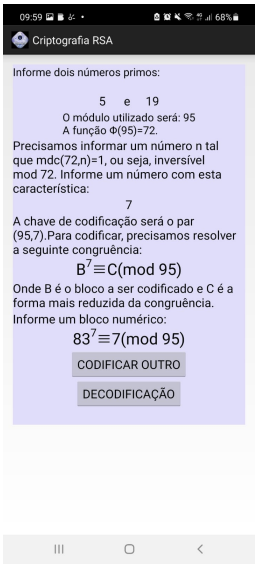
Fonte: Produção do próprio autor (2023)

Figura 41 – 5º Passo no Verso RSA



Fonte: Produção do próprio autor (2023)

Figura 42 – 6º Passo no Verso RSA



Fonte: Produção do próprio autor (2023).

4º Passo: Como atividade a ser entregue via aplicativo de mensagens, codificar a palavra "OBMEP", pelo algoritmo RSA, usando os números primos 7 e 17.

Avaliação: A avaliação se deu através da participação dos alunos e na entrega da atividade proposta no Passo 4, via aplicativo de mensagens.

6ª parte

Duração: 2 aulas

O algoritmo da decodificação

A chave de decodificação será dada pelo par (n, e), onde e é o inverso de $d \pmod{(p-1)\cdot(q-1)}$. O algoritmo de decodificação será dado por:

$$a^e \equiv b \pmod{n} \tag{4.5}$$

1º passo: Apresentar aos estudantes o algoritmo de decodificação e exemplificar usando a palavra que foi codificada na 5ª parte desta sequência. Decodificamos os blocos "a", da palavra "SOL" que foram codificados como $7-59-76$. O objetivo é que estes blocos retornem nos blocos "b" referentes à palavra "SOL". Para isso, precisamos encontrar o valor de e. Lembre-se que $n = 95$ e que escolhemos $d = 7$ para a codificação, então teremos:

$$d \cdot e \equiv 1 \pmod{(p-1)\cdot(q-1)}$$

$$\Rightarrow 7 \cdot e \equiv 1 \pmod{72} \Rightarrow e = 31$$

Portanto, a chave de decodificação será dada por $(95, 31)$.

Decodificando o primeiro bloco:

$$7^{31} \equiv b \pmod{95} \tag{4.6}$$

$$7^{31} \equiv ((7)^2)^{15} \cdot 7 \equiv ((49)^{15} \cdot 7 \equiv ((49)^2)^7 \cdot 49 \cdot 7 \equiv 2401^7 \cdot 343 \equiv 26^7 \cdot 58$$
$$\equiv ((26)^2)^3 \cdot 26 \cdot 58 \equiv 676^3 \cdot 1508 \equiv 11^3 \cdot 83 \equiv (11)^2 \cdot 11 \cdot 83 \equiv 121 \cdot 11 \cdot 83$$
$$\equiv 26 \cdot 11 \cdot 83 \equiv 286 \cdot 83 \equiv 1 \cdot 83 \equiv 83 \pmod{95}$$

Portanto, $7^{31} \equiv 83 \pmod{95}$.
Retornando ao bloco $b = 83$ que corresponde à letra S.

Decodificando o segundo bloco:

$$59^{31} \equiv b \pmod{95} \tag{4.7}$$

$$59^{31} \equiv ((59)^2)^{15} \cdot 59 \equiv ((-36)^2)^{15} \cdot (-36) \equiv ((1296)^{15} \cdot (-36) \equiv 61^{15} \cdot (-36)$$
$$\equiv (-34)^{15} \cdot (-36) \equiv ((-34)^2)^7 \cdot (-34) \cdot (-36) \equiv 1156^7 \cdot 1224 \equiv 16^7 \cdot 84 \equiv ((16)^2)^3 \cdot 16 \cdot (-11)$$
$$\equiv 256^3 \cdot (-176) \equiv 66^3 \cdot (-81) \equiv 66^2 \cdot 66 \cdot 14 \equiv (-29)^2 \cdot (-29) \cdot 14 \equiv 841 \cdot (-29) \cdot 14$$
$$\equiv 81 \cdot (-29) \cdot 14 \equiv (-14) \cdot (-29) \cdot 14 \equiv 406 \cdot 14 \equiv 26 \cdot 14 \equiv 364 \equiv 79 \pmod{95}$$

Portanto, $59^{31} \equiv 79 \pmod{95}$.
Retornando ao bloco $b = 79$ que corresponde à letra O.

Decodificando o terceiro bloco:

$$76^{31} \equiv b \pmod{95} \tag{4.8}$$

$$76^{31} \equiv ((76)^2)^{15} \cdot 76 \equiv ((-19)^2)^{15} \cdot (-19) \equiv (361)^{15} \cdot (-19) \equiv 76^{15} \cdot (-19) \equiv (-19)^{15} \cdot (-19)$$
$$\equiv ((-19)^2)^7 \cdot (-19) \cdot (-19) \equiv 361^7 \cdot 361 \equiv 76^7 \cdot 76 \equiv ((-19)^2)^3 \cdot (-19) \cdot (-19) \equiv 361^3 \cdot 361$$
$$\equiv 76^3 \cdot 76 \equiv 76^2 \cdot 76 \cdot 76 \equiv (-19)^2 \cdot (-19) \cdot (-19) \equiv 361 \cdot 361 \equiv 76 \cdot 76 \equiv (-19) \cdot (-19)$$
$$\equiv 361 \equiv 76 \pmod{95}$$

Portanto, $76^{31} \equiv 76 \pmod{95}$.
Retornando ao bloco $b = 76$ que corresponde à letra L.

O texto decodificado será representado pela Tabela 31.

Tabela 31 – Decodificação da palavra SOL

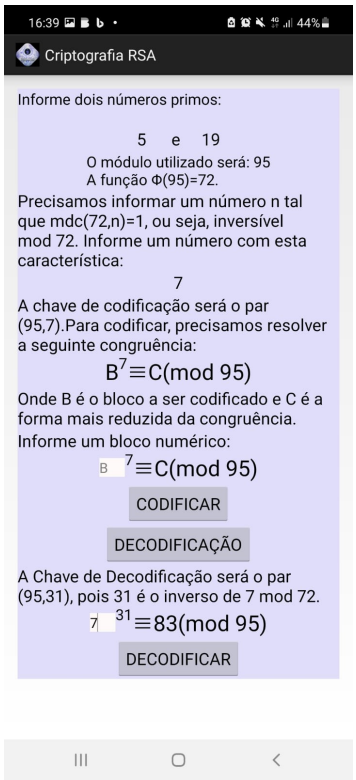
Texto Codificado	Numeração na Tabela ASCII	Código RSA	Caractere Texto Decodificado	Binário correspondente
BEL	7	83	S	01010011
;	59	79	O	01001111
L	76	76	L	01001100

Fonte: Produção do próprio autor (2023).

2º Passo: Cada estudante deve decodificar o código cifrado por eles da palavra "OBMEP" referente à tarefa dada anteriormente. O objetivo desta tarefa é verificar se o valor encontrado em cada bloco após decifrado, corresponde às letras da palavra "OBMEP". Caso não confira, o aluno errou a codificação ou errou a decodificação.

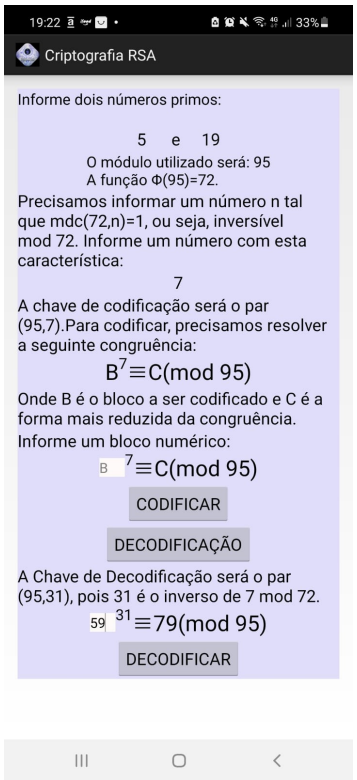
3º passo: Utilizar o Aplicativo Verso RSA para conferir a decodificação dos números obtidos na codificação. Como Exemplo, as Figuras 43 , 44 e 45, demonstram a utilização do aplicativo no processo de decodificação da palavra "SOL".

Figura 43 – Decodificação do bloco $a = 7$



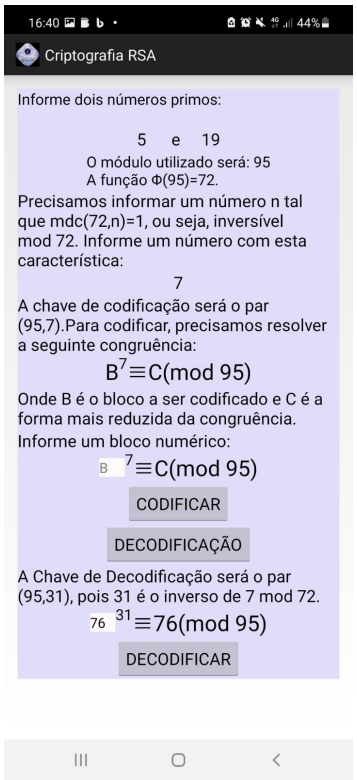
Fonte: Produção do próprio autor (2023)

Figura 44 – Decodificação do bloco $a = 59$



Fonte: Produção do próprio autor (2023)

Figura 45 – Decodificação do bloco $a = 76$



Fonte: Produção do próprio autor (2023)

Avaliação: A avaliação se dará pela participação e pela produção das tarefas solicitadas.

7ª parte

Duração: 2 aulas

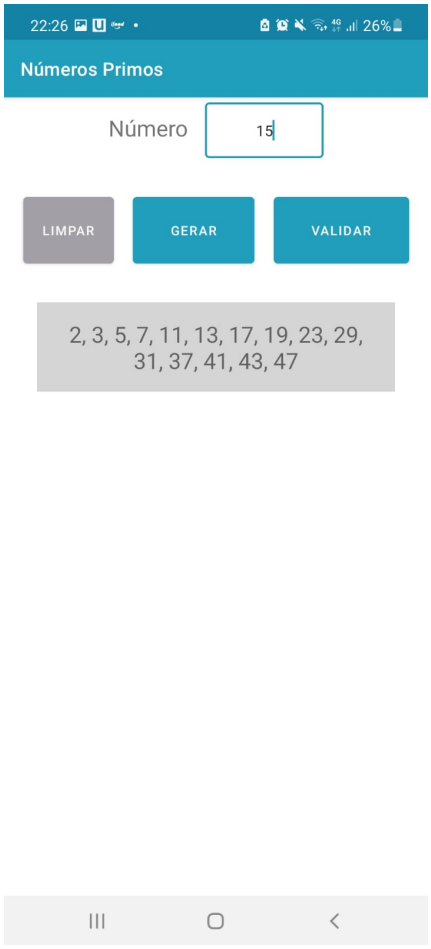
Atividades diversificadas com uso dos aplicativos indicados

Nesta etapa da Sequencia didática, mais uma vez, fizemos uso de aplicativos como ferramenta facilitadora da aprendizagem. Usamos o aplicativo Números Primos e o Aplicativo Verso RSA.

1º Passo As atividades seguintes são inspiradas em atividades propostas em (COUTINHO, 2015).

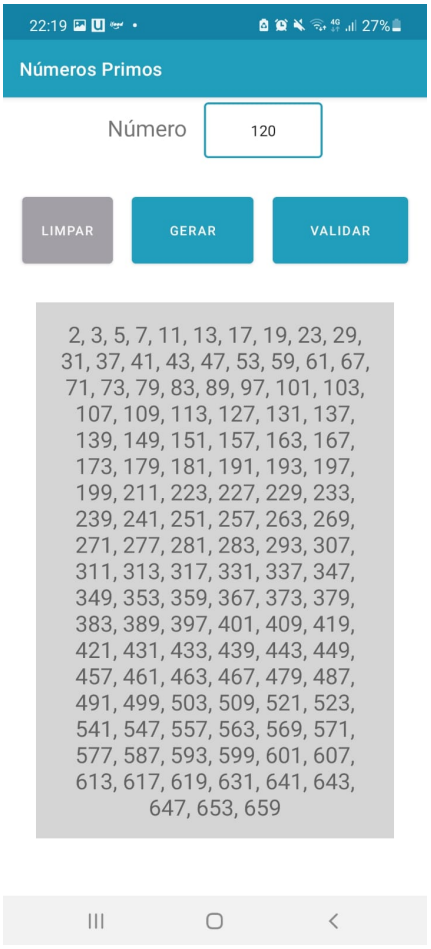
Usando o aplicativo Números Primos, construa uma chave pública usando dois dos 15 primeiros números primos, para utilizar na codificação de mensagens RSA para os colegas. O aplicativo Números Primos gera a quantidade de primos solicitado. As Figuras 46 e 47, mostram a interface do aplicativo Números Primos com as quantidades solicitadas de primos.

Figura 46 – 15 Primeiros números primos



Fonte: Produção do próprio autor (2023).

Figura 47 – 120 Primeiros números primos



Fonte: Produção do próprio autor (2023).

2º Passo: O estudante deve usar a chave pública que construiu na atividade anterior para codificar seu nome com o algoritmo RSA. Deve escrever a chave e a mensagem codificada (nome) em um papel e colocar em um envelope. Os envelopes foram embaralhados e sorteados entre os estudantes para a próxima atividade.

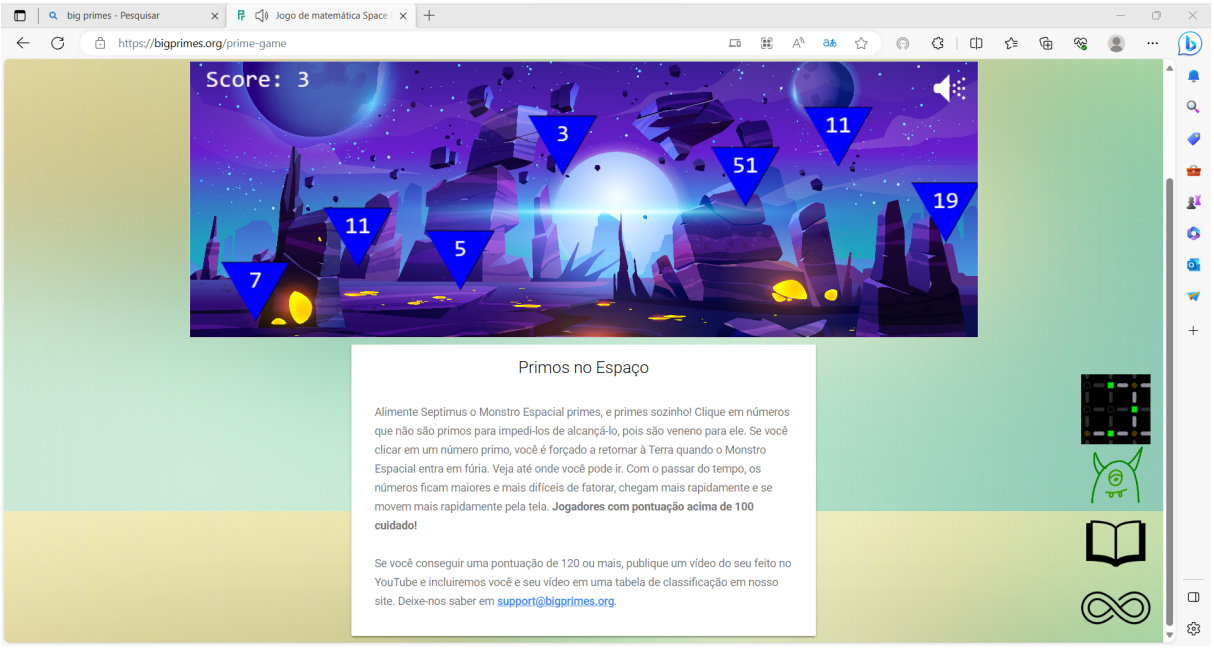
3º Passo: O estudante deve fatorar a chave pública que recebeu. Depois deve encontrar a chave privada e decodificar a mensagem e descobrir de quem era a mensagem.

4º Passo: Para descontração, elabormosr uma competição com o jogo sobre números primos existente no programa Big Primes (disponível em <https://bigprimes.org/prime-game>) utilizando os computadores da escola . O jogo que inicialmente parece um jogo para crianças, se torna muito difícil com o passar das etapas, possuindo até mesmo um ranking com possibilidade de publicação de vídeo com as pontuações superiores a 120. O nome do jogo é "Primos no Espaço" e sua sinopse é dada abaixo:

> Alimente Septimus o Monstro Espacial! Clique em números que não são primos para impedi-los de alcançá-lo, pois são veneno para ele. Se você clicar em um número primo, você é forçado a retornar à Terra quando o Monstro Espacial entra em fúria. Veja até onde você pode ir. Com o passar do tempo, os números ficam maiores e mais difíceis de fatorar, chegam mais rapidamente e se movem mais rapidamente pela tela. Jogadores com pontuação acima de 100 cuidado! Se você conseguir uma pontuação de 120 ou mais, publique um vídeo do seu feito no YouTube e incluiremos você e seu vídeo em uma tabela de classificação em nosso site. Deixe-nos saber em support@bigprimes.org.

A Figura 48 mostra a interface do jogo.

Figura 48 – Jogo Primos no espaço



Fonte: Disponível em: <https://bigprimes.org/prime-game>. Acesso em: 10 de set. de 2023.

Avaliação: A avaliação se deu pela participação nas atividades, no jogo e na produção e decodificação das mensagens RSA.

Finalizamos esta Sequência Didática com a tirinha da Figura 49.

Figura 49 – Tirinha: Encontro Anual de primos

Fonte: Disponível em: <https://dragoesdegaragem.com/cientirinhas/cientirinhas-143/>. Acesso em: 10 de set. de 2023.

5 Conclusão

Após as pesquisas realizadas para a conclusão deste trabalho, pude perceber o quanto a criptografia foi importante no decorrer da história e como teve influência, a ponto de intervir em seus rumos. Foi possível, também observar como ela foi se desenhando e se modelando com o passar do tempo, para se adaptar às novas necessidades e realidades de cada época.

Tendo como objetivo o estudo da Criptografia RSA, foi possível explorar a importância dos números primos para a geração de chaves, bem como a aplicabilidade da aritmética modular no algoritmo desta criptografia. Destacamos também a eficiência e confiabilidade mediante possíveis ataques de força bruta, oferecendo um nível muito elevado de proteção e permitindo o uso seguro de dados importantes do nosso dia a dia como senhas e números de cartão de crédito via internet.

O desenvolvimento da sequência didática, visa ajudar ao professor de matemática a trabalhar de forma suave, os conceitos matemáticos fundamentais para o entendimento do algoritmo de criptografia RSA, sem perder ao mesmo tempo rigor matemático. Desse modo, espero que tanto a dissertação em sua totalidade, quanto a Sequência Didática possam auxiliar outros profissionais que desejem fazer uso dela para trabalhar em suas aulas. O uso da disciplina Eletiva é apenas sugestivo.

Com o surgimento de novas tecnologias, surge também a necessidade de mudança e aperfeiçoamento assim como a própria história da criptografia nos mostra e também é esperado que com a criptografia RSA não será diferente. Os recentes avanços da computação quântica se tornam uma ameaça ao RSA que terá que se aprimorar para resistir.

O estudo de criptografia é algo apaixonante, desde o seu comportamento histórico, até as especificidades de cada método. Desejo continuar a estudar os novos métodos de criptografia de dados, entre eles o de curvas elípticas e desenvolver novos trabalhos e pesquisas sobre eles.

Referências

ACADEMY, K. Theorema do número primo. acesso em 08 de junho de 2023. Disponível em: <https://pt.khanacademy.org/computing/computer-science/cryptography/comp-number-theory/v/prime-number-theorem-the-density-of-primes>. Citado na página 52.

ARAUJO, M. J. V. C. d. Notas de aulas - introdução à álgebra. 2009. Acessado em 05/07/2023. Disponível em: <https://www.ufjf.br/fred_feitosa/files/2009/08/ap.pdf>. Citado 2 vezes nas páginas 47 e 75.

BRASIL, M. d. E. *Base Nacional Comum Curricular*. 3. ed. Brasília: MEC, 2018. Acesso em 04/07/2023. Disponível em: <http://basenacionalcomum.mec.gov.br/>. Citado 2 vezes nas páginas 89 e 95.

CASAGRANDE, J. H. B. Apostila: Eletrônica digital 1, capítulo 3 – circuitos combinacionais. *CEFET/SC*, 2005. Citado na página 79.

COSTA, C.; FIGUEIREDO, L. M. Introdução à criptografia. 2010. Disponível em: <https://canal.cecierj.edu.br/012016/a99b588e1edecbb6543d63cf51e20158.pdf>. Citado 7 vezes nas páginas 16, 19, 21, 22, 24, 26 e 34.

COUTINHO, S. C. Criptografia. *Rio de Janeiro, Programa de Iniciação Científica da OBMEP (PIC-OBMEP)*, 2015. Citado 2 vezes nas páginas 71 e 110.

HEFEZ, A. *Aritmética*. [S.l.]: Sociedade Brasileira de Matemática, 2012. (Coleção Profmat). Citado 7 vezes nas páginas 34, 41, 42, 44, 54, 56 e 75.

MARTZLOFF, J.-C. *A History of Chinese Mathematics*. [S.l.]: Springer Berlin, Heidelberg, 1997. 310 p. Citado na página 73.

OBMEP-IMPA. *Clubes de Matemática da OBMEP*. 2012. Acessado em 21/09/2023. Disponível em: <http://clubes.obmep.org.br/blog/texto_012-contagem-de-divisores-um-segundo-estudo/>. Citado na página 75.

PERRIN, B. Lives, volume iv: Alcibiades and coriolanus. lysander and sulla. Harvard University Press Cambridge, 1916. Citado 2 vezes nas páginas 20 e 34.

ROUSSEAU, C.; SAINT-AUBIN, Y. Matemática e atualidade. *Rio de Janeiro: SBM*, v. 2015, 2015. Citado na página 87.

SAUTOY, M. D. *A Música dos Números Primos: A história de um problema não resolvido na matemática*. [S.l.]: Zahar, 2007. Citado 2 vezes nas páginas 34 e 46.

SEDU-ES. *Itinerário Formativo*. 2021. Acessado em 05/07/2023. Disponível em: <https://novoensinomedio.sedu.es.gov.br/itinerario-formativo>. Citado na página 88.

STALLINGS, W. *Criptografia e segurança de redes. Princípios e práticas, ch. 6*. [S.l.]: Pearson Prentice Hall, 2006. Citado 4 vezes nas páginas 17, 30, 31 e 75.

STEIN M. L.; ULAM, S. M.; WELLS, M. B. A visual display of some properties of the distribution of primes. *American Mathematical Monthly 71*, 1964. Citado na página 53.

TKOTZ, V. Criptografia - segredos embalados para viagem. *[S.l.: s.n.]*, 2005. Citado 6 vezes nas páginas 25, 28, 29, 31, 32 e 33.