



Universidade Federal do Tocantins
Mestrado Profissional em Matemática
PROFMAT

Francisco Claudio Lima Gomes

**Uma proposta de abordagem no Ensino Médio da Criptografia
RSA e sua estrutura matemática**

Gurupi - TO
Maio - 2014

Francisco Claudio Lima Gomes

**Uma proposta de abordagem no Ensino Médio da Criptografia
RSA e sua estrutura matemática**

Dissertação apresentada ao programa de Mestrado Profissional em Matemática em Rede Nacional, coordenado pela Sociedade Brasileira de Matemática e ofertado pela Universidade Federal do Tocantins, sob a orientação do Prof. Dr. Pedro Alexandre da Cruz, como requisito parcial para a obtenção do título de mestre em matemática

Gurupi - TO
Maio - 2014

Dados Internacionais de Catalogação na Publicação (CIP)
Biblioteca da Universidade Federal do Tocantins
Campus Universitário de Palmas

G633p Gomes, Francisco Claudio Lima
 Uma proposta de abordagem no Ensino médio da Criptografia RSA e
 sua estrutura matemática / Francisco Claudio Lima Gomes. - Gurupi,
 2014.
 68f.

 Dissertação de Mestrado – Universidade Federal do Tocantins,
 Programa de Mestrado Profissional em Matemática - PROFMAT, 2014.
 Linha de pesquisa: Matemática.
 Orientador: Prof. Dr. Pedro Alexandre da Cruz.

 1. Criptografia. 2. Algoritmo RSA. 3. Aplicação. I. Cruz, Pedro
 Alexandre. II. Universidade Federal do Tocantins. III. Título.
 CDD 21.ed. 652.8

Bibliotecária: Roseane da Silva Pires
CRB-2 / 1.211


TODOS OS DIREITOS RESERVADOS – A reprodução total ou parcial, de qualquer forma ou por qualquer meio deste documento é autorizado desde que citada a fonte. A violação dos direitos do autor (Lei nº 9.610/98) é crime estabelecido pelo artigo 184 do Código Penal.

Francisco Claudio Lima Gomes

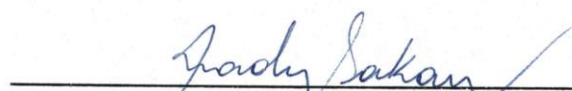
Uma proposta de abordagem no Ensino Médio da Criptografia RSA e sua estrutura matemática

Dissertação apresentada ao programa de Mestrado Profissional em Matemática em Rede Nacional, coordenado pela Sociedade Brasileira de Matemática e ofertado pela Universidade Federal do Tocantins, sob a orientação do Prof. Dr. Pedro Alexandre da Cruz, como requisito parcial para a obtenção do título de mestre em matemática.

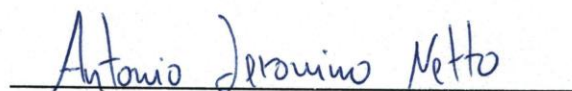
Trabalho aprovado. Gurupi - TO, 23 de maio de 2014:



Prof. Dr. Pedro Alexandre da Cruz
Orientador



Professora Dra.
Lady Sakay



Professor Dr.
Antonio Jeronimo Netto

Gurupi - TO
Maio - 2014

Dedico este trabalho a meu grande amigo Gentil Domingues Filho; a minha querida esposa Vanúzia Alves de Araújo e filhos Claudio de Araújo Gomes e Nicole de Araújo Gomes; aos meus pais José Gomes de Melo e Antônia Solange Pereira Lima; a meus irmãos José Kleeber Lima Gomes, José Kassio Lima Gomes e Antônio Carlos Lima Gomes.

Dedido também a todos os meus alunos, a todos os meus professores, a todos da turma UFT PROFMAT 2012 em especial a Wellington Pereira Braz, Thiago Beirigo Lopes, Leniedson Guedes Dos Santos, Flávio Antônio Nolêto Fernandes.

AGRADECIMENTOS

Agradeço a Gentil Domingues Filho, ao IMPA pela iniciativa de proporcionar o PROFMAT, á CAPES pelo apoio, à UFT, ao meu orientador prof. Dr. Pedro Alexandre da Cruz e a todos os professores do mestrado PROFMAT UFT.

*“Vivemos em uma sociedade extremamente dependente da ciência e tecnologia ,na qual
pouquíssimos sabem alguma coisa sobre ciência e tecnologia”.*
(Carl Sagan)

RESUMO

Este trabalho almeja contribuir para ensino de matemática na segunda etapa do ensino básico no Brasil e tem por objetivos: levar aos estudantes do ensino médio conhecimento sobre a estrutura matemática do algoritmo de criptografia RSA, contribuindo, assim, para a compreensão de alguns fundamentos científico-tecnológicos de segurança em processos produtivos; apresentar aos estudantes do ensino médio a aritmética modular, levando-os a perceber que a matemática é mais ampla e rica do que as operações apresentadas na educação básica; divulgar e disponibilizar material didático sobre o algoritmo de criptografia RSA que possa subsidiar professores interessados em trabalhar o conteúdo de criptografia no ensino médio. A metodologia aplicada foi a pesquisa bibliográfica. Espera-se despertar o interesse de estudantes do ensino médio para a criptografia, e que esse material possa auxiliar os professores que desejem trabalhar esse conteúdo no ensino médio, possibilitando os trabalhos e projetos de ensino com a participação de várias disciplinas como História, Filosofia, Sociologia, Matemática, Física e Informática, possibilitando a construção de conhecimento relativo à criptologia.

Palavras-chaves: Álgebra, números primos, Criptografia RSA.

ABSTRACT

This work aims to contribute to teaching math in the second stage of basic education in Brazil and has the following objectives: to bring high school students knowledge about the mathematical structure of the RSA encryption algorithm, thus contributing to the understanding of some scientific-basics technological security processes; introduce high school students to modular arithmetic, causing them to realize that mathematics is broader and richer than the steps in basic education; disseminate and make available educational material on the RSA encryption algorithm that can support teachers interested in working content encryption in high school. The methodology used was the literature research. It is hoped to interest high school students for the encryption, and that this material can assist teachers who wish to work in middle school this content, enabling work and teaching projects involving several disciplines such as History, Philosophy, sociology, Mathematics, Physics and Informatics, allowing the construction of knowledge on cryptology.

Key-words: Algebra, prime number, RSA Criptography.

Lista de ilustrações

Figura 1 – Ramos da criptologia	18
Figura 2 – Classificação de cifras	19
Figura 3 – Scytalae	20
Figura 4 – Frequência na escrita de português no Brasil	23
Figura 5 – Disco de Alberti	24
Figura 6 – Tábula recta	24
Figura 7 – Alfabeto Della Porta	26
Figura 8 – Enigma	27
Figura 9 – Colossus	27
Figura 10 – Calendário	45
Figura 11 – Período modular primo	62
Figura 12 – Período modular de número composto	63
Figura 13 – Mult. modular	64

Lista de tabelas

Tabela 1 – Processo de divisões sucessivas	35
Tabela 2 – Algoritmo estendido de Euclides	37
Tabela 3 – Exemplo numérico do algoritmo estendido de Euclides	37
Tabela 4 – Primos entre 1 e 50	40
Tabela 5 – Distância média entre primos de 1 a n	43
Tabela 6 – Adição modular	49
Tabela 7 – Multiplicação modular	50

Lista de Quadros

1	Atbash	20
2	Cifras de coluna	21
3	Transposição de colunas	22
4	Frequência de letras na escrita de português no Brasil	22
5	Cifra de Vegenère	25
6	Precodificação	57

Lista de símbolos

\mathbb{N}	Conjunto dos números naturais
\mathbb{Z}	Conjunto dos números inteiros
\mathbb{Z}_+^*	Conjunto dos números inteiros estritamente positivos
\mathbb{Z}_+	Conjunto dos números inteiros não negativos
$=$	Igualdade
\simeq	Aproximado
\neq	É diferente de
\in	Relação de pertença entre elemento e conjunto
\exists	Existe
\nexists	Não existe
\cup	União de conjuntos
\cap	Intersecção de conjuntos
\subset	Contido em
$n(X)$	Números de elementos de um conjunto
\forall	Para todo
\implies	Implicação lógica
$>$	É maior que
$<$	É menor que
\nless	Não é menor que
\geq	É maior ou igual a
\leq	É menor ou igual a
∞	Símbolo matemático do infinito
$ x $	Módulo de um número x

x^{-1}	Inverso de um número x
x^n	n -ésima potência de um número x
$f(x)$	Representação de uma função
$n!$	Fatorial de um número n
	Divide
†	Não divide
\equiv	Congruência modular
$\not\equiv$	Incongruência modular
\ln	Logaritmo natural
e	número irracional base do logaritmo neperiano
\lim	Limite
$[x]_n$	Representante de classe modular com período n
$\phi(n)$	Função ϕ de Euler
$\text{mod } k$	Período na aritmética modular
■	Demonstração finalizada

Sumário

1	INTRODUÇÃO	16
2	CONTEXTO HISTÓRICO	18
2.1	Conceitos iniciais	18
2.2	Cronologia da criptologia	19
2.2.1	Antiguidade	19
2.2.2	Criptografia durante a Idade Média	21
2.2.3	Algumas cifras da Idade Moderna	22
2.2.4	Tópicos de criptografia durante o século XX	26
3	CONCEITOS BÁSICOS DA TEORIA DOS NÚMEROS	29
3.1	O conjunto dos números naturais	30
3.2	O conjunto dos números inteiros	31
3.3	O algoritmo de Euclides	34
3.4	Números primos	37
3.4.1	Técnicas de abordagem de primos: tentativas de equacioná-los	39
4	ARITMÉTICA MODULAR	45
4.1	Congruência	46
4.1.1	Caracterização e propriedades de congruência	46
4.1.2	Sistema completo de restos SCR	47
4.2	A aritmética do relógio	48
4.2.1	Soma e subtração	48
4.2.2	Multiplicação	49
4.2.3	Potenciação modular	50
4.2.4	Inverso multiplicativo módulo n	50
4.3	O pequeno Teorema de Fermat	51
5	A CRIPTOGRAFIA RSA	55
5.1	O problema de distribuição de chaves	55
5.2	Usando o algoritmo RSA	56
5.3	Entendendo o mecanismo do algoritmo RSA	60
6	APLICAÇÃO EM SALA DE AULA	61
6.1	O inverso multiplicativo a partir do MMC	61
6.2	Por que o $\text{mdc}(a, n) = 1$?	62

6.3	Criando uma tabela de multiplicação modular em planilha eletrônica	63
6.4	Algoritmo estendido de Euclides	64
6.5	Criptografando com algoritmo RSA	64
6.6	Usando mais de dois números primos	65
	Considerações finais	66
	Referências	67

1 INTRODUÇÃO

A construção e difusão do conhecimento, como forma e instrumento de acesso à cidadania, necessita de prática escolar direcionada para a autonomia de seus estudantes, possibilitando-lhes participação ativa em atividades científicas ou culturais. Para isso, conhecer as bases da tecnologia da produção de conhecimento é fundamental. O aparato computacional de hoje possibilita apresentar e explorar conteúdos matemáticos mais complexos e com maior profundidade. Por isso, alguns tópicos já deveriam ter sido contemplados no ensino médio, entre eles noções de recorrência e criptologia. A criptologia acompanha a história das civilizações, tendo sido decisiva em guerras e, hoje, é de valor inestimável para a segurança no comércio eletrônico, nas comunicações entre pessoas e entre Estados (BURNET; PEINE, 2002). Pode-se dizer extremamente vulnerável, ou mesmo excluído, quem dela não faz uso daí a importância de se buscar compreender seus fundamentos.

A LDB (Lei de Diretrizes e Bases da Educação) em seu art. 35 destaca, entre as finalidades do ensino médio, no inciso IV, a compreensão dos fundamentos científico-tecnológicos dos processos produtivos, relacionando teoria a prática, no ensino de cada disciplina. O art. 36 da LDB estabelece como diretrizes do currículo de ensino médio o destaque a educação tecnológica básica entre outras; ainda, em seu parágrafo único, estabelece que ao final do ensino médio o educando demonstre domínio dos princípios científicos e tecnológicos que amparam a produção moderna e conhecimento das formas contemporâneas de linguagem (BRASIL, 1996). De acordo com os PCN's (Parâmetros Curriculares Nacionais) a Matemática no Ensino Médio é formativa no sentido de estruturar o pensamento e o raciocínio dedutivo (BRASIL, 2000).

Complementarmente à determinação legal, há estudos realizados por Piagetianos nas sociedades ocidentais mostrando que os adolescentes são capazes de estabelecer hipóteses e inferir, sua mente pode realizar operações mentais formais (GARDNER, 1994). Dessa forma, é razoável e interessante que se desafie o adolescente com atividades cada vez mais complexas visando seu desenvolvimento intelectual.

O conhecimento da criptologia, que compreende a criptografia e a criptoanálise, aproxima o estudante de uma das bases que suportam a comunicação moderna e cumpre os preceitos legais. A criptografia está presente quando se usa o cartão de crédito ou se faz uma transação pela internet.

A privacidade é cada vez mais necessária e espera-se que os e-mails fiquem somente entre os interessados; que os segredos mercadológicos e as estratégias de crescimento das empresas sejam resguardados; que os bancos transmitam diariamente a movimentação de

sua praça sem que isso se torne público. Os Estados precisam guardar informações, mantê-las em segredo, vê-se que há intensa necessidade de segurança da informação por Estados, empresas e, por parte das pessoas, há uma intensa necessidade de privacidade. A criptografia vem em atendimento a essa demanda.

Apesar de toda a justificativa para abordar criptologia, há uma lacuna que pode ser facilmente verificada. Os livros adotados no ensino médio pouca atenção dão à criptologia, que foi fundamental durante a Segunda Guerra Mundial. O autor deste trabalho consultou livros de História, Sociologia, matemática das redes federal, estadual e particular de ensino na cidade de Gurupi, Estado do Tocantins, durante o primeiro bimestre de 2014, e encontrou quase nenhuma referência ao tema criptografia. Uma menção é encontrada na página 150 do livro *matemática interativa* do 7º ano do ensino básico do autor Alexandre Luís Trovon de Carvalho (CARVALHO, A.; REIS, 2009).

É, portanto, importante que se leve ao conhecimento dos estudantes de ensino médio esse conteúdo por satisfazer as exigências legais e, ainda, possibilitar a elaboração de projetos pedagógicos com o tema criptografia em que diversas disciplinas, como Informática, História, Sociologia, Filosofia, Física e Matemática, possam participar e colaborar. Por isso, a escola deveria oferecer algum conteúdo no âmbito da criptografia, criptoanálise ou ambas nos currículos de ensino médio.

No capítulo 2 é feito um breve resumo do contexto histórico da criptografia desde a antiguidade, passando pela Idade Média e o pós guerra. Também serão descritas, no âmbito do ensino médio, a modalidade simétrica e a necessidade da criptografia assimétrica como o algoritmo RSA.

Em seguida, no capítulo 3, apresentam-se as principais definições, conceitos e teoremas referentes à Teoria Clássica dos Números visando garantir o entendimento, a segurança e o funcionamento do Algoritmo RSA.

No capítulo 4 são apresentados os conceitos de aritmética modular com suas operações e propriedades. Mostra-se também o Pequeno Teorema de Fermat e a função ϕ de Euler que permitem o funcionamento do algoritmo RSA.

No capítulo 5, apresenta-se um breve histórico da criptografia RSA e, com base nos fundamentos dos capítulos anteriores, descreve-se e explica-se a implementação matemática do Algoritmo RSA em linhas gerais.

No capítulo 6, trabalha-se uma aplicação em sala de aula do algoritmo RSA com a utilização de planilha eletrônica.

Nas considerações finais há sugestão para estudo e adaptação, para o Ensino Médio, de outras modalidades de criptografia que estão em fase de estudo e implementação.

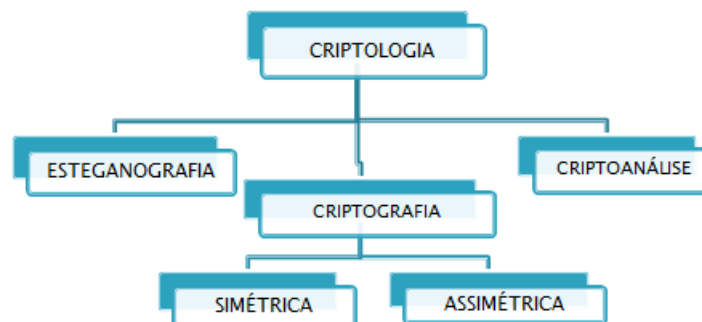
2 CONTEXTO HISTÓRICO

2.1 Conceitos iniciais

A preocupação em esconder ou embaralhar as mensagens foi praticada, por povos antigos como os egípcios, babilônios, assírios, romanos, etc. Para esconder a mensagem entra em ação a esteganografia. A arte da esteganografia consiste em ocultar a existência de uma mensagem (COUTO, 2008).

Mas se a intenção for impedir a leitura da mensagem por pessoas não autorizadas, modificando seus caracteres por substituição ou permutação, então usa-se a criptografia. A codificação é a mudança das características de um sinal com uma finalidade específica. Essa finalidade pode ser transmissão, exibição ou arquivamento. Por exemplo, pode-se converter texto, som ou imagem de forma a arquivá-los em HDs, que são dispositivos de armazenamento de dados dos computadores. Já a cifragem é alteração de símbolos(grafemas) da mensagem original como meio de torná-la acessível apenas aos autorizados (COUTO, 2008). Entende-se por algoritmo o conjunto de regras e procedimentos lógicos perfeitamente definidos que levam à solução de um problema em um número finito de etapas (HOUAISS, 2009). As figuras 1 e 2 foram elaboradas pelo autor com base em (COUTO, 2008)

Figura 1 – Ramos da criptologia



Fonte: elaborado pelo autor

A mensagem cifrada é o resultante da aplicação de um algoritmo invariável associado a uma determinada chave (variável ou não). O sistema e a chave precisam ser de conhecimento do emissor e do receptor (COUTO, 2008) como será descrito nos capítulos à frente.

A criptografia convencional é composta por 5 elementos que são: o texto plano, também chamado de texto limpo ou texto claro (conteúdo original); o algoritmo criptográfico; a chave secreta; o texto cifrado e o algoritmo de decriptografia (COUTO, 2008). O algo-

ritmo criptográfico converte o texto limpo em texto cifrado, o algoritmo de decryptografia conferte o texto cifrado em texto claro e a chave é um modo específico de se executar tais algoritmos.

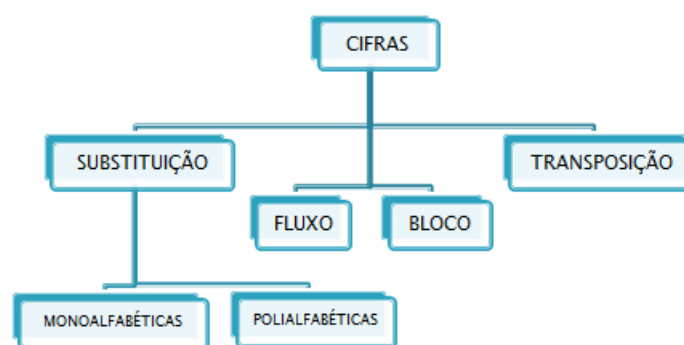
Naturalmente a busca por segredos de estado, mensagens inimigas durante as guerras ou mais recentemente segredos industriais, além do simples desafio à inteligência humana, estimulou a busca de métodos de quebra de cifras por meio da detecção da chave para acesso não autorizado à mensagem. Esse ramo chama-se criptoanálise que consiste em um conjunto de técnicas e métodos para a decifração de caracteres de uma escrita de sistema desconhecido (HOUAISS, 2009). Mais recentemente algumas empresas estão contratando os criptoanalistas para pesquisarem fraquezas em sistemas por elas desenvolvidos.

2.2 Cronologia da criptologia

2.2.1 Antiguidade

Os estudiosos consideram como primeiro documento de escrita cifrada alguns hieróglifos egípcios, encontrados na tumba de Khnumhotep, a aproximadamente 1900 a.C. Em aproximadamente 1500 a.C. houve o desenvolvimento da esteganografia pelas culturas egípcia, chinesa, indiana e mesopotâmica. Situações como raspar o cabelo, tatuar uma mensagem, deixar o cabelo crescer, enviar ao destinatário que raspará novamente para que a leitura seja efetuada é um exemplo.

Figura 2 – Classificação de cifras



Fonte: elaborado pelo autor

Há muitos exemplos de esteganografia: escrever um texto e esconder a mensagem em meio ao texto; escritas na parte interna de caixas para transporte de cera ou mensagens adequadamente embaladas para serem engolidas por animais, transportada em seus estômagos e depois recuperadas (COUTO, 2008).

Os hebreus, entre 600 e 500 a.C. usaram uma cifra de substituição conhecida como ATBASH que consistia em substituir uma letra do alfabeto por sua simétrica em relação

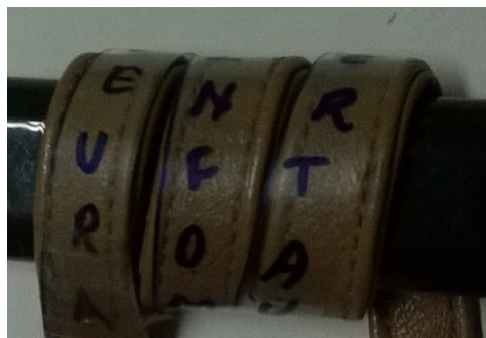
aos extremos do abecedário, como exemplo a cifra ATBASH usando o alfabeto latino teria cada letra substituída pela letra diretamente abaixo conforme a sequencia mostrada no quadro 2.1 que foi adaptado a partir de (COUTO, 2008).

Quadro 1 – Atbash

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

Há indícios de que, no mesmo período, os espartanos usavam um bastão conhecido como scytalae ou Bastão de Licurgo para criptografar. Esse método consistia em amarrar uma tira de couro em um bastão, escrever a mensagem sobre o couro e na direção do comprimento do bastão, quando desenrolado a mensagem ficava embaralhada (COUTO, 2008).

Figura 3 – Scytalae



Fonte: elaborado pelo autor

Por volta de 300 a.C., na Índia, um livro chamado de Artha–sastra, continha a compilação de vários métodos de criptoanálise. Seu provável autor se chamava Kautilya e tal livro era restrito ao uso diplomático. O matemático grego Euclides sintetizou o conhecimento de geometria e teoria dos números. O grego Eratóstenes criou um método para separar os números primos em um intervalo de 1 a n conhecido como crivo de Eratóstenes (COUTO, 2008). Os escribas de Uruk, Iraque atualmente, identificavam seus trabalhos convertendo as letras de seus nomes para números e adicionando a seus trabalhos, isso se dá em torno de 130 a.C e é uma forma bem interessante de autenticação(COUTO, 2008).

A cifra de César

O general romano Júlio Cesar (100 a 44 A.C.) foi um dos primeiros a usar em documentos oficiais um método de cifragem que consistia em substituir qualquer letra

da mensagem por outra, três posições à frente (COUTO, 2008). Assim, a letra A deveria ser substituída pela letra D e a letra Z pela letra C. Como exemplo, a expressão CRIPTOGRAFIA RSA passaria a ser:

FULSWRJUDILD UVD.

2.2.2 Criptografia durante a Idade Média

A idade média é um período compreendido, não exatamente, entre os anos 476 e 1453. No século VIII, o árabe Al-Khalil fica famoso no império bizantino por decifrar um criptograma antigo supondo que a parte inicial do texto era “Em nome de Deus”, este método ficou conhecido como Método da Palavra Provável foi usado para decifrar trabalhos da máquina Enigma no período da 2ª Guerra Mundial (COUTO, 2008).

Duas inovações são apresentadas. Primeiro, no século IX, o árabe Al-Kindi usa análise de frequência para decifrar mensagens criptográficas, sendo um dos primeiros estudiosos da matemática estatística, seu livro Risalah fi Istikhraj al Mu’amma é a obra, sobre criptologia, mais antiga conservada. Segundo, entre os séculos XII e XIII, o árabe Ibn Dunaanir inova ao usar as cifras algébricas, que consiste em substituir letras por números e submetê-los a operações aritméticas (COUTO, 2008).

Algumas cifras antigas

As cifras clássicas podem se entendidas como algoritmos de transposição (permuta entre os símbolos que compõem a mensagem) ou algoritmos de substituição nos quais as letras são trocadas por outras letras ou símbolos (COUTO, 2008).

Cifras de colunas

Na cifra de colunas a mensagem é distribuída, de cima para baixo, em uma grade que depois é quebrada em blocos de k termos da esquerda para a direita, por exemplo:

PARABENIZO AO IMPA E A UFT A INICIATIVA DO PROFMAT

Quadro 2 – Cifras de coluna

P	A	N	O	I	A	U	P	A	I	A	V	O	O	A
A	B	I	A	M	E	F	E	I	C	T	A	P	F	T
R	E	Z	O	P	A	T	L	N	I	I	D	R	M	.

Em seguida o texto será separado usando uma chave de 7 caracteres da esquerda para a direita ficando assim:

PANOIAU PAIAVOO AABIAME FEICTAP FTREZOP ATLNIID RM

Faz-se necessário o conhecimento do tamanho da tabela e da chave para se decriptar (COUTO, 2008). OS quadros 2 e 3 foram elaborados pelo autor.

Há também a transposição de colunas. Escolhe-se uma palavra chave como **MODULAR** e constrói-se uma tabela para distribuir as letras da mensagem:

Quadro 3 – Transposição de colunas

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

O restante dos espaços da tabela devem ser preenchidos com quaisquer caracteres, neste exemplo foram escolhidas X, W, K, J e P. O texto encriptado consiste na sequência formada pelas colunas, em ordem alfabética das letras da palavra chave (COUTO, 2008). O texto cifrado é:

EIFNVFJ-ROELAPX-BOUIIOK-PIPPCDA-AZAEIOT-NMTIAMP-AAATRW

2.2.3 Algumas cifras da Idade Moderna

A idade moderna compreende o período que vai da queda de Constantinopla (1453 a.C) até a Revolução Francesa (1789). A análise de frequência tornou-se uma importante ferramenta para os criptoanalistas. Com base no trabalho da analista de sistema Viktoria Tkotz (COUTO, 2008), o quadro 4 apresenta a frequência das letras na língua portuguesa.

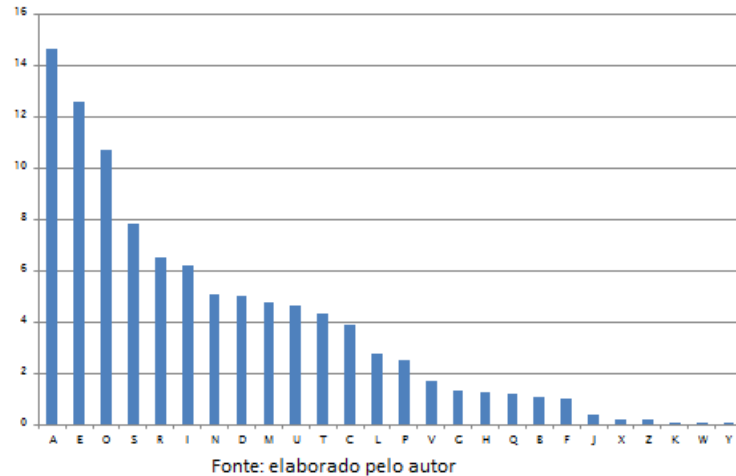
Quadro 4 – Frequência de letras na escrita de português no Brasil

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

A resposta à análise de frequência inicialmente foram as cifras homofônicas em que quanto maior a frequência de uma letra mais símbolos há para substituí-la. Assim, em um grupo de 100 símbolos, a letra A poderia ser representada por 14 ou 15 diferentes símbolos. O quadro 4 tem por fonte (COUTO, 2008. pg. 74).

Para efeito de visualização gerou-se o gráfico abaixo a partir da tabela de frequência de letras em português no Brasil.

Figura 4 – Frequência na escrita de português no Brasil

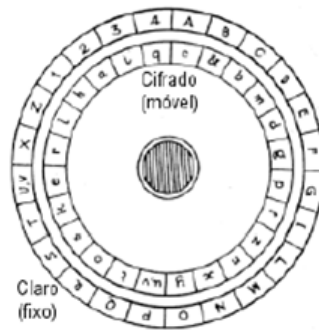


Em 1467, aproximadamente, o arquiteto italiano Leon Battista Alberti (1404 - 1472) inventa e publica a primeira cifra polialfabética e também cria um disco para facilitar a cifragem que fica conhecido como Disco de Alberti (COUTO, 2008). Dessa maneira se dificultava o uso da análise de frequência para decifração de textos. Alberti é considerado o pai da criptologia ocidental. O disco de Alberti era composto por dois discos concêntricos divididos em 24 partes igualmente espaçadas conforme figura 5. Externamente um disco fixo apresentava o alfabeto latino ordenado com 20 letras (excluídas h, j, k, w e y), no outro, que podia girar, o alfabeto latino aleatoriamente distribuído e os números de 1 a 4. Naturalmente era necessário que o destinatário também tivesse igual disco e conhecesse uma determinada letra chave (COUTO, 2008).

A cifragem começava com a escolha de uma letra chave no disco móvel (por exemplo a letra p) que era alinhada com determinada letra do disco externo, que tinha suas letras escritas em maiúsculo. Escreviam-se três ou quatro letras da mensagem substituindo a correspondente letra do disco interno pela letra alinhada no disco externo conforme chave previamente combinada entre emissor e destinatário. Para mudar bastava alinhar a letra, conforme chave preestabelecida, a qualquer outra letra do disco externo e continuar substituindo as letras do texto claro pelas letras alinhadas do disco externo (COUTO, 2008).

Em 1518 foi escrito o que é considerado o primeiro livro impresso sobre criptologia pelo alemão Johannes Trithemius (1462 - 1516) que também inventou uma cifra esteganográfica. No final do século XIV ele criou uma tabela, conhecida como tábula recta (tabela reta de Trithemius), para cifras polialfabéticas semelhantes às de Alberti. Para

Figura 5 – Disco de Alberti



Fonte: www.dm.ufscar.br/~caetano/fiae2004/G6/disco.htm

cifrar usando a tabela reta mantem-se a primeira letra da mensagem, ou seja, a primeira letra não é substituída; a segunda letra é substituída pela letra imediatamente abaixo (segunda linha); a terceira letra da mensagem deve ser substituída por letra da terceira linha pertencente à mesma coluna da substituída e assim sucessivamente (COUTO, 2008). Por exemplo, a palavra TOCANTINS é cifrada mantendo-se o *T*, substituindo-se o *O* pelo *P*, o *C* por *E*, o *A* por *D* e assim seguidamente conforme figura 6. Ao final do processo tem-se: TPEDRYOUA. Após 26 deslocamentos volta-se para a primeira linha.

Figura 6 – Tábula recta

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

Fonte: elaborado pelo autor com base em Couto, pg 78

Giovan Batista Belaso (1505 - ?), usando uma tabela semelhante, estabelece um método conhecido como cifra de Vigenère em 1553. Os deslocamentos na cifra de Vigenère

estão associados a uma chave. Escolhida a chave o processo de cifragem consiste trocar uma letra por outra pertencente à mesma coluna. A sequência de letras da palavra chave diz, respectivamente, em que linha procurar a letra substituta. Por exemplo, escolhendo-se a chave: GRITO, deve-se buscar substituta para a primeira letra do texto claro na intersecção de sua própria coluna com a linha iniciada por G; deve-se substituir a segunda letra do texto claro na coluna em que ela se encontra intersecção com a linha iniciada pela letra R e assim sucessivamente. Após o uso da última letra da chave repete-se o processo a partir da primeira letra, que no caso é a letra G (COUTO, 2008). Como exemplo será cifrando: MATEMATICA usando a chave GRITO.

Usando a tábula recta figura 6 a primeira busca é feita sempre na primeira linha, então busca-se o M e desce por sua coluna, que é a 14^a, até a linha iniciada por G, que é a 8^a e que é a primeira letra da palavra chave, encontra-se T nessa intersecção. Assim a letra M será substituída pela letra T.

Localiza-se na primeira linha da tábula recsta a segunda letra a ser substituída (A). Sua substituta está na mesma coluna da letra A(2^a coluna) na altura da linha iniciada pela letra R (19^a linha), a intersecção da 2^a coluna com a 19^a linha apresenta a letra S, assim a letra A é substituída por S. A palavra chave é usada de forma cíclica como já foi mencionado. Quadro 5 elaborado pelo autor.

Quadro 5 – Cifra de Vegenère

texto	M	A	T	E	M	A	T	I	C	A
chave	G	R	I	T	O	G	R	I	T	O
cifra	T	S	C	Y	B	H	L	R	W	P

Um sistema de chave dupla foi criado por Giambattista Della Porta (1535 – 1615) em 1563. A cifra é composta de 11 alfabetos, conforme figura 5, em que as letras de uma mesma coluna são cambiáveis na cifragem (COUTO, 2008).

Uma palavra chave era usada e determinava o uso dos alfabetos. Como exemplo, usando a palavra chave for NATO, para cifra o texto ENSINO MÉDIO. Procura-se o alfabeto que contenha a letra N (primeira letra da palavra chave). Esse alfabeto é MN conforme figura 5, nele as letras E e Y estão na mesma coluna e, por isso, o E deve ser substituído por Y. Na sequência busca-se o alfabeto que contenha a letra A (segunda letra da palavra chave). Esse alfabeto é AB e nele N e A estão na mesma coluna, o N é substituído por A. Para encontra o substituto de S procura-se um alfabe que tenha a letra T que é o ST e, nele, a letra S deve ser substituída por B e assim seguidamente. A chave é usada ciclicamente, ou seja, ao se usar a ultima letra volta-se a usar a primeira e a segunda, e assim sucessivamente. O resultado é a cifra: YABOGB QWXVK.

Figura 7 – Alfabeto Della Porta

Alfabeto	Letras intercambiáveis												
AB	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
CD	A	B	C	D	E	F	G	H	I	J	K	L	M
	Z	N	O	P	Q	R	S	T	U	V	W	X	Y
EF	A	B	C	D	E	F	G	H	I	J	K	L	M
	Y	Z	N	O	P	Q	R	S	T	U	V	W	X
GH	A	B	C	D	E	F	G	H	I	J	K	L	M
	X	Y	Z	N	O	P	Q	R	S	T	U	V	W
IJ	A	B	C	D	E	F	G	H	I	J	K	L	M
	W	X	Y	Z	N	O	P	Q	R	S	T	U	V
KL	A	B	C	D	E	F	G	H	I	J	K	L	M
	V	W	X	Y	Z	N	O	P	Q	R	S	T	U
MN	A	B	C	D	E	F	G	H	I	J	K	L	M
	U	V	W	X	Y	Z	N	O	P	Q	R	S	T
OP	A	B	C	D	E	F	G	H	I	J	K	L	M
	T	U	V	X	W	Y	Z	N	O	P	Q	R	S
QR	A	B	C	D	E	F	G	H	I	J	K	L	M
	S	T	U	V	W	X	Y	Z	N	O	P	Q	R
ST	A	B	C	D	E	F	G	H	I	J	K	L	M
	R	S	T	U	V	W	X	Y	Z	N	O	P	Q
UV	A	B	C	D	E	F	G	H	I	J	K	L	M
	Q	R	S	T	U	V	W	X	Y	Z	N	O	P
WX	A	B	C	D	E	F	G	H	I	J	K	L	M
	P	Q	R	S	T	U	V	W	X	Y	Z	N	O
YZ	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	P	Q	R	S	T	U	V	W	X	Y	Z	N

Fonte: elaborado pelo autor com base em Couto, 2008. pg.82

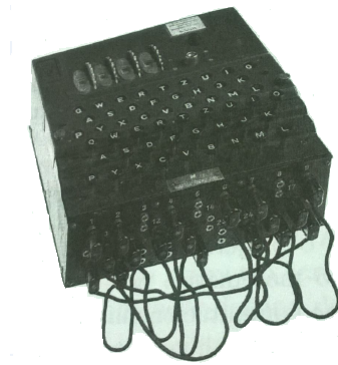
2.2.4 Tópicos de criptografia durante o século XX

O italiano Guglielmo Marconi (1874 – 1937) patenteia o rádio em 1901 iniciando a comunicação à distância e sem fio. Em 1917 o norte americano Gilbert Sandford Vernam (1890 – 1960) cria uma máquina de encriptar polialfabética que usa uma chave totalmente randômica. Em 1919 uma máquina cifrante com base em rotores é patenteada pelo holandês Hugo Alexander Koch (1870 – 1928) que repassa sua criação a Arthur Scherbius, empresário que fabrica e vende ao exército alemão a máquina que fica conhecida como Enigma (COUTO, 2008).

Em 1929 o norte americano Lester S. Hill (1891 – 1961) apresenta um método de cifragem a partir do uso de operações matriciais, tal método ficou conhecido como cifra de Hill. Nos anos 30, William Friedman (1891 – 1969) cria a máquina SIGABA, também conhecida como Conversor M-134. Enquanto a máquina ENIGMA contava com 4 ou 5 rotores, o M-134 contava com 15 rotores sendo 5 para controle dos passos e 10 para transformação de caracteres (COUTO, 2008).

Os japoneses apresentaram, em 1937, a máquina Púrpura, que usava relês (um interruptor eletromecânico) telefônicos em substituição aos rotores e isso aumentava o

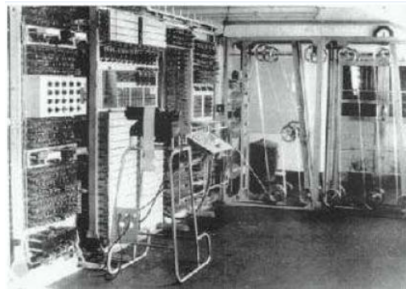
Figura 8 – Enigma



Fonte: Terada, 2008. pg 20

número de permutações a cada passo. Em 1943 os ingleses põem em ação a partir do Centro de Estudos Criptológicos da Inglaterra, situado em Bletchley Park, um computador para analisar e quebrar códigos, chamado Colossus (COUTO, 2008).

Figura 9 – Colossus



Fonte: Fonseca, 2007. pg 106

Na década de 60 o alemão Horst Feistel (1915 – 1990), à frente de uma equipe de pesquisa da IBM, traz a público a cifra Lúçifer, uma cifra de bloco cuja versão DTD-1 passa a ser usada nos caixas eletrônicos nos anos 70. O governo americano analisa a cifra Lucifer em 1976, com a ajuda da NSA (National Security Agency ou Agência Nacional de Segurança) e NBS (National Bureau of Standards ou Escritório Nacional de Padrões), sugerem algumas modificações e passam a usá-la como padrão de encriptação agora conhecida como DES (Data Encryption Standard ou padrão de encriptação de dados) (COUTO, 2008).

Durante muito tempo a criptografia foi feita usando-se chaves simétricas, que é o uso da mesma chave tanto para cifrar quanto para decifrar e isso, de certa forma, é um problema pois, há dificuldade na maneira de comunicar essa chave ou no gerenciamento de múltiplas chaves em comunicação com um número elevado de pessoas.

Bailey Whitfield Diffie (1944 -) e Martin Eduward Hellman (1945 -) sugerem o uso de chave pública, com base em uma função de via única, em seu livro *New Directions in Cryptography*. Na criptografia a natureza das chaves passa a se dar de duas formas:

podem ser simétricas ou assimétricas. O uso de chaves assimétricas, em que o emissor e o destinatário da mensagem possuem chaves diferentes com uma operando de forma inversa à outra, resolveu os problemas de distribuição e gerenciamento de chaves.

Os pesquisadores Ronald L. Rivest (1947 -), Adi Shamir (1952 -) e Leonard M. Adleman (1945 -) atendem à sugestão de Diffie e Hellman e apresentam, em um artigo de 1977, a cifra RSA (primeira letra do nome de cada pesquisador), uma cifra de chave pública, qual era tanto processo de criptografia quanto para assinatura digital (COUTO, 2008).

Antes do século 20 a criptoanálise podia ser tentada com papel e caneta mas as inovações como as máquinas baseadas em rotores durante as grandes guerras mundiais tornaram essa tarefa extremamente complicada. Ainda sim foi possível ao gênio de Alan Turing e sua equipe, cujo trabalho assentou as bases para a computação. O computador pode efetuar uma quantidade de cálculos que é impossível de realizar à mão por uma pessoa.

As mensagens são convertidas em bits, que é a unidade base na linguagem dos computadores, e então são encriptadas. Esse trabalho pode ser feito, pelo menos, de duas formas: algoritmo de fluxo ou algoritmo de bloco. O algoritmo de *fluxo* executa bit a bit a mensagem clara e alguns algoritmo de fluxo são o RC4 e one-time-pad que é o único considerado matematicamente inquebrável, por ter a chave do tamanho da mensagem. O algoritmo de *blocos* que junta um "pacote" de bits e encripta todo o bloco de uma vez, alguns exemplares são o DES, IDEA E RC5 (CARVALHO, D., 2000).

Cada bit pode assumir dois valores 0 ou 1 e cada vez que se acrescenta um bit dobra-se a quantidade de escritas possíveis naquele espaço. Uma chave de 10 bits é que equivale a 1024 possibilidade.

Em 1990 são publicados os primeiros experimentos em criptografia quântica baseados no artigo pioneiro em 1984 de Charles H. Bennett, norte-americano, e Gilles Brassard (1955 -), canadense. Em 1999 o padrão DES de 56 bits foi, mais uma vez, quebrado por um computador chamado Deep Crack depois de trabalhar por 22 horas e 15 minutos, em resposta o governo americano adota o triple-DES, a aplicação tripla do algoritmo DES com chaves de 64 bits. No ano 2000 o DES é substituído pelo AES (Advanced Encryption Standard ou padrão de encriptação avançado) que antes se chamava algoritmo Rijndael (COUTO, 2008).

3 CONCEITOS BÁSICOS DA TEORIA DOS NÚMEROS

A construção matemática se dá por meio de axiomas ou postulados, conjecturas e teoremas. Como um castelo que é construído bloco a bloco tal é a matemática. Infelizmente, por dificuldades diversas esse castelo não tem sido construído em todas as salas de ensino médio brasileiro. Quem é professor de matemática sabe que o tempo ou os recursos nem sempre permitem a apresentação dos conteúdos mencionando princípios, postulados ou qualquer demonstração. O professor deve lançar mão dos melhores recursos metodológicos para promover a aprendizagem significativa a seus estudantes e é importante que ele considere, também e sempre que possível, a estrutura axiomática, os teoremas e suas demonstrações.

DEFINIÇÃO 1: Proposição é uma afirmação que pode assumir, um e somente um valor, verdade ou falsidade.

Parte do trabalho matemático consiste em analisar proposições e determinar sua veracidade ou falsidade.

DEFINIÇÃO 2: Postulado ou axioma é uma verdade aceita sem prova a partir da qual se provam outras proposições que são os teoremas.

DEFINIÇÃO 3: Uma conjectura é uma proposição que ainda não foi nem provada nem refutada.

Há, entre outras, duas importantes técnicas de demonstração: a demonstração por absurdo e o princípio da indução finita. A primeira consiste em encontrar uma contradição em uma proposição tomada como verdadeira. Se sua veracidade leva a contradição então, conclui-se que sua negação será aceita com valor lógico verdadeiro; a segunda consiste em verificar se uma propriedade se estende aos sucessores a partir de um primeiro e particular caso ou de antecessores.

No escopo da técnica de criptografia RSA o conjunto universo é o conjunto dos números inteiros e de grande importância são seus subconjuntos e chamados respectivamente de inteiros não-negativos (\mathbb{Z}_+) e conjuntos dos naturais (\mathbb{N}). A teoria dos números serve de base para grande parte dos sistemas de criptografia sendo que a segurança de um sistema depende do tamanho da chave e do tempo computacional de quebra de cifras (STALING, 2011).

3.1 O conjunto dos números naturais

O conjunto dos números naturais é intuitivamente aceito e se presta à contagem. Se um estudante de ensino médio for perguntado sobre os número naturais é bem provável que ele o enumere alguns elementos como: $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

Matematicamente essa descrição nao é suficiente para dizer o que é o conjunto dos números natuais e, por isso, a formalização do conjunto dos naturais foi realizada pelo matemático italiano Giuseppe Peano (1858 - 1932) em quatro axiomas conhecidos como axiomas de Peano (LIMA; CARVALHO; MORGADO, 2003):

1. Todo número natural tem um único sucessor;
2. Números naturais diferentes têm sucessores diferentes;
3. Existe um único número natural, chamado *um* e representado por 1, que não é sucessor de nenhum outro;
4. Seja X um conjunto de números naturais. Se $1 \in X$ e se, além disso, o sucessor de todo elemento de X ainda pertence a X, entao $X = \mathbb{N}$.

Observa-se que o elemento zero não consta na formalização. Esse elemento não é um número natural mas, para atender algumas propriedades (a exemplo do elemento neutro) e operações, ele tem sido considerado e apresentado nos livros de ensino básico como número natural.

Princípio da Indução Finita

O princípio da indução finita é uma poderosa forma de demonstração usando sequências relacionadas aos naturais.

PROPOSIÇÃO 1: (Primeira forma do princípio da indução finita - P.I.F.) Suponha que a todo natural n esteja associada uma afirmação $P(n)$ em que:

- i) $P(1)$ é verdadeira;
- ii) $P(n+1)$ é verdadeira sempre que $P(n)$ for verdadeira,

Então $P(n)$ é verdadeira para qualquer n .

EXEMPLO 1: Observando que $1 = 1^2$; $(1 + 3) = 2^2$ e $(1 + 3 + 5) = 3^2$, pode se conjecturar se a soma dos primeiros n números impares equivale a n^2 . Pode-se obter a resposta pelo uso do P.I.F.

Representando os números pares por $2k$ e os números ímpress por $(2k-1)$, com $k \in \mathbb{N}$:

- i) satisfeita, pois $1 = 1^2$;
- ii) Suponha a propriedade válida para $(2k-1)$,

$$\begin{aligned}
[1 + 3 + 5 + \dots + (2k - 1)] &= k^2, \text{ acrescentando mais um termo} \\
(1 + 3 + 5 + \dots + (2k - 1) + (2k + 1)) &= k^2 + (2k + 1) \\
&= k^2 + 2k + 1 \\
&= (k + 1)^2 \quad \blacksquare
\end{aligned}$$

3.2 O conjunto dos números inteiros

No conjunto dos naturais a diferença entre dois de seus elementos a e b , representada por $a - b$, só está estabelecida quando $a > b$. O conjunto dos inteiros é conhecido desde a segunda etapa da educação básica (do 6º ao 9º anos) sendo possível atualizar sua definição e dar sentido à expressão $(b - a)$ por meio de uma ampliação do conjunto dos naturais. Nessa ampliação busca-se dar sentido para toda solução de $(a + x = b)$ com a e b naturais, obtendo, de forma única $(x = b - a)$ (DOMINGUES, 1991). Tem-se que:

- $1 - 1 = 2 - 2 = \dots = n - n = 0$ (classe da diferença entre iguais);
- $0 - 1 = 1 - 2 = \dots = k - (k+1) = -1$;
- $0 - m = 1 - (m+1) = \dots = k - (m+k) = -m$;
- $m - 0 = (m+1) - 1 = \dots = (m+k) - k = +m$.

Assim, surge o conjunto dos números inteiros, representado por \mathbb{Z} e nele o zero é definido com o representante de classe de diferença entre iguais. Para mais detalhes consultar (DOMINGUES, 1991). Assim, o conjunto dos inteiros é:

$$\mathbb{Z} = \{\dots - 3, -2, -1, 0, +1, +2, +3, \dots\}$$

Na sequência são apresentadas algumas operações no conjunto dos inteiros e suas propriedades.

Adição em \mathbb{Z}

Para a operação de adição, verificam-se as seguintes propriedades:

- i) $(a + b) + c = a + (b + c)$, a , b e c (associativa);
- ii) $a + b = b + a$, a e b (comutativa);
- iii) $\exists 0 \in \mathbb{Z} \mid a + 0 = 0 + a = a$, $\forall a \in \mathbb{Z}$ (elemento neutro da adição);
- iv) $\forall a \in \mathbb{Z}, \exists b \in \mathbb{Z} \mid a + b = b + a = 0$, (elemento simétrico).

O elemento simétrico, ou oposto de a , é único e representado por $-a$.

PROPOSIÇÃO 2: Quaisquer que sejam a , b e c , quando $a + c = b + c$, então $a = b$ (lei do cancelamento)(DOMINGUES, 1991).

DEMONSTRAÇÃO como há elemento simétrico para todo inteiro (item iv da adição em \mathbb{Z} pode-se somar o simétrico ao elementos repetido (b) em cada membro da equação:

$$\begin{aligned} a + b &= b + c \\ a + b - b &= b + c - b \\ a + (b - b) &= (b - b) + c \\ a + 0 &= 0 + c \\ a &= c. \end{aligned}$$

■

DEFINIÇÃO 4: Para m , n inteiros, o elemento m será menor ou igual a n , simbolicamente $m \leq n$, se $n = m + r$, com r inteiro não negativo.

DEFINIÇÃO 5: Dado um elemento qualquer de \mathbb{Z} , o seu módulo, ou valor absoluto, é definido pelas condições seguintes:

$$|a| = \begin{cases} a, & \text{se } a \geq 0 \\ -a, & \text{se } a < 0 \end{cases}$$

Multiplicação em \mathbb{Z}

As propriedades da multiplicação em \mathbb{Z} são:

- i) $(ab)c = a(bc)$, $\forall a, b \text{ e } c \in \mathbb{Z}$ (associativa);
- ii) $ab = ba$, $\forall a \text{ e } b \in \mathbb{Z}$ (comutativa);
- iii) $a \cdot 1 = a$, $\forall a \in \mathbb{Z}$ (elemento neutro da multiplicação);
- iv) $ab = 0$ $a = 0$ ou $b = 0$ (lei do anulamento do produto);
- v) $a(b + c) = ab + ac$, $\forall a, b \text{ e } c \in \mathbb{Z}$ (a multiplicação é distributiva em relação à soma).

DEFINIÇÃO 6: O conjunto dos múltiplos de um número inteiro k , em \mathbb{Z} , é o resultado da multiplicação de k pelos elementos de \mathbb{Z} . Indicando por $M(k)$ o conjunto dos múltiplos de k , tem-se:

$$M(k) = \{\dots, -4k, -3k, -2k, -k, 0, +k, +2k, +3k, +4k, \dots\}$$

$M_{(k)}$ representa o conjunto dos números pares dados por $M_{(2k)} = \{\dots, -4, -2, 0, 2, 4, 6, \dots\}$ ao passo que o conjunto dos ímpares é dado por $M_{(2k+1)} = \mathbb{Z} - M_{(2k)}$. Tem-se que $M_{(2k+1)} = \{\dots, -5, -3, -1, 1, 3, 5, \dots\}$ (DOMINGUES, 1991).

TEOREMA 1 - (Teorema de Eudoxius): Dados a e b inteiros, com $b \neq 0$ então a é múltiplo de b ou se encontra entre dois múltiplos de b , isto é, correspondendo a cada par de inteiros a e $b \neq 0$ existe um inteiros q tal que (STALLING, 2011),

$$\text{para } b > 0, qb \leq a \leq (q+1)b; \text{ e}$$

$$\text{para } b < 0, qb \leq a \leq (q-1)b.$$

DEMONSTRAÇÃO

Considere $a > 0$ e $b > 0$ (os casos em que a ou b negativo podem ser demonstrados de forma análoga), há duas possibilidades:

- i) Se $a = wb$, com $w \in \mathbb{Z}$ não há o que provar;
- ii) se $a \neq wb$ existe um menor inteiro k que satisfaz a condição: $a < kb$.
a relação entre $(k-1)b$ e a é tal que:

- $a \neq kb$, pelo item ii e;
- $a \not< (k-1)b$ pois contraria a hipótese de k ser o menor inteiro a satisfazer $a < kb$;

por tanto $a > (k-1)b$ e a está entre dois múltiplos consecutivos de b . ■

DEFINIÇÃO 7: Se $a = bc$ para algum c , a e b inteiros, então é dito que b divide a . Quando isso acontece também se diz que b é divisor de a ou que a é múltiplo de b (ou divisível por b). Quando b divide a usa-se a notação $b|a$ e quando b não divide a , $b \nmid a$. O elemento c tal que $a = bc$ é chamado quociente de a por b e indicado por $c = \frac{a}{b}$ (também é comum $a : b$) (DOMINGUES, 1991).

EXEMPLO 2: Nas notações abaixo 3 divide 21 pois se pode escrever o vinte e um tendo o três como fator, já o 4 não divide 29 pois não lhe é fator.

- $3|21$, pois $21 = 7 \cdot 3$;
- $4 \nmid 29$, pois $\nexists k$ tal que $29 = 4 \cdot k$.

DEFINIÇÃO 8: Um número m é dito mínimo múltiplo comum (MMC) de a e b , se:

- i) $m \geq 0$;
- ii) $a|m$ e $b|m$ (m é múltiplo de a e de b);

iii) $a|m'$ e $b|m'$, então $m|m'$ (todo múltiplo de a e b é também múltiplo de m)(DOMINGUES, 1991).

3.3 O algoritmo de Euclides

TEOREMA 2 - (Algoritmo de Euclides): Sejam $a, b \in \mathbb{Z}$, $b \neq 0$, há um par, e é único, de inteiros q e r , tais que $a = b \cdot q + r$, em que $0 \leq r < |b|$. O elemento a é chamado de dividendo, o elemento b é o divisor, q é dito quociente e r é o resto na divisão euclidiana de a por b (CARVALHO, D, 2000).

DEMONSTRAÇÃO

Pelo Teorema de Eudoxius, considere, por simplificação, já que os outros casos são demonstrados similarmente, $b > 0$, existe q satisfazendo:

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

O que implica $0 \leq a - bq$ e $a - bq < b$. Ao se definir $r = a - bq$, há garantia da existência de q e r . Para mostrar a unicidade, considera-se a existência de outro par de inteiros q' e r' tais que:

$$a = q'b + r', \text{ com } 0 \leq r' < |b|.$$

tem-se que $(qb + r) - (q'b + r') = 0 \Rightarrow b(q - q') = (r' - r) \Rightarrow b|(r' - r)$.

Como $r < |b|$ e $r' < |b|$, tem-se que $|r' - r| < |b|$ e b divide $|r' - r|$, deve-se ter $r' - r = 0 \Rightarrow r' = r$ e $q = q'$. ■

EXEMPLO 3: Seja a divisão de $a = 22$ por $b = 3$, tem-se: $22 = 7 \cdot 3 + 1$.

É possível, por conveniência, que toda divisão seja feita com os módulos do dividendo e do divisor. Deve-se considerar que o resto terá o mesmo sinal que o dividendo e que o quociente será positivo quando dividendo e divisor tiverem mesmo sinal e negativo quando tiverem sinais opostos. Nos exemplos seguintes, por simplicidade expositiva, as divisões serão feitas com divisor e dividendo positivos.

DEFINIÇÃO 9: O máximo divisor comum (MDC) entre dois inteiros a e b quaisquer é o número d que satisfaz as seguintes condições:

- i) $d > 0$;
- ii) $d|a$ e $d|b$, ou seja, existem $k \in \mathbb{Z}$ e $w \in \mathbb{Z}$ tais que $a = kd$ e $b = wd$;
- iii) Se $c|a$ e $c|b$ então $c|d$, com $c \in \mathbb{Z}$ (DOMINGUES, 1991).

PROPOSIÇÃO 3: Se $a|b$, então $\text{mdc}(a, b) = |a|$.

DEMONSTRAÇÃO - por (DOMINGUES, 1991): Observa-se que $|a|$ satisfaz os 3 quesitos para ser mdc.

PROPOSIÇÃO 4: Se $a = qb + r$ e $d = \text{mdc}(a, b)$, então $d = \text{mdc}(b, r)$. E se $d = \text{mdc}(b, r)$, então $d = \text{mdc}(a, b)$.

DEMONSTRAÇÃO - por (DOMINGUES, 1991):

Sendo $d = \text{mdc}(a, b)$ e $c = \text{mdc}(b, r)$. Sabes-e que $d|a$ e $d|b$ o que implica em $d|bq$. Assim $d|(a - bq)$ o que equivale a $d|r$. Pela propriedade iii do mdc qualquer inteiro que divida b e divida r também divide o mdc entre b e r , Assim $d|c$; De outra forma se $c|b$ e $c|r$, como $(bq + r) = a$, então $c|b$ e $c|a$ e, pela mesma propriedade iii do mdc, c divide o mdc entre a e b , ou seja, $c|d$; Das duas constatações acima em que $c|d$ e $d|c$ conclui-se que $d = c$. ■

Existe um artifício para cálculo de mdc a partir da proposição 4 que consiste em converter cada divisor no próximo dividendo e cada resto no próximo divisor. Esse artifício esta esquematizado na tabela 1 em que q_n representa o n-ésimo quociente e r_n o n-ésimo resto. A tabela 1 foi elaborada pelo autor.

Tabela 1 – Processo de divisões sucessivas

	q_1	q_2	q_3	...	$q_{(n-2)}$	$q_{(n-1)}$	q_n
a	b	r_1	r_2	...	$r_{(n-3)}$	$r_{(n-2)}$	$r_{(n-1)}$
r_1	r_2	r_3	...	$r_{(n-2)}$	$r_{(n-1)}$	0	

Apresenta-se, também, uma aplicação numérica do uso desse processo de divisões sucessivas que é, ainda hoje, uma das melhores formas de se computar mdc entre dois inteiros, principalmente para grandes números.

Na divisão, pelo do algoritmo de Euclides, estima-se valor máximo para cada quociente, subtrai-se do dividendo o produto do quociente pelo divisor obtendo-se cada resto, até que o último resto seja menor que o divisor. Assim, a divisão para e obtêm-se quociente e resto, únicos. Isto sempre acontece, pois a sequência dos restos obtidos é formada por números inteiros positivos e decrescentes.

EXEMPLO 4: Calcule o mdc entre 301 e 84

	3	1	1	2	2
301	84	49	35	14	7
49	35	14	7	0	

Então, pelo processo descrito o mdc entre 301 e 84 é 7.

TEOREMA 3 - (teorema de Bachet-Bézout): Sejam a e b inteiros e $d = \text{mdc}(a, b)$, então existem inteiros x_0 e y_0 de forma que:

$$ax_0 + by_0 = d$$

Essa identidade, para os números inteiros, foi provada pelo matemático francês Claude Gaspard Bachet de Méziriac (1581 – 1638). O matemático francês Étienne Bézout (1730 – 1783), provou o equivalente do resultado para polinômios. Essa expressão, na verdade é uma versão simplificada por haver apenas dois inteiros.

DEMONSTRAÇÃO - por (NETO, 2012): Considere dois inteiros a e b cujo $\text{mdc}(a, b) = d$, isso significa que existem k_1 e k_2 inteiros tais que $a = k_1d$ e $b = k_2d$. Considere, também, S como o conjunto de todas as combinações lineares entre a e b , ou seja, $S = ax_0 + by_0 \forall x_0, y_0 \in \mathbb{Z}$ e T como o conjunto dos múltiplos de d , ou seja, $T = d\mathbb{Z}$.

A prova se dá em duas etapas:

Primeira parte: é fácil provar que $S \subset T$, pois $ax_0 + by_0 = k_1dx_0 + k_2dx_0 = d(k_1x_0 + k_2x_0)$ que pertence a $d\mathbb{Z}$.

Segunda parte: consiste em mostrar que $T \subset S$. Para isso, faz-se $x_0 = a$ e $y_0 = 0$. Assim, verifica-se a existência de elementos estritamente positivos em S , nesse caso a^2 . O conjunto dos elementos estritamente positivos de S apresenta um menor elemento que será denotado d' .

$d' = ax_0' + by_0'$ por pertencer a S , para algum x_0' e algum y_0' inteiros. Dessa forma, $d' = k_1dx_0' + k_2dy_0' \implies d' = d(k_1x_0' + k_2y_0')$. Isso significa que $d|d'$, então $d' \leq d$. d' não pode ser menor que d pois contraria a hipótese de ser d o menor elemento positivo de S . Conclui-se que $d' = d$ e, assim, pode-se escrever: $ax_0 + by_0 = d$.

COROLÁRIO 1: Dois números a e b são primos entre si ou coprimos, isto é, não apresentam fatores comuns, se e somente se, existem x_0 e $y_0 \in \mathbb{Z}$ tais que $ax_0 + by_0 = 1$.

DEMONSTRAÇÃO: Sejam dois inteiros a e b cujo $\text{mdc}(a, b) = 1$. Pelo teorema de Bezout existem x_0 e y_0 tais que $ax_0 + by_0 = 1$. Por outro lado, considerando a expressão $ax_0 + by_0 = 1$, sendo $1 > 0$, $1|a$, $1|b$. Se $c|a$ e $c|b$, então $c|(ax_0 + by_0)$, o que equivale a $c|1$ conforme item iii da definição 9, $c = 1$. ■

Há um dispositivo chamado de algoritmo estendido de Euclides que facilita o cálculo dos coeficientes para escrever o $\text{mdc}(a, b)$ em função de a e b . O dispositivo é uma tabela em que a primeira coluna é a dos "restos", a segunda coluna é a dos quocientes, a terceira coluna é a dos coeficientes de a e a última coluna é dos coeficientes de b . A tabela 2 foi elaborada pelo autor.

O preenchimento das duas primeiras colunas é feita usando o algoritmo de Euclides. Ao se dividir a por b é gerado o quociente q_1 e resto r_1 . Dividindo-se b por r_1 são gerados q_2 e r_2 e assim seguidamente.

As outras duas colunas referentes aos coeficientes x_0 e y_0 são preenchidas da seguinte

Tabela 2 – Algoritmo estendido de Euclides

restos	quociente	coef. de a (x_0)	coef. de b (y_0)
a	*	(1)a	(0)b
b	*	(0)a	(1)b
r_1	q_1	(1)a	$(-q_1)b$
r_2	q_2	$(-q_2)a$	$[1 - q_2q_1]b$
r_3	q_3	$(1 + q_2q_3)a$	$[-q_1 - (q_3 - q_1q_2q_3)]b$

forma: o coeficiente de a da n-ésima linha é o coeficiente de a da (n-2)-ésima linha menos o produto do coeficiente de a da (n-1)-ésima linha pelo quociente da n-ésima linha.

Para os coeficientes de b a forma é semelhante. O coeficiente da n-ésima linha é o coeficiente de b da (n-2)-ésima linha menos o produto do coeficiente de b da (n-1)-ésima linha pelo quociente da n-ésima linha.

EXEMPLO 5: Considere $a = 19$ e $b = 8$.

Tabela 3 – Exemplo numérico do algoritmo estendido de Euclides

restos	quociente	coef. de a (x_0)	coef. de b (y_0)
19	*	(1)	(0)
8	*	(0)	(1)
3	2	$[(1)-(0).2] = 1$	$[(0)-(1).2] = -2$
2	2	$[(0)-(1).2] = -2$	$[(1)-(-2).2] = 5$
1	1	$[(1)-(-2).1] = 3$	$[(-2)-(5).1] = -7$

Quando o resto é igual ao mdc sabe-se que o processo findou. Dessa forma podem ser encontrados os coeficientes para se escrever o resto em função de $a = 19$ e $b = 8$, especificamente da última linha se tira: $1 = (3)19 + (-7)8$. Os números 8 e 19 coprimos, ou seja, primos entre si. A tabela 3 foi elaborada pelo autor.

3.4 Números primos

Os números primos e algumas de suas propriedades fundamentais serão apresentados e justificados nesta seção devido a sua extrema importância para o algoritmo de criptografia RSA.

DEFINIÇÃO 10: Um número $p \in \mathbb{Z}$ é dito primo se:

- i) $|p| \neq 0$;
- ii) $|p| \neq 1$;
- iii) p tem como seus únicos divisores ± 1 e $\pm p$.

DEFINIÇÃO 11: Número composto é um número inteiro não nulo, diferente de 1 e não primo (DOMINGUES, 1991).

TEOREMA 4 - (Teorema Fundamental da Aritmética em \mathbb{Z}): Seja $a \in \mathbb{Z}$, $a \neq 0$ e $a \neq \pm 1$. Existem números primos $p_1, p_2, \dots, p_n \in \mathbb{Z} (n \geq 1)$, todos com módulo maior que 1, de maneira que:

$$a = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \dots p_n \text{ ou } a = -p_1 \cdot p_2 \cdot p_3 \cdot p_4 \dots p_n$$

de acordo com $a > 0$ ou $a < 0$. Essa decomposição é única, desconsiderando a ordem dos fatores (DOMINGUES, 1991).

DEMONSTRAÇÃO: Caso a seja primo nada há para provar; caso a seja composto ele pode ser escrito como produto de dois ou mais fatores. Considere um inteiro a positivo escrito como produto de dois fatores, assim $a = p_1 \cdot a_1$, com p_1 o menor dos divisores de a . Afirma-se que p_1 é primo pois caso contrário existiria um k , $1 < k < p_1$ tal que $k|a$ contradizendo o fato de ser p_1 o menor dos fatores de a . Repetindo-se esse processo chega-se a: $a = p_1 \cdot p_2 \cdot p_3 \dots p_n$. ■

Sobre a decomposição em fatores primos

I) Na decomposição $a = p_1 \cdot p_2 \dots p_r$, conforme o teorema 4, nem sempre todos os fatores são diferentes entre si. A reunião de possíveis fatores iguais leva à expressão:

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \dots p_n^{\alpha_n}$$

II) pode ser conveniente que, às vezes, ao lidar com dois ou mais números maiores que 1, estejam eles escritos como potências dos mesmos primos. Isso é possível, obviamente, desde que se utilizem expoentes nulos, como no exemplo a seguir:

$$120 = 2^3 \cdot 3^1 \cdot 5^1 \cdot 7^0 \text{ e } 350 = 2^1 \cdot 3^0 \cdot 5^2 \cdot 7^1$$

III) De I e II decorre, considerando ainda o teorema fundamental da aritmética, o seguinte critério:

Dado $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \dots p_n^{\alpha_n}$, conforme I ou II, então um número b é divisor de a se, e somente se, $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \dots p_n^{\beta_n}$ em que $0 \leq \beta_i \leq \alpha_i$ com $(i = 1, 2, \dots, n)$.

De fato, se $b|a$, o teorema fundamental da aritmética garante não haver fatores primos de b que não sejam fatores primos de a . Mas nem todos os fatores primos de a precisam estar na decomposição de b em primos. Daí os possíveis expoentes nulos em fatores de b , mesmo que não os haja em a . Quanto à recíproca, tomando $c = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot p_3^{\gamma_3} \dots p_n^{\gamma_n}$, em

que $\gamma_i = \alpha_i - \beta_i$ com ($i = 1, 2, \dots, s$), então $c \in \mathbb{Z}$ e $cb = a$. Logo $b|a$ (SANTOS, 2009).

PROPOSIÇÃO 5 - (Euclides): O conjunto dos números primos é infinito.

DEMONSTRAÇÃO: A demonstração consiste em considerar o produtos de todos os supostos finitos primos e formar o números composto $n = p_1 \cdot p_2 \cdot \dots \cdot p_k$, seu sucessor $(n+1) = p_1 \cdot p_2 \cdot \dots \cdot p_r + 1$ quando dividido por todos os fatores primos deixa resto 1 e, portanto, não é divisível por nenhum número além de 1 e $(n+1)$ sendo, então, primo. ■

PROPOSIÇÃO 6: Se n não é primo, então n possui, necessariamente, um fator primo menor ou igual a \sqrt{n} .

DEMONSTRAÇÃO - por (SANTOS, 2009): Sendo n composto é possível escrevê-lo como $n = n_1 \cdot n_2$ em que $1 < n_1 < n$ e $1 < n_2 < n$. Sem perda de generalidade considere $n_1 \leq n_2$. Logo $n_1 \leq \sqrt{n}$ pois, caso contrário, ter-se-ia $n = n_1 \cdot n_2 > \sqrt{n} \cdot \sqrt{n} > n$, o que é absurdo. ■

Para testar se um número é primo, é suficiente dividi-lo apenas pelos primos $\leq \sqrt{n}$. Este processo é chamado Crivo de Eratóstenes e será mostrado na próxima seção.

3.4.1 Técnicas de abordagem de primos: tentativas de equacioná-los

Os registros evidenciam Eratóstenes como um dos primeiros a tentar sistematizar o conjunto dos números primos, e seu método é tido como o primeiro ou um dos mais antigo algoritmo de procura de primos. Seu algoritmo conhecido como crivo de Eratóstenes possibilita separar os primos de um conjunto finito de inteiros. Abaixo há a descrição do crivo de Eratóstenes bem como outras tentativas de localização e organização de primos que foram e continuam a ser pesquisadas desafiando os maiores matemáticos. A questão de localização dos números primos ainda está em aberto e há um prêmio para quem resolver tal problema. É importante observar os trabalhos dos matemáticos, como abordaram essa situação, abaixo um pequeno relato histórico dessas tentativas, além do crivo houve uso fórmulas polinomiais, exponenciais, fatoriais e uma abordagem que leva a uma estimativa logarítmica de detecção de primos (COUTINHO, 2003).

ABORDAGEM 1: (verificação): Provavelmente os primeiros a buscar disputam, apenas, da tentativa direta. Ao dividir um número por seus antecessores podia se detectar se era composto ou primo.

ABORDAGEM 2: (Crivo de Eratóstenes): Inicialmente o crivo de Eratóstenes consiste em tabelar uma quantidade finita de inteiros positivos, manter os primos e eliminar seus múltiplos compostos, em ordem crescente, dos primos identificados. Por exemplo, analisar-se-á o conjunto A dos primeiros 50 inteiros positivos, ou seja,

$$A = \{x \in \mathbb{Z}_+^* \mid 1 \leq x \leq 50\}$$

Elimina-se o 1 por não ser primo, mantém-se o 2 que é o primeiro primo e o único par, eliminam-se todos os seus múltiplos; mantém-se o 3 e eliminam-se todos os seus múltiplos;

Lembrando-se de que todo número n tem um fator menor ou igual a \sqrt{n} e sendo $\sqrt{50} \simeq 7$, só é necessário, então, eliminar até os múltiplos de 7. Ao final tem-se o conjunto de todos os primos pertencentes ao conjunto inicial. A tabela 4 foi elaborada pelo autor.

Tabela 4 – Primos entre 1 e 50

-	2	3	-	5	-	7	-	-	-
11	-	13	-	-	-	17	-	19	-
-	-	23	-	-	-	-	-	29	-
31	-	-	-	-	-	37	-	-	-
41	-	43	-	-	-	47	-	-	-

ABORDAGEM 3: (fórmulas polinomiais): A fórmula polinomial é uma das mais simples na busca de “geração” de primos. Um polinômio tem a forma: $f(x) = a_n x^n + a_{(n-1)} x^{(n-1)} + \dots + a_1 x^1 + a_0$, em que $a_n, a_{(n-1)}, \dots, a_1$ e a_0 são coeficientes inteiros. Espera-se que $f(m)$ seja primo para todo m inteiro positivo (COUTINHO, 2003).

EXEMPLO 6: Seja o polinômio $f(x) = 2x^2 + 5$, nele os primeiros 4 valores numéricos de inteiros positivos resultam em primos. $f(1) = 7$; $f(2) = 13$; $f(3) = 23$ e $f(4) = 37$.

Exemplos de polinômios que fornecem primos para determinado intervalo:

- i) $f(n) = n^2 + n + 41$, válida para $0 \leq n < 40$;
- ii) $f(n) = 2n^2 + 29$, válida para $0 \leq n \leq 28$;
- iii) $f(n) = n^2 + n + 17$, válida para $0 \leq n \leq 16$;
- iv) $f(n) = 3n^2 + 3n + 23$, válida para $0 \leq n \leq 21$. (FILHO, 1981).

Pode-se perguntar se é possível um polinômio que forneça somente valores numéricos primos, a resposta é não conforme o teorema abaixo:

TEOREMA 5: Seja $p(x)$ um polinômio de coeficientes inteiros, há infinitos números inteiros k tais que $f(k)$ é composto.

DEMONSTRAÇÃO - por (COUTINHO, 2003): Será mostrado um caso particular de um polinômio de grau 3, mas o procedimento em outros graus é semelhante. Seja um polinômio na forma:

$$f(x) = a_3 x^3 + a_2 x^2 + a_1 x^1 + a_0, \text{ com } a_3 > 0.$$

Considere um inteiro k satisfazendo a condição $f(k) = p$, com p primo. Para um inteiro positivo h qualquer pode-se calcular $f(k + hp)$, obtendo-se:

$$\begin{aligned} f(k + hp) &= a_3(k + hp)^3 + a_2(k + hp)^2 + a_1(k + hp) + a_0 \\ f(k + hp) &= a_3[(k^3 + 3k^2(hp) + 3k(hp)^2 + (hp)^3)] + a_2[(k^2 + 2k(hp) + (hp)^2)] + a_1(k + hp) + a_0 \\ &= a_3k^3 + 3a_3k^2(hp) + 3a_3k(hp)^2 + a_3(hp)^3 + a_2k^2 + 2a_2k(hp) + a_2(hp)^2 + a_1k + a_1hp + a_0 \\ &= (a_3k^3 + a_2k^2 + a_1k + a_0) + [3a_3k^2(hp) + 3a_3k(hp)^2 + a_3(hp)^3 + 2a_2k(hp) + a_2(hp)^2 + a_1hp] \\ &= p + p[3a_3k^2h + 3a_3kp(h)^2 + a_3h(hp)^2 + 2a_2kh + a_2p(h)^2 + a_1h] \end{aligned}$$

Ajusta-se h para que $[3a_3k^2h + 3a_3kp(h)^2 + a_3h(hp)^2 + 2a_2kh + a_2p(h)^2 + a_1h] > 1$ o que é possível posto que há um termo em h^3 e, para grandes valores, ele se sobrepõe aos demais termos de menor grau. Com essa condição satisfeita, haverá infinitos valores numérico compostos a partir de $f(x)$. ■

ABORDAGEM 4: (fórmulas exponenciais):

A abordagem exponencial ficou famosa devido a Fermat e Mersene.

DEFINIÇÃO 12: Um número é dito perfeito se a soma de seus divisores positivos é igual ao dobro de seu módulo. Assim 28 é perfeito pois os divisores de 28 são (1,2,4,7,14 e 28) cuja soma é 56 e $56 = 2 \cdot (28)$ (COUTINHO, 2003) .

Era sabido por Euclides que os números da forma $2^{(n-1)} \cdot (2^n - 1)$ são perfeitos sempre que $2n - 1$ é primo (COUTINHO, 2003).

Martin Mersenne (1588 - 1648) que foi contemporâneo de Fermat, Descartes e Pascal, tendo trocado correspondências matemáticas com esses e outros matemáticos afirmou que os números da forma $M(n) = 2^n - 1$ seriam primos para $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ e 257 . Os números de expressão $M(n) = 2^n - 1$ ficaram conhecidos como números de Mersenne (COUTINHO, 2003).

PROPOSIÇÃO 7: Expoente composto gera um número de Mersenne $M(n)$ composto.

VERIFICAÇÃO:

Seja $n = ab$, com a, b e n inteiros. Pode-se escrever a expressão $2^{ab} - 1$ como:

$$2^{ab} - 1 = (2^a - 1) \cdot [2^{a(b-1)} + 2^{a(b-2)} + 2^{a(b-3)} + \dots + 2^a + 1].$$

No entanto, o fato de n ser primo não garante que $M(n)$ seja primo. O $M(11) = 2047 = 23 \cdot 89$. São números de Mersenne alguns dos maiores primos conhecidos e embora

seus números não sejam todos primos ainda assim tem sido neles que se buscam primos com mais frequência (COUTINHO, 2003).

Em 1640 Fermat escreve a um matemático conhecido como cavalheiro Frenicle e lhe apresenta a fórmula $F(n) = 2^{2^n} + 1$ conjecturando, após poucas verificações, ser uma fórmula que fornece apenas números primos. Por exemplo, $F(0) = 3$; $F(1) = 5$; $F(2) = 17$; $F(3) = 257$; $F(4) = 65537$ e $F(5) = 4294967297$, nesta última Fermat comete um erro que seria detectado por Euler quase 100 anos depois. Euler verificou que $F(5) = (641) \times (6700417)$ sendo, portanto, um número composto e não primo como supôs Fermat. Há poucos números primos de Fermat conhecidos, diferente dos números de Mersenne que são mais comuns (COUTINHO, 2003). Os números de Mersenne são empregados em algoritmos para determinar se um número muito grande é primo ou composto.

ABORDAGEM 5: (fórmula fatorial)

DEFINIÇÃO 13: Seja k um inteiro positivo e não nulo, o fatorial de um número, representado por $k!$, é o produto deste número por todos os seus antecessores até a unidade, isto é,

$$k! = k(k-1)(k-2)\dots 3.2.1$$

Considere $h(p)$ uma função calculada de forma semelhante ao fatorial de um número mais que tenha por domínio apenas números primos. Assim, $h: \mathbb{Z}_+ \rightarrow \mathbb{Z}_+$ tal que $h(p)$ é o produto de todos os primos menores ou iguais a p (COUTINHO, 2003).

EXEMPLO(S) 7:

$$h(2) = 2; \quad h(3) = 3 \times 2 = 6; \quad h(5) = 5 \times 3 \times 2 = 30, \quad \text{e} \quad h(7) = 7 \times 5 \times 3 \times 2 = 210.$$

Considere agora a função $h'(p) = h(p) + 1$.

$$h'(2) = 3; \quad h'(3) = 7; \quad h'(5) = 31; \quad h'(7) = 211.$$

Um contra exemplo é suficiente para mostrar que ela fornece também números compostos. Calculando $h'(13)$ verifica-se: $h'(13) = 30031 = 59 \times 509$ (COUTINHO, 2003).

ABORDAGEM 6 - (fórmula logarítmica): O desafio de encontrar o próximo primo ou uma fórmula que forneça apenas primos estimulou e continua a estimular muitos matemáticos. Diferentemente dos outros que focavam no próximo primo, Gauss se perguntou sobre quantos primos há entre 1 e um inteiro n qualquer. Gauss se dedicou ao estudo de uma *função conhecida como função de contagem dos números primos* denotada

por $\pi(n)$ que fornece a quantidade de primos de 1 até n (SPENTHOF; SOUZA, 2013, pg.18).

EXEMPLO(S)8:

$\pi(1) = 0$; $\pi(\sqrt{5}) = 1$; $\pi(10) = 4$; $\pi(50) = 15$.

A proporção de números primos de 1 a n é dada por $\frac{\pi(n)}{n}$ e a distribuição média de primos em determinado intervalo de 1 a n é $\frac{n}{\pi(n)}$. Gauss construiu uma tabela no intuito de estudar a distribuição de primos. Abaixo uma tabela semelhante adaptada de (SPENTHOF; SOUZA, 2013) pg.18.

Tabela 5 – Distância média entre primos de 1 a n

n	$\pi(n)$	$\frac{n}{\pi(n)}$
10^3	168	6
10^4	1.229	8,1
10^5	9592	10,4
10^6	78498	12,7
10^7	664.579	15,0
10^8	5.761.455	17,4
10^9	50.847.534	19,7
10^{10}	455.052.511	22,0

Gauss observou que ao multiplicar n por 10 a distribuição média de primos no intervalo de 1 a n fica acrescida de 2,3 aproximadamente. Sabendo que as funções logarítmicas apresentam a propriedade de converter produto em soma ele conjecturou uma base na qual o logaritmo de n expressasse a distribuição média de primos no intervalo de 1 a n . Gauss verificou que essa base poderia ser a base e , dessa forma:

$$\frac{n}{\pi(n)} \simeq \ln(n) \implies \pi(n) \simeq \frac{n}{\ln(n)}$$

A conjectura de Gaus foi retomada por Charles-Jean de La Vallée Poussin (1866 - 1962) e Jacques Hadamard (1865 -1963), que em 1896, de forma independente, provaram que quando n tende ao infinito a razão entre a distribuição média de primos no intervalo dividida pela razão entre n e $\ln(n)$ tende a unidade (SPENTHOF; SOUZA, 2013). Matematicamente:

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{\frac{n}{\ln(n)}} = 1$$

Pode-se, então, estimar a quantidade de primos em um dado intervalo $x_{1,2} = x_2 - x_1$ pela expressão:

$$\pi(x_{1,2}) \simeq \frac{(x_2)}{\ln x_2} - \frac{(x_1)}{\ln x_1}.$$

EXEMPLO 9: Sabendo que $\ln 5 \simeq 1,609$ estime quantos primos há no intervalo entre 625 e 78125.

Representando por δ o intervalo em questão, tem -se :

$$\delta \simeq \frac{78.125}{\ln(78.125)} - \frac{625}{\ln(625)} \rightarrow \delta \simeq \frac{78.125}{11,26} - \frac{625}{6,44} \rightarrow \delta \simeq (6938 - 97) \simeq 6841,$$

ou seja, existem aproximadamente 6841 primos entre 625 e 78125.

4 ARITMÉTICA MODULAR

Os conceitos de aritmética modular, cujo conjunto universo são os inteiros, é trabalhado nos cursos de graduação, mestrado ou doutorado, mas esse conteúdo, ou pelo menos a parte essencial dele, não está fora de alcance do raciocínio de estudantes de ensino médio, em especial aos estudantes do 3º ano, e, por isso, podem-lhes ser apresentado. Pode-se perguntar se os estudantes têm base para aprender. É bem verdade que os estudantes brasileiros têm um déficit em matemática e isso pode dificultar a apresentação de alguns conteúdos, mas o raciocínio e o potencial para a compreensão e apreensão de saberes estão de pronto, desde que o procedimento de ensino aprendizagem respeite o tempo, o ritmo e a comunicação de cada estudante. Desafiar nossos jovens e contribuir em sua formação é uma questão de procedimento, ou seja, de como abordar o conteúdo, para qualquer disciplina.

O conceito de congruência bem como sua notação foi introduzido por Karl Friedrich Gauss (1777 - 1855) em 1801. As operações com aritmética modular são usadas nos cálculos de fenômenos periódicos e em muito ampliaram o poder computacional (COUTINHO, 2003).

Exemplos de fenômenos cíclicos estão relacionados ao tempo, como o passar das horas, dias e meses que podem ser organizados em relógios, calendários, de acordo com as fases da lua, com estações do ano, etc.

Assim, supondo que hoje é quinta-feira dia 10 de abril, que dia da semana será quando se passarem 134 dias? Essa resposta será apresentada nas páginas seguintes.

Figura 10 – Calendário

abril de 2014						
D	S	T	Q	Q	S	S
		1	2			
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

Fonte: elaborado pelo autor

Pode-se resolver facilmente questões como essa fazendo uso da aritmética modular.

4.1 Congruência

DEFINIÇÃO 14: Sejam a , b e n inteiros dados, sendo $n > 1$. Diz-se que a e b são congruentes módulo n , e denota-se por $a \equiv b \pmod{n}$, se $n|(a - b)$ (NETO, 2012).

EXEMPLO(S) 10:

- $7 \equiv 5 \pmod{2}$, pois $2|(7 - 5)$;
- $13 \equiv -35 \pmod{12}$, pois $12|[13 - (-35)]$
- $38 \equiv 10 \pmod{7}$, pois $7|(38 - 10)$.

4.1.1 Caracterização e propriedades de congruência

PROPOSIÇÃO 8: Sejam $a \in \mathbb{Z}$ e $n \in \mathbb{Z}$, com $n > 1$, se r é o resto na divisão de a por n , então $a \equiv r \pmod{n}$ ou, $n|(a - r)$.

DEMONSTRAÇÃO: Basta considerar a divisão a a partir do Teorema de Euclides:

$$a = nq + r \rightarrow$$

$$(a - r) = nq \rightarrow$$

$$n|(a - r) \rightarrow a \equiv r \pmod{n}. \quad \blacksquare$$

PROPOSIÇÃO 9: $a \equiv b \pmod{n}$ se, e somente se, a e b deixam o mesmo resto na divisão por n .

DEMONSTRAÇÃO:

Primeira parte da demonstração:

Considere $a - b = kn$, $k \in \mathbb{Z}$. Seja a divisão de b por n , isto é, $b = q_1n + r$, então

$a = b + kn \implies a = q_1n + r + kn \implies a = (q_1 + k)n + r$ e a deixa o mesmo resto na divisão por n .

Segunda parte da demonstração:

Seja $a = q_1n + r$ e $b = q_2n + r \implies (a - b) = (q_1 - q_2)n \implies a \equiv b \pmod{n}. \quad \blacksquare$

PROPOSIÇÃO 10: Considerando-se os inteiros a , b , c e n , tal que $n > 1$, tem-se:

i) $a \equiv a \pmod{n}$

ii) $a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$

iii) $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$

DEMONSTRAÇÃO:

$$\text{i) } n|0 \implies n|(a-a) \implies a \equiv a \pmod{n}$$

$$\text{ii) } a \equiv b \pmod{n} \implies (a-b) = kn \implies (b-a) = (-k)n \implies b \equiv a \pmod{n}$$

$$\text{iii) } a \equiv b \pmod{n} \implies (a-b) = k_1n \text{ e } b \equiv c \implies (b-c) = k_2n, \text{ somando-se } (a-b) \text{ e } (b-c): \\ (a-b) + (b-c) = (k_1+k_2)n \implies a \equiv c \pmod{n} \quad \blacksquare$$

Há outras propriedades que podem ser provadas a partir das propriedades acima e serão omitidas nesse trabalho.

4.1.2 Sistema completo de restos SCR

DEFINIÇÃO 15: Um sistema de restos módulo n é o conjunto $S = \{r_1, r_2, r_3, \dots, r_n\}$ de n inteiros, formado pelos restos possíveis na divisão de um inteiro positivo qualquer por n . Dessa forma, um inteiro arbitrário a é congruente módulo n a um único elemento de S .

Dados a e n inteiros com $n > 0$ e a não negativo, a divisão de a por n satisfaz à relação:

$$a = q \cdot n + r, \text{ com } 0 < r < n$$

Essa relação constitui o algoritmo da divisão de Euclides que é uma divisão com resto estabelecida inicialmente para os naturais, mas que se estende ao conjunto dos inteiros. O número a se encontra entre qn e $q(n+1)$ conforme o teorema de Eudoxius. O termo a é chamado dividendo, q é o quociente, n é o divisor e r é o resto.

Pelo algoritmo de Euclides, quando se divide um inteiro a por n , os únicos restos (resíduos) possíveis são $0, 1, 2, \dots, (n-1)$. Diz-se, então, que r_1, r_2, \dots, r_n formam um sistema completo de resíduos módulo n . O resto r pode assumir os valores desde 0 até $(n-1)$, ou seja, todo número inteiro dividido por n deixa um único resto $0 \leq r < n$. Este resto é chamado de resíduo de a módulo n (DOMINGUES, 1991). Este n é chamado de período de construção. O conjunto dos restos possíveis constituem um sistema completo de restos SCR módulo n . Como a semana tem sete dias, pode-se perguntar sobre os restos possíveis na divisão por 7 , que é o conjunto $S_7 = \{0, 1, 2, 3, 4, 5, 6\}$. Também é possível escrever todos os inteiros na forma: $a_0 = 0 + 7q$; $a_1 = 1 + 7q$; $a_2 = 2 + 7q$; \dots ; $a_6 = 6 + 7q$.

Classe de resíduos

Há muitos inteiros que são congruentes módulo n e, portanto, deixam o mesmo resto módulo n , com $0 \leq r < n$. Esses inteiros forma uma classe pois são todos congruentes módulo n e essa classe usa um representante para as devidas operações. Na sequência os representante considerando $n = 7$ que representa a quantidade de dias da semana.

$$[0]_7 = \{\dots, -14, -7, 0, 7, 14, 21, \dots\}$$

$$[1]_7 = \{\dots, -13, -6, 1, 8, 15, 22, \dots\}$$

$$[2]_7 = \{\dots, -12, -5, 2, 9, 16, 23, \dots\}$$

$$[3]_7 = \{\dots, -11, -4, 3, 10, 17, 24, \dots\}$$

$$[4]_7 = \{\dots, -10, -3, 4, 11, 18, 25, \dots\}$$

$$[5]_7 = \{\dots, -9, -2, 5, 12, 19, 26, \dots\}$$

$$[6]_7 = \{\dots, -8, -1, 6, 13, 20, 27, \dots\}$$

A classe $[0]_7$ representa o conjunto de elementos congruentes a 0 (mod 7), ou seja o conjunto dos inteiros que deixa resto 0 na divisão por 7, ou de forma equivalente $x \equiv 0 \pmod{7}$, com $x \in \mathbb{Z}$. Da mesma forma a classe $[5]_7$ representa o conjunto dos inteiros que deixa resto 5 quando dividido por 7. É um esses restos específicos quais sejam $\{0, 1, 2, 3, 4, 5, 6\}$ que irão aparecer como representantes de classe modular e como resultado de toda e qualquer operação modular com período 7.

É fácil a observação de que qualquer sequência de n inteiros consecutivos compõe um sistema completo de restos SCR.

Observando um calendário percebe-se que dois dias que diferem entre si por um múltiplo de 7 correspondem ao mesmo dia da semana. Por exemplo, se dia 1 é segunda-feira, então os dias 8, 15, 22 e 29 (possibilidades no intervalo de um mês) também serão segunda-feira, pois diferem entre si por um múltiplo de 7 que é a quantidade de dias da semana.

4.2 A aritmética do relógio

Por questão de simplicidade na notação a operações módulo n serão marcadas por um subíndice n. Por exemplo $[a]_n$ significa que a será submetido a uma operação modular com período n.

Há, pelo menos, duas maneiras de se proceder. A redução a um elemento de classe residual pode ser feita com os termos ou com o resultado. As operações e propriedades apresentadas abaixo foram baseadas em (STALING, 2011).

4.2.1 Soma e subtração

DEFINIÇÃO 16: Sejam a e b, inteiros, a soma e a subtração módulo n é dada conforme as expressões abaixo:

$$[a]_n + [b]_n = [a + b]_n$$

$$[a]_n - [b]_n = [a - b]_n$$

EXEMPLO 11: Supondo que hoje é uma quinta-feira de abril e que a semana começa no domingo, que dia da semana será quando se passarem 134 dias?

$[5]_7 + [134]_7 = [134 + 5]_7 = [139]_7 = [6]_7 =$ sexta-feira. Ou seja, ao se considerar o domingo como o dia 1, a segunda-feira como dia 2 e assim sucessivamente, a quinta-feira será dia 5 então dizer que dia da semana será 134 dias após a quinta é continuar a contagem ou somar 134 a 5 e depois separar em pacotes de 7 dias (que é uma semana) o resto é o dia procurado, nesse caso sexta-feira.

PROPOSIÇÃO 11: Sejam a , b e c inteiros, as operações de soma e subtração apresentam as seguintes propriedades:

$$[a]_n \pm ([b]_n \pm [c]_n) = ([a]_n \pm [b]_n) \pm [c]_n, \text{ associativa;}$$

$$[a]_n \pm [b]_n = \pm [b]_n + [a]_n, \text{ comutativa;}$$

$$[a]_n \pm [0]_n = [a]_n, \text{ elemento neutro;}$$

$$[a]_n \pm [n - a]_n = \pm [n]_n = [0]_n = 0, \text{ elemento oposto ou inverso aditivo.}$$

Tabela 6 – Adição modular

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	0	1	2	3	4	5	6
[1]	1	2	3	4	5	6	0
[2]	2	3	4	5	6	0	1
[3]	3	4	5	6	0	1	2
[4]	4	5	6	0	1	2	3
[5]	5	6	0	1	2	3	4
[6]	6	0	1	2	3	4	5

As tabelas 6 e 7 foram elaboradas pelo autor.

4.2.2 Multiplicação

DEFINIÇÃO 17: Sejam a e b , inteiros, a multiplicação módulo n é dada conforme a expressão abaixo:

$$[a]_n \cdot [b]_n = [a \cdot b]_n$$

EXEMPLO 12: $[5]_{11} \cdot [7]_{11} = [5 \cdot 7]_{11} = [35]_{11} = [2]_{11}$.

PROPOSIÇÃO 12: Sejam a , b e c inteiros, a operação de multiplicação apresenta as seguintes propriedades:

$$[a]_n \cdot ([b]_n \cdot [c]_n) = ([a]_n \cdot [b]_n) \cdot [c]_n, \text{ associativa;}$$

$$[a]_n \cdot [b]_n = [b]_n \cdot [a]_n, \text{ comutativa;}$$

$$[a]_n \cdot [1]_n = [a]_n, \text{ elemento neutro multiplicativo;}$$

$$[a]_n \cdot ([b]_n + [c]_n) = [a]_n \cdot [b]_n + [a]_n \cdot [c]_n, \text{ distributiva em relação a adição.}$$

Tabela 7 – Multiplicação modular

x	[1]	[2]	[3]	[4]	[5]	[6]	[0]
[1]	1	2	3	4	5	6	0
[2]	2	4	6	1	3	5	0
[3]	3	6	2	5	1	4	0
[4]	4	1	5	2	6	3	0
[5]	5	3	1	6	1	2	0
[6]	6	5	4	3	2	1	0
[0]	0	0	0	0	0	0	0

4.2.3 Potenciação modular

DEFINIÇÃO 18: Dado um inteiro a , a k -ésima potência de a é definida por:

$$a^k = a.a.a\dots a \text{ (} k \text{ vezes)}$$

Considerando $[E]_{(mod\ n)}$ o conjunto de potência de a módulo n , em que $\text{mdc}(a, n) = d$. Esse conjunto é dado por:

$$[E]_{(mod\ n)} = \{a^1, a^2, a^3, \dots, a^j, \dots\}$$

Embora o conjunto pareça infinito ele não o é, pois o tratamento modular é finito e gera conjuntos com, no máximo $(n - 1)$ elementos e, por isso, haverá repetições, um comportamento cíclico.

Dessa forma não é preciso se preocupar com as potências de expoentes maiores que $(n - 1)$ pois terão correspondentes nas potências com expoentes menores (COUTINHO, 2003).

4.2.4 Inverso multiplicativo módulo n

PROPOSIÇÃO 13: Se $\text{mdc}(a, n) = 1$, então a é invertível módulo n , ou seja, existe o inverso a^{-1} tal que $a.a^{-1} = 1 \pmod{n}$, em que $0 < a < n$ e $0 < a^{-1} < n$.

DEMONSTRAÇÃO: Considere $\text{mdc}(a, n) = 1$, então, pelos Teorema de Bezout, existem números inteiros x e y tais que $ax + by = 1$, ou ainda, $ax = 1 - ny$, dessa forma $ax = 1 + (-y)n$. Logo, $ax \equiv 1 \pmod{n}$ e daí x é o inverso de a módulo n , que indica-se $x \equiv a^{-1}$. ■

PROPOSIÇÃO 14: Há uma única classe para o inverso modular de determinado elemento de sistema de resíduos completo é único.

DEMONSTRAÇÃO: Considerando dois inversos modulares a^{-1} e b^{-1} tais que $0 < a^{-1} < n$ e $0 < b^{-1} < n$, para cada par de inteiros a e n tais que $\text{mdc}(a, n) = 1$, tem-se que $ab^{-1} \equiv 1 \equiv aa^{-1}$ e daí, como $\text{mdc}(a, n) = 1$ pode-se cancelar a na congruência obtendo-se $a^{-1} \equiv b^{-1}$. ■

Com a existência do inverso multiplicativo a divisão se torna possível. Como 3 e 5 são inversos multiplicativos módulo 7, então é possível a divisão de 6 por 5 em forma modular:

$$6 \div 5 \pmod{7} \equiv 6 \cdot 5^{-1} \pmod{7} \equiv 6 \cdot 3 = 18 \equiv 4 \pmod{7}.$$

4.3 O pequeno Teorema de Fermat

O algoritmo RSA tem por base a função ϕ de Euler, em especial, a aplicação do pequeno Teorema de Fermat. Tanto a função de Euler quanto o Pequeno Teorema de Fermat serão apresentados e explicados na sequência.

PROPOSIÇÃO 15 : Seja o conjunto de inteiros $A = \{r_1, r_2, \dots, r_n\}$ um SCR (sistema completo de resíduos) módulo n . Considere $k \in \mathbb{Z}$ tal que $\text{mdc}(k, n) = 1$. Afirma-se que o conjunto $B = \{kr_1, kr_2, \dots, kr_n\}$ também constitui um SRC.

DEMONSTRAÇÃO: Sejam kr_1 e kr_2 dois elementos do conjunto B arbitrariamente escolhidos. Considere, por hipótese, $kr_1 \equiv kr_2$ então $kr_1 = k_1n + r$ e $kr_2 = k_2n + r$, com k_1 e $k_2 \in \mathbb{Z}$, de forma que $kr_2 - k_2n = kr_1 - k_1n$, o que implica em $kr_2 - kr_1 = k_2n - k_1n$. Chega-se a $k(r_2 - r_1) = n(k_2 - k_1)$, como $\text{mdc}(k, n) = 1$ tem-se que $n | (r_2 - r_1)$ o que é absurdo por se ter partido de um sistema de resíduos completo que são incongruentes, entre si, módulo n . ■

Sendo $\text{mdc}(a, n) = 1$, então a multiplicação de a por elementos primos com n produz, pelo mesmo argumento acima, um conjunto de elementos também primos a n .

Por um contra exemplo mostra-se a necessidade de se ter $\text{mdc}(k, n) = 1$. Considere $n = 12$ e $k = 3$, cujo $\text{mdc}(12, 3) = 3$. O sistema de resíduos completo módulo 12 é:

$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$, multiplicando por 3:

$\{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33\}$, reduzindo módulo 12 tem-se:

{0, 3, 6, 9, 0, 3, 6, 9, 0, 3, 6, 9}

Deixando de ser um sistema completo como se pode verificar pois o sistema de resto passa a ser composto pelos múltiplos do mdc, nesse caso 3.

TEOREMA 6 - (Pequeno Teorema de Fermat): Sendo p um número primo e a um inteiro tal que $p \nmid a$, então:

$$a^{(p-1)} \equiv 1 \pmod{p}$$

DEMONSTRAÇÃO: considerando-se a proposição 15 e tomando de um inteiro qualquer a , em que $p \nmid a$, seus primeiros $(p - 1)$ múltiplos, isto é: $a, 2a, 3a, \dots, (p - 1)a$, tem-se que nenhum é congruente a 0 módulo p , ou seja, p não divide qualquer deles. Além disso, dois quaisquer elementos são incongruentes módulo p (FILHO, 1981). Assim:

$$a.2a.3a.....(p-1)a \equiv 1.2.3.....(p-1) \pmod{p}$$

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

$$a^{(p-1)} \equiv 1 \pmod{p}. \quad \blacksquare$$

O pequeno Teorema de Fermat é uma aplicação aos números primos de um teorema mais abrangente devido a Euler.

DEFINIÇÃO 19: A função $\phi : \mathbb{Z}_+^* \rightarrow \mathbb{Z}_+^*$, conhecida como função "fi" de Euler quantifica, para cada $m \in \mathbb{Z}_+^*$, os coprimos de m no intervalo $0 \leq k \leq m$, ou seja, fornece quantos elementos desse intervalo satisfazem a condição $\text{mdc}(m, k) = 1$.

EXEMPLO 13: Seja $m = 10$ e o conjuntos de inteiros $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. $\phi_{(10)} = 4$ que representa a quantidade de coprimos de 10 que, neste intervalo, são 1, 3, 7, 9.

Como um número primo p tem em sua classe de resíduos apenas um elemento congruente, que é o zero, então a $\phi(p) = (p - 1)$.

Seja p^α a potência qualquer de um número primo, com $\alpha > 0$. O conjunto de divisores de p^α é $\{1, p, p^2, \dots, p^{(\alpha-1)}\}$, Com $p^{(\alpha-1)}$ elementos. Assim $\phi_{(p^\alpha)} = p^\alpha - p^{(\alpha-1)}$. Pondo-se em evidência p^α , tem-se: $p^\alpha(1 - \frac{1}{p})$.

Dado um número $N = p_1^\alpha \cdot p_2^\beta \cdot p_3^\gamma$, pretende-se calcular a quantidade de inteiros coprimos no intervalo de zero a N . A demonstração desse caso particular se estende aos demais casos, ou seja, uma maneira de calcular a quantidade de coprimos com um determinado número é baseada nesse procedimento.

Da união de conjuntos tem-se que:

$$n(A \cup B) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C).$$

A quantidade de números com fatores comuns a p^α é $p^{\alpha-1}$. Assim, dado um número $N = p_1^\alpha \cdot p_2^\beta \cdot p_3^\gamma$, a quantidade de números sem fatores comuns a N é:

$$\begin{aligned}
\phi(N) &= N - \frac{N}{p_1} - \frac{N}{p_2} - \frac{N}{p_3} + \frac{N}{p_1 \cdot p_2} + \frac{N}{p_1 \cdot p_3} + \frac{N}{p_2 \cdot p_3} - \frac{N}{p_1 \cdot p_2 \cdot p_3} \implies \\
\phi(N) &= N \left[1 - \frac{1}{p_1} - \frac{1}{p_2} - \frac{1}{p_3} + \frac{1}{p_1 \cdot p_2} + \frac{1}{p_1 \cdot p_3} + \frac{1}{p_2 \cdot p_3} - \frac{1}{p_1 \cdot p_2 \cdot p_3} \right] \implies \\
\phi(N) &= N \left[\frac{p_1 p_2 p_3 - p_3 p_2 - p_1 p_3 - p_2 p_1 + p_3 + p_2 + p_1 - 1}{p_1 p_2 p_3} \right] \implies \\
\phi(N) &= N \left[\frac{p_2 p_3 (p_1 - 1) - p_3 (p_1 - 1) - p_2 (p_1 - 1) + (p_1 - 1)}{p_1 \cdot p_2 \cdot p_3} \right] \implies \\
\phi(N) &= N \left[\frac{(p_1 - 1)(p_3 p_2 - p_3 - p_2 + 1)}{p_1 \cdot p_2 \cdot p_3} \right] \implies \\
\phi(N) &= N \left[\frac{(p_1 - 1)[p_3 (p_2 - 1) - (p_2 - 1)]}{p_1 \cdot p_2 \cdot p_3} \right] \implies \\
\phi(N) &= N \left[\frac{(p_1 - 1)(p_2 - 1)(p_3 - 1)}{p_1 \cdot p_2 \cdot p_3} \right] \implies \\
\phi(N) &= p_1^\alpha \cdot p_2^\beta \cdot p_3^\gamma \left[\frac{(p_1 - 1)(p_2 - 1)(p_3 - 1)}{p_1 \cdot p_2 \cdot p_3} \right] \implies \\
\phi(N) &= \left[p_1^\alpha \left(1 - \frac{1}{p_1} \right) \right] \left[p_2^\beta \left(1 - \frac{1}{p_2} \right) \right] \left[p_3^\gamma \left(1 - \frac{1}{p_3} \right) \right] \implies \\
\phi(N) &= \phi(p_1) \cdot \phi(p_2) \cdot \phi(p_3). \quad \blacksquare
\end{aligned}$$

Dessa forma, se $\text{mdc}(m, n) = 1$, a quantidade de números coprimos ao produto $m \cdot n$ é dado pelo produto dos coprimos de m com os coprimos de n , ou seja, $\phi_m \cdot \phi_n$, a função ϕ_n é uma função multiplicativa.

DEFINIÇÃO 20: Um sistema reduzido de resíduos módulo n (SRR) é um conjunto de $\phi(n)$ inteiros $r_1, r_2, r_3, \dots, r_i, \dots, r_{\phi_n}$, tais que $\text{mdc}(r_i, n) = 1$, e se $i \neq j$, então $r_i \not\equiv r_j \pmod{n}$ (SANTOS, 2009).

PROPOSIÇÃO 16: Dado $r_1, r_2, r_3, \dots, r_i, \dots, r_{\phi_n}$ um sistema reduzido de resíduos módulo n e a um inteiro tal que $\text{mdc}(a, n) = 1$, então $ar_1, ar_2, ar_3, \dots, ar_i, \dots, r_{\phi_n}$ é, também, um sistema reduzido de resíduos módulo n (SANTOS, 2009).

DEMONSTRAÇÃO: Sejam ar_1 e ar_2 dois elementos do conjunto reduzido de resíduos módulo n arbitrariamente escolhidos. Considere, por hipótese, $ar_1 \equiv ar_2$ então $ar_1 = a_1 n + r$ e $ar_2 = a_2 n + r$, com a_1 e $a_2 \in \mathbb{Z}$, de forma que $ar_2 - a_2 n = ar_1 - a_1 n$, o que implica em $ar_2 - ar_1 = a_2 n - a_1 n$. Chega-se a $a(r_2 - r_1) = n(a_2 - a_1)$, como $\text{mdc}(a, n) = 1$ tem-se que $n | (r_2 - r_1)$ o que é absurdo por se ter partido de um sistema reduzido de resíduos que são incongruentes, entre si, módulo n . \blacksquare

TEOREMA 7 - (Euler): Se n é um inteiro positivo e $\text{mdc}(a, n) = 1$, então:

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

DEMONSTRAÇÃO: O raciocínio é semelhante ao apresentado na proposição 15 e com base na proposição 16. Seja $B = \{a_1, a_2, a_3, \dots, a_{\phi_n}\}$ elementos de um sistema reduzido de resíduos e a um inteiro de maneira que $\text{mdc}(a, n) = 1$. O produto de a pelos

elementos do conjunto B gera um conjunto $B' = \{a.a_1, a.a_2, a.a_3, \dots, a.a_{\phi_n}\}$, que também é um sistema reduzido de resíduos. Assim,

$$(aa_1).(aa_2).(aa_3)\dots(aa_{\phi_n}) \equiv a_1.a_2.a_3\dots a_{\phi_n} \pmod{n}$$

$$a^{\phi(n)}(a_1.a_2.a_3\dots a_{\phi_n}) \equiv a_1.a_2.a_3\dots a_{\phi_n} \pmod{n}$$

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



5 A CRIPTOGRAFIA RSA

A criptografia realizada antes do sistema de chave pública se baseava em substituição ou permutação. A criptografia de chave assimétrica é tida como a maior revolução na história da criptografia.

O algoritmo RSA se baseia no conceito de função unidirecional, uma função unidirecional é aquela em que facilmente se pode determinar o valor numérico da função mas dificilmente se consegue o valor numérico de sua inversa, ela também tem a propriedade de que cada elemento do domínio tenha um inverso único. Assim como o RSA, também são baseados em funções unidirecionais os sistemas criptográficos de chave elíptica, Diffe-Hellman e DSS (STALING, 2011).

Em 1976 Diffie e Hellman publicaram um artigo em que apresentavam uma nova técnica para criptografia, desafiando os criptoanalistas a encontrarem um algoritmo para o sistema de chave assimétrica. Um dos primeiros trabalhos foi desenvolvido por Ron Rivest, Adi Shamir e Len Adleman, no MIT (STALING, 2011).

5.1 O problema de distribuição de chaves

A comunicação secreta exige o conhecimento de chaves e algoritmos para se concretizar. A criptografia assimétrica surge para responder a duas demandas do contexto da criptografia simétrica:

- a) o problema de distribuição das chaves e
- b) o problema das assinaturas digitais (STALING, 2011).

Em relação à distribuição de chaves considere um grupo de 80 pessoas que precisam de comunicação segura entre duas quaisquer pessoas do grupo. Utilizando a criptografia simétrica há necessidade de $\frac{80 \cdot 79}{2} = 3160$ chaves. Não deve ser fácil o gerenciamento dessas chaves (CARVALHO, D., 2000).

Representando por R o remetente e D o destinatário e usando um algoritmo com a propriedade comutativa tem-se a seguinte possibilidade:

1. R escolhe uma chave particular, ch_R ;
2. D escolhe uma chave particular, ch_D ;
3. R encripta o texto com sua chave e manda para D;
4. D encripta a mensagem recebida com sua chave e reenvia a R;

5. R descripta o texto com sua chave e o remete a D;
6. D descripta o texto com sua chave e tem acesso à mensagem original.

Há uma comparação interessante para melhor entendimento dos passos acima, primeiro R escreve a mensagem colocando-a em uma caixa e trancando com um cadeado que só ele tem a chave; ao receber a caixa, D acrescenta outro cadeado cuja chave só D tem e devolve a caixa para R; R destranca seu cadeado e envia a caixa a D que finalmente destranca seu cadeado tendo acesso à mensagem (CARVALHO, D., 2000).

Os dois principais problemas são: primeiro nem todo algoritmo opera comutativamente e segundo a mensagem transitou três vezes entre remetente e destinatário o que aumenta a chance de interceptação por um terceiro e torna a comunicação extremamente lenta (CARVALHO, D., 2000).

Os passos na criptografia assimétrica ou de chave pública seriam:

1. D escolhe duas chaves, uma privada a qual apenas D conhece e uma pública que é acessível a todos;
2. R usa a chave pública de D para encriptar uma mensagem e enviá-la a D;
3. D usa sua chave particular para decriptar a mensagem.

O comparativo é: D escolhe um cadeado que só ele tem a chave e o distribui aberto a quem o quiser; R escreve uma mensagem e a tranca em uma caixa a ser enviada a D; D usa sua chave particular para abrir a caixa e ter acesso à mensagem. Dessa forma R e D mantêm comunicação segura e a mensagem transitou apenas uma vez pelo canal.

5.2 Usando o algoritmo RSA

Precodificação

Pode-se considerar uma primeira etapa chamada de precodificação subdividida em três passos.

- i) primeiro se converte em números a mensagem a ser encriptada;
- ii) são escolhidos os parâmetros p e q , dois primos que são essenciais ao algoritmos RSA e a partir do qual se obtém as chaves pública e privada;
- iii) por último a mensagem convertida em números é dividida em blocos B , tais que $B < pq$ ou, como veremos mais adiante, $B < n$ ($n = pq$). O quadro 6 tem por fonte (COUTINHO, 2003, pg. 181).

Observa-se, no quadro 6, a numeração ser iniciada a partir do dez, evitando ambiguidade, assim todas as letras são representadas por dois algarismos. Dessa forma o

Quadro 6 – Precodificação

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

14 representa E e não AD. O espaço entre palavras é representado pelo número 99. A explicação de como funciona o algoritmo RSA foi feito com base no trabalho de S. Collier Coutinho. Para mais detalhes consulte (COUTINHO, 2003).

Suponha a mensagem DIA D. O primeiro passo consiste em converter em números conforme a tabela acima:

13 - 18 - 10 - 9 - 9 - 13

O segundo passo é a escolha de dois primos, por exemplo, 7 e 11 que geram o número $n = 7 \cdot 11 = 77$. O número n , neste caso 77, irá compor a chave pública e a chave privada. Na criptografia convencional são escolhido primos da ordem de 10^{100} (COUTINHO, 2003), vê-se que é computacionalmente muito difícil descobrir p e q por fatoração. Os computadores caseiros atualmente precisariam de milhões de anos nessa tarefa.

O terceiro passo consiste em quebrar a mensagem em blocos menores que n , nesse caso em blocos menores que 77. Por exemplo: 13 - 18 - 10 - 9 - 9 - 13. Observe que o 99, por ser maior que 77, não pode figurar como bloco e, daí a sua quebra em dois blocos 9 e 9. Os blocos podem ser escolhidos de modo a não representarem nenhuma unidade linguística eliminando, assim, a possibilidade de análise de frequência de grafemas, por exemplo: 1 - 31 - 8 - 10 - 9 - 9 - 1 - 3. Deve-se ter o cuidado de não usar zero no início de cada bloco (COUTINHO, 2003).

Cifrando

A codificação pode ser realizada em duas etapas. Primeiro é preciso gerar as chaves pública e privada; o segundo passo consiste no tratamento modular da mensagem.

Para o estabelecimento das chaves pública e privada calcula-se $\phi(n)$ e dois números e e d tais que $ed \equiv 1 \pmod{\phi(n)}$:

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

$$\phi(77) = (7-1)(11-1)$$

$$\phi(77) = 60$$

O emissor precisa de uma chave pública $Pu = \{e, n\}$ e o receptor precisa da chave privada $Pr = \{d, n\}$ lembrando que $\text{mdc}(e, \phi(n)) = 1$ e $\text{mdc}(d, \phi(n)) = 1$. Para o caso em questão escolhe-se $e = 7$. Pelo Teorema de Euler tem-se que:

$$7^{\phi(60)} \equiv 1$$

$$60 = 2^2 \cdot 3 \cdot 5 \implies \phi(60) = 60(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 16$$

$$7^{16} = 7 \cdot 7^{15}, \text{ o inverso de } 7 \text{ é } 7^{15} \pmod{60}.$$

$$7^4 = 2401 \equiv 1 \pmod{60}$$

$$7^{15} = 7^4 \cdot 7^4 \cdot 7^4 \cdot 7^3 \equiv 343 \equiv 43 \pmod{60}.$$

Então a chave pública é $(7, 77)$ e a chave privada é $(43, 77)$ pois, $7 \cdot 43 \equiv 1 \pmod{n}$ e, assim um é inverso do outro.

Atualmente os blocos processados podem ter até 309 dígitos. O processo de cifra-gem e decifração pode ser assim esquematizado: considerando M um bloco de texto claro e C um bloco de texto cifrado. Para cifrar usa-se a chave pública, ou seja, o par $(7, 77)$ da seguinte forma.

$$C = M^e \pmod{n}$$

O texto cifrado será o resto na divisão de M^e por n . Assim, os blocos $B_1 = 13$, $B_2 = 18$, $B_3 = 10$, $B_4 = 9$, $B_5 = 9$ e $B_6 = 13$ que representam a mensagem O DIA D serão tratado como segue:

$$B_1 = B_6 = 13$$

$$13^2 = 169 \equiv 15 \pmod{77}$$

$$13^6 = (13^2)^3 \equiv 15^3 = 3375 \equiv 64 \pmod{77}$$

$$13^7 = 13^6 \cdot 13 \equiv 64 \cdot 13 = 832 \equiv \mathbf{62}$$

$$B_2 = 18$$

$$18^2 = 324 \equiv 16 \pmod{77}$$

$$18^6 \equiv 16^3 = 4096 \equiv 15 \pmod{77}$$

$$18^7 = 18^6 \cdot 18 \equiv 15 \cdot 18 = 270 \equiv \mathbf{39} \pmod{77}$$

$$B_3 = 10$$

$$10^2 = 100 \equiv 23 \pmod{77}$$

$$10^6 \equiv 23^3 = 12167 \equiv 1 \pmod{77}$$

$$10^7 = 10^6 \cdot 10 \equiv 1 \cdot 10 = 10 \equiv \mathbf{10} \pmod{77}$$

$$B_4 = B_5 = 9$$

$$9^2 = 81 \equiv 4 \pmod{77}$$

$$9^6 \equiv 4^3 = 64 \pmod{77}$$

$$9^7 = 9^6 \cdot 9 \equiv 64 \cdot 9 = 576 \equiv \mathbf{37} \pmod{77}$$

A mensagem cifrada é, então: 62 - 39 - 10 - 37 - 37 - 62

Para decifrar deve-se usar

$$M = C^d \pmod{n}$$

O texto decifrado é o resto da divisão de C^d por n .

$$B'_1 = B'_6 = 62$$

$$62^2 = 3844 \equiv 71 \pmod{77}$$

$$62^4 \equiv 71^2 = 5041 \equiv 36 \pmod{77}$$

$$62^8 \equiv 36^2 = 1296 \equiv 64 \pmod{77}$$

$$62^{16} \equiv 64^2 = 4096 \equiv 15 \pmod{77}$$

$$62^{32} \equiv 15^2 = 225 \equiv 71 \pmod{77}$$

$$62^{40} = 62^{32} 62^8 \equiv 71 \cdot 64 = 4544 \equiv 1 \pmod{77}$$

$$62^{43} = (62^{32} 62^8) 62^2 62 \equiv 1 \cdot 71 \cdot 62 = 4402 \equiv \mathbf{13} \pmod{77}$$

$$B'_2 = 39$$

$$39^2 = 1521 \equiv 58 \pmod{77}$$

$$39^4 \equiv 58^2 = 3364 \equiv 53 \pmod{77}$$

$$39^8 \equiv 53^2 = 2809 \equiv 37 \pmod{77}$$

$$39^{16} \equiv 37^2 = 1369 \equiv 60 \pmod{77}$$

$$39^{32} \equiv 60^2 = 3600 \equiv 58 \pmod{77}$$

$$39^{40} = 39^{32} 39^8 \equiv 58 \cdot 37 = 2146 \equiv 67 \pmod{77}$$

$$39^3 = 39^2 39 \equiv 58 \cdot 39 = 2262 \equiv 29 \pmod{77}$$

$$39^{43} = 39^{40} 39^3 \equiv 67 \cdot 29 = 1943 \equiv \mathbf{18} \pmod{77}$$

$$B'_3 = 10$$

$$10^2 = 100 \equiv 23 \pmod{77}$$

$$10^4 \equiv 23^2 = 529 \equiv 67 \pmod{77}$$

$$10^8 \equiv 67^2 = 4489 \equiv 23 \pmod{77}$$

$$10^{16} \equiv 23^2 = 529 \equiv 67 \pmod{77}$$

$$10^{32} \equiv 67^2 = 4489 \equiv 23 \pmod{77}$$

$$10^{40} = 10^{32} 10^8 \equiv 23 \cdot 23 = 529 \equiv 67 \pmod{77}$$

$$10^{42} = 10^{40} 10^2 \equiv 67 \cdot 23 = 1541 \equiv 1 \pmod{77}$$

$$10^{43} = 10^{42} 10 \equiv 1 \cdot 10 = 10 \equiv \mathbf{10} \pmod{77}$$

$$\begin{aligned}
B'_4 &= B_5 = 37 \\
37^2 &= 1369 \equiv 60 \pmod{77} \\
37^4 &= 37^2 \cdot 37^2 \equiv 60^2 \equiv 58 \pmod{77} \\
37^8 &= 37^4 \cdot 37^4 \equiv 58 \cdot 58 = 3364 \equiv 53 \pmod{77} \\
37^{16} &= 37^8 \cdot 37^8 \equiv 53 \cdot 53 = 2809 \equiv 37 \pmod{77} \\
37^{32} &= 37^{16} \cdot 37^{16} \equiv 37 \cdot 37 = 1369 \equiv 60 \pmod{77} \\
37^{40} &= 37^{32} \cdot 37^8 \equiv 60 \cdot 53 = 3180 \equiv 23 \pmod{77} \\
37^{42} &= 37^{40} \cdot 37^2 \equiv 23 \cdot 60 = 1380 \equiv 71 \pmod{77} \\
37^{43} &= 37^{42} \cdot 37 \equiv 71 \cdot 37 = 2627 \equiv \mathbf{9} \pmod{77}
\end{aligned}$$

5.3 Entendendo o mecanismo do algoritmo RSA

O que ocorre é: $M = C^d \pmod{n} = (M^e)^d \pmod{n} = M^{ed} \pmod{n} \equiv M^1 \pmod{n}$.

Lembrando que $e \cdot d = 1 \pmod{\phi(n)}$, há, pela própria definição de congruência, uma expressão equivalente que é $e \cdot d = k \cdot \phi(n) + 1$. Uma vez que $\phi(n) = (p-1)(q-1)$, é necessário mostrar que: $M^{e \cdot d} = M^{k \cdot (p-1) \cdot (q-1) + 1} \pmod{n} = M$

Há dois casos:

Caso 1: $p \mid M$, ou seja, M é divisível por p , nesse caso $M \equiv 0 \pmod{p}$ e, por tanto, $M^{k \cdot (p-1) \cdot (q-1) + 1} \equiv 0 \pmod{p}$. Assim, $p \mid [M^{k \cdot (p-1) \cdot (q-1) + 1} - M]$, ou seja, $M^{k \cdot (p-1) \cdot (q-1) + 1} \pmod{p} = M \pmod{p}$ (11).

Caso 2: Não há fatores comuns entre M e P além da unidade, ou seja $p \nmid M$, pelo Teorema de Euler $M^{\phi(n)} \equiv 1 \pmod{n}$ então:

$$\begin{aligned}
&M^{k \cdot (p-1) \cdot (q-1) + 1} \pmod{p} \\
&= M \cdot M^{k \cdot (p-1) \cdot (q-1)} \pmod{p} \\
&= M [M^{(p-1)}]^{k \cdot (q-1)} \pmod{p} \\
&= M [1]^{k \cdot (q-1)} \pmod{p} \\
&= M \pmod{p}
\end{aligned}$$

Por raciocínio semelhante se demonstra que $M^{k \cdot (p-1) \cdot (q-1) + 1} \pmod{q} = M \pmod{q}$.

Observa-se que:

$$\begin{aligned}
M^{k \cdot (p-1) \cdot (q-1) + 1} - M &= 0 \pmod{p} \text{ e} \\
M^{k \cdot (p-1) \cdot (q-1) + 1} - M &= 0 \pmod{q} \text{ então:}
\end{aligned}$$

Como $\text{mdc}(p, q) = 1$, deve existir um número inteiro r tal que:

$$\begin{aligned}
M^{k \cdot (p-1) \cdot (q-1) + 1} - M &= r(pq) \\
M^{k \cdot (p-1) \cdot (q-1) + 1} - M &= (n)r
\end{aligned}$$

■

6 APLICAÇÃO EM SALA DE AULA

As atividades visam reforçar a explicação e fazer as verificações a partir dos conhecimentos matemáticos desenvolvidos até o ensino médio. O ideal é que o foco seja a discussão e a compreensão do algoritmo RSA. Dessa forma busca-se apresentar uma justificativa usando a matemática de nível médio. Simplificar não é tão fácil quanto possa parecer e, para o professor, o desafio é apresentar conteúdos complexos buscando maneiras diversas para atender a todos os estudantes. Assim, são apresentadas na sequências alguns tópicos para discussão em sala.

É importante que se discuta sobre segurança no trato com a informação, sobre o direito à privacidade. O ideal é chamar para participar o professor de História, Filosofia, Física, Informática, Sociologia, entre outros, para discussão sobre sociedade.

6.1 O inverso multiplicativo a partir do MMC

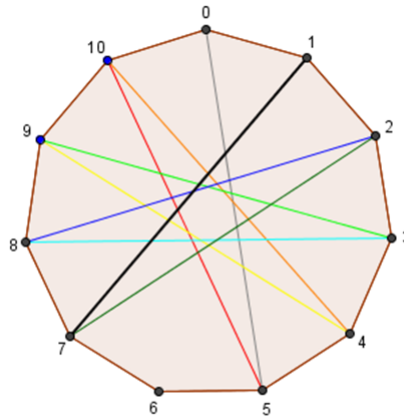
O MMC é apresentado ainda no ensino fundamental e, nem sempre sua aplicação é enfatizada. O MMC pode ser usado para soma ou subtração de frações, comparar raízes com índices diferentes e, também, nos problemas de se determinar encontros em atividades cíclicas. Por exemplo, um ônibus A sai de uma estação a cada 35 minutos, um ônibus B sai a cada 45 minutos, se os dois saírem juntos às 7:00h da manhã em que horas estarão juntos novamente na estação?

Pode ser interessante e estimulante que se aborde a parte histórica, a estrutura matemática como definições e propriedades e, também, a aplicabilidade de cada conteúdo. No caso do MMC, além da aplicações citadas acima é possível usá-lo para demonstrar, com conteúdo próprio do ensino básico, a existência de inverso multiplicativo modular quando um determinado elemento de classe residual (a) e o período modular (n) não apresentam fatores comuns, ou seja, $\text{mdc}(a, n) = 1$.

Pode-se escolher um polígono regular qualquer. Neste exemplo escolheu-se o polígono regular de 11 lados. Poder-se-ia de dois em dois, três em três, quatro em quatro, k em k , etc. Como exemplo a contagem será de cinco em cinco e o objetivo é verificar a existência de inverso modular e encontrá-lo.

O que ocorre é que o MMC entre 5 e 11 é 55. O que isso significa? Significa que, começando do zero e contando de cinco em cinco só se pode voltar ao zero depois de percorrer 55 números. A sequência nos inteiros é (5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55), mas como se está contando e operando de forma modular, no terceiro passo não se encontrará o 15 mas um número que lhe é congruente módulo 11, nesse caso o 4. A partir

Figura 11 – Período modular primo



Fonte: elaborado pelo autor

do 4, contando-se mais 5 obtem-se o 9 que é congruente a 20 módulo 11. Dessa forma a sequência obtida é (5, 10, 4, 9, 3, 8, 2, 7, 1, 6, 0), verifique. As figuras 11 e 12 foram elaboradas pelo autor usando o Geogebra.

A sequência pode ser encontrada com a ajuda de retas, assim os estudantes podem desenhar um polígono regular e, com a ajuda de uma régua ligar os pontos sequencias que distam cinco unidades. Quando se passa pela unidade, basta contar quantos seguimentos de reta foram traçados e esse número representa o inverso de 5 módulo 11. No exemplo apresentado foram traçados 9 seguimentos de reta até se chegar ao 1. Então $9 \times 5 = 45 = 4 \times 11 + 1$, isto é, $9 \times 5 \equiv 1 \pmod{11}$. O números 9 e 5 são inverso multiplicativos modulares para o período 11.

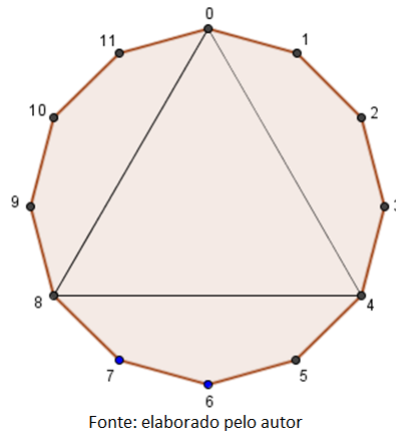
É interessante reforçar o emprego do MMC. Cada ponto só será repetido 55 pontos depois, neste caso, e 55 contado de cinco em cinco resulta 11, ou seja, os 11 pontos do polígono serão visitados antes de qualquer repetição. Ao se contar de cinco em cinco o que se faz é multiplicar a sequência de restos do 11 por 5 e o efeito é uma permutação dessa sequência, isto é, $5 \times (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10) = (5, 10, 4, 9, 3, 8, 2, 7, 1, 6, 0)$.

Agora, usando esse processo, determine o inverso do 2, do 3, 4, 6, 7, 8, 9 e 10 módulo 11. Procure analisar outros poligonos regulares primos como o polígono de 13 lados, de 17 lados, de 19 lados e verifique se eles também apresentam essa propriedade.

6.2 Por que o $\text{mdc}(a, n) = 1$?

Agora recorre-se a um polígono regular com um número composto de lados para analisar o que ocorre quando há fator em comum entre um multiplicador qualquer e o período modular. Foi escolhido um dodecágono regular para representar os restos possíveis na divisão por 12.

Figura 12 – Período modular de número composto



Ao se contar de 4 em 4 percebe-se nem todos os pontos serão visitados. A sequência é (4, 8, 0), isso significa que ao se multiplicar o conjuntos dos resto possíveis de 12 por 4 o resultado não é mais um sistema completo de resíduos. $4 \times (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11) = (4, 8, 0)$. Se alguns elementos não são alcançados então eles não apresentam inverso, por exemplo, não existe um número inteiro que multiplicado por 4 resulte em 1 módulo 12. Pelo exposto, verifica-se que para haver inverso modular entre a e n é necessário que o $\text{mdc}(a, n)$ seja 1.

6.3 Criando uma tabela de multiplicação modular em planilha eletrônica

O procedimento para criar uma tabela multiplicativa modular é necessário informar o período e criar uma linha e uma coluna com o SCR do número escolhido. Por exemplo, para uma tabela multiplicativa modular o comando é:

$$= \text{mod}(\$A2*B\$1; \text{período})$$

Observar a figura 13 em que foi escolhido o período 11.

Descartando a linha de zeros e a coluna de zeros pode-se notar uma propriedade interessante de progressão aritmética que permanece. A soma dos extremos dos dez valores restantes após a eliminação das linhas e colunas nulas resultam em um valor constante que, neste caso, é o período modular, para este exemplo o 11. Dessa forma é possível preencher a tabela usando o oposto somativo modular. A terceira linha, por exemplo, que representa multiplicar por 3 o SCR do 11 pode ser preenchida considerando que o primeiro elemento é 3 e o último é $(11 - 3)$, ou seja, o último é 8. O segundo número é 6 e o penúltimo é $(11 - 6) = 5$; o terceiro é 9 e o antepenúltimo é $(11 - 9) = 2$. Assim a

Figura 13 – Mult. modular

H7		fx = =MOD(\$A7*\$H\$1;11)										
A	B	C	D	E	F	G	H	I	J	K	L	M
	1	2	3	4	5	6	7	8	9	10	11	
1	1	2	3	4	5	6	7	8	9	10	0	
2	2	4	6	8	10	1	3	5	7	9	0	
3	3	6	9	1	4	7	10	2	5	8	0	
4	4	8	1	5	9	2	6	10	3	7	0	
5	5	10	4	9	3	8	2	7	1	6	0	
6	6	1	7	2	8	3	9	4	10	5	0	
7	7	3	10	6	2	9	5	1	8	4	0	
8	8	5	2	10	7	4	1	9	6	3	0	
9	9	7	5	3	1	10	8	6	4	2	0	
10	10	9	8	7	6	5	4	3	2	1	0	
11	0	0	0	0	0	0	0	0	0	0	0	

Fonte: elaborado pelo autor

sequência, obtida por propriedade de P.A. é (3, 6, 9, 1, 4, 7, 10, 2, 5, 8). A figura 13 foi elaborada pelo autor usando uma planilha eletrônica.

6.4 Algoritmo estendido de Euclides

Use uma planilha eletrônica para estabelecer x_0 e y_0 , coeficiente que possibilitam escrever o mdc (a, b) em função de a e b conforme tabela 2.

- entre 13 e 5;
- entre 6 e 21;
- entre 11 e 7.

6.5 Criptografando com algoritmo RSA

Essa atividade consiste em criptografar mensagens pequenas como UFT usando o algoritmo RSA por um grupo (metade da sala) e decodificar por outro grupo (outra metade da turma) com o auxílio de uma planilha eletrônica.

PRECODIFICAÇÃO:

- passo: converta as letras para seus representantes numéricos conforme tabela de precodificação apresentada no capítulo 5;
- passo: use os primos $p = 7$ e $q = 13$;
- passo: considere cada letra e seu correspondente numérico um bloco, estabeleça b_1, b_2, b_3 ;

CODIFICANDO

- passo: calcule $n = p \cdot q$
- passo: calcule $\phi(n) = (p - 1)(q - 1)$;
- passo: gere a chave pública (e, n) escolhendo e tal que $\text{mdc}(e, \phi(n)) = 1$;

4º passo: determine \mathbf{d} tal que $\mathbf{ed} \equiv 1 \pmod{\phi(n)}$;

5º passo: Determina $c_1 = b_1^e$; $c_2 = b_2^e$ e $c_3 = b_3^e$;

DECODIFICANDO

Calcule $b_1 = c_1^d$; $b_2 = c_2^d$ e $b_3 = c_3^d$

6.6 Usando mais de dois números primos

É possível que o algoritmo RSA use três ou mais primos. Descreva esse processo e responda porque há preferência para o uso de apenas dois números primos no algoritmo de criptografia RSA.

Considerações Finais

O que se busca neste trabalho é apresentar o algoritmo de criptografia RSA, no ensino médio. É um tema que faz parte do cotidiano e mesmo assim poucos têm conhecimento sobre tais procedimentos, pouco se discute sobre a criptografia que tem possibilitado o comércio eletrônico, as comunicações e, de certa forma, a dinâmica do mundo nas últimas décadas.

O objetivo de proporcionar material sobre o algoritmo de criptografia RSA para professores interessados em abordar esse tema no Ensino Médio foi alcançado.

É interessante perceber que a exploração do potencial computacional em sala de aula ainda é pouca. Neste trabalho foi mostrado que a computação é bem vinda e pode auxiliar os estudantes na lida com números considerados grandes.

Cumpriu-se, também, a proposta de apresentação da aritmética modular. Espera-se que esse conhecimento possa auxiliar os estudantes quando da análise de situações ou questões de natureza cíclica.

O trabalho, conforme proposto, apresenta um relato da criptografia através dos tempos, descreve a estrutura dos inteiros através de seus blocos de construção conhecidos como números primos, considera as abordagens na tentativa de organização e previsão de números primos. Apresenta os números compostos e a forma única de decomposição em fatores primos e mostra também o algoritmo de Euclides, a partir do qual se estrutura a aritmética do relógio.

São apresentados o Pequeno Teorema de Fermat e a função ϕ (fi) de Euler que potencializam os cálculos exponenciais e permitem ao algoritmo RSA toda sua funcionalidade.

Fica a proposta de pesquisa sobre outras modalidades de criptografia como a baseada em curvas elípticas, a criptografia quântica e os algoritmos baseados em sistemas biológicos, com o desafio de adaptar a esses algoritmos aos estudantes do ensino médio.

Entre as atividades propostas, talvez, a mais importante seja a que sugere um trabalho conjunto com outras disciplinas como Física, Matemática, História, Filosofia e Informática em que se pode refletir sobre necessidades próprias do nosso tempo como segurança, privacidade, cidadania, direito à informação, direito à expressão e à participação na construção de uma cidadania global que se aponta.

Referências

- BRASIL, Ministério de Educação e Cultura. LDB - Lei nº 9394/96, de 20 de dezembro de 1996. Estabelece as diretrizes e bases da Educação Nacional. Brasília: MEC, 1996.
- BRASIL, Ministério de Educação e Cultura. PCN. Parâmetros Curriculares Nacionais – Apresentação. Brasília, DF: MEC/SEF, 2000.
- BURNETT, Steve; PEINE, Stephen. *Criptografia e Segurança*: o guia oficial do RSA. Rio de Janeiro: Campus, 2002.
- CARVALHO, Alexandre Luís Trovon; REIS, Lourisnei Fortes *Matemática interativa*. Tatui: Casa Publicadora Brasileira, 2009.
- CARVALHO, Daniel Balparda de. *Segurança de dados com Criptografia*: métodos e algoritmos. Rio de Janeiro: Book Express, 2000. p.22-30
- COUTO, Sérgio Pereira. *Códigos & Cifras*: da antiguidades à Era Moderna. Rio de Janeiro: Nova Terra, 2008. p. 2-108
- COUTINHO, Severino Collier. *Números inteiros e criptografia RSA*. 2ª ed. Rio de Janeiro: IMPA, 2003. p.53-189
- FILHO, Edgard de Alencar. *Teoria elementar dos números*. São Paulo: Nobel, 1981.
- FONSECA FILHO, Clézio. *História da computação*: O caminho do pensamento e da tecnologia. Porto Alegre: EdipuRS, 2007.
- GARDNER, Howard. *Estruturas da mente*: A Teoria das Inteligências Múltiplas. Porto Alegre: Artes Médias Sul, 1994 p. 103.
- DOMINGUES, Higyno H. *Fundamentos de Aritmética*. São Paulo: Atual, 1991. p. 52-114
- HOUAISS, Antônio; VILLAR, Mauro de Salles. *Dicionário Houaiss da língua portuguesa*. Rio de Janeiro: Objetiva, 2009.
- <http://www.dm.ufscar.br/caetano/iae2004/G6/disco.htm>. Acessado em 08 de abril de 2014.
- LIMA, Elon Lages; CARVALHO, Paulo Cezar P.; WAGNER, Eduardo; MORGADO, Augusto C. *A matemática do Ensino Médio*. Rio de Janeiro: IMPA, 2003.

NETO, Antônio Caminha Muniz. *Tópicos de Matemática Elementar*. Rio de Janeiro:SBM, 2012.

TERADA, Routho. *Segurança de Dados: Criptografia em redes de computador*. 2ª ed. São Paulo: Edgard Blucher, 2008.

SANTOS, José Plínio de Oliveira. *Teoria dos Número*.3ª ed. Rio de Janeiro: IMPA, 2009.

SPENTHOF, Roberto Luiz; SOUZA, Josiney Alves de. Primos: da aleatoriedade ao padrão. **SBM**, (professor de matemática online). Número 1, volume, 2013.

STALING, William. *Criptografia e Segurança de Redes*. 4ª ed. São Paulo: Pearson, 2011.p.182-202