PAULO FRANCISCO DE ARAÚJO

APLICAÇÕES DE CRIPTOGRAFIA NO ENSINO MÉDIO

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação do Mestrado Profissional em Matemática em Rede Nacional, para obtenção do título de *Magister Scientiae.*

VIÇOSA
MINAS GERAIS - BRASIL
2017

PAULO FRANCISCO DE ARAÚJO

APLICAÇÕES DE CRIPTOGRAFIA NO ENSINO MÉDIO

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação do Mestrado Profissional em Matemática em Rede Nacional, para obtenção do título de *Magister Scientiae*.

APROVADA: 14 de março de 2017.

Allan de Oliveira Moura

Walter Teófilo Huaraca Vargas

Anderson Tiago da Silva
(Orientador)

A minha amada esposa Cassiana, minhas filhas Maria Paula e Alice, aos meus pais Julio e Terezinha e às minhas irmãs.

"A matemática é o alfabeto com o qual Deus escreveu o universo"

Pitágoras

Agradecimentos

Agradeço primeiramente a Deus princípio e fundamento de todas as coisas. Pela Sua presença constante em minha vida e por todas as bênçãos e graças derramadas em minha vida. A Ti toda honra e toda glória.

A minha amada esposa Cassiana por todo amor, paciência, dedicação e apoio incondicionais e às nossas filhas Maria Paula e Alice por todo carinho e amor.

Aos meus pais Julio e Terezinha por sempre acreditarem em mim e às minhas irmãs pelo carinho.

Ao meu orientador, Anderson Tiago da Silva pela paciência, pelas correções e pela parceria, meu muito obrigado.

Aos professores do PROFMAT/UFV que foram essenciais para conclusão de mais esta etapa da minha vida.

A família Grupo de Oração Nossa Senhora de Fátima por serem presença constante na minha vida e por estarem em constante intercessão a Deus para que eu alcançasse mais esta vitória.

Aos meus amigos de turma do PROFMAT 2015 pelo companheirismo.

A todos aqueles que direta e indiretamente contribuíram para a realização de mais este sonho.

Sumário

Lista de Figuras

Lista de Tabelas

Resumo

ARAÚJO, Paulo Francisco, M. Sc., Universidade Federal de Viçosa, março de 2017. **O ensino de matrizes utilizando os conceitos de criptografia.** Orientador: Anderson Tiago da Silva.

Este trabalho aborda conceitos da Teoria dos Números que é essencial para o desenvolvimeto da Criptografia RSA e da Criptografia ElGamal que, juntamente com a Teoria de Matrizes, se torna essencial para o desenvolvimento da Cifra de Hill. É apresentado também um software matemático que pode ser de grande ajuda para o desenvolvimento da Teoria de Matrizes no ensino Médio.

Abstract

ARAÚJO, Paulo Francisco, M. Sc., Universidade Federal de Viçosa, March, 2017. **The theaching of matrices using the concepts of cryptography.** Advisor: Anderson Tiago da Silva.

This work approaches concepts of Number Theory that is essential for the development of RSA Cryptography and ElGamal Cryptography which, together with Matrix Theory, becomes essential for the development of the Hill Cipher. It is also presented of mathematical software that can be of great help for the development of Matrix Theory in High School.

Introdução

Ao analisarmos os livros de Matemática do ensino médio, percebemos que estes, em sua maioria, abordam o conteúdo a ser estudado de tal modo que privilegiam a conceituação e não a aplicação, fazendo com que o ensino esteja voltado para a utilização de fórmulas que, por sua vez, estão longe da realidade dos alunos, fazendo com que os educandos tenham muitas dificuldades no aprendizado da matéria e também que o ensino da Matemática fracasse. A falta de aplicação, conforme nos diz LIMA [17], é considerada o grande problema dos livros didáticos brasileiros. Tal forma de se abordar os diferentes conceitos matemáticos leva, na grande maioria das vezes, a uma dificuldade na aprendizagem, além de um desinteresse pela referida matéria pois, os estudantes não conseguem visualizar a aplicabilidade do conteúdo estudado no seu cotidiano. Partindo desse contexto, conforme nos diz SANCHES [23], podem manifestar-se os seguintes aspectos:

> *Dificuldades em relação ao desenvolvimento cognitivo e à construção da experiência matemática; do tipo da conquista de noções básicas e princípios numéricos, da conquista da numeração, quanto à prática das operações básicas, quanto à mecânica ou quanto à compreensão do significado das operações. Dificuldades na resolução de problemas, o que implica a compreensão do problema, compreensão e habilidade para analisar o problema e raciocinar matematicamente.*
> *Dificuldades quanto às crenças, às atitudes, às expectativas e aos fatores emocionais acerca da matemática. Questões de grande interesse e que com o tempo podem dar lugar ao fenômeno da ansiedade para com a matemática e que sintetiza o acúmulo de problemas que os alunos maiores experimentam diante do contato com a matemática.*
> *Dificuldades relativas à própria complexidade da matemática, como seu alto nível de abstração e generalização, a complexidade dos conceitos e algoritmos. A hierarquização dos conceitos matemáticos, o que implica ir assentando todos os passos antes de continuar, o que nem sempre é possível para muitos alunos; a natureza lógica e exata de*

seus processos, algo que fascinava os pitagóricos, dada sua harmonia e sua "necessidade", mas que se torna muito difícil pra certos alunos; a linguagem e a terminologia utilizadas, que são precisas, que exigem uma captação (nem sempre alcançada por certos alunos), não só do significado, como da ordem e da estrutura em que se desenvolve.
Podem ocorrer dificuldades mais intrínsecas, como bases neurológicas, alteradas. Atrasos cognitivos generalizados ou específicos. Problemas linguísticos que se manifestam na matemática; dificuldades atencionais e motivacionais; dificuldades na memória, etc.
Dificuldades originadas no ensino inadequado ou insuficiente, seja porque a organização do mesmo não está bem sequenciado, ou não se proporcionam elementos de motivação suficientes; seja porque os conteúdos não se ajustam às necessidades e ao nível de desenvolvimento do aluno, ou não estão adequados ao nível de abstração, ou não se treinam as habilidades prévias; seja porque a metodologia é muito pouco motivadora e muito pouco eficaz. (p. 174)

Ao ensinar uma determinada matéria, o professor deve instigar seus alunos a pensar por si mesmos e estimulá-los de tal forma que sejam capazes de buscar seus próprios aprendizados. Para que isso ocorra, o educador deve ensinar seus alunos a perguntar. Segundo BARBOSA [4], esse é o caminho da educação:

> *O que o professor deveria ensinar - porque ele próprio deveria sabê-lo - seria, antes de tudo, ensinar a perguntar. Porque o início do conhecimento, repito, é perguntar. E somente a partir de perguntar é que se deve sair em busca de resposta e não o contrário.*

E além disso, de acordo com a proposta curricular do Currículo Básico Comum, CBC [21]:

> *Um dos principais objetivos do ensino de Matemática, em qualquer nível, é o de desenvolver habilidades para a solução de problemas. Esses problemas podem advir de situações concretas observáveis ("contextualizadas") ou não. No primeiro caso, é necessária uma boa capacidade de usar a linguagem matemática para interpretar questões formuladas verbalmente. Por outro lado, problemas interessantes, que despertam a curiosidade dos estudantes, podem surgir dentro do próprio contexto matemático, em que novas situações podem ser exploradas e o conhecimento aprofundado, num exercício contínuo da imaginação.*

Hoje, muito tem se falado em um ensino contextualizado. E a contextualização dos conteúdos, deve fazer com que o aluno saia do papel de um mero expectador e passe a ser capaz de aplicar o conhecimento adquirido nas diversas situações do seu cotidiano.

Conforme o PCN+ [6],

> *Aprender Matemática de uma forma contextualizada, integrada e relacionada a outros conhecimentos traz em si o desenvolvimento de competências e habilidades que são essencialmente formadoras, à medida que instrumentalizam e estruturam o pensamento do aluno, capacitando-o para compreender e interpretar situações, para se apropriar de linguagens específicas, argumentar, analisar e avaliar, tirar conclusões próprias, tomar decisões, generalizar e para muitas outras ações necessárias à sua formação.(p. 111)*

Ainda nesse sentido, de acordo com a proposta curricular do Currículo Básico Comum, CBC [21]:

> *O ensino da Matemática deve evidenciar o caráter dinâmico, em constante evolução, do conhecimento matemático. Devido ao fato de que mesmo conhecimentos matemáticos mais antigos possuem ainda hoje aplicações, existe uma tendência de considerá-los como algo pronto e estático. O que ocorre é exatamente o contrário: a cada dia, surgem novas questões matemáticas e até novas áreas de pesquisas, (por exemplo, a criptografia), e não cessam as demandas de outras áreas (por exemplo, Biologia, Economia) por modelos matemáticos mais efetivos e sofisticados.*
>
> *[· · ·]Isto significa que o projeto pedagógico para a Matemática deve ser elaborado de forma articulada com as outras disciplinas e que, sempre que possível, seja ressaltada a relação entre os conceitos abstratos com as suas aplicações e interpretações em situações concretas, tanto na aula de Matemática quanto na disciplina que está sendo utilizada. (p. 14-15)*

Nesse sentido, uma das formas de se contextualizar o ensino da matemática no Ensino Médio é através da criptografia. Este assunto pode ser encontrado em [8], e pode ser associado ao ensino de matemática. Trabalhando de forma contextualizada, estaremos propiciando aos alunos uma visão diferenciada da matemática e proporcionando a eles uma aprendizagem satisfatória desta disciplina.

Segundo TAMAROZZI [28], o tema criptografia possibilita o desenvolvimento de atividades didáticas envolvendo diversos conteúdos dos ensinos fundamental e médio e se constituem em material útil para exercícios, atividades e jogos de fixação, onde o professor pode utilizá-los para fixação da matéria. Sendo assim, o presente trabalho visa aplicar de forma contextualizada e integrada a outros conhecimentos alguns métodos criptográficos, de tal forma que ofereça ao professor uma ferramenta de trabalho que o possibilite desenvolver alguns conceitos abordados no ensino médio, de forma mais eficaz, oferecendo assim aos alunos, a oportunidade de uma aprendizagem significativa destes temas.

Capítulo 1

História da Criptografia

A história da criptografia é precedida pela esteganografia, nome derivado de duas palavras gregas *steganos,* que significa coberto, e *graphein,* que significa escrever, ou seja, é a arte de se escrever ocultamente. E inicia-se da necessidade do ser humano de transmitir uma mensagem sem que outros, mesmo que consigam interceptá-la, possam tomar conhecimento do seu conteúdo. Data-se do quinto século antes de Cristo os primeiros relatos que se têm do uso destas mensagens secretas. Ao observarmos a história, verificamos que reis e rainhas utilizaram dessa técnica para envio de mensagens secretas de tal forma que os possibilitava comunicar com seus aliados sem o risco de que o conteúdo de suas mensagens caíssem nas mãos inimigas. Dessa forma, guerras foram vencidas graças ao uso dessa técnica que hoje conhecemos como criptografia.

Uma das primeiras técnicas para o envio de mensagens secretas, conforme nos diz SINGH [26] foi a utilizada por Demerato, que decidiu enviar uma mensagem para advertir os espartanos dos planos de invasão do rei Xerxes. A mensagem foi enviada "raspando a cera de um par de tabuletas de madeira, e escrevendo embaixo o que Xerxes pretendia fazer, depois a mensagem foi coberta novamente com cera. Deste modo, as tabuletas pareciam estar em branco e não causariam problemas com os guardas ao longo da estrada."

Outra forma que também foi utilizada para envio de mensagens, foi a utilizada por Histaeu, que raspou a cabeça do mensageiro e escreveu a mensagem no seu couro cabeludo e, assim que o cabelo cresceu o mensageiro foi enviado ao destinatário. Assim que chegou ao seu destino o mensageiro informou que a mensagem estava em seu couro cabeludo e, sendo raspada sua cabeça novamente, o destinatário teve conhecimento da mensagem que lhe fora enviada.

Existem várias outras formas de se transmitir uma mensagem secreta. A primeira que envolve um aparelho criptográfico militar é o citale espartano figura

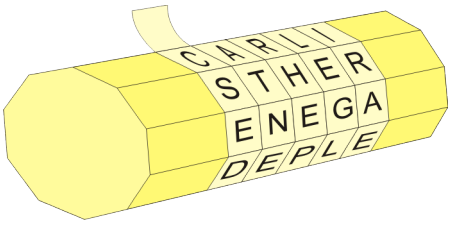


Figura 1.1: Citale Espartano

1.1. Este, consiste em um bastão de madeira no qual é envolvido uma tira de couro ou pergaminho onde é escrita a mensagem no comprimento do citale e, após ser desenrolado o pergaminho ou a tira de couro, temos uma sequência de letras sem sentido. Para que a mensagem possa ser compreendida é necessário que o receptor ou o destinatário tenha um outro citale com o mesmo diâmetro do qual foi utilizado para escrever a mensagem enviada.

Outro exemplo de ocultação de mensagem é a chamada cifra de deslocamento de César ou simplesmente a cifra de César que consiste, conforme descreve SINGH [26], num alfabeto cifrado onde o alfabeto original foi deslocado um determinado número de casas. Esse método de cifragem é conhecido como cifra de substituição monoalfabética pois, cada letra da mensagem é substituída sempre pela letra correspondente do alfabeto cifrado, conforme tabela abaixo:

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

Tabela 1.1: Cifra de César

A partir daí, os árabes desenvolveram uma técnica para decifrar as mensagens que utilizavam a cifra de substituição monoalfabética que ficou conhecida como criptoanálise. A partir da análise de frequência na utilização das letras na língua de origem, no caso do emissor, estuda-se a frequência das letras na mensagem codificada. Então, substituindo tais letras de acordo com a frequência em que elas aparecem, possivelmente, conseguiremos decifrar a mensagem codificada. Essa técnica ficou conhecida como análise de frequência e é atribuída ao filósofo árabe

Abu Yusef Ya'qub ibn Is-haq ibn as-Sabbah ibn omran ibn Ismail al-Kindi, mais conhecido como al-Kindi.

A partir da observação feita por al-Kindi a cifra de substituição monoalfabética caiu em desuso, sendo necessário o desenvolvimento de outras formas de cifragem de mensagens. Por volta de 1460, Leon Battista Alberti, " propôs o uso de dois ou mais alfabetos cifrados, usados alternadamente, de modo a confundir os criptoanalistas em potencial"retirado de SINGH [26].

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

Tabela 1.2: Exemplo de dois alfabetos cifrados com os quais podemos codificar uma mensagem alternando entre eles.

Para cifrar, por exemplo a palavra ABRAÇO, utilizando os dois alfabetos cifrados, substituímos a primeira letra da palavra original de acordo com o alfabeto cifrado 1 e segunda letra da palavra original pela letra correspondente no alfabeto cifrado 2 e assim, sucessivamente. Assim, teríamos como resposta a palavra cifrada FOOGBJ. Observe que a letra **A** na palavra original, aparece cifrada por duas letras diferentes, **F** e **G** e nisto consiste a vantagem dessa forma de cifragem.

Como Alberti e outros estudiosos de seu trabalho não conseguiram aperfeiçoar ao máximo esta técnica de cifragem, coube então a Blaise de Vigenère, diplomata francês, no ano de 1562, "formar uma nova cifra, coerente e poderosa."Tal cifra ficou conhecida como *chiffre indéchiffrable*, cifra indecifrável.

Para decifrar uma palavra ou frase que nos foi enviada, precisamos saber qual das linhas do quadrado de Vigenère foi utilizada para cifrar a referida palavra ou frase. Para isso, o remetente deve fornecer uma palavra chave que é escrita, repetidas vezes, acima da palavra ou frase, de modo que cada letra da palavra chave corresponda a uma letra da palavra ou frase cifrada. A referida cifra ficou conhecida como a cifra indecifrável, devido à impossibilidade de ser decifrada através da análise de frequência e por possuir um grande número de chaves.

Como exemplo, vamos cifrar a palavra BRASIL utilizando a palavra chave LUA. Seguindo o algoritmo descrito acima, temos:

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

Figura 1.2: Quadrado de Vigenère

Palavra chave	l	u	a	l	u	a
Palavra a ser cifrada	B	R	A	S	I	L
Palavra cifrada	M	L	A	D	C	L

Tabela 1.3: Exemplo de cifragem utilizando o quadrado de Vigenère

Para obter a letra **M**, primeira letra da palavra cifrada acima, encontramos a letra que é a interseção da 11ª linha, que começa com a letra **l**, e que corresponde com a primeira letra da palavra chave, com a 2ª coluna, que inicia com a letra **B**, que corresponde a primeira letra da palavra a ser cifrada. Obtemos a segunda letra, **L**, da palavra cifrada acima, encontrando a letra que é a interseção da 20ª linha, que começa com a letra **u**, e que corresponde à segunda letra da palavra chave, com a 18ª coluna, que inicia com a letra **R**, que corresponde a segunda letra da palavra a ser cifrada. Procedendo de forma análoga para as outras letras encontramos a palavra cifrada, **MLADCL**, acima.

A partir daí, surgiu um novo questionamento, como conseguir decifrar a cifra de Vigenère? Então, aproximadamente 300 anos depois, um oficial prussiano da infantaria, Friedrich Kasinski conseguiu detectar um "ponto fraco"na cifra de

Vigenère. Ele verificou que a palavra chave se repete. E verificou ainda que, se for possível determinar o comprimento da palavra chave, será possível utilizar a análise de frequência em cada bloco da palavra ou frase codificada conseguindo, então, decifrar a referida mensagem. E, graças a esta descoberta, a cifra de Vigenère não era mais considerada segura.

Observando algumas das técnicas que foram utilizadas acima, vemos que foi criado um método para ocultar a mensagem, ou seja, foi-se usado um *algoritmo*. Observe que só será possível decifrar tais mensagens se tivermos em mãos, o que chamamos de *chave*. Na cifra de César, por exemplo, o algoritmo utilizado, foi a substituição do alfabeto original pelo alfabeto cifrado e a chave é o alfabeto cifrado utilizado para codificar a mensagem. Assim sendo, só será possível decifrar a mensagem com o referido alfabeto cifrado em mãos, ou seja, a segurança da mensagem depende em manter o segredo da chave.

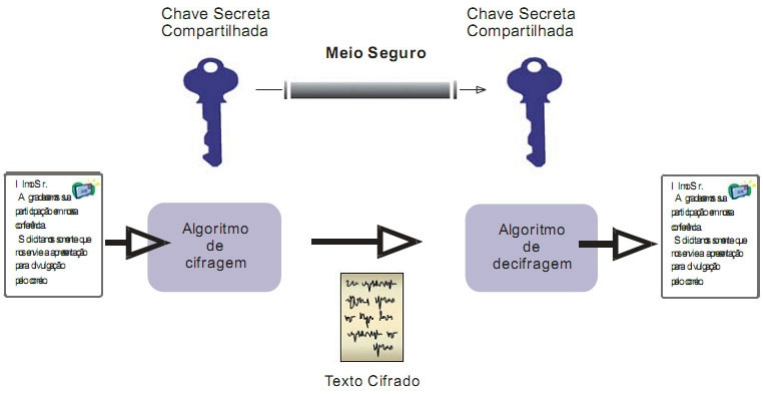


Figura 1.3: Para decifrar a mensagem recebida, o destinatário deve conhecer a chave e o algoritmo de codificação.

Com o avanço da tecnologia, deu-se um grande salto em relação às comunicações através do uso de sistemas informatizados. Como não poderia deixar de ser, as atividades realizadas via comunicação eletrônica dependem do sigilo em suas operações, principalmente as transações financeiras e o envio de mensagens via internet. Dessa forma, a criptografia, diferentemente de outros métodos utilizados na antiguidade, não oculta a mensagem mas sim o seu significado. Daí o nome criptografia, do qual, cripto que vem da palavra grega kriptos e significa "oculto,"e grafia, da palavra grega graphia e significa "escrita,"ou seja, criptografia é arte da escrita oculta.

Durante a Segunda Guerra Mundial houve um embate entre decifradores britânicos e fazedores de códigos alemães onde, estes últimos se sagraram vencedores. Os britânicos construíram uma máquina decifradora, chamada de Colossus, para combater a cifra alemã Lorenz. E, a partir da Colossus foi desenvolvida a

criptografia na segunda metade do século XX.

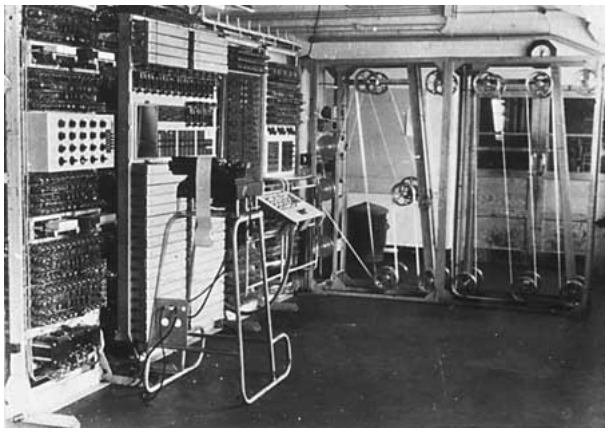


Figura 1.4: Máquina Colossus utilizada para quebrar a cifra alemã Lorenz

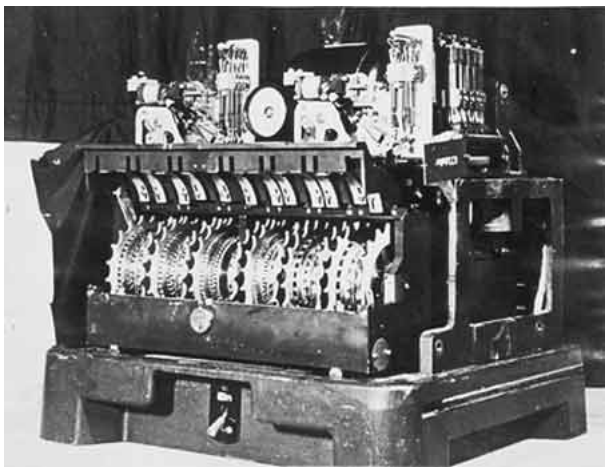


Figura 1.5: Máquina alemã Lorenz

O desenvolvimento da criptografia foi de extrema importância pois conforme encontrado em SAUTOY [25]:

> *Antes de 1977, quem quisesse enviar uma mensagem secreta depararia com um problema essencial, o emissor e o receptor da mensagem teriam de se encontrar para decidir qual cifra - o método de codificação - usariam para, a partir daí, poderem se comunicar. Os generais espartanos, por exemplo, precisavam concordar sobre as dimensões da cítala.*
>
> *Já, na Segunda Guerra Mundial, os alemães utilizaram uma máquina para criptografar e descriptografar mensagens, chamada Enigma. Nessa época Enigma foi considerada uma máquina extremamente eficiente ao ponto dos franceses e britânicos pensarem que a sua cifra fosse inquebrável. Mesmo com toda a capacidade de cifragem da máquina*

> *Enigma e, por isso foi produzida em série, Berlim tinha que enviar agentes para fornecer aos capitães dos barcos U e aos comandantes dos tanques os livros que descreviam as configurações da máquina para codificar as mensagens de cada dia. Naturalmente, se um inimigo pusesse as mãos no livro de códigos, o jogo terminava.*

Assim, com o avanço da internet se tornou ainda mais imprescindível a segurança para as conversas e transações eletrônicas e, a criptografia veio de encontro a estas necessidades e seu desenvolvimento trouxe segurança e confidencialidade para os dados que estão disponíveis na rede. A partir dessa necessidade de segurança na transmissão de dados em 1978 foi criado por, R. L. Rivest, A. Shamir e L. Adleman o mais conhecido dos métodos de criptografia de chave pública, o RSA que pode ser encontrado em [8].

Neste trabalho iremos descrever três métodos criptográficos, a cifra de Hill, que foi desenvolvida pelo americano Lester S. Hill em 1929 que pode auxiliar na aprendizagem e fixação dos conceitos de matrizes, a criptografia RSA e a criptografia ElGamal que, juntamente com a cifra de Hill, nos permitirão explorar noções de aritmética modular, além de seus métodos de cifragem e decodificação de mensagens.

Capítulo 2

Pré-Requisitos

O texto a seguir, bem como suas demonstrações, foi desenvolvido utilizando as referências [2], [8], [11], [12], [13], [19], [20], [22] e [24].

2.1 Teoria dos Números

2.1.1 Algoritmo de Euclides

Antes de enunciarmos o algoritmo da divisão vamos descrever a segunda forma do princípio de indução que usaremos na demonstração do algoritmo da divisão.

Proposição 2.1.1 *(Indução - segunda forma)[[12] pág 17] Suponhamos que seja dada uma afirmação $a(n)$ dependendo de $n \in \mathbb{N}$ tal que:*

(i) $a(0)$ *é verdadeira.*

(ii) Para cada inteiro $m > 0, a(m)$ é verdadeira sempre que $a(k)$ for verdadeira para $0 \leq k < m$.

Então, $a(n)$ é verdadeira para todo $n \in \mathbb{N}$.

Demonstração:

Vide [12].

Teorema 2.1.1 *(Algoritmo da Divisão)[[12], pág 17] Sejam $n, d \in \mathbb{N}$ e $d > 0$. Então existem únicos $q, r \in \mathbb{N}$, tais que*

$$n = qd + r$$

e $0 \leq r < d$.

Demonstração:

Provaremos a existência usando indução sobre n.

Se $n < d$ existem $q = 0, r = n$, assim podemos assumir $n \geq d > 0$.

Então temos $0 \leq n - d < n$ e, pela hipótese (ii) de indução (segunda forma) segue que existem $q_1, r \in \mathbb{N}$ tais que $n - d = q_1 d + r$ onde $0 \leq r < d$ e daí segue que $n = (q_1 + 1)d + r$ onde $0 \leq r < d$. Assim existem $q = q_1 + 1$ e $r \in \mathbb{N}$ como queríamos demonstrar.

Provaremos agora a unicidade. Suponhamos que existam $q_1, r_1, q_2, r_2 \in \mathbb{N}$ tais que $n = q_1 d + r_1$, $0 \leq r_1 < d$ e $n = q_2 d + r_2$, $0 \leq r_2 < d$. Daí, segue que, $q_1 d + r_1 = q_2 d + r_2$ onde $0 \leq r_1 < d$ e $0 \leq r_2 < d$. Como $d > 0$ é suficiente provarmos que $r_1 = r_2$ pois nesse caso teríamos $q_1 d = q_2 d$, ou seja, $q_1 = q_2$. Suponhamos, por absurdo, que $r_1 \neq r_2$, por exemplo, $r_1 > r_2$. Nesse caso teríamos:

$$0 < r_1 - r_2 = (q_2 - q_1)d.$$

Mas também $r_1 - r_2 < d$ pois $r_1 < d$ e $r_2 < d$, e daí segue que:

$$0 < r_1 - r_2 = (q_2 - q_1)d < d$$

o que é um absurdo, e isto termina a demonstração do teorema.

Teorema 2.1.2 *Sejam a e b dois inteiros positivos. Então existe um inteiro positivo que é o máximo divisor comum de a e b.*

Demonstração:

Sejam a e b dois inteiros positivos. Sem perda de generalidade, suponhamos $a \leq b$. Se $a = 1$, $a = b$ ou $a \mid b$, então $(a, b) = a$.

Dessa forma, vamos supor $1 < a < b$, e $a \nmid b$. Pelo algoritmo da divisão existem r_1 e q_1 inteiros positivos tais que $b = aq_1 + r_1$, com $r_1 < a$.

Agora, temos dois casos a analisar:

i) Se $r_1 \mid a$, então existe k inteiro tal que $a = kr_1$. Como $b = aq_1 + r_1$, e $a = kr_1$, temos $b = kr_1 q_1 + r_1 = r_1(kq_1 + 1)$, ou seja, $r_1 \mid b$ e, portanto, $(a, b) = r_1$.

ii) Se $r_1 \nmid a$, efetuando a divisão de a por r_1, obtemos $a = r_1 q_2 + r_2$, com q_2, r_2 inteiros positivos e $r_2 < r_1$. O que nos dá, novamente, duas possibilidades:

1) Se $r_2 \mid r_1$, por uma justificativa análoga à do item i), temos que $(a, b) = r_2$.

2) Se $r_2 \nmid r_1$, efetuando a divisão de r_1 por r_2, obteremos $r_1 = r_2 q_3 + r_3$, com $r_3 < r_2$.

Observe que o processo acima é finito pois, caso contrário, teríamos encontrado uma sequência decrescente de inteiros positivos $a > r_1 > r_2 > r_3 > \ldots$ que não teria um menor elemento, contrariando assim, o Princípio da Boa Ordem.

Logo, sendo r_n este menor elemento, com $r_n \mid r_n - 1$, temos que $(a, b) = r_n$.

Portanto, quaisquer dois inteiros positivos admitem máximo divisor comum.

Vamos representar o algoritmo descrito acima em forma de diagrama.

	q_1	q_2	q_3	$\cdots$	q_{n-1}	q_n	q_{n+1}
b	a	r_1	r_2	$\cdots$	r_{n-2}	r_{n-1}	$r_n = (a, b)$
r_1	r_2	r_3	r_4	$\cdots$	r_n	0	

Exemplo 2.1.1 *Encontre o máximo divisor comum de* 1200 *e* 38.

	31	1	1	2	1	2
1200	38	22	16	6	4	2=(1200,38)
22	16	6	4	2	0	

Logo, $(1200, 38) = 2$.

Definição 2.1.1 *Sejam a e b números inteiros não simultaneamente nulos. Dizemos que o inteiro d é o máximo divisor comum de a e b, se satisfaz as seguintes condições:*

i) $d \mid a$ *e* $d \mid b$;

ii) Se existe um inteiro c tal que $c \mid a$ e $c \mid b$ então $c \mid d$.

Definição 2.1.2 *Seja p um inteiro, com $p > 1$. Dizemos que p é um número primo se ele for divisível apenas por* 1 *e por ele mesmo.*

Observe que, se p é um número primo e $p \nmid n$ então $(p, n) = 1$. Dessa forma, para verificarmos se um número inteiro qualquer é primo, basta verificar se os únicos divisores deste número são 1 e ele mesmo.

Uma outra forma de encontrarmos números primos é através do Crivo de Eratóstenes que descreveremos abaixo.

2.1.2 Crivo de Eratóstenes

O crivo de Eratóstenes é um dos mais antigos métodos para se determinar todos os números primos menores ou iguais a um número n. Daremos um passo a passo de como determinar tais números primos.

Passo 1- Escrevemos os números de 2 até n.

Passo 2- A partir do primeiro número primo da lista, excluímos todos os múltiplos deste número.

Passo 3- O número seguinte que não foi riscado também é primo. Assim, basta repetirmos o passo 2.

Passo 4- O crivo pára quando, na sequência do passo 3, o quadrado do número seguinte que não foi riscado for maior do que n.

Exemplo 2.1.2 *Determinar todos os números primos até* 100.

Solução: Consideremos a tabela abaixo com todos os números de 2 até 100.

	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

Agora, riscamos todos os múltiplos de 2.

	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

O próximo número não riscado é o número 3. Vamos riscar agora, todos os seus múltiplos.

	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

Seguindo o mesmo raciocínio, vamos riscar todos os múltiplos de 5.

	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

Múltiplos de 7.

	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~~

Observe que já temos todos os números primos menores do que 100 pois, o próximo número que não foi riscado é o número 11 e, como $11^2 = 121 > 100$, o crivo pára.

Logo, os números primos menores do que 100 são:

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89$ e 97.

2.2 Grupos

Definição 2.2.1 ([11], pág 121) *Um conjunto G com uma operação $(G, .)$*

$$G \times G \to G$$
$$(a, b) \mapsto a.b$$

é um grupo se as condições seguintes são satisfeitas:

(i) A operação é associativa, isto é,

$$a.(b.c) = (a.b).c, \forall a, b, c \in G.$$

(ii) Existe um elemento neutro, isto é,

$$\exists e \in G \text{ tal que } e.a = a.e = a, \forall a \in G.$$

(iii) Todo elemento possui um elemento inverso, isto é,

$$\forall a \in G, \exists b \in G \text{ tal que } a.b = b.a = e.$$

O grupo é abeliano ou comutativo se:

(iv) A operação é comutativa, isto é,

$$a.b = b.a = e, \forall a, b \in G.$$

2.3 Subgrupos

Definição 2.3.1 ([11], pág 128) *Seja $(G, .)$ um grupo. Um subconjunto não-vazio H de G é um subgrupo de G (denotado por $H < G$) quando, com a operação de G, o conjunto H é um grupo, isto é, quando as condições seguintes são satisfeitas:*

0) $h_1.h_2 \in H, \forall h_1, h_2 \in H.$

i) $h_1.(h_2.h_3) = (h_1.h_2).h_3, \forall h_1, h_2, h_3 \in H.$

ii) $\exists e_h \in H$ *tal que* $e_h.h = h.e_h = h, \forall h \in H.$

iii) Para cada $h \in H$, *existe* $k \in H$ *tal que* $h.k = k.h = e_h.$

Proposição 2.3.1 ([11], pag 128) *Seja H um subconjunto não vazio do grupo G. Então H é um subgrupo de G se, e somente se, as duas condições seguintes são satisfeitas:*

1) $h_1.h_2 \in H, \forall h_1, h_2 \in H.$

2) $h^{-1} \in H, \forall h \in H.$

Demonstração: Veja [11].

Definição 2.3.2 ([11], pag 131) *A ordem de um grupo G é o número de elementos em G, e será denotada por $\mid G \mid$. Se α é um elemento desse grupo, a ordem de α é a ordem do subgrupo gerado por α, e será denotada por $\mathcal{O}(\alpha)$.*

2.4 Congruências

2.4.1 Introdução

Na Teoria dos números, uma área de extrema importância é a parte em que lidamos com congruência. Esta área foi desenvolvida, no início do século XIX, por Carl Friedrich Gauss. A simbologia que adotamos até hoje é devida a Gauss que a apresentou através do seu livro *Disquisitionis Arithmeticae*, publicado em 1801.

Definição 2.4.1 *Sejam a e b inteiros e m um inteiro não nulo. Dizemos que a é congruente a b módulo m, e escrevemos $a \equiv b \pmod{m}$, se os restos da divisão de a e b por m forem iguais.*

Proposição 2.4.1 *Se a e b são inteiros e m um inteiro não nulo, tem-se que $a \equiv b \pmod{m}$ se, e somente se, $m \mid (a-b)$.*

Demonstração:

Suponha que $a \equiv b \pmod{m}$. Então, existem inteiros q_1, q_2 e r tais que $a = mq_1 + r$ e $b = mq_2 + r$. Logo,

$$a - b = (mq_1 + r) - (mq_2 + r) = m(q_1 - q_2)$$

e, portanto, $m \mid (a-b)$.

Reciprocamente, suponha que $m \mid (a-b)$. Fazendo-se a divisão de a e b por m, pelo algoritmo da divisão, existem inteiros q_1, r_1, q_2 e r_2 tais que $a = mq_1 + r_1$ e $b = mq_2 + r_2$ com $0 \leq r_1 < m$ e $0 \leq r_2 < m$. Assim, $a - b = m(q_1 - q_2) + (r_1 - r_2)$. Como $m \mid m(q_1 - q_2)$, devemos ter $m \mid (r_1 - r_2)$. Logo, $r_1 = r_2$ pois, $\mid r_1 - r_2 \mid < m$ e, portanto, $a \equiv b \pmod{m}$.

Exemplo 2.4.1

$$11 \equiv 2 \pmod{3}$$

pois,

$$11 - 2 = 9$$

e

$$3 \mid 9.$$

Agora, descreveremos algumas propriedades das congruências.

Proposição 2.4.2 *Sejam a, b e c números inteiros e seja m um inteiro positivo. Temos:*

i) Propriedade reflexiva: $a \equiv a \pmod{m}$.

ii) Propriedade simétrica: Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.

iii) Propriedade transitiva: Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

Demonstração:

i) Observe que $m \mid 0$. Como $0 = a - a$, segue que $m \mid (a - a)$. Logo, $a \equiv a \pmod{m}$.

ii) Suponha que $a \equiv b \pmod{m}$. Então, existe um inteiro k, tal que $a - b = km$. Daí, temos que $b - a = -(km) = (-k)m$. Portanto, $b \equiv a \pmod{m}$.

iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $m \mid (a-b)$ e $m \mid (b-c)$. Logo, $m \mid [(a-b)+(b-c)]$ e, daí que, $m \mid (a-c)$. Portanto, $a \equiv c \pmod{m}$.

Enunciaremos agora, alguns teoremas que mostram que a adição, subtração e multiplicação de ambos os lados de uma congruência, preservam a congruência.

Teorema 2.4.1 *Sejam a, b, c e m inteiros, com $m > 0$, tais que $a \equiv b \pmod{m}$. Então:*

i) $a + c \equiv b + c \pmod{m}$.

ii) $a - c \equiv b - c \pmod{m}$.

iii) $ac \equiv bc \pmod{m}$.

Demonstração: Se $a \equiv b \pmod{m}$, então $m \mid (a-b)$.

i) Temos,

$$a - b = (a-b) + (c-c) = (a+c) - (b+c).$$

Portanto, $m \mid [(a+c)-(b+c)]$ e, consequentemente, $a+c \equiv b+c \pmod{m}$.

ii) Note que,

$$a - b = (a-b) + (c-c) = (a-c) - (b-c).$$

Logo, $m \mid [(a-c)-(b-c)]$ e, portanto, $a - c \equiv b - c \pmod{m}$.

iii) Se $m \mid (a-b)$, então, $m \mid (a-b)c$. Daí, temos que $m \mid (ac-bc)$. Logo, $ac \equiv bc \pmod{m}$.

Exemplo: Como $19 \equiv 3 \pmod{8}$, temos, pelo teorema anterior, que:

$$23 = 19 + 4 \equiv 3 + 4 = 7 \pmod{8}$$

$$17 = 19 - 2 \equiv 3 - 2 = 1 \pmod{8}$$

$$57 = 19 \times 3 \equiv 3 \times 3 = 9 \pmod{8}$$

Teorema 2.4.2 *Sejam a, b, c, d e m inteiros, com $m > 0$, tais que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$. Então:*

i) $a + c \equiv b + d \pmod{m}$.

ii) $a - c \equiv b - d \pmod{m}$.

iii) $ac \equiv bd \pmod{m}$.

Demonstração: Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $m \mid (a-b)$ e $m \mid (c-d)$.

i) Temos

$$(a+c)-(b+d) = a+c-b-d = (a-b)+(c-d)$$

e, como $m \mid (a-b)+(c-d)$ segue que, $m \mid (a+c)-(b+d)$. Portanto, $a+c \equiv b+d \pmod{m}$.

ii) Observe que

$$(a-c)-(b-d) = a-c-b+d = (a-b)-(c-d)$$

e, como $m \mid (a-b)-(c-d)$ segue que, $m \mid (a-c)-(b-d)$. Portanto, $a-c \equiv b-d \pmod{m}$.

iii) Note que,

$$ac-bd = ac-bc+bc-bd = c(a-b)+b(c-d).$$

Como $m \mid (a-b)$ e $m \mid (c-d)$ segue que $m \mid c(a-b)$ e $m \mid b(c-d)$. Logo, $m \mid c(a-b)+b(c-d)$ e, daí que, $m \mid (ac-bd)$. Portanto, $ac \equiv bd \pmod{m}$.

Teorema 2.4.3 *Sejam a, b, c, n e m inteiros, com $m, n > 0$ e $a \equiv b \pmod{m}$. Então, $a^n \equiv b^n \pmod{m}$.*

Demonstração: Provaremos por indução sobre n. Para $n = 1$ a proposição é verdadeira pois, por hipótese, $a \equiv b \pmod{m}$. Agora, suponha que para um inteiro $k > 1$ a proposição seja verdadeira, ou seja, $a^k \equiv b^k \pmod{m}$. Então, temos:

$$a^{k+1} - b^{k+1} = a^k a - b^k b.$$

Como, $a \equiv b \pmod{m}$ e, por hipótese de indução, $a^k \equiv b^k \pmod{m}$ temos que $a^{k+1} \equiv b^{k+1} \pmod{m}$. Portanto, a proposição é verdadeira para todo inteiro positivo n.

Teorema 2.4.4 (Pequeno Teorema de Fermat) *Seja p um número primo e $a \in \mathbb{Z}$. Então $a^p \equiv a \pmod{p}$.*

Demonstração: Provaremos por indução sobre a. Para $a = 1$, temos $1 \equiv 1 \pmod{p}$.

Agora, suponhamos que $p \mid (a^p - a)$. Temos então:

$$\begin{aligned}(a+1)^p - (a+1) &= \binom{p}{0}a^p + \binom{p}{1}a^{p-1} + \cdots \binom{p}{p-1}a + \binom{p}{p} - (a+1) \\ &= a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots \binom{p}{p-1}a + 1 - (a+1) \\ &= a^p - a + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots \binom{p}{p-1}a + 1 - 1 \\ &= (a^p - a) + \sum_{k=1}^{p-1}\binom{p}{k}a^{p-k}.\end{aligned}$$

Por hipótese de indução $p \mid (a^p - a)$ e, como $p \mid \binom{p}{k}$, para todo $1 \leq k \leq p-1$, segue que $p \mid [(a^p - a) + \sum_{k=1}^{p-1}\binom{p}{k}a^{p-k}]$ e, portanto $p \mid [(a+1)^p - (a+1)]$.

Logo, $a^p \equiv a \pmod{p}$ para todo $a \in \mathbb{Z}$.

Exemplo 2.4.2 *Seja $p = 7$ um número primo. Pelo teorema acima, dado $a = 2$ temos $2^7 \equiv 2 \pmod{7}$.*

Devemos mostrar que $7 \mid (2^7 - 2)$. Observe que $2^7 = 128$ e, como $128 - 2 = 126 = 2 \times 3^2 \times 7$, que é divisível por 7. Daí, segue o resultado.

Corolário 2.4.1 (Pequeno Teorema de Fermat) *Seja p um número primo e a um inteiro não divisível por p, então p divide $a^{p-1} - 1$.*

Exemplo 2.4.3 *Sejam $p = 7$ um número primo e $a = 2$. Observe que $7 \nmid 2$. Pelo corolário acima, temos $2^{7-1} \equiv 1 \pmod{7}$.*

Devemos mostrar que $7 \mid (2^6 - 1)$. Observe que $2^6 = 64$ e, como $64 - 1 = 63 = 7 \times 9$, que é divisível por 7. Daí, segue o resultado.

2.4.2 Classes Residuais

Na seção anterior, vimos que a congruência módulo m é uma relação de equivalência pois, ela é reflexiva, simétrica e transitiva. Dessa forma, podemos considerar a classe residual de um inteiro a qualquer, módulo m. Assim, a classe de equivalência do inteiro a, será denotada como segue:

$$\overline{a} = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\}.$$

Na divisão euclidiana, se r é o resto da divisão de qualquer inteiro por m então, $0 \leq r \leq m-1$, ou seja, o conjunto das classes residuais módulo m tem exatamente m elementos. Denotaremos o conjunto das classes residuais módulo m por $\mathbb{Z}_m$.

Assim,

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

Antes de enunciarmos a primeira proposição, definiremos as operações de adição e multiplicação em $\mathbb{Z}_m$.

Teorema 2.4.5 ([12], pág 30) *Seja m um inteiro tal que $m \geq 2$.*

(a)

$$\begin{aligned} + : \mathbb{Z}_m \times \mathbb{Z}_m &\to \mathbb{Z}_m \\ (\overline{x}, \overline{y}) &\rightsquigarrow \overline{x+y} = \overline{x} + \overline{y} \end{aligned}$$

e

$$\begin{aligned} \cdot : \mathbb{Z}_m \times \mathbb{Z}_m &\to \mathbb{Z}_m \\ (\overline{x}, \overline{y}) &\rightsquigarrow \overline{x \cdot y} = \overline{x} \cdot \overline{y} \end{aligned}$$

definem duas operações chamadas soma e produto no conjunto $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \cdots, \overline{m-1}\}$.

(b) As operações acima definidas gozam das propriedades:

i) Associatividade da soma;

ii) Existência de elemento neutro da soma;

iii) Existência de inverso aditivo;

iv) Comutatividade da soma;

v) Associatividade do produto;

vi) Existência da unidade;

vii) Comutatividade do produto;

viii) Distributividade do produto em relação à soma;

Por isso dizemos que $(\mathbb{Z}_m, +, \cdot)$ é um anel comutativo com unidade $\overline{1}$.

c) O anel $(\mathbb{Z}_m, +, \cdot)$ é um domínio de integridade (isto é, sem divisores de zero) se, e somente se, m é um número primo.

d) Se $m = p$ é um número primo então $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{p-1}\}$ além das propriedades listadas em (b), goza das seguintes propriedades:

ix) $\mathbb{Z}_p$ *não possui divisores de zero;*

x) Se $\overline{0} \neq \overline{x} \in \mathbb{Z}_p$ *então existe* $\overline{y} \in \mathbb{Z}_p$ *tal que* $\overline{x} \cdot \overline{y} = \overline{y} \cdot \overline{x} = \overline{1}$ *(isto é, os elementos diferentes de* $\overline{0}$ *possuem inverso multiplicativo).*

Por isso dizemos que $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{p-1}\}$ *é um corpo.*

Demonstração: Vamos demonstrar o item (x) da letra (d).

Suponhamos que $n = p \geq 2$ é um número primo e seja $\overline{0} \neq \overline{x} \in \mathbb{Z}_p$. Podemos escolher x tal que $0 < x < p$ pois $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{p-1}\}$. Ora, p primo e $1 \leq x < p$ implica que $(x, p) = 1$ e, portanto, existem $r, s \in \mathbb{Z}$ tais que $xr + ps = 1$ e daí, segue que:

$$\overline{xr + ps} = \overline{1}$$

e, como $\overline{p} = \overline{0}$ teremos finalmente $\overline{x} \cdot \overline{r} = \overline{1}$, como queríamos mostrar.

Para as outras demonstrações vide [12].

Definição 2.4.2 *Um elemento* $\overline{a} \in \mathbb{Z}_m$ *é um elemento invertível se existe* $\overline{b} \in \mathbb{Z}_m$ *tal que* $\overline{a}.\overline{b} = \overline{1}$.

Proposição 2.4.3 *Um elemento* $\overline{a}$ *pertencente a* $\mathbb{Z}_m$ *é invertível sobre a multiplicação se, e somente se,* $(a, m) = 1$.

Demonstração: Seja $\overline{a} \in \mathbb{Z}_m$ um elemento invertível. Então,pela definição 2.4.2, existe $\overline{b} \in \mathbb{Z}_m$ tal que $\overline{a}\overline{b} = \overline{ab} = \overline{1}$. Logo, $ab \equiv 1 \pmod{m}$, ou seja, $m \mid (ab - 1)$. Assim, se existisse um primo p tal que p dividisse a e m ao mesmo tempo, então p dividiria 1, o que seria um absurdo. Logo, $(a, m) = 1$.

Reciprocamente, se $(a, m) = 1$, então a identidade de Bezoult nos garante que existem b e y tais que $ab + my = 1$. Logo, $m \mid ab - 1$ e, daí que $ab \equiv 1 \pmod{m}$, ou seja, $\overline{ab} = \overline{a}\overline{b} = \overline{1}$. Portanto, $\overline{a}$ é invertível em $\mathbb{Z}_m$.

Exemplo 2.4.4 *Consideremos a multiplicação em* $\mathbb{Z}_4$. *Neste caso, consideraremos apenas os símbolos* $\overline{0}, \overline{1}, \overline{2}$ *e* $\overline{3}$. *Na tabela da multiplicação em* $\mathbb{Z}_4$, *temos:*

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Observe, no exemplo acima que, $(1, 4) = 1 = (3, 4)$ que, pelo teorema acima, são os únicos elementos invertíveis em $\mathbb{Z}_4$.

Proposição 2.4.4 *O conjunto $\mathbb{Z}_m^*$ é fechado para a operação de multiplicação se, e somente se, m é primo.*

Demonstração:

Suponhamos, primeiramente que m não seja primo, ou seja, existem $x, y < m$ tais que $m = xy$. Como $x, y < m$, temos que $x, y \in \mathbb{Z}_m^*$ e, daí que, $\overline{x}.\overline{y} = \overline{x.y} = \overline{m} = \overline{0}$. O que é uma contradiçao pois, $\overline{0} \notin \mathbb{Z}_m^*$.

Reciprocamente, o conjunto $\mathbb{Z}_m^*$ não será fechado para a operação de multiplicação se existirem $x, y \in \mathbb{Z}_m^*$ tais que $\overline{x}.\overline{y} = \overline{0}$, ou seja, $xy \equiv 0 \pmod{m}$ e , daí que, $m|xy$. Como, por hipótese, m e primo, temos que $m|x$ ou $m|y$. Se $m|x$, existe um inteiro k tal que $x = km$. Logo,

$$\overline{x} = \overline{k.m} = \overline{k}.\overline{m} = \overline{k}.\overline{0} = \overline{0}.$$

Portanto, $\overline{x} = \overline{0}$ o que é um absurdo pois $\overline{x} \in \mathbb{Z}_m^*$.

Analogamente, se $m|y$, mostramos que $\overline{y} = \overline{0}$, o que será um absurdo.

Portanto, o conjunto $\mathbb{Z}_m^*$ é fechado para a operação de multiplicação se, e somente se, m é primo.

Observação 2.4.1 *A partir de agora iremos trabalhar com o conjunto $\mathbb{Z}_p^*$, com p primo.*

2.5 Subgrupo $\mathbb{Z}_p$

Definição 2.5.1 *Um grupo multiplicativo G é chamado de cíclico se existir $a \in G$ tal que $G = \{a^n; n \in \mathbb{Z}\}$ e, vamos denotar por, $\langle a \rangle = G$, e diremos que a é um gerador de G.*

Afirmamos que $\mathbb{Z}_p^*$, com p primo, é um grupo multiplicativo.

De fato, Sejam $\overline{a}$ e $\overline{b}$ elementos de $\mathbb{Z}_p^*$. Como as operações de adição e multiplicação de inteiros estão bem definidas em $\mathbb{Z}_p^*$, resta mostrar que dado $a \in \mathbb{Z}_p^*$ existe $b \in \mathbb{Z}_p^*$ tal que $ab \equiv 1 \pmod{p}$, ou seja, existe um inteiro x tal que, $ab - px = 1$. Como $a < p$ pois, $a \in \mathbb{Z}_p^*$, temos $(a, p) = 1$ e, daí que, a equação diofantina $ab - px = 1$ tem solução.

Portanto, $\mathbb{Z}_p^*$ é um grupo multiplicativo.

Definição 2.5.2 *Dizemos que um elemento $b \in \mathbb{Z}_p^*$ é uma raiz primitiva de $\mathbb{Z}_p^*$ quando b for um gerador de $\mathbb{Z}_p^*$.*

Exemplo 2.5.1 *Mostremos que $(\mathbb{Z}_5^*, .)$ é um grupo cíclico.*

Demostração:

Como $(\mathbb{Z}_5^*, .) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, temos, calculando todas as potências de $2, 3$ e 4 que são congruentes módulo 5 a $1, 2, 3$ ou 4, que:

$$2^1 \equiv 2 \pmod 5$$

$$2^2 \equiv 4 \pmod 5$$

$$2^3 \equiv 3 \pmod 5$$

$$2^4 \equiv 1 \pmod 5.$$

$$3^1 \equiv 3 \pmod 5$$

$$3^2 \equiv 4 \pmod 5$$

$$3^3 \equiv 2 \pmod 5$$

$$3^4 \equiv 1 \pmod 5.$$

$$4^1 \equiv 4 \pmod 5$$

$$4^2 \equiv 1 \pmod 5$$

$$4^3 \equiv 4 \pmod 5$$

$$4^4 \equiv 1 \pmod 5.$$

Observe, pela definição acima, que $\overline{2}$ e $\overline{3}$ são geradores de $(\mathbb{Z}_5^*, .)$, ou seja, $\langle\overline{2}\rangle = (\mathbb{Z}_5^*, .)$ e, $\langle\overline{3}\rangle = (\mathbb{Z}_5^*, .)$.

2.5.1 O Teorema Chinês dos Restos

Teorema 2.5.1 ([14], pág 253) *Sejam $m_1, m_2, m_3, \cdots, m_r$ inteiros positivos primos entre si. Então o sistema de congruências*

$$x \equiv c_1 \pmod{m_1},$$

$$x \equiv c_2 \pmod{m_2},$$

$$\vdots$$

$$x \equiv c_r \pmod{m_r}$$

tem uma única solução módulo $M = m_1 m_2 \cdots m_r$. *As soluções são*

$$x = M_1 y_1 c_1 + \cdots + M_r y_r c_r + tM,$$

onde $t \in \mathbb{Z}$, $M_i = \dfrac{M}{m_i}$ *e* y_i *é solução de* $M_i Y \equiv 1 \pmod{m_i}$, *com* $i = 1, \ldots, r$.

Demonstração:

Vamos inicialmente, provar que x é uma solução simultânea desse sistema. De fato, como $m_i \mid M_j$ se $i \neq j$, e $M_i Y_i \equiv 1 \pmod{m_i}$, segue-se que

$$x = M_1 y_1 c_1 + \cdots + M_r y_r c_r \equiv M_i y_i c_i \equiv c_i \pmod{m_i}.$$

Por outro lado, se x' é outra solução do sistema, então

$$x \equiv x' \pmod{m_i}$$

para todo $i = 1, \ldots, r$. Como $(m_i, m_j = 1)$, para todo $i \neq j$, segue-se que $[m_i, \ldots, m_r] = m_1 \cdots m_r = M$ e, consequentemente, $x \equiv x' \pmod{[m_i, \ldots, m_r]}$.

Portanto, $x \equiv x' \pmod{M}$.

2.5.2 A Função de Euler

Definição 2.5.3 *Seja* m *um inteiro positivo. A função fi de Euler,* $\varphi(m)$ *é definida como o número de inteiros não negativos menores do que* m *e que são primos com* m. *Assim,* $\varphi(m) = \#\{a \in \mathbb{Z}_+^* : a < m \quad e \quad (a, m) = 1\}$. *Observe que, se* m *for primo,* $\varphi(m) = m - 1$.

Propriedades da função fi de Euler

Teorema 2.5.2 *Sejam* $m, n \in \mathbb{N}$ *com* $(m, n) = 1$. *Então*

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

Demonstração: O resultado é facilmente verificado se $m = 1$ ou $n = 1$. Então, vamos supor $m > 1$ e $n > 1$. Assim, consideremos a tabela abaixo formada pelos números naturais de 1 até nm.

Observe que a tabela acima forma um sistema completo de resíduos módulo nm. Mas, estamos interessados no sistema reduzido de resíduos módulo nm, ou seja,

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

queremos determinar todos os números de 1 a nm que são primos com nm. Assim, queremos determinar t, tal que $(t, nm) = 1$. Mas,

$$(t, mn) = 1 \Leftrightarrow (t, n) = (t, m) = 1.$$

Dessa forma, para calcular $\varphi(mn)$ devemos determinar na tabela acima os inteiros que são primos com n e m ao mesmo tempo. Assim, se na r-ésima linha tivermos $(m, r) = d > 1$ então nenhum termo dessa linha será primo com nm pois, todos os termos são da forma $km+r$, onde $0 \leq k \leq n-1$ e estes são todos divisíveis por d. Logo, os elementos que são primos com m estão necessariamente nas colunas restantes e, num total de $\varphi(m)$ elementos. Agora, vejamos quais são os elementos primos com n em cada uma dessas linhas.

Como $(n, m) = 1$, os elementos da linha $k, m + k, \ldots, (n-1)m + k$ são todos primos com n e formam um sistema completo de resíduos módulo n. Logo, cada uma dessas linhas possui uma quantidade de $\varphi(n)$ elementos primos com n e, consequentemente primos com nm. Logo, o número de elementos simultaneamente primos com n e m é $\varphi(n)\varphi(m)$. Portanto, $\varphi(nm) = \varphi(n)\varphi(m)$.

Teorema 2.5.3 *Seja p um número primo e α um inteiro positivo temos:*

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

Demonstração:

Pela definição de φ, temos que $\varphi(p^\alpha)$ é a quantidade de inteiros positivos que são primos com p^α. Note que, a quantidade de números menores do que p^α é um total de p^α. Observe também que os números que não são primos com p^α são $\{p, 2p, 3p, 4p, \cdots, p^2, p^3, \cdots, p^\alpha\}$ e são em quantidade de $p^{\alpha-1}$. Dessa forma, a quantidade de inteiros positivos que são primos com p^α é:

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

Teorema 2.5.4 *Se* $n = p_1^{\alpha_1}.p_2^{\alpha_2}.p_3^{\alpha_3}.\cdots.p_r^{\alpha_r}$ *então:*

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

Demonstração:

Pelo teorema 2.5.3, temos:

$$\varphi(p^{\alpha_i}) = p^{\alpha_i} - p^{\alpha_i-1}.$$

E, pelo teorema 2.5.2:

$$\begin{aligned}
\varphi(p_1^{\alpha_1}.p_2^{\alpha_2}.p_3^{\alpha_3}.\cdots.p_r^{\alpha_r}) &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_r^{\alpha_r}) \\
&= \left(p_1^{\alpha_1}-p_1^{\alpha_1-1}\right)\left(p_2^{\alpha_2}-p_2^{\alpha_2-1}\right)\cdots\left(p_r^{\alpha_r}-p_r^{\alpha_r-1}\right) \\
&= p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right)\cdots p_r^{\alpha_r}\left(1-\frac{1}{p_r}\right) \\
&= p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right) \\
&= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)
\end{aligned}$$

Portanto,

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

2.6 Matrizes e suas Propriedades

2.6.1 Introdução

Neste capítulo serão revisadas as definições de Matrizes, assim como as operações entre seus elementos. O texto desenvolvido a seguir, bem como suas demonstrações, foi desenvolvido utilizando as referências em [5] e [16].

2.6.2 Matrizes

Definição 2.6.1 (Matriz) *Uma matriz* A *é dada por* $A = (a_{ij})_{m\times n}$ *com* $1 \leqslant i \leqslant m$ *e* $1 \leqslant j \leqslant n$ *onde o elemento* (a_{ij}) *é o elemento da* i*-ésima linha e da* j*-ésima coluna.*

Se $m = n$ *dizemos que a matriz* A *é quadrada.*

Abaixo nomearemos algumas matrizes especiais:

a) **Matriz nula -** é a matriz em que todos os elementos (a_{ij}) são iguais a zero.

b) **Matriz linha -** é toda matriz do tipo $A = (a_{1j})_{1\times n}$, com $1 \leqslant j \leqslant n$, ou seja, é a matriz que tem uma única linha.

c) **Matriz coluna -** é toda matriz do tipo $A = (a_{i1})_{1\times m}$, com $1 \leqslant i \leqslant m$, ou seja, é a matriz que tem uma única coluna.

d) **Matriz quadrada de ordem** n **-** é toda matriz do tipo $n \times n$, isto é, é uma matriz que tem o número de linhas igual ao número de colunas.

e) **Matriz diagonal -** é toda matriz quadrada em que os elementos que não pertencem à diagonal principal são iguais a zero, ou seja, $a_{ij} = 0$ para todo $i \neq j$.

f) **Matriz identidade -** é uma matriz diagonal em que os elementos da diagonal principal são iguais a 1, ou seja, $a_{ij} = 1$ para todo $i = j$. Denotaremos a matriz identidade de ordem n por I_n ou $I_{n\times n}$.

Observação: Duas matrizes são iguais quando seus elementos correspondentes forem iguais. Dessa forma, dadas as matrizes $A = (a_{ij})_{m\times n}$ e $B = (b_{ij})_{m\times n}$ com $1 \leqslant i \leqslant m$ e $1 \leqslant j \leqslant n$ a igualdade $A = B$ se dará quando $a_{ij} = b_{ij}$.

2.6.3 Operações com Matrizes

Adição

A matriz soma é obtida somando-se os elementos que ocupam a mesma posição em cada uma das matrizes que estão sendo somadas. Dessa forma, só é possível realizar a soma de matrizes que têm a mesma ordem.

Assim, sendo $B = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{bmatrix}$ e $C = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{bmatrix}$,

a soma $A = B + C$, é dada por:

$$A = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{bmatrix} + \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{bmatrix}$$

$$= \begin{bmatrix} b_{11} + c_{11} & b_{12} + c_{12} & \cdots & b_{1n} + c_{1n} \\ b_{21} + c_{21} & b_{22} + c_{22} & \cdots & b_{2n} + c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} + c_{m1} & b_{m2} + c_{m2} & \cdots & b_{mn} + c_{mn} \end{bmatrix}$$

A matriz A é dita a matriz soma de B com C.

Definição 2.6.2 *Uma matriz A' é dita oposta da matriz A quando $A + A' = 0$ e denotaremos $A' = -A$ e a chamaremos de matriz oposta da matriz A.*

Observação: Na definição acima, 0 representa a matriz nula.

A partir daí, podemos definir a diferença entre duas matrizes.

Definição 2.6.3 *Dadas duas matrizes $A = a_{ij}$ e $B = b_{ij}$, a diferença entre as matrizes A e B é dada pela soma da matriz A com a oposta da matriz B e escreveremos $A - B$.*

Propriedades da Adição de Matrizes

Sejam A, B e C matrizes de mesma ordem.

i) **Comutativa**

$$A + B = B + A.$$

De fato,

$$[A + B]_{ij} = a_{ij} + b_{ij} = b_{ij} + a_{ij} = B + A.$$

ii) **Associativa**

$$(A + B) + C = A + (B + C)$$

pois,

$$[(A + B) + C]_{ij} = (a_{ij} + b_{ij}) + c_{ij} = a_{ij} + (b_{ij} + c_{ij}) = [A + (B + C)]_{ij}$$

iii) **Existência e elemento neutro**

Seja $0_{m\times n}$ a matriz nula. Temos:

$$A + 0 = 0 + A = A$$

iv) **Existência de simétrico**

$$A + (-A) = 0.$$

De fato,

$$A + (-A) = a_{ij} - a_{ij} = 0.$$

2.6.4 Multiplicação de uma Matriz por um escalar

Seja k um número qualquer e $A = a_{ij}$ uma matriz qualquer. O produto de k pela matriz A será denotado por $kA = ka_{ij}$, para todo i, j. Assim, para efetuarmos o produto de um número qualquer por uma matriz, basta multiplicarmos cada elemento da matriz pelo número dado.

Propriedades da Multiplicação por Escalar

Sejam α e β escalares e A e B matrizes quaisquer.

i) **Associativa**

$$\alpha(\beta A) = (\alpha\beta)A.$$

ii) **Distributiva**

$$(\alpha + \beta)A = \alpha A + \beta B.$$

$$\alpha(A + B) = \alpha A + \alpha B.$$

iii) **Existência de elemento neutro**

$$1A = A.$$

2.6.5 Produto de Matrizes

O produto de duas matrizes $A = (a_{ij})_{m\times n}$ e $B = (b_{jl})_{n\times l}$ é a matriz $C = (c_{il})_{m\times l}$ onde c_{il} é dado por:

$$c_{il} = a_{i1}b_{1l} + a_{i2}b_{2l} + a_{i3}b_{3l} + \cdots + a_{in}b_{nl}.$$

Para escrevermos na forma de somatório, verifique que os índices i da matriz A e l da matriz B se mantém fixos enquanto o índice j varia de 1 até n. Daí, temos:

$$\sum_{j=1}^{n} = a_{ij}b_{jl}.$$

Propriedades do Produto de Matrizes

Sejam $A = (a_{ij})_{m\times n}, B = (b_{ij})_{n\times p}$ e $C = (c_{ij})_{p\times q}$ matrizes tais que o produto exista.

i) **Associativa**

$$A(BC) = A(BC).$$

De fato,

$$\begin{aligned}
[A(BC)]_{ij} &= \sum_{k=1}^{n} a_{ik}\left(\sum_{l=1}^{p} b_{kl}c_{lj}\right) \\
&= \sum_{k=1}^{n}\sum_{l=1}^{p} a_{ik}(b_{kl}c_{lj}) \\
&= \sum_{k=1}^{n}\sum_{l=1}^{p} (a_{ik}b_{kl})c_{lj} \\
&= \sum_{l=1}^{p}\sum_{k=1}^{n} (a_{ik}b_{kl})c_{lj} \\
&= \sum_{l=1}^{p}\left(\sum_{k=1}^{n} (a_{ik}b_{kl}\right)c_{lj} \\
&= (AB)C
\end{aligned}$$

ii) **Distributividade**

$$A(B + C) = AB + AC.$$

$$\alpha(AB) = \alpha A\alpha B.$$

iii) **Elemento neutro**

Se A é uma matriz $m \times n$, então existe I_n e I_m tais que,

$$AI_n = A$$

e

$$I_m A = A.$$

2.6.6 Transposta de uma Matriz

Seja A uma matriz. A transposta da matriz A será a matriz obtida quando transformamos as linhas da matriz A em colunas. Denotaremos por A^t a transposta da matriz A. Assim, sendo

$$A = (a_{ij})_{m\times n}$$

então

$$A^t = (a_{ji})_{n\times m}.$$

Propriedades da Matriz Transposta

i) $(A^t)^t = A$.

ii) $(A + B)^t = A^t + B^t$.

iii) $(AB)^t = B^t A^t$.

iv $(\alpha A)^t = \alpha A^t$.

2.6.7 Determinantes

Seja M o conjunto das matrizes quadradas $n \times n$. O determinante, denotado por $detA$, onde $A \in M$, é determinado como se segue:

i) Se A é de ordem 1, então $A = (a_{11})$ e, $detA = a_{11}$.

ii) Se A é de ordem 2, então $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ e, $detA = a_{11}a_{22} - a_{12}a_{21}$.

iii) Se A é de ordem 3, então $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$ e, $detA = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{32}a_{21} - a_{13}a_{22}a_{31} - a_{23}a_{32}a_{11} - a_{33}a_{21}a_{12}$.

Podemos calcular o determinante de uma matriz usando permutação. Mas antes de o definirmos dessa forma, daremos a definição de permutação.

Definição 2.6.4 *Dada uma permutação dos inteiros* $1, 2, \ldots, n$, *existe uma inversão quando um inteiro precede outro menor que ele.*

Como exemplo, consideremos as permutações de $1, 2, 3$ e observemos em cada permutação o número de inversões:

Permutação	Número de Inversões
(1 2 3)	0
(1 3 2)	1
(2 1 3)	1
(2 3 1)	2
(3 1 2)	2
(3 2 1)	3

De maneira geral, podemos calcular o determinante como se segue:

Definição 2.6.5 *O determinante da matriz A é definido por*

$$detA = \sum_{\rho} (-1)^J a_{1j_1} a_{2j_2} \dots a_{nj_n},$$

onde $J = J(j_1, j_2, \dots, j_n)$ é o número de inversões da permutação $(j_1, j_2, \dots, j_n)$ e ρ indica que a soma é estendida a todas as $n!$ permutações de $(1 \ \ 2 \ \ 3 \ \ \dots \ \ n)$.

Observações:

i) Se a permutação $(j_1, j_2, \dots, j_n)$ tem um número par de inversões, o coeficiente $(-1)^J$ do termo correspondente na somatória terá sinal positivo, caso contrário, terá sinal negativo.

ii) Em cada termo da somatória, existe um e apenas um elemento de cada linha, e um e apenas um elemento de cada coluna da matriz.

iii) Através de uma reordenação conveniente dos termos, mostra-se que também é possível definir um determinante por

$$detA = \sum_{\rho} (-1)^J a_{j_1 1} a_{j_2 2} \dots a_{j_n n}$$

variando os primeiros e deixando fixos os segundos índices.

Propriedades dos Determinantes

i) Se todos os elementos de uma linha ou coluna de uma matriz A são nulos, $detA = 0$.

ii) $detA^t = detA$.

iii) Se multiplicarmos uma linha ou coluna de uma matriz M por uma constante k, o determinante da nova matriz $M^{'}$ será o produto de k pelo determinante de M, ou seja, $detM^{'} = kdetM$.

iv) Se trocarmos a posição de duas linhas ou colunas de uma matriz A, o determinante da nova matriz $A^{'}$ será dado por, $detA^{'} = -detA$.

v) O determinante de uma matriz que tem duas linhas ou colunas iguais é zero.

vi) De um modo geral, $det(A + B) \neq detA + detB$.

vii) O determinante não se altera se somarmos a uma linha outra linha multiplicada por uma constante.

viii) $det(AB) = detA.detB$.

Definição 2.6.6 *Sejam $A_{n\times n}$ uma matriz e a_{ij} um elemento de A. O cofator do elemento a_{ij}, denotado por c_{ij}, é obtido da seguinte forma:*

$$c_{ij} = (-1)^{i+j} detA_{ij},$$

onde $detA_{ij}$ é o determinante da submatriz A obtido ao excluir a $i-$ésima linha e $j-$ésima coluna da matriz A, $i, j = 1, 2, \ldots, n$.

Definição 2.6.7 *Chama-se matriz dos cofatores da matriz $A_{n\times n}$, denotada por $\overline{A}$ à matriz:*

$$\overline{A} = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{bmatrix},$$

onde c_{ij} são os cofatores dos respectivos elementos a_{ij} da matriz A.

Definição 2.6.8 (Matriz Adjunta) *A matriz adjunta da matriz $A_{n\times n}$, denotada por $adj(A)$, é a matriz transposta dos cofatores de A.*

$$adj(A) = (\overline{A})^t$$

2.6.8 Matriz Inversa

Definição 2.6.9 *Seja A uma matriz quadrada de ordem n. Chamamos de inversa de A a matriz B tal que $AB = BA = I_n$, onde I_n é a matriz identidade de ordem n. Escrevemos A^{-1} para a inversa de A.*

Observações: [[5], pág 75-76]

i) Se A e B são matrizes quadradas de mesma ordem, ambas inversíveis (isto é, existem A^{-1} e B^{-1}), então AB é inversível e $(AB)^{-1} = B^{-1}.A^{-1}$.

ii) Se A é uma matriz quadrada e existe uma matriz B tal que $BA = I$, então A é inversível, ou seja, A^{-1} existe e, além disso, $B = A^{-1}$.

iii) Nem toda matriz tem inversa.

De fato,

Basta verificar que a matriz $A = \begin{pmatrix} 0 & 2 \\ 0 & 1 \end{pmatrix}$ não tem inversa.

Suponhamos que uma matriz A de ordem n tenha inversa, isto é, existe A^{-1} tal que $AA^{-1} = I_n$. Usando determinantes, temos:

$$det(AA^{-1}) = detAdetA^{-1}$$

e, como $det(I_n) = 1$, segue que:

$$detAdetA^{-1} = 1.$$

Desse produto concluímos que, se A tem inversa:

i) $detA \neq 0$;

ii) $detA^{-1} = \dfrac{1}{detA}$;

Teorema 2.6.1 *Uma matriz quadrada A admite uma inversa se, e somente se, $detA \neq 0$. Nesse caso,*

$$A^{-1} = \frac{1}{detA} adj(A).$$

A demonstração do teorema acima pode ser encontrada em [5].

Exemplo 2.6.1 *Seja*

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$$

temos $detA = 3 \neq 0$ *e, portanto existe a inversa de A. Calculemos* A^{-1} *através da relação* $A^{-1} = \frac{1}{detA} adj(A)$.

$$\overline{A} = \begin{pmatrix} 3 & 0 \\ -2 & 1 \end{pmatrix}$$

e

$$adj(A) = \begin{pmatrix} 3 & 0 \\ -2 & 1 \end{pmatrix}.$$

Então,

$$A^{-1} = \frac{1}{detA} adj(A) = \frac{1}{3} \begin{pmatrix} 3 & -2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \frac{-2}{3} \\ 0 & \frac{1}{3} \end{pmatrix}.$$

2.7 Geogebra

O Geogebra é um programa matemático que oferece recursos para auxiliar no aprendizado dos alunos. Ele tem ferramentas que podem auxiliar no ensino da aritmética, álgebra, geometria e cálculo. Nesta seção, iremos utilizar o Geogebra para operarmos com matrizes. Para utilizarmos o referido software, é necessário que o tenhamos instalado no nosso computador. Para baixá-lo, basta acessarmos o endereço eletrônico `https://www.geogebra.org/download`.

Tendo efetuado a instalação do geogebra no seu computador, para abri-lo, basta darmos dois cliques, com o botão esquerdo do mouse, no ícone do geogebra que estará na sua área de trabalho.

Ao abrí-lo, aparecerá uma tela conforme a figura abaixo:

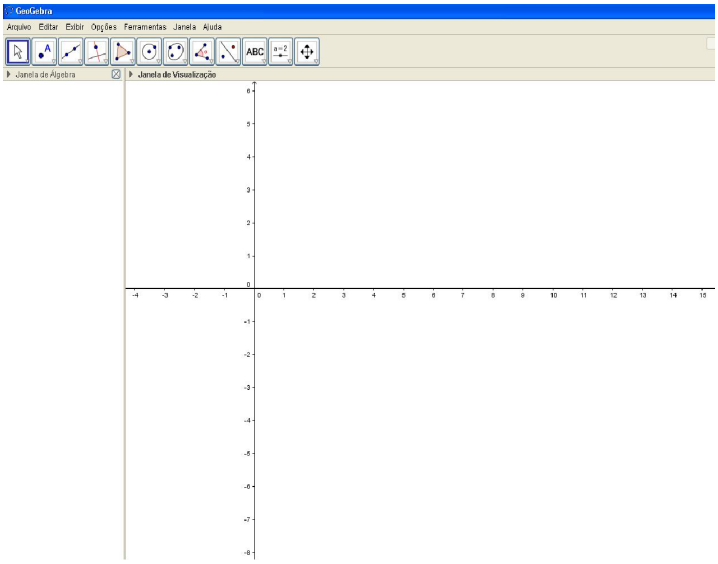
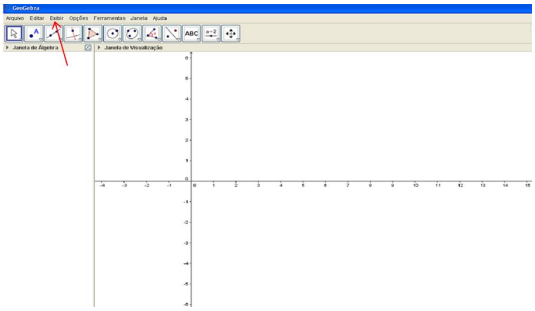


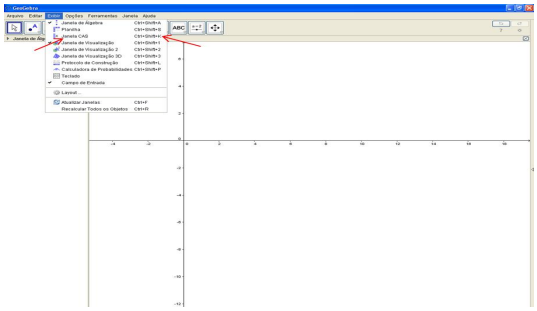
Figura 2.1: Tela inicial do Geogebra

Observe que nesta tela há duas janelas: a janela de Álgebra à esquerda e a janela de Visualização à direita.

Na barra de tarefas, dê um clique, com o botão direito do mouse, no menu Exibir e, em seguida selecione Janela CAS. Se preferir, após aberto o Geogebra podemos utilizar o atalho CTRL+SHIFT+K que a Janela CAS é aberta automaticamente.



(a) Menu Exibir do Geogebra



(b) Acessando a janela CAS

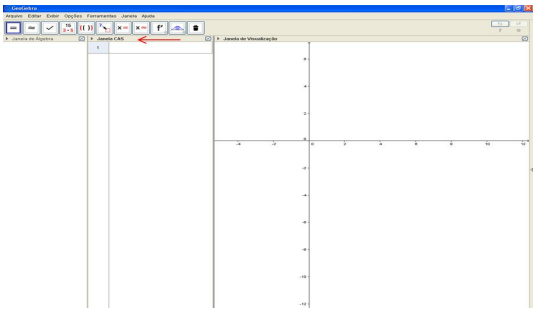
Observe que, a tela do Geogebra está dividida e três janelas:

1) Janela da esquerda - Janela de Álgebra;

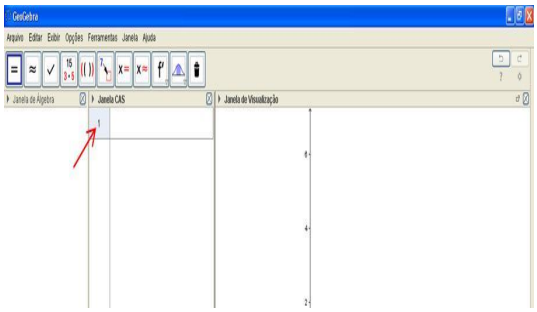
2) Janela central - Janela CAS;

3) Janela da direita - Janela de Visualização;

Após aberta a janela CAS, teremos a seguinte tela no nosso computador:



(c) Janela CAS



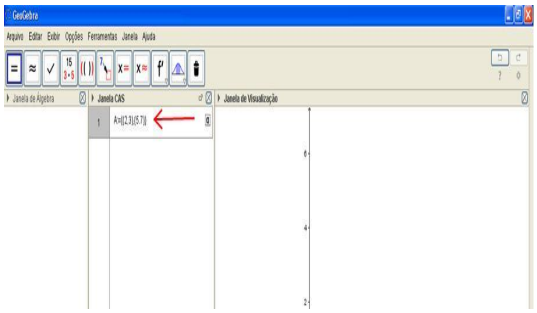
(d) Célula 1 na janela CAS

Como estamos interessados na janela CAS, iremos trabalhar com a janela central.

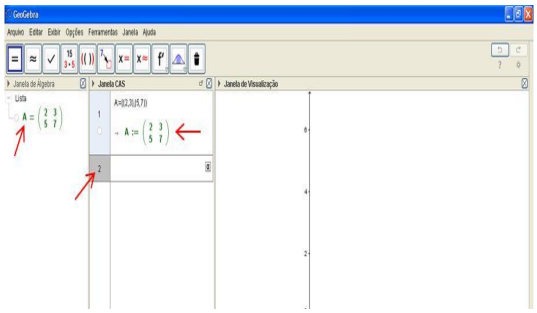
2.7.1 Inserindo Matrizes no Geogebra

Podemos observar na janela CAS que, ao abrí-la, aparece uma célula numerada com o numeral 1 e, será nesta célula que iremos entrar com os dados da nossa matriz.

Para inserirmos a matriz $A = \begin{pmatrix} 2 & 3 \\ 5 & 7 \end{pmatrix}$, digitamos na célula 1, conforme figura abaixo e, ao clicarmos no botão Enter, o geogebra nos retorna a matriz A, na janela CAS e na janela de Álgebra e, imediatamente aparece, na janela CAS, uma outra célula numerada com o numeral 2 a qual também usaremos para entrar com os nossos dados.



(e) Inserindo Matrizes



(f) Inserindo Matrizes

Procedendo de forma análoga, vamos inserir as matrizes $B = \begin{pmatrix} -5 & 8 \\ -1 & -9 \end{pmatrix}$, $C = \begin{pmatrix} 1 & 4 \end{pmatrix}$ e $D = \begin{pmatrix} 7 \end{pmatrix}$ e, a seguir vamos operar com estas matrizes.

2.7.2 Operando com Matrizes

Adição

Após inseridas as matrizes A, B e C na janela CAS e, sendo $E = A + B$ basta digitarmos na célula 5, conforme figura abaixo, que o geogebra nos retorna o resultado da soma da matriz A com a matriz B.

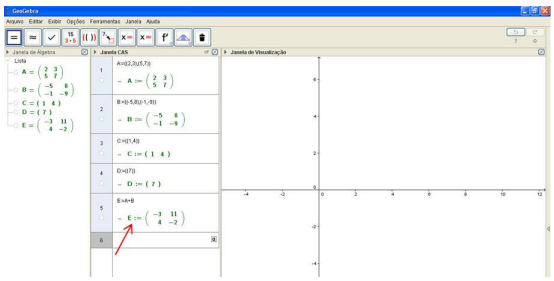


Figura 2.2: Adição de Matrizes

Multiplicação

Sendo $F = AB$ o produto da matriz A pela matriz B, basta inserirmos na célula do geogebra tal como se segue.

Lembrando que o sinal da multiplicação é dado pelo símbolo $*$.

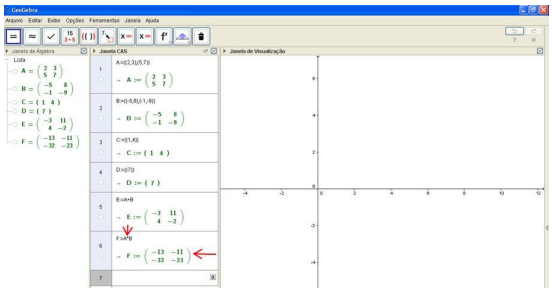


Figura 2.3: Multiplicação de Matrizes

Multiplicação por um escalar

Para inserirmos um escalar na janela CAS, clicamos com o cursor do mouse sobre a célula em branco e, logo após clicamos com o botão esquerdo do mouse no ícone que está à direita nesta célula.

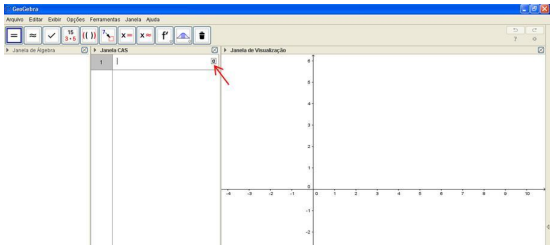


Figura 2.4: Inserindo um escalar

Após clicar neste ícone, basta escolher com qual escalar vamos querer trabalhar. No nosso caso, escolhemos λ e atribuímos o valor 2. Observe que, sempre que entramos com um dado na célula, este aparece também na janela de Álgebra.

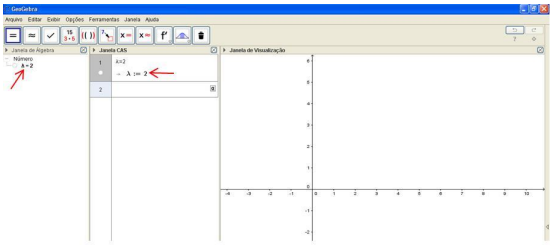


Figura 2.5: Inserindo um escalar

Após termos entrado com o escalar e com a matriz na janela CAS, podemos efetuar a multiplicação desta matriz pelo escalar.

Matriz Transposta

Na janela CAS, para encontrarmos a transposta G de uma matriz qualquer, basta digitarmos $G := MatrizTransposta[< Matriz >]$, onde no lugar de $< Matriz >$ digitaremos a matriz a qual queremos determinar a transposta.

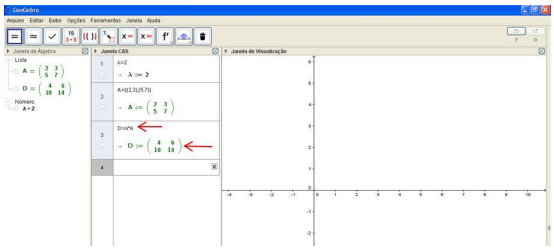


Figura 2.6: Multiplicação de uma matriz por um escalar

Por exemplo, determine as matrizes $G = A^t$ e $H = B^t$ das matrizes $A = \begin{pmatrix} 2 & 3 \\ 5 & 7 \end{pmatrix}$ e $B = \begin{pmatrix} -5 & 8 \\ -1 & -9 \end{pmatrix}$. A solução encontra-se na figura abaixo:

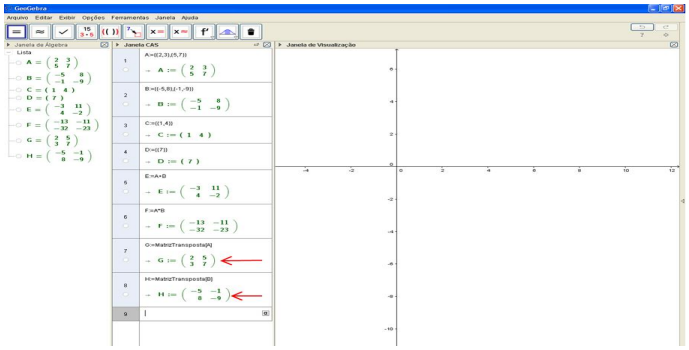
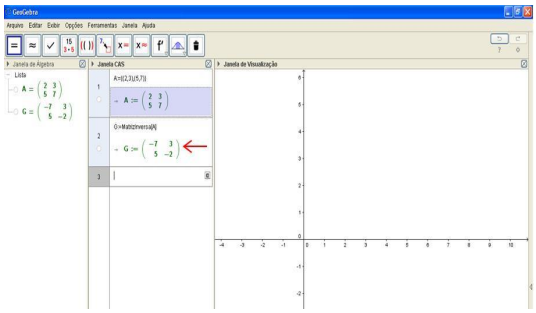


Figura 2.7: Transposta das Matrizes A e B

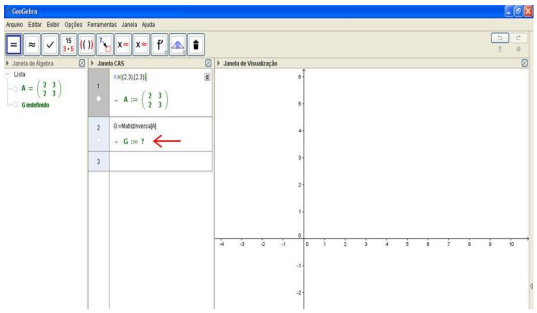
Matriz Inversa

Para invertermos uma determinada matriz na janela CAS basta, após termos inserido esta matriz em uma determinada célula, basta digitarmos em uma célula em branco $MatrizInversa[< Matriz >]$, onde no lugar de $< Matriz >$ digitaremos a matriz a qual queremos determinar a sua inversa.

No caso da matriz não ser invertível, como por exemplo a matriz $A = \begin{pmatrix} 2 & 3 \\ 2 & 3 \end{pmatrix}$, o geogebra nos retorna, sendo $G = A^{-1}$, $G :=?$, vide figura abaixo:



(a) Inversa de uma matriz



(b) Inversa de uma matriz

Determinante

Para calcularmos o determinante de uma matriz dada, digitamos na janela CAS do geogebra, $Determinante[< Matriz >]$, onde no lugar de $< Matriz >$ digitaremos a matriz a qual queremos obter seu determinante.

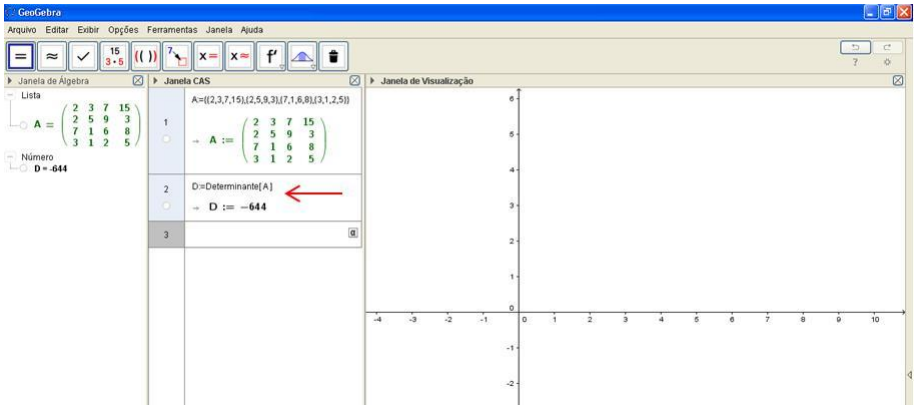


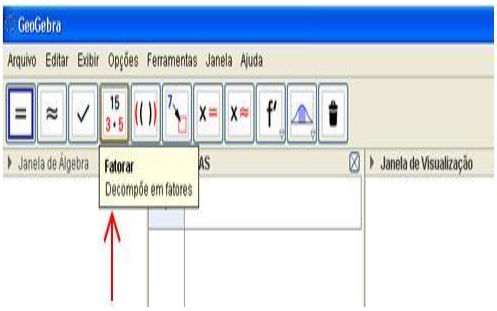
Figura 2.8: Cálculo do determinante de uma matriz

Fatoração de números

Na janela CAS do geogebra existe uma ferramenta muito útil para a decomposição de um número em fatores primos. No capítulo 3, quando formos falar de Criptografia RSA, veremos que, se conseguirmos fatorar o número n, que é produto de dois números primos p e q, conseguiremos, caso seja interceptada, decifrar a mensagem que foi enviada a um destinatário qualquer.

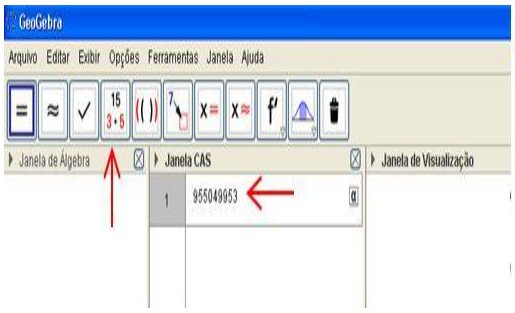
Na barra de ferramentas da janela CAS, existe um ícone destinado a decompor em fatores, ou seja, decompõe um número qualquer em fatores primos.

(a) Barra de ferramentas da janela CAS

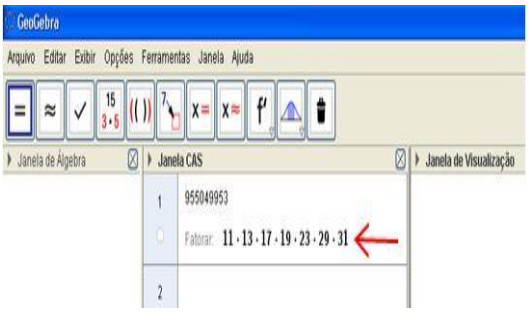


(b) Ícone para decomposição de números em fatores primos

Como exemplo, vamos decompor o número 955049953 em fatores primos. Para isso, devemos entrar com este número em uma célula vazia e, logo após clicamos no ícone fatorar que irá nos devolver a decomposição deste número em fatores primos.



(c) Decompondo um número em fatores primos



(d) Número 955049953 decomposto em fatores primos

Uma observação importante é que, esta ferramenta nos dá o resultado da fatoração de forma rápida e eficiente podendo também ser utilizada pelo professor em sala de aula para auxílio no desenvolvimento deste conteúdo.

2.8 LibreOffice Calc

O LibreOffice Calc é um programa de planilha eletrônica e assemelha-se ao Lotus $1-2-3$, da IBM, e ao Excel, da Microsoft. O Calc é destinado à criação de planilhas e tabelas, permitindo ao usuário a inserção de equações matemáticas e auxiliando na elaboração de gráficos de acordo com os dados presentes na planilha.

O Calc utiliza o formato ODF como padrão, embora reconheça e exporte arquivos em formatos de outras planilhas eletrônicas, além de exportar arquivos em PDF sem a necessidade de instalação de uma extensão, assim como todos os aplicativos da suíte LibreOffice.

O Calc possui o recurso de fórmulas em linguagem natural, permitindo a criação de uma fórmula sem a necessidade de aprendizagem de códigos específicos.

Ao abrir uma planiha no LibreOffice Calc, aparecerá uma tela conforme a figura 2.9. Observe a semelhança do ambiente Calc com uma planilha do Excel, conforme mencionado acima. Utilizaremos o Calc para podermos construir uma calculadora modular, conforme figura 2.10, para nos auxiliar nos cálculos dos exercícios envolvendo congruências.

Inserindo dados na planilha Calc

Conforme figura 2.10, iremos construir uma calculadora para nos fornecer resultados de congruências da forma $a^x \equiv k \pmod{p}$.

Para distinguir os valores que serão atribuídos às variáveis módulo p, a, x, a^x e k vamos inserir estas variáveis nas células $C5, C7, C9, C11$ e $C13$, respectiva-

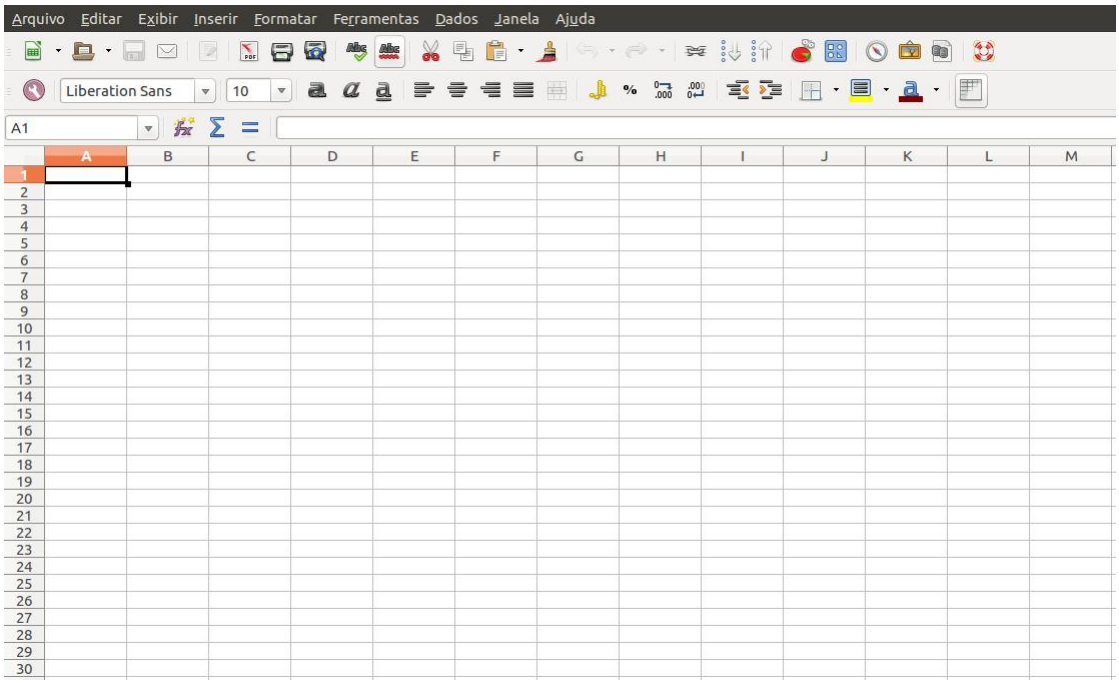


Figura 2.9: Planilha Calc do LibreOffice

	A	B	C	D	E	F	G	H
1	**Calculadora Modular para cálculo de potências menores do que $2x10^8$**							
2								
3			a^x≡k mod(p)					
4								
5			**Módulo p**	31				
6								
7			**a**	3				
8								
9			**x**	15				
10								
11			**a^x**	14348907				
12								
13			**k**	30				

Figura 2.10: Calculadora Modular para cálculo de de potências

mente. Nas células $D5, D7, D9, D11$ e $D13$ iremos inserir os valores de módulo p, a, x, a^x e k, respectivamente.

Após inseridos os valores das variáveis módulo p, a, x e k, podemos inserir as fórmulas. Vamos calcular o valor de a^x. Para isso, vamos selecionar a célula $D11$, que irá nos retornar, após ser calculado pelo LibreOffice Calc, o valor de a^x. Então, em $D11$, vamos digitar a fórmula como se segue, $= D7\hat{}D9$ e clicamos na tecla ENTER no teclado do computador. O LibreOffice Calc nos retornará o resultado do cálculo da potência a^x.

Para obtermos o valor de k, selecionamos a célula $D13$ e digitamos $= SE(D7\hat{}D9 < 200000000; MOD((D7\hat{}D9); D5);$ "$Potencia\, excessiva$") e clicamos ENTER, ob-

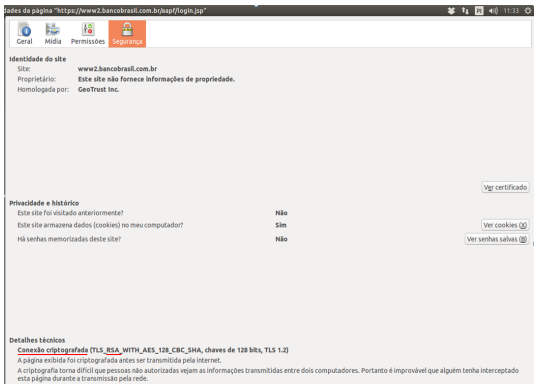
tendo o valor de k. Esta última fórmula nos diz que, se a potência que calculamos for menor do que 2.10^8 então calcule o resto da divisão desta potência pelo valor de módulo de p. Caso contrário, nos dê como resposta Potência excessiva.

Conforme dito anteriormente, esta calculadora irá nos auxiliar no cálculo de congruências das atividades que serão propostas.

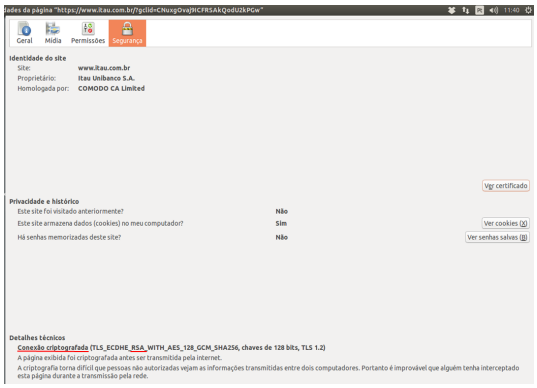
Capítulo 3

Métodos Criptográficos

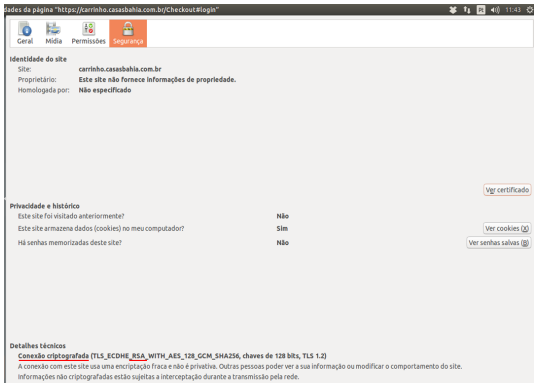
A criptografia é um excelente exemplo de aplicação da matemática pois está inserida no nosso cotidiano. Ela é utilizada, por exemplo, em transações bancárias via *internet*, na proteção de compras efetuadas *on line*, em sites do governo e no envio de mensagens via *whatsapp*.



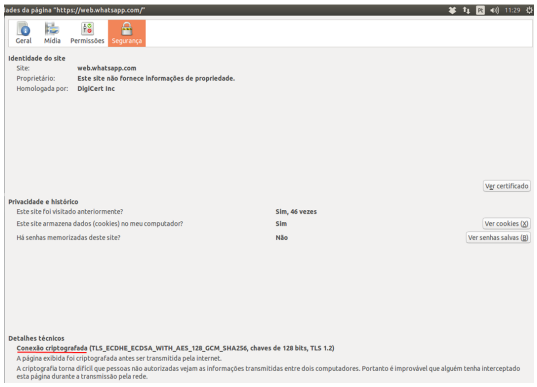
(a) Criptografia em transações bancárias



(b) Criptografia em transações bancárias



(c) Proteção de compras *on line*



(d) Mensagens via *whatsapp*

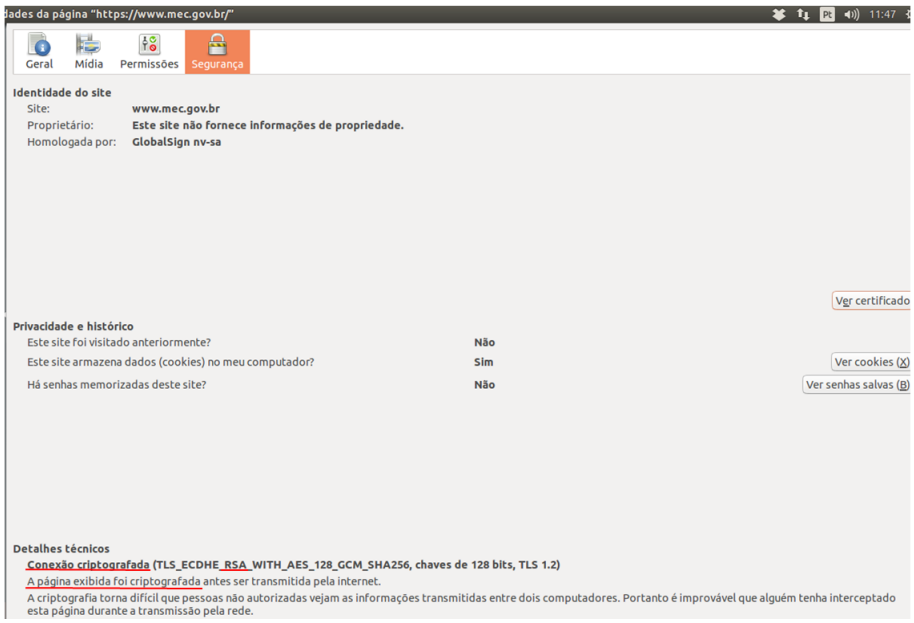


Figura 3.1: Sites do governo

Nesse sentido, o referido capítulo tem como objetivo apresentar três métodos criptográficos que podem ser utilizados para o ensino de Matemática no Nível Médio.

3.1 Introdução

Nesta seção iremos estudar o conceito de congruência para matrizes, a fim de que, ao final, sejamos capazes de entender o sistema criptográfico de Hill ou cifra de Hill. Para elaboração deste texto utilizamos as seguintes referências [5] e [22].

Definição 3.1.1 (Congruência entre Matrizes) *Sejam A e B matrizes $n \times k$ com entradas a_{ij} e b_{ij} inteiras e seja m um inteiro positivo. Dizemos que A é congruente a B módulo m e escrevemos $A \equiv B \pmod{m}$ se $a_{ij} \equiv b_{ij} \pmod{m}$ para todos $1 \leq i \leq n$ e $1 \leq j \leq k$.*

Caso contrário, escrevemos $A \not\equiv B \pmod{m}$.

Exemplo 3.1.1 *Observe que*

$$\begin{pmatrix} 5 & 17 & 9 \\ 4 & 15 & 8 \end{pmatrix} \equiv \begin{pmatrix} -2 & 3 & 2 \\ -3 & 1 & 1 \end{pmatrix} \pmod 7$$

pois, $5 \equiv -2 \pmod 7, 17 \equiv 3 \pmod 7, 9 \equiv 2 \pmod 7, 4 \equiv -3 \pmod 7, 15 \equiv 1 \pmod 7$ *e* $8 \equiv 1 \pmod 7$.

Já

$$\begin{pmatrix} 5 & 17 & 9 \\ 4 & 15 & 8 \end{pmatrix} \not\equiv \begin{pmatrix} -2 & 3 & 2 \\ -3 & 1 & 2 \end{pmatrix} \pmod 7$$

pois, $5 \equiv -2 \pmod 7, 17 \equiv 3 \pmod 7, 9 \equiv 2 \pmod 7, 4 \equiv -3 \pmod 7, 15 \equiv 1 \pmod 7$ *e* $8 \not\equiv 2 \pmod 7$.

Proposição 3.1.1 *Sejam A e B matrizes $n \times k$ com $A \equiv B \pmod m$, C uma matriz $k \times p$ e D uma matriz $p \times n$ todas com entradas inteiras. Então, $AC \equiv BC \pmod m$ e $DA \equiv DB \pmod m$.*

Demonstração: Sejam a_{ij} as entradas da matriz A e b_{ij} as entradas da matriz B com $1 \leq i \leq n$ e $1 \leq j \leq k$ e seja c_{ij} as entradas da matriz C, com $1 \leq i \leq k$ e $1 \leq j \leq p$. Observe que os elementos da i-ésima linha e j-ésima coluna das matrizes AC e BC são $\sum_{t=1}^{n} a_{it}c_{tj}$ e $\sum_{t=1}^{n} b_{it}c_{tj}$, respectivamente. Como $A \equiv B \pmod m$, temos $a_{it} \equiv b_{it} \pmod m$.

Logo, pelo teorema 2.4.2, $\sum_{t=1}^{n} a_{it}c_{tj} \equiv \sum_{t=1}^{n} b_{it}c_{tj}$ e, portanto $AC \equiv BC \pmod m$.

Analogamente se prova que $DA \equiv DB \pmod m$.

Definição 3.1.2 (Matriz Inversa) *Se A e A^{-1} são matrizes $n \times n$ com entradas inteiras tais que $A^{-1}A \equiv AA^{-1} \equiv I \pmod m$, onde $I = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$ é a matriz identidade de ordem n, então dizemos que A^{-1} é a matriz inversa da matriz A módulo m.*

Se A^{-1} é uma inversa módulo m da matriz A e $B \equiv A^{-1} \pmod m$, então pela proposição 3.1.1 B é uma inversa módulo m de A pois, $BA \equiv A^{-1}A \equiv I \pmod m$.

Se B_1 e B_2 são inversas módulo m da matriz A então $B_1 \equiv B_2 \pmod m$.

De fato:

Supondo B_1 e B_2 inversas módulo m da matriz A temos, pela proposição 3.1.1 que $B_1A \equiv B_2A \equiv I \pmod{m}$. Daí, temos que $B_1AB_1 \equiv B_2AB_1 \pmod{m}$. Sendo $AB_1 \equiv I \pmod{m}$, concluímos que $B_1 \equiv B_2 \pmod{m}$.

Exemplo 3.1.2 *Se*

$$\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}\begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 6 & 10 \\ 10 & 16 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{5}$$

e,

$$\begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} 11 & 25 \\ 5 & 11 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{5}$$

então a matriz $\begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix}$ *é uma inversa da matriz* $\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$ *módulo* 5.

A seguir enunciaremos uma proposição que nos mostra como obter, facilmente, a inversa de uma matriz 2×2 módulo m.

Proposição 3.1.2 *Sejam* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *uma matriz de números inteiros tais que* $\Delta = detA = ad - bc$ *e o inteiro positivo* m *são primos entre si. Então a matriz* $A^{-1} = \Delta^{-1}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, *onde* Δ^{-1} *é o inverso de* Δ *módulo* m, *é a matriz inversa de* A *módulo* m.

Demonstração: Para verificarmos que a matriz A^{-1} é uma inversa da matriz A módulo m, basta mostrarmos que $AA^{-1} \equiv A^{-1}A \equiv I \pmod{m}$. Assim, temos:

$$\begin{aligned}
AA^{-1} &\equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix}\Delta^{-1}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\
&\equiv \Delta^{-1}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\
&\equiv \Delta^{-1}\begin{pmatrix} ad-bc & 0 \\ 0 & -bc+ad \end{pmatrix} \\
&\equiv \Delta^{-1}\begin{pmatrix} \Delta & 0 \\ 0 & \Delta \end{pmatrix} \\
&\equiv \begin{pmatrix} \Delta^{-1}\Delta & 0 \\ 0 & \Delta^{-1}\Delta \end{pmatrix} \\
&\equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
&= I \pmod{m}
\end{aligned}$$

e,

$$\begin{aligned} A^{-1}A &\equiv \Delta^{-1}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &\equiv \Delta^{-1}\begin{pmatrix} ad-bc & 0 \\ 0 & -bc+ad \end{pmatrix} \\ &\equiv \Delta^{-1}\begin{pmatrix} \Delta & 0 \\ 0 & \Delta \end{pmatrix} \\ &\equiv \begin{pmatrix} \Delta^{-1}\Delta & 0 \\ 0 & \Delta^{-1}\Delta \end{pmatrix} \\ &\equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= I \pmod{m} \end{aligned}$$

Portanto, A^{-1} é uma inversa de A módulo m.

Exemplo 3.1.3 *Seja* $A = \begin{pmatrix} 3 & 2 \\ 2 & 2 \end{pmatrix}$. *Observe que* $detA = 2$ *e* 6 *é um inverso de* $detA = 2$ *módulo* 11. *Assim,*

$$A^{-1} \equiv 6\begin{pmatrix} 2 & -2 \\ -2 & 3 \end{pmatrix} \equiv \begin{pmatrix} 12 & -12 \\ -12 & 18 \end{pmatrix} \equiv \begin{pmatrix} 1 & 10 \\ 10 & 7 \end{pmatrix} \pmod{11}$$

é uma inversa da matriz A.

Proposição 3.1.3 *Se* A *é uma matriz de números inteiros* $n \times n$ *e* m *é um inteiro positivo, tais que* $(detA, m) = 1$ *então a matriz* $A^{-1} = \Delta^{-1}adj(A)$ *é uma inversa de* A *módulo* m, *onde* Δ^{-1} *é o inverso de* Δ *módulo* m.

Demonstração: Como $(detA, m) = 1$ temos que $detA \neq 0$. Assim, pelo teorema 2.6.1, temos:

$$A^{-1} = \frac{1}{detA}adj(A).$$

Multiplicando ambos os lados da igualdade acima por A, temos:

$$AA^{-1} = \frac{1}{detA}Aadj(A) = I.$$

Logo,

$$Aadj(A) = det(A)I.$$

Como $(detA, m) = 1$, existe $\Delta^{-1} = \Delta = detA$ que é o inverso de $\Delta = detA$ módulo m. Então:

$$A(\Delta^{-1}adj(A)) = A(adj(A)\Delta^{-1}) = (Aadj(A))\Delta^{-1} = \Delta I\Delta^{-1} = \Delta\Delta^{-1}I = I$$

e,

$$(\Delta^{-1}adj(A))A = \Delta^{-1}(adj(A)A) = \Delta^{-1}\Delta I = I.$$

Portanto, a matriz $A^{-1} = \Delta^{-1}adj(A)$ é uma inversa de A módulo m.

3.2 A Cifra de Hill

A n-cifra de Hill é um sistema de criptografia polialfabético, criado em 1929 por Lester S. Hill(1891-1961) e que consiste na cifragem da mensagem a ser enviada, quebrando-a em blocos de n letras, utilizando a multiplicação de matrizes. Caso o número de caracteres (letras) da mensagem a ser cifrada, desconsiderando os espaços entre as palavras, não seja múltiplo de n, completamos o último bloco com letras aleatórias, desde que estas letras não alterem o sentido da mensagem.

Figura 3.2: Lester S. Hill

Cada letra da mensagem a ser codificada será substituída pelo seu valor correspondente na tabela abaixo, que chamaremos tabela de conversão.

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

Tabela 3.1: Tabela de conversão

3.2.1 Cifrando uma mensagem utilizando a n-cifra de Hill

Para cifrar um texto qualquer, por exemplo, TEOREMA DE PITÁGORAS, utilizando a $2-$cifra de Hill, nesse caso, $n = 2$, procedemos da seguinte forma:

Passo 1: Como $n = 2$, escolhemos uma matriz $A_{2\times 2}$, de entradas inteiras em $\mathbb{Z}_{26}$, que será nossa matriz codificadora e que também tenha inversa módulo 26, conforme proposição 3.1.2.

Passo 2: Unimos todas as palavras do texto a ser cifrado desconsiderando os acentos e os espaços entre elas. Assim, teremos:

TEOREMADEPITAGORAS

Passo 3: A cada letra da palavra acima associaremos a um P_i, $i = 1, 2, \ldots, l$ onde l é a quantidade de letras do texto a ser cifrado, ou seja,

$$P_1 \to T,$$

$$P_2 \to E,$$

$$P_3 \to O,$$

$$P_4 \to R,$$

$$\vdots$$

$$P_{18} \to S.$$

Passo 4: Substituímos cada letra do texto comum pelo seu correspondente numérico na tabela 3.1, obtendo:

$$P_1 \to 19,$$

$$P_2 \to 4,$$

$$P_3 \to 14,$$

$$P_4 \to 17,$$

$$\vdots$$

$$P_{18} \to 18.$$

Passo 5: Como, no nosso caso, $n = 2$, agruparemos os $P_{i's}$ em pares P_1P_2, P_3P_4,

$P_5P_6, \ldots, P_{17}P_{18}$ e os converteremos em matrizes coluna,

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix}, \begin{pmatrix} P_3 \\ P_4 \end{pmatrix}, \begin{pmatrix} P_5 \\ P_6 \end{pmatrix}, \ldots, \begin{pmatrix} P_{17} \\ P_{18} \end{pmatrix}$$

2×1. Caso a quantidade de letras do texto original não seja múltiplo de n, acrescentamos, ao final do texto, letras aleatórias até completarem o último bloco, desde que estas letras não alterem o sentido da mensagem.

Passo 6: Efetuamos o produto AP, onde A é a matriz que foi escolhida no passo 1, por cada uma das matrizes coluna 2×1, obtidas no passo 5, que chamaremos de P. Em seguida, determinamos o correspondente numérico de $AP \pmod{26}$ obtendo, assim, seu correspondente cifrado

$$C = \begin{pmatrix} C_1 \\ C_2 \end{pmatrix}$$

da matriz coluna

$$P = \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}$$

2×1. Observe que, para cada par P_1P_2, P_3P_4, $P_5P_6, \ldots, P_{17}P_{18}$, obteremos, respectivamente, os seus correspondentes cifrados C_1C_2, C_3C_4, $C_5C_6, \ldots, C_{17}C_{18}$.

Passo 7: Agora, basta converter cada vetor cifrado no seu equivalente alfabético, conforme tabela 3.1.

Assim, para determinar o bloco cifrado, digamos C_1C_2 correspondente ao bloco P_1P_2 da mensagem a ser criptografada utilizaremos a relação:

$$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} \equiv A \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} mod(26) \tag{3.-12}$$

$$C \equiv APmod26$$

onde $C = \begin{pmatrix} C_1 \\ C_2 \end{pmatrix}$ é uma matriz 2×1, A é uma matriz de ordem 2 com $(detA, 26) = 1$ e $P = \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}$ é o bloco a ser cifrado.

Como exemplo, consideremos a mensagem:

CIFRA DE HILL

e consideremos $n = 3$.

A partir do passo a passo dado acima, temos:

Passo 1: Consideremos a matriz de cifragem

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 5 & 7 & 5 \\ 4 & 6 & 3 \end{pmatrix}$$

vemos que $detA = 7$ e, como $(detA, 26) = 1$ temos que 15 é o inverso de $detA$ módulo 26. Assim, pela proposição 3.1.3, a matriz inversa de A módulo 26 é:

$$A^{-1} = \begin{pmatrix} 21 & 24 & 17 \\ 23 & 21 & 20 \\ 4 & 4 & 7 \end{pmatrix}.$$

Passo 2: O texto a ser cifrado ficará da seguinte forma:

CIFRADEHILL

Passo 3:

$$P_1 \to C,$$

$$P_2 \to I,$$

$$P_3 \to F,$$

$$P_4 \to R,$$

$$P_5 \to A,$$

$$P_6 \to D,$$

$$P_7 \to E,$$

$$P_8 \to H,$$

$$P_9 \to I,$$

$$P_{10} \to L,$$

$$P_{11} \to L.$$

Passo 4:

$$P_1 \to 2,$$

$$P_2 \to 8,$$

$$P_3 \to 5,$$

$$P_4 \to 17,$$

$$P_5 \to 0,$$

$$P_6 \to 3,$$

$$P_7 \to 4,$$

$$P_8 \to 7,$$

$$P_9 \to 8,$$

$$P_{10} \to 11,$$

$$P_{11} \to 11.$$

Passo 5: Agrupando os $P_{i's}$, e convertendo em matrizes coluna 3×1, temos:

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix}, \begin{pmatrix} P_4 \\ P_5 \\ P_6 \end{pmatrix}, \begin{pmatrix} P_7 \\ P_8 \\ P_9 \end{pmatrix}, \begin{pmatrix} P_{10} \\ P_{11} \end{pmatrix}.$$

Observe que a última matriz coluna, é uma matriz 2×1 e não uma matriz 3×1, conforme dito anteriormente. Sendo assim, faz-se necessário acrescentar uma letra, por exemplo X, ao final do texto para completar o último bloco. Assim, a mensagem a ser criptografada será CIFRADEHILLX e, podemos notar que esta letra não altera o significado da mensagem.

Substituindo esta última letra pelo seu correspondente numérico, a última matriz coluna será:

$$\begin{pmatrix} P_{10} \\ P_{11} \\ P_{12} \end{pmatrix}.$$

Passo 6: Daí, criptografando o primeiro bloco da mensagem, obteremos:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 & 3 \\ 5 & 7 & 5 \\ 4 & 6 & 3 \end{pmatrix} \begin{pmatrix} 2 \\ 8 \\ 5 \end{pmatrix} mod(26) \equiv \begin{pmatrix} 7 \\ 13 \\ 19 \end{pmatrix} mod(26)$$

Para o segundo bloco, teremos:

$$\begin{pmatrix} C_4 \\ C_5 \\ C_6 \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 & 3 \\ 5 & 7 & 5 \\ 4 & 6 & 3 \end{pmatrix} \begin{pmatrix} 17 \\ 0 \\ 3 \end{pmatrix} mod(26) \equiv \begin{pmatrix} 0 \\ 22 \\ 25 \end{pmatrix} mod(26)$$

Para o terceiro bloco, temos:

$$\begin{pmatrix} C_7 \\ C_8 \\ C_9 \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 & 3 \\ 5 & 7 & 5 \\ 4 & 6 & 3 \end{pmatrix} \begin{pmatrix} 4 \\ 7 \\ 8 \end{pmatrix} mod(26) \equiv \begin{pmatrix} 16 \\ 5 \\ 4 \end{pmatrix} mod(26)$$

finalmente, para o quarto bloco, temos:

$$\begin{pmatrix} C_{10} \\ C_{11} \\ C_{12} \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 & 3 \\ 5 & 7 & 5 \\ 4 & 6 & 3 \end{pmatrix} \begin{pmatrix} 11 \\ 11 \\ 23 \end{pmatrix} mod(26) \equiv \begin{pmatrix} 24 \\ 13 \\ 23 \end{pmatrix} mod(26)$$

Logo, os blocos cifrados serão representados pelos números

7 13 19 0 22 25 16 5 4 24 13 23

Passo 7: Convertendo a mensagem cifrada em texto, obtemos:

GNT AWZ QFE YNX.

Que será a mensagem cifrada a ser enviada para o destinatário.

3.2.2 Decifrando uma mensagem utilizando a n-cifra de Hill

Para cada bloco da mensagem criptografada, o bloco decodificado será determinado pela relação

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \equiv A^{-1} \begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} \pmod{26} \tag{3.-11}$$

$$P \equiv A^{-1}C \pmod{26}$$

onde $P = \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix}$ é o bloco descriptografado; $C = \begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix}$ é o bloco cifrado e A^{-1} é a matriz inversa da matriz A. Agora, vamos dar um passo a passo de como decifrar uma mensagem utilizando a relação acima.

Passo 1: Obtemos a matriz inversa A^{-1} da matriz de cifragem, no nosso caso, da matriz A.

Passo 2: Efetuamos a multiplicação $A^{-1}C$ da matriz inversa A^{-1} por cada bloco C, matriz coluna, da mensagem cifrada e determinamos o correspondente numérico de $A^{-1}C$ módulo 26 obtendo assim, o bloco decodificado P da mensagem original.

Vamos agora decodificar a mensagem que foi codificada acima.

Como, $A^{-1} = \begin{pmatrix} 21 & 24 & 17 \\ 23 & 21 & 20 \\ 4 & 4 & 7 \end{pmatrix}$ é a inversa da matriz A módulo 26, obtemos, descriptografando o primeiro bloco da mensagem cifrada:

$$\begin{aligned} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} &\equiv A^{-1} \begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} mod(26) \\ &\equiv \begin{pmatrix} 21 & 24 & 17 \\ 23 & 21 & 20 \\ 4 & 4 & 7 \end{pmatrix} \begin{pmatrix} 7 \\ 13 \\ 19 \end{pmatrix} = \begin{pmatrix} 782 \\ 814 \\ 213 \end{pmatrix} \\ &\equiv \begin{pmatrix} 2 \\ 8 \\ 5 \end{pmatrix} mod(26). \end{aligned}$$

Descriptografando o segundo bloco, temos:

$$\begin{aligned}\begin{pmatrix} P_4 \\ P_5 \\ P_6 \end{pmatrix} &\equiv A^{-1}\begin{pmatrix} C_4 \\ C_5 \\ C_6 \end{pmatrix} mod(26) \\ &\equiv \begin{pmatrix} 21 & 24 & 17 \\ 23 & 21 & 20 \\ 4 & 4 & 7 \end{pmatrix}\begin{pmatrix} 0 \\ 22 \\ 25 \end{pmatrix} = \begin{pmatrix} 953 \\ 962 \\ 263 \end{pmatrix} \\ &\equiv \begin{pmatrix} 17 \\ 0 \\ 3 \end{pmatrix} mod(26).\end{aligned}$$

Para o terceiro bloco, obtemos:

$$\begin{aligned}\begin{pmatrix} P_7 \\ P_8 \\ P_9 \end{pmatrix} &\equiv A^{-1}\begin{pmatrix} C_7 \\ C_8 \\ C_9 \end{pmatrix} mod(26) \\ &\equiv \begin{pmatrix} 21 & 24 & 17 \\ 23 & 21 & 20 \\ 4 & 4 & 7 \end{pmatrix}\begin{pmatrix} 16 \\ 5 \\ 4 \end{pmatrix} = \begin{pmatrix} 524 \\ 553 \\ 112 \end{pmatrix} \\ &\equiv \begin{pmatrix} 4 \\ 7 \\ 8 \end{pmatrix} mod(26).\end{aligned}$$

E, para quarto bloco da mensagem:

$$\begin{aligned}\begin{pmatrix} P_{10} \\ P_{11} \\ P_{12} \end{pmatrix} &\equiv A^{-1}\begin{pmatrix} C_{10} \\ C_{11} \\ C_{12} \end{pmatrix} mod(26) \\ &\equiv \begin{pmatrix} 21 & 24 & 17 \\ 23 & 21 & 20 \\ 4 & 4 & 7 \end{pmatrix}\begin{pmatrix} 24 \\ 13 \\ 23 \end{pmatrix} = \begin{pmatrix} 1207 \\ 1285 \\ 309 \end{pmatrix} \\ &\equiv \begin{pmatrix} 11 \\ 11 \\ 23 \end{pmatrix} mod(26).\end{aligned}$$

Logo, o bloco descriptografado será:

2 8 5 17 0 3 4 7 8 11 11 23

e, com o auxílio da tabela de conversão, conseguimos ler a mensagem que nos foi enviada.

3.2.3 Quebrando a cifra de Hill

O teorema abaixo nos dá uma ideia de como proceder para quebrarmos a cifra de Hill sem que conheçamos a chave decodificadora. Antes de enunciarmos o referido teorema, vamos definir o que são operações elementares sobre linhas de uma matriz.

Definição 3.2.1 *Chamamos de operações elementares sobre linhas (colunas) de uma matriz A, as seguintes operações:*

i) A permutação de duas linhas (colunas) da matriz A.

ii) Efetuar a multiplicação de uma linha (coluna) da matriz por um escalar $\alpha \neq 0$, ou seja, sendo l_i esta linha, temos $l_i = \alpha l_i$.

iii) Somar a uma linha (coluna) da matriz um múltiplo de uma outra linha (coluna), ou seja, $l_i = l_i + \alpha l_j$, onde l_i e l_j são linhas da referida matriz.

Teorema 3.2.1 *Sejam $p_1, p_2, \cdots, p_n$ os n vetores linearmente independentes da mensagem original da n-cifra de Hill sendo desconhecida a matriz A e sejam $c_1, c_2, \cdots, c_n$ os vetores correspondentes do texto cifrado. Se,*

$$P = \left(\begin{array}{c|c|c|c} p_1 & p_2 & \cdots & p_n \end{array} \right)$$

é uma matriz de vetores coluna $p_1, p_2, \cdots, p_n$ e,

$$C = \left(\begin{array}{c|c|c|c} c_1 & c_2 & \cdots & c_n \end{array} \right)$$

é uma matriz de vetores coluna $c_1, c_2, \cdots, c_n$, então uma sequência de operações elementares sobre linhas que reduz C^T a matriz identidade I reduz P^T à matriz $(A^{-1})^T$ que é a transposta da matriz A^{-1}.

A demonstração deste teorema pode ser encontrada em [9].

3.3 Criptografia RSA

Iniciaremos nesta seção o estudo da criptografia RSA. Para elaboração deste texto foram utilizadas as referências [8] e [27].

A criptografia RSA é um sistema criptográfico de chave pública assimétrica baseado em funções matemáticas. Nesse sistema são utilizadas duas chaves relacionadas onde, qualquer uma das chaves pode ser usada para criptografar ou descriptografar a mensagem. Essas chaves são chamadas de chave pública ou chave de cifragem. A chave pública fica disponível para que qualquer usuário possa utilizá-la para criptografar suas mensagens e a chave privada ou chave de decodificação, que é de conhecimento somente do destinatário, fica disponível para que este possa descriptografar a mensagem que ele receber. Este sistema criptográfico foi desenvolvido pelos pesquisadores, Ron Rivest, Adi Shamir e Len Adleman, do laboratório de ciência da computação do *Massachusetts Intitute of Technology* - MIT, em 1977 e publicado em 1978. A partir daí, o RSA, que traz as iniciais dos nomes, Rivest, Shamir e Adleman, tem sido o criptossistema de chave pública mais utilizado até os dias de hoje, veja [27] "o desenvolvimento da criptografia de chave pública é a maior e talvez a única verdadeira revolução na história da criptografia" e isto se dá devido a impossibilidade, até o momento, de quebra da chave de decodificação pois, os algoritmos computacionais que existem não são eficientes para a fatoração de números inteiros, muito grandes, em fatores primos. Daí a necessidade de cada vez mais se descobrir números primos cada vez maiores.

Figura 3.3: Ron Rivest, Adi Shamir e Len Adleman

3.3.1 Codificando mensagens com o RSA

Para se utilizar o método RSA, primeiro devemos converter a mensagem a ser enviada em uma sequência de números onde, cada letra do nosso alfabeto será substituída pelo seu correspondente numérico, conforme tabela abaixo. Nesse método não faremos distinção entre letras maiúsculas e minúsculas e desconsideraremos também os acentos das palavras. Além disso, os espaços entre as palavras serão substituídos pelo número 99.

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

Tabela 3.2: Tabela de conversão para o método RSA

Observe que, ao escolhermos a representação de cada letra do nosso alfabeto por um algarismo de dois dígitos, estaremos evitando ambiguidades no momento da conversão da mensagem original em uma sequência numérica. Por exemplo, se na tabela acima a letra A fosse representada pelo número 1, a letra B pelo número 2 e assim por diante, teríamos que a letra L teria o mesmo correspondente numérico que AB, que nosso caso seria 12. Dessa forma, ao descriptografar a mensagem, não saberíamos se 12 é o correspndente numérico de AB ou da letra L.

Daremos agora um passo a passo de como criptografar mensagens utilizando o método RSA e logo após um exemplo de aplicação do referido método.

1) Convertemos a mensagem a ser criptografada em uma sequência numérica conforme a tabela de conversão para o método RSA.

2) Escolhemos dois números primos distintos quaisquer, suficientemente grandes, que chamaremos de p e q.

3) Determinamos n o primeiro parâmetro a ser utilizado na cifragem, de forma que $n = pq$.

4) Calculamos o valor de $\varphi(n)$ que é a função fi de Euler e, como $n = pq$, com p, q primos temos $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$.

5) Determinamos e o segundo parâmetro que será utilizado na codificação de tal forma que e seja relativamente primo com $\varphi(n)$, ou seja, $(e, \varphi(n)) = 1$ e $1 < e < \varphi(n)$.

6) Quebramos a mensagem em blocos de tamanho $M < n$.

7) Codificamos cada bloco da mensagem utilizando a seguinte relação:

$$C(b) \equiv b^e \pmod{n},$$

onde b é o bloco da mensagem original e $C(b)$ é o bloco cifrado.

Observação: O par (n, e) é a chave pública ou chave se cifragem.

Exemplo 3.3.1 *Vamos criptografar a mensagem Trabalhando com criptografia RSA.*

Seguindo os passos acima, teremos:

1) A sequência numérica ficará da seguinte forma:

$$292710111021171023132499122422991227182529241627101518109927 2810$$

2) Sejam $p = 17$ e $q = 19$.

3) $n = pq = 323$.

4) $\varphi(n) = \varphi(323) = (17 - 1)(19 - 1) = 288$.

5) Vamos considerar $e = 5$ e, observe que $(5, 288) = 1$.

6) Como $n = 323$, devemos quebrar a mensagem em blocos de tamanho aleatório, desde que o valor numérico de cada bloco seja menor do que $n = 323$. Assim, quebrando a mensagem em blocos, obtemos:

$$2 - 92 - 7 - 101 - 110 - 211 - 7 - 102 - 313 - 249 - 91 - 224 - 229 - 91$$

$$227 - 182 - 52 - 92 - 41 - 6 - 27 - 101 - 51 - 8 - 109 - 92 - 72 - 8 - 10$$

7) Para o primeiro bloco, ou seja, para $b = 2$, temos:

$$C(2) \equiv 2^5 \pmod{323}.$$

Logo, $C(2) = 32$.

Para o segundo bloco, $b = 92$, temos:

$$\begin{aligned} C(92) &\equiv 92^5 \pmod{323} \\ &\equiv 92^2 \times 92^2 \times 92 \pmod{323} \\ &\equiv 66 \times 66 \times 92 \pmod{323} \\ &\equiv 157 \times 92 \pmod{323} \\ &\equiv 232 \pmod{323}. \end{aligned}$$

Logo, $C(92) = 232$.

Para o terceiro bloco, $b = 7$, temos:

$$\begin{aligned} C(7) &\equiv 7^5 \pmod{323} \\ &\equiv 7^3 \times 7^2 \pmod{323} \\ &\equiv 20 \times 49 \pmod{323} \\ &\equiv 11 \pmod{323}. \end{aligned}$$

Logo, $C(7) = 11$.

Continuando com o mesmo raciocínio, obteremos a seguinte sequência de blocos codificados:

$$32-232-11-271-230-317-11-68-130-146-211-192-77-211-75$$

$$292-86-232-300-24-278-271-204-145-181-232-21-145-193$$

Dessa forma, a mensagem a ser enviada para o destinatário será:

$$32-232-11-271-230-317-11-68-130-146-211-192-77-211-75$$

$$292-86-232-300-24-278-271-204-145-181-232-21-145-193$$

3.3.2 Decifrando mensagens com o RSA

Para decodificar a mensagem que recebemos, iremos seguir um passo a passo, conforme fizemos para codificação da mensagem que nos foi enviada, em seguida, decodificaremos a mensagem codificada no exemplo acima.

1) Determinamos d, tal que $de \equiv 1 \pmod{\varphi(n)}$.

   Observe que o valor de d pode ser calculado utilizando o Algoritmo de

Euclides descrito na seção 2.1.1 na página 12.

2) Decodificamos cada bloco da mensagem utilizando a relação:

$$D(a) \equiv a^d \pmod{n},$$

onde a é um bloco da mensagem codificada.

Observação: O par (n, d) é a chave privada ou chave de decodificação.

Enunciaremos logo abaixo um teorema que garante que o algoritmo RSA funciona.

Teorema 3.3.1 *Sejam $C(b)$ um bloco qualquer da mensagem criptografada e $D(a)$ um bloco da mensagem decodificada. Então, $D(C(b)) = b$.*

Demonstração:

Das relações $C(b) \equiv b^e \pmod{n}$ e $D(a) \equiv a^d \pmod{n}$, temos:

$$D(C(b)) \equiv D(b^e) \equiv (b^e)^d \equiv b^{ed} \pmod{n} \tag{3.-32}$$

Como d é o inverso de e módulo $\varphi(n)$, temos que $ed \equiv 1 \pmod{\varphi(n)}$ e, daí que, existe um inteiro k tal que $ed = k\varphi(n) + 1$. Mas, $\varphi(n) = (p-1)(q-1)$. Assim, temos: $ed = k(p-1)(q-1) + 1$ e, substituindo em 3.3.2, temos:

$$D(C(b)) \equiv b^{k(p-1)(q-1)+1} \pmod{n} \tag{3.-32}$$

Como $n = pq$, temos:

$$D(C(b)) \equiv b^{k(p-1)(q-1)+1} \pmod{pq} \tag{3.-32}$$

Observe que, pelo fato de p e q serem primos, basta mostrar:

i) $b^{k(p-1)(q-1)+1} \equiv b \pmod{p}$

ii) $b^{k(p-1)(q-1)+1} \equiv b \pmod{q}$.

De fato:

i) Se $p \mid b$ então $0 \equiv b \equiv b^{k(p-1)(q-1)+1} \pmod{pq}$. O que mostra $D(C(b)) = b$.

Se $p \nmid b$ então pelo Pequeno Teorema de Fermat, temos:

$$b^{p-1} \equiv 1 \pmod{p}$$

e daí que,

$$(b^{p-1})^{k(q-1)} \equiv 1^{k^(q-1)} \equiv 1 \pmod{p}.$$

Multiplicando esta equivalência por b, obtemos

$$b^{k(p-1)(q-1)+1} \equiv b \pmod{p}.$$

Analogamente provamos ii).

Portanto, $D(C(b)) = b$ para todo bloco $C(b)$ da mensagem criptografada.

Exemplo 3.3.2 *Vamos descriptografar a mensagem*

$$32 - 232 - 11 - 271 - 230 - 317 - 11 - 68 - 130 - 146 - 211 - 192 - 77 - 211 - 75$$

$$292 - 86 - 232 - 300 - 24 - 278 - 271 - 204 - 145 - 181 - 232 - 21 - 145 - 193$$

que recebemos.

Seguindo o procedimento descrito acima, temos:

1) Sabemos que $n = 323$, $e = 5$ e $\varphi(323) = 288$. Daí, como $de \equiv 1 \pmod{\varphi(n)}$, temos $d = 173$.

   Utilizando o Algoritmo de Euclides, temos:

	57	1	1	2
$\varphi(323) = 288$	$e = 5$	3	2	1
3	2	1	0	

$$1 = 3 - 2.1 \tag{3.-32}$$

$$2 = 5 - 3.1 \tag{3.-32}$$

$$3 = 288 - 5.57 \tag{3.-32}$$

Substituindo 3.3.2 em 3.3.2, obtemos:

$$1 = 2.3 - 5 \tag{3.-32}$$

Agora, substituindo 3.3.2 em 3.3.2, encontramos:

$$1 = 2.288 + 5(-115) \tag{3.-32}$$

Como $173 \equiv -115 \pmod{288}$, temos que 3.3.2 é equivalente, módulo 288, a

$$1 = 2.288 + 5.173 \tag{3.-32}$$

Logo, $d = 173$ é o inverso de e módulo 288.

2) Decodificando o primeiro bloco, $D(32) = 32^{173}$, da mensagem, temos:

$$\begin{aligned}
D(32) &\equiv 32^{173} \pmod{323} \\
&\equiv [(32)^2]^{86} \times 32 \\
&\equiv 55^{86} \times 32 \\
&\equiv [(55)^2]^{43} \times 32 \\
&\equiv 118^{43} \times 32 \\
&\equiv [(118)^2]^{21} \times 118 \times 32 \\
&\equiv 35^{21} \times 118 \times 32 \\
&\equiv [(35)^2]^{10} \times 35 \times 118 \times 32 \\
&\equiv 256^{10} \times 35 \times 118 \times 32 \\
&\equiv [(256)^2]^5 \times 35 \times 118 \times 32 \\
&\equiv 290^5 \times 53 \\
&\equiv [(290)^2]^2 \times 290 \times 53 \\
&\equiv 120^2 \times 290 \times 53 \\
&\equiv 188 \times 290 \times 53 \\
&\equiv 2
\end{aligned}$$

Portanto, $D(32) = 2$.

Procedendo de forma análoga para todos os outros blocos da mensagem criptografada, determinaremos os blocos da mensagem original e, com o auxílio da tabela de conversão, conseguiremos ler a mensagem que nos foi enviada.

3.3.3 Por que o RSA é seguro?

Sabemos que para criptografar a mensagem, necessitamos dos parâmetros n e e, que são parâmetros públicos acessíveis a qualquer usuário, onde $n = pq$ com p e q primos suficientemente grandes. Já, para decodificar uma mensagem, precisamos dos parâmetros d e e. Mas para calcular d precisamos saber quem é $\varphi(n)$ e, para calcularmos $\varphi(n)$ é preciso fatorar n.

Sabemos que $n = pq$. Temos:

$$\begin{aligned} \varphi(n) &= (p-1)(q-1) \\ &= pq - p - q + 1 \\ &= n - (p+q) + 1 \end{aligned}$$

Daí, temos $p + q = n + 1 - \varphi(n)$ e $n = pq$. Logo, p e q são raízes da equação do segundo grau $x^2 - (n + 1 - \varphi(n)) + n = 0$. O que nos mostra que precisamos fatorar n para determinar $\varphi(n)$.

Assim, a dificuldade da quebra do código RSA está na dificuldade em se fatorar o número n. Como até o momento não existem algoritmos rápidos e eficientes de fatoração para o caso de n ser suficientemente grande, a segurança do RSA estará garantida quanto maior forem os primos p e q.

3.4 Criptografia ElGamal

O criptosistema ElGamal é um algoritmo de chave pública, criado pelo egípcio Taher ElGamal em 1984 e se baseia no problema do logaritmo discreto. A segurança do referido criptosistema advém da dificuldade em se calcular logaritmos discretos de um grupo cíclico finito.

Antes de mostrarmos como criptografar utilizando o criptosistema ElGamal, apresentaremos as definições e alguns exemplos para calcular o logaritmo discreto de um grupo $(\mathbb{Z}_p^*, .)$.

3.4.1 Logaritmos Discretos

Definição 3.4.1 *Sejam $a, b \in \mathbb{Z}_p^*$ com $b \equiv a^n \pmod{p}, 0 \leqslant n \leqslant p-1$. Dizemos que n é o logaritmo discreto de b na base a módulo p e escrevemos $n = \log_a(b)$.*

Exemplo 3.4.1 *Do exemplo 2.5.1, temos:*

$$2^1 \equiv 2 \pmod{5}$$

$$2^2 \equiv 4 \pmod{5}$$

$$2^3 \equiv 3 \pmod{5}$$

$$2^4 \equiv 1 \pmod{5}.$$

E, daí que, $\log_2(2) \pmod{5} = 1$; $\log_2(4) \pmod{5} = 2$; $\log_2(3) \pmod{5} = 3$; $\log_2(1) \pmod{5} = 4$.

Observação 3.4.1

i) Como $\langle \overline{2} \rangle = (\mathbb{Z}_5^*, .)$ e, portanto uma raiz primitiva de $\mathbb{Z}_5^*$, para todo $a \in \mathbb{Z}_5^*$ podemos encontrar seu logaritmo discreto.

ii) Se $\overline{\alpha} \in \mathbb{Z}_5^*$ não é uma raiz primitiva de $\mathbb{Z}_5^*$ então, nem sempre existe o seu logaritmo discreto. Considere, por exemplo, $\overline{4} \in \mathbb{Z}_5^*$. Temos que $\log_4(3)$ *não existe pois, $n \in \mathbb{Z}$ tal que* $4^n \equiv 3 \pmod{5}$.

Vejamos agora como criptografar uma mensagem utilizando o algoritmo ElGamal.

3.4.2 Geração de chaves

Para gerarmos as chaves que serão utilizadas para criptografar uma mensagem, seguiremos os seguintes passos:

1) Primeiro escolhemos um primo p suficientemente grande e um gerador a do grupo multiplicativo $\mathbb{Z}_p^*$ dos inteiros módulo p.

2) Escolhemos a chave privada b, com $b \in \mathbb{Z}_p^*$ tal que $1 < b < p-1$.

3) Agora, para determinarmos a chave pública, calculamos $\alpha \equiv a^b \pmod{p}$. Assim, a chave pública é (p, a, α).

3.4.3 Criptografando uma mensagem

De posse da chave pública, qualquer pessoa poderá enviar uma mensagem criptografada para o detentor da chave privada.

Com a chave pública, (p, a, α), em mãos, para criptografar uma mensagem M, procedemos da seguinte forma:

1) Após converter a mensagem em uma sequência numérica, quebramos a referida mensagem em um conjunto de inteiros $(m_1, m_2, \ldots, m_r)$ onde $1 \leq m_i \leq p-1$, com $1 \leq i \leq r$. Os inteiros $m_1, m_2, \ldots, m_r$ serão codificados um a um.

2) Para criptografar uma mensagem, o emissor escolhe um inteiro x, com $1 \leq x \leq p-2$ para ser sua chave particular e, a partir dessa chave, calcula $\beta \equiv a^x \pmod{p}$.

3) Para criptografar cada bloco $m_1, m_2, \ldots, m_r$ da mensagem M, basta calcular $\gamma_i \equiv m_i.\alpha^x \pmod{p}, 1 \leq i \leq r$. A mensagem cifrada a ser enviada para o destinatário será os conjuntos de pares $(\beta, \gamma_i), 1 \leq i \leq r$.

3.4.4 Descriptografando uma mensagem

Após receber os conjuntos de pares $(\beta, \gamma_i), 1 \leq i \leq r$, para descriptografá-los, basta seguir os seguintes passos:

1) Para cada par $(\beta, \gamma_i), 1 \leq i \leq r$, calcula-se $y \equiv \beta^{p-1-b} \pmod{p}$. Nesse passo, o receptor da mensagem criptografada está usando a chave privada b.

2) Para descriptografar a mensagem, basta calcular, para cada γ_i, $m_i \equiv y.\gamma_i \pmod{p}$, com $1 \leq i \leq r$, que obteremos a mensagem M.

Observe que, para todo par (β, γ_i) da mensagem codificada,

$$m_i \equiv y.\gamma_i,$$

para todo $1 \leq i \leq r$.

De fato:

$$y \equiv \beta^{p-1-b} \equiv \beta^{p-1}\beta^{-b} \pmod{p}.$$

Pelo corolário 2.4.1, temos:

$$\beta^{p-1} \equiv 1 \pmod{p}$$

e, como

$$\beta \equiv a^x \pmod{p},$$

temos:

$$y \equiv \beta^{-b} \equiv (a^x)^{-b} \equiv a^{-bx} \pmod{p}.$$

Daí, como $\alpha \equiv a^b \pmod{p}$, temos:

$$\begin{aligned} y.\gamma_i &\equiv a^{-bx} m_i.\alpha^x \pmod{p} \\ &\equiv a^{-bx} m_i.(a^b)^x \pmod{p} \\ &\equiv m_i \end{aligned}$$

Logo, $m_i \equiv y.\gamma_i$, para todo $1 \leq i \leq r$.

Exemplo 3.4.2 *Vamos criptografar e descriptografar a palavra AMOR.*

Seguindo os passos acima para gerar a chave pública, temos:

1) Vamos escolher um primo $p = 29$. Assim, estaremos trabalhando com o grupo $\mathbb{Z}_{29}^* = \{\overline{1}, \overline{2}, \overline{3}, \ldots, \overline{28}\}$ e consideremos o número $a = 3$ que é um dos geradores deste grupo.

2) Tomemos $b = 10$ para ser a chave privada.

3) Calculando $a^b = 3^{10} \equiv 5 \pmod{29}$, temos que $\alpha = 5$. Logo, a chave pública é $(29, 3, 5)$.

Criptografando a mensagem:

1) A mensagem, convertida em uma sequência numérica, de acordo com a tabela 3.2 será, $10 - 22 - 24 - 27$, one $m_1 = 10, m_2 = 22, m_3 = 24$ e $m_4 = 27$.

2) Seja $x = 13$ uma outra chave particular, temos:

$$a^x = 3^{13} \equiv 19 \pmod{29}.$$

Logo, $\beta = 19$.

3) Criptografando cada bloco da mensagem, temos:

$m_1.\alpha^x = 10.5^{13} \equiv 2 \pmod{29}$.

Logo, $\gamma_1 = 2$.

$m_2.\alpha^x = 22.5^{13} \equiv 16 \pmod{29}$.

Logo, $\gamma_2 = 16$.

$m_3.\alpha^x = 24.5^{13} \equiv 28 \pmod{29}$.

Logo, $\gamma_3 = 28$.

$m_4.\alpha^x = 27.5^{13} \equiv 17 \pmod{29}$.

Logo, $\gamma_4 = 17$.

Portanto, os conjuntos de pares a serem enviados ao destinatário serão

$$(19, 2); (19, 16); (19, 28); (19, 17).$$

Descriptografando a mensagem:

1) Calculando $\beta^{p-1-b} = 19^{29-1-10} = 19^{18} \equiv 5 \pmod{29}$. Logo, $y = 5$.

2) Para o primeiro par:

$y.\gamma_1 = 5.2 \equiv 10 \pmod{29}$.

Logo, $m_1 = 10$.

Para o segundo par:

$y.\gamma_2 = 5.16 \equiv 22 \pmod{29}$.

Logo, $m_2 = 22$.

Para o terceiro par:

$y.\gamma_3 = 5.28 \equiv 24 \pmod{29}$.

Logo, $m_3 = 24$.

Para o quarto bloco:

$y.\gamma_4 = 5.17 \equiv 27 \pmod{29}$.

Logo, $m_4 = 27$.

Portanto a sequência numérica descriptografada é $10 - 22 - 24 - 27$ que, substituindo pelo corresponte na tabela 3.2, obtemos a palavra AMOR.

3.5 Ataques ao Criptossistema ElGamal

Os possíveis ataques ao criptossistema ElGamal, estão relacionados em tentar recuperar a chave particular x ou forjar assinaturas sem recuperar a chave particular x.

Para mais detalhes de como recuperar a chave particular e como forjar assinaturas, vide [10].

Capítulo 4

Aplicações em Sala de Aula

As atividades desenvolvidas neste capítulo foram elaboradas para serem trabalhadas com alunos da segunda série do Ensino Médio. Tal fato se deve pois, em algumas atividades, exige-se o conhecimento prévio dos alunos de outros conteúdos que foram ministrados no ano anterior e de conteúdos que são desenvolvidos a partir da segunda série do Nível Médio.

4.1 Atividades referentes à Congruência

Atividade 1

Questão 8 - 1ª Fase - OBMEP-2013:

Marcos fez cinco provas de Matemática. Suas notas, em ordem crescente, foram 75, 80, 84, 86 e 95. Ao digitar as notas de Marcos na ordem em que as provas foram realizadas, o professor notou que as médias das duas primeiras provas, das três primeiras, das quatro primeiras e das cinco provas eram números inteiros. Qual foi a nota que Marcos tirou na última prova?

A) 75

B) 80

C) 84

D) 86

E) 95

Solução:

Para a média das três e das quatro primeiras notas, vamos analisar os restos das divisões das cinco notas por três e por quatro, respectivamente. Temos:

$$75 \equiv 0 \pmod 3, \textit{ deixa resto } 0 \textit{ quando dividido por } 3;$$

$$80 \equiv 2 \pmod 3, \textit{ deixa resto } 2 \textit{ quando dividido por } 3;$$

$$84 \equiv 0 \pmod 3, \textit{ deixa resto } 0 \textit{ quando dividido por } 3;$$

$$86 \equiv 2 \pmod 3, \textit{ deixa resto } 2 \textit{ quando dividido por } 3;$$

$$95 \equiv 2 \pmod 3, \textit{ deixa resto } 2 \textit{ quando dividido por } 3.$$

Para determinar quais são as três primeiras notas basta somar os restos das divisões feitas acima e verificar se esta soma é divisível por três. Após esta análise observamos que as três primeiras notas são, não necessariamente nessa ordem, 80, 86 e 95.

$$75 \equiv 3 \pmod 4, \textit{ deixa resto } 3 \textit{ quando dividido por } 4;$$

$$80 \equiv 0 \pmod 4, \textit{ deixa resto } 0 \textit{ quando dividido por } 4;$$

$$84 \equiv 0 \pmod 4, \textit{ deixa resto } 0 \textit{ quando dividido por } 4;$$

$$86 \equiv 2 \pmod 4, \textit{ deixa resto } 2 \textit{ quando dividido por } 4;$$

$$95 \equiv 3 \pmod 4, \textit{ deixa resto } 3 \textit{ quando dividido por } 4.$$

Somando os restos das divisões por 4, verificamos que, as quatro primeiras notas são, não necessariamente nessa ordem, 75, 80, 86 e 95.

Portanto, a última nota que Marcos tirou na prova foi 84.

Alternativa C.

Atividade 2

Problema 4.3 - página 83 [15]:

Mostre que $10^n \equiv 1 \pmod 9$, para todo número natural n.

Solução:

O teorema 2.4.3 nos afirma que $10^n \equiv 1 \pmod 9$. Vamos então mostrar isso.

Queremos mostrar que $9 \mid 10^n - 1$, ou seja, que $10^n - 1$ é um múltiplo de 9. Temos:

$$10^n - 1 = 1\underbrace{000\ldots00}_{n \text{ zeros}} - 1 = \underbrace{999\ldots999}_{n \text{ vezes}} = 9 \times \underbrace{111\ldots111}_{n \text{ vezes}}.$$

Portanto, $9 \mid 10^n - 1$.

Atividade 3

Exercício:

Mostre que $3^{18} - 2^{18}$ é divisível por 7.

Solução:

Temos:

$$3^{18} = (3^3)^6 \equiv (-1)^6 \equiv 1 \pmod 7$$

Observe que usamos a letra c do teorema 2.4.1 pois,

$$28 \equiv 0 \pmod 7 \Rightarrow 28 - 1 = 27 \equiv 0 - 1 = -1 \pmod 7$$

e,

$$2^{18} = (2^3)^6 \equiv (-1)^6 \equiv 1 \pmod 7$$

pelo mesmo teorema citado acima.

Logo, $3^{18} - 2^{18} \equiv 1 - 1 = 0 \pmod 7$ e, portanto, $3^{18} - 2^{18}$ é divisível por 7.

4.2 Atividades referentes à Cifra de Hill

Estas atividades deverão ser apresentadas para alunos do segundo ano do Ensino Médio e tem por objetivo despertar o interesse nos alunos para o estudo de Matrizes. Além disso, poderão ser utilizadas para a fixação das operações com Matrizes. A sugestão é que se divida a sala em grupos para que um grupo possa criptografar a mensagem e o outro grupo possa descriptografá-la.

Atividade 1

Criptografe a mensagem *Vai chover hoje* utilizando a 2-cifra de Hill e a matriz de cifragem $A = \begin{pmatrix} 3 & 3 \\ 1 & 2 \end{pmatrix}$.

Grupo 1 - Criptografando uma mensagem: Passo a passo

Passo 1- Os alunos deverão quebrar a mensagem em blocos de duas letras. Eles deverão observar que será necessário acrescentar a letra X ao final do último bloco.

Passo 2- Converter a mensagem acima em uma sequência numérica de acordo com a tabela 3.1.

A sequência numérica que eles deverão obter será:

21 0 8 2 7 14 21 4 17 7 14 9 4 23

Passo 3- Converter a sequência numérica em matrizes coluna 2×1.

Passo 4- Após efetuarem o cálculo do determinante da matriz A, eles deverão chegar ao resultado esperado, a saber, $detA = 3$ e concluírem que a matriz possui inversa A^{-1} pois, $(detA, 26) = 1$ podendo então, criptografar a mensagem utilizando a referida matriz.

Passo 5- Cifrar a mensagem através da relação 3.-12.

Passo 6- Converter a mensagem cifrada em texto, conforme tabela 3.1.

Passo 7- Enviar a mensagem cifrada para o outro grupo a fim de eles possam descriptografá-la.

Grupo 2 - Descriptografando uma mensagem: Passo a passo

Passo 1- Converter o texto cifrado em uma sequência numérica, conforme tabela 3.1.

Passo 2- Tendo em mãos a matriz A, verificar, após efetuarem o cálculo do determinante da matriz A, que a matriz possui inversa A^{-1} pois, $(detA, 26) = 1$.

Passo 3- Determinar o inverso de $detA$ módulo 26.

Passo 4- Determinar a inversa da matriz A utilizando a proposição 3.1.2.

Passo 5- Descriptografar a mensagem através da relação 3.-11.

Passo 6- Converter a mensagem decodificada em texto, conforme tabela 3.1.

Passo 7- Ler a mensagem.

Atividade 2

João recebeu a seguinte mensagem criptografada:

DG TA LI BT KJ.

Sabendo que a matriz de cifragem utilizada foi a matriz $A = \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix}$, obtenha a mensagem original.

Resolução da atividade

Passo 1- Converter o texto cifrado em uma sequência numérica, conforme tabela 3.1.

Passo 2- Tendo em mãos a matriz A, verificar, após efetuarem o cálculo do determinante da matriz A, que a matriz possui inversa A^{-1} pois, $(detA, 26) = 1$.

Passo 3- Determinar o inverso de $detA$ módulo 26.

Passo 4- Determinar a inversa da matriz A utilizando a proposição 3.1.2.
Os alunos deverão obter $A^{-1} = \begin{pmatrix} 5 & 11 \\ 16 & 5 \end{pmatrix} \pmod{26}$.

Passo 5- Descriptografar a mensagem através da relação 3.-11.

Passo 6- Converter a mensagem decodificada em texto, conforme tabela 3.1.
A mensagem decodificada deverá ser a seguinte:

DA RK NI GH TX.

Passo 7- Ler a mensagem.

DARK NIGHT.

4.3 Atividades envolvendo a criptografia RSA

Atividade 1

Determine o inverso de 3 módulo 127 utilizando o Algoritmo de Euclides.

Solução:

Utilizando o Algoritmo de Euclides, temos:

	42	3
127	3	1
1	0	

Temos:

$$1 = 127 + 3.(-42) \tag{4.0}$$

Como $85 \equiv -42 \pmod{127}$, temos que 4.3 é equivalente, módulo 127, a

$$1 = 127 + 3.85 \tag{4.0}$$

Logo, 85 é o inverso de 3 módulo 127.

Atividade 2

Determine o inverso de 5 módulo 127 utilizando o Algoritmo de Euclides.

Solução:

Utilizando o Algoritmo de Euclides, temos:

	25	2	2
127	5	2	1
2	1	0	

Assim,

$$1 = 5 - 2.2 \tag{4.0}$$

$$2 = 127 - 5.25 \tag{4.0}$$

Substituindo a equação 4.3 na equação 4.3, temos:

$$1 = 127.(-2) + 5.51 \tag{4.0}$$

Logo, 51 é o inverso de 5 módulo 127.

Atividade 3

Nesta atividade sugerimos que se divida a sala em grupos para que um grupo possa criptografar a mensagem e o outro grupo possa descriptografá-la. Sugerimos ainda que o professor esteja atento aos alunos para que eles façam, com muita atenção o passo a passo.

Criptografe a mensagem **BOM DIA** utilizando os primos $p = 7$ e $q = 11$.

Grupo 1 - Criptografando uma mensagem: Passo a passo

Passo 1- Os alunos deverão converter a mensagem na sequência numérica,

$$11242299131810,$$

conforme a tabela 3.2.

Passo 2- Com os primos $p = 7$ e $q = 11$ em mãos, determinar o parâmetro de cifragem $n = pq = 77$.

Passo 3- Calcular a função $\varphi(n) = \varphi(pq) = (p-1)(q-1) = 60$.

Passo 4- Determinar o parâmetro ϵ de tal forma que $(\epsilon, \varphi(n)) = 1$, com $1 < \epsilon < \varphi(n)$. Para facicitar os cálculos, podemos considerar $\epsilon = 7$.

Passo 5- Quebra-se a mensagem em blocos de tamanho $M < n = 77$. Um exemplo de como podemos quebrar a referida mensagem é dado abaixo:

$$11 - 2 - 42 - 29 - 9 - 13 - 18 - 10$$

Passo 6- Codificamos a mensagem de acordo com a relação

$$C(b) \equiv b^e \pmod{n}.$$

Para os blocos acima, temos:

$$\begin{aligned} C(11) &\equiv 11^7 \pmod{77} \\ &\equiv 11^2 \times 11^2 \times 11^2 \times 11 \pmod{77} \\ &\equiv 44 \times 44 \times 44 \times 11 \pmod{77} \\ &\equiv 11 \times 44 \times 11 \pmod{77} \\ &\equiv 44 \times 44 \pmod{77} \\ &\equiv 11 \pmod{77} \end{aligned}$$

Logo, $C(11) = 11$.

$$\begin{aligned} C(2) &\equiv 2^7 \pmod{77} \\ &\equiv 128 \pmod{77} \\ &\equiv 51 \pmod{77}. \end{aligned}$$

Logo, $C(2) = 51$.

$$\begin{aligned} C(42) &\equiv 42^7 \pmod{77} \\ &\equiv 42^2 \times 42^2 \times 42^2 \times 42 \pmod{77} \\ &\equiv 70 \times 70 \times 70 \times 42 \pmod{77} \\ &\equiv 49 \times 70 \times 42 \pmod{77} \\ &\equiv 42 \times 42 \pmod{77} \\ &\equiv 70 \pmod{77} \end{aligned}$$

Logo, $C(42) = 70$.

$$\begin{aligned} C(29) &\equiv 29^7 \pmod{77} \\ &\equiv 29^2 \times 29^2 \times 29^2 \times 29 \pmod{77} \\ &\equiv 71 \times 71 \times 71 \times 29 \pmod{77} \\ &\equiv 36 \times 71 \times 29 \pmod{77} \\ &\equiv 15 \times 29 \pmod{77} \\ &\equiv 50 \pmod{77} \end{aligned}$$

Logo, $C(29) = 50$.

$$\begin{aligned} C(9) &\equiv 9^7 \pmod{77} \\ &\equiv 9^2 \times 9^2 \times 9^2 \times 9 \pmod{77} \\ &\equiv 4 \times 4 \times 4 \times 9 \pmod{77} \\ &\equiv 37 \pmod{77} \end{aligned}$$

Logo, $C(9) = 37$.

$$\begin{aligned} C(13) &\equiv 13^7 \pmod{77} \\ &\equiv 13^2 \times 13^2 \times 13^2 \times 13 \pmod{77} \\ &\equiv 15 \times 15 \times 15 \times 13 \pmod{77} \\ &\equiv 71 \times 15 \times 13 \pmod{77} \\ &\equiv 64 \times 13 \pmod{77} \\ &\equiv 62 \pmod{77} \end{aligned}$$

Logo, $C(13) = 62$.

$$\begin{aligned} C(18) &\equiv 18^7 \pmod{77} \\ &\equiv 18^2 \times 18^2 \times 18^2 \times 18 \pmod{77} \\ &\equiv 16 \times 16 \times 16 \times 18 \pmod{77} \\ &\equiv 25 \times 16 \times 18 \pmod{77} \\ &\equiv 15 \times 18 \pmod{77} \\ &\equiv 39 \pmod{77} \end{aligned}$$

Logo, $C(18) = 39$.

$$\begin{aligned} C(10) &\equiv 10^7 \pmod{77} \\ &\equiv 10^2 \times 10^2 \times 10^2 \times 10 \pmod{77} \\ &\equiv 23 \times 23 \times 23 \times 10 \pmod{77} \\ &\equiv 67 \times 23 \times 10 \pmod{77} \\ &\equiv 1 \times 10 \pmod{77} \\ &\equiv 10 \pmod{77} \end{aligned}$$

Logo, $C(10) = 10$.

Passo 7- Enviar a mensagem criptografada para o destinatário.

A mensagem a ser envada será:

$$11 - 51 - 70 - 50 - 37 - 62 - 39 - 10.$$

Grupo 2 - Decifrando uma mensagem: Passo a passo

Passo 1- Determinar d, o inverso de ϵ módulo $\varphi(n)$, ou seja, $d\epsilon \equiv 1 \pmod{\varphi(77)}$. Assim, como $\epsilon = 7$ e $\varphi(77) = 60$, temos: $7d \equiv 1 \pmod{60}$, e daí que $d = 43$ pois, $7 \times 43 = 301 = 5 \times 60 + 1$.

Utilizando o Algoritmo de Euclides, temos:

	8	1	1	3
$\varphi(77) = 60$	$\epsilon = 7$	4	3	1
4	3	1	0	

$$1 = 4 - 3.1 \tag{4.-42}$$

$$3 = 7 - 4.1 \tag{4.-41}$$

$$4 = 60 - 7.8 \tag{4.-40}$$

Substituindo 4.-41 em 4.-42, obtemos:

$$1 = 4.2 - 7 \tag{4.-39}$$

Agora, substituindo 4.-40 em 4.-39, encontramos:

$$1 = 2.60 + 7(-17) \tag{4.-38}$$

Como $43 \equiv -17 \pmod{60}$, temos que 4.-38 é equivalente, módulo 60, a

$$1 = 2.60 + 7.43 \tag{4.-37}$$

Logo, $d = 43$ é o inverso de ϵ módulo 60.

Passo 2- Decodificamos a mensagem de acordo com a relação

$$D(a) \equiv a^d \pmod{n}.$$

$$\begin{aligned} D(11) &\equiv 11^{43} \pmod{77} \\ &\equiv [(11)^7]^6 \times 11 \pmod{77} \\ &\equiv 11^6 \times 11 \pmod{77} \\ &\equiv 11^7 \pmod{77} \\ &\equiv 11 \pmod{77} \end{aligned}$$

Logo, $D(11) = 11$.

$$\begin{aligned} D(51) &\equiv 51^{43} \pmod{77} \\ &\equiv [(51)^3]^{14} \times 51 \pmod{77} \\ &\equiv 57^{14} \times 51 \pmod{77} \\ &\equiv (57^2)^7 \times 51 \pmod{77} \\ &\equiv 15^7 \times 51 \pmod{77} \\ &\equiv (15^2)^3 \times 15 \times 51 \pmod{77} \\ &\equiv 71^3 \times 15 \times 51 \pmod{77} \\ &\equiv 15 \times 15 \times 51 \pmod{77} \\ &\equiv 71 \times 51 \pmod{77} \\ &\equiv 2 \pmod{77} \end{aligned}$$

Logo, $D(51) = 2$.

$$\begin{aligned} D(70) &\equiv 70^{43} \pmod{77} \\ &\equiv [(70)^3]^{14} \times 70 \pmod{77} \\ &\equiv 42^{14} \times 70 \pmod{77} \\ &\equiv (42^2)^7 \times 70 \pmod{77} \\ &\equiv 70^7 \times 70 \pmod{77} \\ &\equiv (70^2)^3 \times 70 \times 70 \pmod{77} \\ &\equiv 49^3 \times 49 \pmod{77} \\ &\equiv 49^2 \times 49^2 \pmod{77} \\ &\equiv 14 \times 14 \pmod{77} \\ &\equiv 42 \pmod{77} \end{aligned}$$

Logo, $D(70) = 42$.

$$\begin{aligned}
D(50) &\equiv 50^{43} \pmod{77} \\
&\equiv [(50)^3]^{14} \times 50 \pmod{77} \\
&\equiv 29^{14} \times 50 \pmod{77} \\
&\equiv (29^2)^7 \times 50 \pmod{77} \\
&\equiv 71^7 \times 50 \pmod{77} \\
&\equiv (71^3)^2 \times 71 \times 50 \pmod{77} \\
&\equiv 15^2 \times 71 \times 50 \pmod{77} \\
&\equiv 71 \times 71 \times 50 \pmod{77} \\
&\equiv 36 \times 50 \pmod{77} \\
&\equiv 29 \pmod{77}
\end{aligned}$$

Logo, $D(50) = 29$.

$$\begin{aligned}
D(37) &\equiv 37^{43} \pmod{77} \\
&\equiv [(37)^3]^{14} \times 37 \pmod{77} \\
&\equiv 64^{14} \times 37 \pmod{77} \\
&\equiv (64^2)^7 \times 37 \pmod{77} \\
&\equiv 15^7 \times 37 \pmod{77} \\
&\equiv (15^2)^3 \times 15 \times 37 \pmod{77} \\
&\equiv 71^3 \times 15 \times 37 \pmod{77} \\
&\equiv 15 \times 15 \times 37 \pmod{77} \\
&\equiv 71 \times 37 \pmod{77} \\
&\equiv 9 \pmod{77}
\end{aligned}$$

Logo, $D(37) = 9$.

$$\begin{aligned} D(62) &\equiv 62^{43} \pmod{77} \\ &\equiv [(62)^3]^{14} \times 62 \pmod{77} \\ &\equiv 13^{14} \times 62 \pmod{77} \\ &\equiv (13^2)^7 \times 62 \pmod{77} \\ &\equiv 15^7 \times 62 \pmod{77} \\ &\equiv (15^2)^3 \times 15 \times 62 \pmod{77} \\ &\equiv 71^3 \times 15 \times 62 \pmod{77} \\ &\equiv 15 \times 15 \times 62 \pmod{77} \\ &\equiv 71 \times 62 \pmod{77} \\ &\equiv 13 \pmod{77} \end{aligned}$$

Logo, $D(62) = 13$.

$$\begin{aligned} D(39) &\equiv 39^{43} \pmod{77} \\ &\equiv [(39)^3]^{14} \times 39 \pmod{77} \\ &\equiv 29^{14} \times 39 \pmod{77} \\ &\equiv (29^2)^7 \times 39 \pmod{77} \\ &\equiv 71^7 \times 39 \pmod{77} \\ &\equiv (71^3)^2 \times 71 \times 39 \pmod{77} \\ &\equiv 15^2 \times 71 \times 39 \pmod{77} \\ &\equiv 71 \times 71 \times 39 \pmod{77} \\ &\equiv 36 \times 39 \pmod{77} \\ &\equiv 18 \pmod{77} \end{aligned}$$

Logo, $D(39) = 18$.

$$\begin{aligned} D(10) &\equiv 10^{43} \pmod{77} \\ &\equiv [(10)^3]^{14} \times 10 \pmod{77} \\ &\equiv 76^{14} \times 10 \pmod{77} \\ &\equiv (76^2)^7 \times 10 \pmod{77} \\ &\equiv 1^7 \times 10 \pmod{77} \\ &\equiv 10 \pmod{77} \end{aligned}$$

Logo, $D(10) = 10$.

Passo 3- Substituímos cada bloco numérico por seu correspondente na tabela 3.2 e lemos a mensagem.

$$11 - 2 - 42 - 29 - 9 - 13 - 18 - 10$$

$$11242299131810$$

4.4 Atividades envolvendo a criptografia ElGamal

Atividade 1

Determine os logaritmos discretos, $\log_3(7) \pmod{11}$ e $\log_3(5) \pmod{11}$.

Solução:

Queremos determinar o valor de n, tal que $3^n \equiv 7 \pmod{11}$. Calculando as potências de 3 e determinando seus restos módulo 11, temos:

$$3^1 = 3 \equiv 3 \pmod{11}$$
$$3^2 = 9 \equiv 9 \pmod{11}$$
$$3^3 = 27 \equiv 5 \pmod{11}$$
$$3^4 = 81 \equiv 4 \pmod{11}$$
$$3^5 = 243 \equiv 1 \pmod{11}$$
$$3^6 = 729 \equiv 3 \pmod{11}$$
$$3^7 = 2187 \equiv 9 \pmod{11}$$
$$3^8 = 6561 \equiv 5 \pmod{11}$$
$$3^9 = 19683 \equiv 4 \pmod{11}$$
$$3^{10} = 59049 \equiv 1 \pmod{11}$$

Logo, $\log_3(7) \pmod{11}$ não existe e, $\log_3(5) \pmod{11} = 3$ e $\log_3(5) \pmod{11} = 8$.

Atividade 2

Calcular, conforme atividade 1, $\log_3(7) \pmod{11}$ e $\log_3(5) \pmod{11}$ utilizando a calculadora de logaritmos discretos.

O professor pode disponibilizar aos alunos o site `https://www.alpertron.com.ar/LOGDI.HTM` que fornece uma calculadora de logaritmos discretos para que eles possam calcular os referidos logaritmos e, em seguida conferir as respostas da atividade 1.

O site acima irá abrir a seguinte janela:

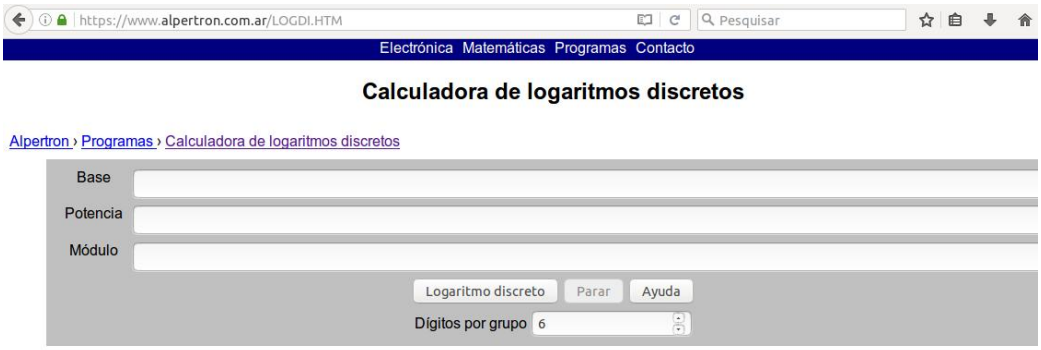


Figura 4.1: Calculadora de logaritmos discretos

Para se efetuar o cálculo do logaritmo discreto $\log_3(7) \pmod{11}$, na caixa de entrada *Base* digita-se a base do logaritmo discreto que, neste caso é 3; na caixa de entrada *Potência* digita-se o logaritmando que é 7 e, na caixa *Módulo* digitamos qual módulo estamos trabalhando que, nesse caso específico é 11.

Após entrar com estes dados, teremos a janela abaixo, conforme figura 4.2: Para calcular o resultado, basta clicarmos no botão *Logaritmo discreto* e, logo

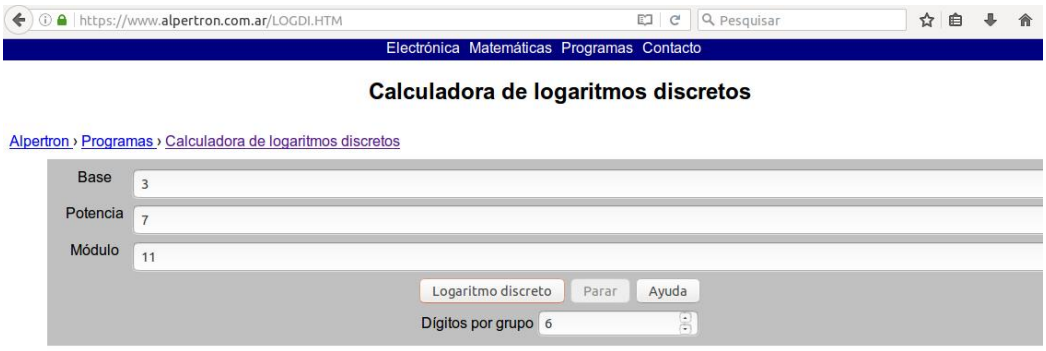


Figura 4.2: Inserindo dados na calculadora de logaritmos discretos

após nos será dada a tela conforme figura 4.3.

Observe que, na primeira linha temos, *Calcular exp tal que* $3^{exp} \equiv 7 \pmod{11}$, o que queremos calcular e, na segunda linha temos a resposta *Nenhum valor de exp satisfaz a congruência.*

Figura 4.3: Resposta do cálculo do logaritmo discreto

A figura 4.4 nos mostra o cálculo de $\log_3(5) \pmod{11}$. Observe que na segunda linha obtivemos, $exp = 3 + 5k$, como reposta.

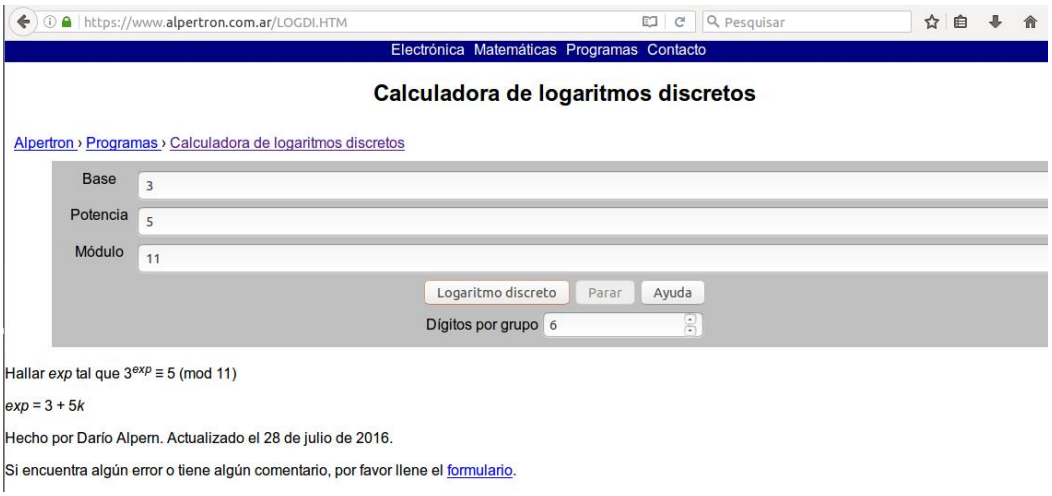


Figura 4.4: Resposta do cálculo do logaritmo discreto

Agora, vamos analisar a resposta que nos foi dada. Como estamos trabalhando com uma congruência módulo 11 em $\mathbb{Z}_p^*$, temos que exp é um inteiro positivo menor do que 11, ou seja, devemos ter $3+5k < 11$, obtendo $k = 0$ ou $k = 1$. Logo, teremos como resposta $exp = 3$ ou $exp = 8$. Que foram as respostas encontradas acima.

Capítulo 5

Conclusão

Este trabalho teve como objetivo, apresentar alguns métodos criptográficos que podem ser trabalhados no ensino Médio, possibilitando ao aluno compreender a aplicabilidade da matemática. Conforme nos sugere o Currículo Básico Comum, um dos principais objetivos do ensino da matemática é despertar a curiosidade nos estudantes com problemas interessantes que advém de situações concretas do seu dia-a-dia.

Sendo assim, a criptografia, por fazer parte do cotidiano dos alunos, se torna um método muito eficaz para o desenvolvimento de conceitos Matemáticos, não somente no Ensino Médio, como também no Ensino Fundamental e, a partir daí, torna-se um motivador para a aprendizagem da Matemática.

Pode-se perceber também que é possível utilizar a tecnologia computacional dentro da sala de aula auxiliando os alunos na compreensão dos assuntos e execução de atividades. Além disso, a criptografia possibilita a interação aluno/aluno e motiva o trabalho em grupo, como foi sugerido em algumas atividades a serem desenvolvidas.

A partir deste trabalho, sugere-se ao professor trabalhar, na medida do possível, aqueles conteúdos que permitem a aplicabilidade de forma mais didática de maneira a motivar o interesse dos alunos pelos conteúdos estudados.

Espera-se, também, que as atividades que foram propostas sejam somente o ponta-pé inicial para que o educador possa buscar outras formas de explanação dos conteúdos abordados pois, ao inserirmos novos métodos de ensino, a matemática se torna cada vez mais atrativa. As ferramentas computacionais que foram indicadas serviram apenas para dar uma noção de como a informática pode nos ser útil em sala de aula. Sendo assim, sugere-se ao professor que busque outros softwares para que possa, de maneira eficaz, estimular o ensino/aprendizagem da matemática através da sua interação com outras áreas de conhecimento.

Referências Bibliográficas

[1] ALMEIDA, Cinthia Soares de. **Dificuldades de Aprendizagem em Matemática e a Percepção dos Professores em Relação a Fatores Associados ao Insucesso nesta Área.**

Disponível em: `www.ucb.br/sites/100/103/TCC/12006/CinthiaSoaresdeAlmeida.pdf`

[2] Andreescu, Titu et al. **Number Theory: Structures, Examples and Problems.**

Disponível em: https://blngcc.files.wordpress.com/2008/11/andreescu-andrica-problems-on-number-theory.pdf Acessado em 05/09/2016.

[3] ARAÚJO, Robson Ricardo de. **Anéis de inteiros de corpos de números e aplicações.** São José do Rio Preto: SP, 2015. Dissertação de Mestrado - Universidade Estadual Paulista "Júlio de Mesquitra Filho." Instituto de Biociências, Letras e Ciências Exatas, 2015.

Disponível em: `http://repositorio.unesp.br/bitstream/handle/11449/127767/000846496.pdf?sequence=1`

[4] BARBOSA, Jonei Cerqueira. **Modelagem na Educação Matemática: Contribuições para o Debate Teórico.** In: REUNIÃO ANUAL DA ANPED, 24., 2001, Caxambu. Anais... Rio de Janeiro: ANPED, 2001. 1 CD-ROM.

Disponível em: `www.ufrgs.br/espmat/disciplinas/funcoes_modelagem/modulo_I/modelagem_barbosa.pdf`. Acessado em 01/06/2016.

[5] BOLDRINI, José Luiz, et al. **Álgebra Linear.** São Paulo: Harper e Row do Brasil, 1980. 3ª Edição.

[6] BRASIL. Secretaria de Educação Média e Tecnológica. **Parâmetros Curriculares Nacionais Mais Ensino Médio: Orientações Complementa-**

res aos Parâmetros Curriculares Nacionais - PCN+ . Brasília: MEC, 2002.

Disponível em: `http://portal.mec.gov.br/seb/arquivos/pdf/CienciasNatureza.pdf`. Acessado em 18/04/2016.

[7] COLOSSUS, Machine.

Disponível em: `http://www.alanturing.net/turing_archive/archive/infopages/ColossusPhoto.html`. Acessado em 12/07/2016.

[8] COUTINHO, S. C. **Números Inteiros e Criptografia RSA.** Rio de Janeiro: IMPA, 2001.

[9] EISENBERG, MURRAY **Hill Ciphers and Modular Linear Algebra.**

Disponível em: `http://apprendre-en-ligne.net/crypto/hill/Hillciph.pdf` Acessado em 03/11/2016.

[10] ELGAMAL, Taher; **A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms.**

Disponível em: `http:http://groups.csail.mit.edu/cis/crypto/classes/6.857/papers/elgamal.pdf` Acessado em 20/12/2016.

[11] GARCIA, Arnaldo; LEQUAIN, Yves. **Elementos de Álgebra.** Rio de Janeiro: RJ. IMPA/PROJETO EUCLIDES, 2005.

[12] GONÇALVES, Adilson. **Introdução à Álgebra.** Rio de Janeiro: IMPA, 2007.

[13] HEFEZ, Abramo. **Elementos de Aritmética.** SBM, 2005.

[14] HEFEZ, Abramo. **Aritmética.** SBM, 2014.

[15] HEFEZ, Abramo. **Iniciação à Aritmética.** Rio de Janeiro: IMPA, 2015.

Disponível em: `http://www.obmep.org.br/docs/apostila1.pdf` Acessado em 23/12/2016.

[16] IEZZI, Gelson; HAZZAN, Samuel. **Fundamentos de Matemática Elementar - Volume 4.** São Paulo: S.P. Atual Editora, 1977. 2ª Edição.

[17] LIMA, Elon Lages. **Exame de Textos-Análise de Livros de Matemática para o Ensino Médio.** Rio de Janeiro: RJ. IMPA/SBM, 2001.

[18] LORENZ, Machine.

Disponível em: http://www.alanturing.net/turing_archive/archive/infopages/LorenzPhoto.html

[19] MAIER, Rudolf R. **Teoria dos Números.** Notas de aula Brasília: D.F. 2005

Disponível em: http://www.mat.unb.br/~maierr/tnotas.pdf Acessado em 26/10/2016.

[20] MARTINEZ, Fabio E. Brochero et al. **Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro.** Livraria Virtual, Impa.

Disponível em: http://www.mat.ufmg.br/~fbrocher/TN/Teoria_dos_numeros_Um_passeio_com_primos_3ed.pdf Acessado em 26/10/2016.

[21] MG. **Proposta Curricular do Currículo Básico Comum de Matemática.**

Disponível em: http://crv.educacao.mg.gov.br/sistema_crv/banco_objetos_crv/%7B4DA513B4-3453-4B47-A322-13CD37811A9C%7D_Matem%C3%A1tica%20final.pdf Acessado em 22/12/2016.

[22] ROSEN, Kenneth H. **Elementary Number Theory and its Applications.** 1984.

[23] SANCHES, Maria Helena Figueiredo. **Efeitos de uma Estratégia Diferenciada do Ensino do Conceito de Matrizes.** Campinas: SP, 2002. Dissertação de Mestrado - Universidade Estadual de Campinas. Faculdade de Educação, 2002.

[24] SANTOS, J. P. **Introdução à Teoria dos Números.** Coleção Matemática Universitária. Rio de Janeiro: IMPA 2009.

[25] SAUTOY, Marcus du. **A Música dos Números Primos: A História de um Problema não Resolvido na Matemática.** Rio de Janeiro: RJ. Zahar, 2007.

[26] SINGH, Simon. **O Livro dos Códigos: A Ciência do Sigilo - do Antigo Egito à Criptografia Quântica** 7ª Edição - Rio de Janeiro: Record, 2008.

[27] STALLINGS, William. **Criptografia e Segurança de Redes: Princípios e Práticas.** 4ª Edição - São Paulo: SP. Pearson Prentice Hall, 2008.

Disponível em: http://docslide.com.br/download/link/criptografia-e-seguranca-de-redes-4a-edicaopdf Acessado em 28/09/2016.

[28] TAMAROZZI, Antônio Carlos. **Codificando e Decifrando Mensagens.** Revista do Professor de Matemática, São Paulo: Sociedade Brasileira de Matemática, n. 45, 2001.

[29] LibreOffice Calc.

Disponível em:https://pt.wikipedia.org/wiki/LibreOffice#cite_note-LibreOffice_.28BrOffice.29_download-23 Acessado em 21/12/2016.