UNIVERSIDADE ESTADUAL DE MARINGÁ
CENTRO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL – PROFMAT
(Mestrado)

DARCI DALA COSTA

A MATEMÁTICA E OS CÓDIGOS SECRETOS:
UMA INTRODUÇÃO À CRIPTOGRAFIA

Maringá – PR
2014

DARCI DALA COSTA

A MATEMÁTICA E OS CÓDIGOS SECRETOS:
UMA INTRODUÇÃO À CRIPTOGRAFIA

Trabalho de Conclusão de Curso apresentado ao Programa de Mestrado profissional em Matemática em Rede Nacional – PROFMAT do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como requisito parcial para obtenção do título de Mestre.
Área de concentração: Matemática.

Orientador: Prof. Dr. JOSINEY ALVES DE SOUZA

Maringá – PR
2014

Ficha Catalográfica

D136m **Dala Costa, Darci**

A Matemática e os códigos secretos: uma introdução à criptografia/

Darci Dala Costa.- Maringá: UEM/PROFMAT,2014.

xi, 67 p.: gráficos, tabelas.

Inclui bibliografia

Dissertação (mestrado) Universidade Estadual de Maringá, 2014

Orientador: Prof. Dr. Josiney Alves de Souza

1. Criptografia. 2. Criptografia – História. 3. Criptografia aplicada à Matemática. 4. Criptografia – Método RSA. 5. Matemática. 6. Teoria dos números. 7. Linguagem codificada. I. Título

CDD 20ª ed. 005.82

512.7

513

Bibliotecária – Hebe Negrão de Jimenez -CRB 101/9

DARCI DALA COSTA

A MATEMÁTICA E OS CÓDIGOS SECRETOS: UMA INTRODUÇÃO À CRIPTOGRAFIA

Trabalho de Conclusão de Curso, apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática tendo a Comissão Julgadora composta pelos membros:

COMISSÃO JULGADORA:

Prof. Dr. Josimey Alves de Souza
DMA/Universidade Estadual de Maringá (Presidente)

Prof. Dr. Simão Nicolau Stelmastchuk
Universidade Estadual do Paraná – União da Vitória - PR

Prof. Dr. Emerson Luiz do Monte Carmelo
DMA/Universidade Estadual de Maringá

Aprovada em: 24 de fevereiro de 2014.
Local de defesa: Auditório do Departamento de Matemática do Centro de Ciências Exatas, Bloco F67, campus da Universidade Estadual de Maringá.

Dedico este trabalho à minha Família: com amor, por tudo que significam pra mim e com gratidão, por suportarem os momentos em que fui mais estudante do que pai ou marido.

Agradecimentos

Ao concluir este trabalho agradeço:

A CAPES, pela oportunidade e pelo fundamental apoio financeiro.

À minha esposa, Neiva, meus filhos Vitor e Thais pelo apoio e compreensão.

Ao professor Josiney Alves de Souza, pela orientação e disponibilidade.

Aos meus colegas de Curso, especialmente a Graciele Muller, Reges Gaieski, Maycon Pavei Boff e Vanderlei Veríssimo, o “Povo do Oeste” pelas viagens divertidas.

A todos os professores que se dispuseram a ministrar aulas para nossa turma.

Resumo

Neste trabalho buscamos mostrar, de forma sintetizada, a evolução da criptografia desde a civilização grega até os dias atuais. Apresentamos as formas de criptografar que tiveram algum destaque histórico, bem como algumas sugestões de exercícios que podem ser trabalhados em aulas de Matemática fazendo uso delas. Incluímos, também, alguns elementos da Teoria dos Números, com o objetivo de auxiliar o entendimento de uma das formas de criptografia aqui apresentadas: o Método RSA.

Palavras chave: Criptografia, Teoria dos Números, Criptografia RSA.

Abstract

In this work, we seek showing, in a synthetic form, the evolution of the cryptography, from the Greek civilization until the present days. We introduce the ways of encrypting that had some historic prominence, as well as some suggestions of exercises which can be worked in the math classes doing the use of them. We include, also, some elements of the Number Theory, with the purpose of helping the understanding of one of the forms of encryption presented here: the RSA method.

Key words: Cryptography, Number Theory, RSA Encryption.

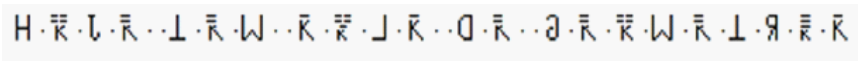
“ A engenhosidade humana não pode arquitetar uma escrita secreta que a própria engenhosidade humana não possa resolver.”

Edgar Allan Poe

Sumário

Introdução

Você é capaz de entender o significado da mensagem abaixo?



Essa mensagem foi codificada, ou seja, o texto original foi substituído por símbolos com o objetivo de dificultar a leitura, ocultando, assim, o significado.

A arte de usar símbolos diferenciados para representar mensagens é quase tão antiga quanto a própria escrita. Atualmente, esse procedimento recebe o nome de criptografia, termo cuja origem vem do grego kryptós (escondido) e gráphein (escrita). De modo geral, essa técnica pode ser entendida como o ato de aplicar um determinado código a fim de manter secreto o conteúdo de certas informações.

Antes de existir os meios de comunicação atuais, os exércitos dependiam de mensageiros para transmitir ordens e informações às tropas. Entretanto, se o arauto fosse capturado e a mensagem caísse em mãos inimigas, dados sigilosos poderiam ser revelados. Diante disso, era prudente que o conteúdo estivesse codificado. Desse modo, os adversários permaneceriam alheios à significação.

Convém ressaltar que cifrar o texto era apenas uma maneira de dificultar a leitura, não uma garantia absoluta de segurança com relação ao envio da mensagem. Os exércitos deveriam possuir uma rede eficiente de envio de informações, pois, se estas não chegassem ao destinatário, pouco importaria o fato de estarem codificadas ou não.

Com a invenção do telégrafo, as mensagens poderiam percorrer grandes distâncias rapidamente, sem a necessidade de um mensageiro. Contudo, embora fosse muito mais prático enviar um telegrama, não havia meios de garantir que a linha estivesse imune a possíveis interceptações. Tal incerteza fez com que surgissem maneiras próprias de comunicação – por meio de códigos –, formadas por frases cifradas ou de sentido modificado.

Outra evolução importante foi o surgimento do telefone, o qual permitia conversas a longas distâncias. Todavia, assim como o telégrafo, o telefone também poderia ser grampeado, o que colocaria em risco conversas confidenciais. Para contornar a situação, novamente entra em cena a linguagem em código – neste caso, evidentemente, no nível da fala.

Nos tempos atuais, mesmo com o advento de toda a tecnologia relacionada à Internet, a necessidade de o homem constituir novos sistemas semióticos não se extinguiu. Afinal, os dados dos usuários são transmitidos via cabo telefônico ou rádio, e as informações que viajam através desses meios estão sujeitas aos mesmos perigos enfrentados em dispositivos como o telégrafo e

o telefone. Então, o remédio também é o mesmo: a utilização de mensagens cifradas.

Em face do exposto, o trabalho ora aduzido almeja explorar, ainda que nos limites de nossas possibilidades, o riquíssimo campo da criptografia. Com efeito, apresentar-se-ão aqui alguns métodos semióticos desenvolvidos no decorrer da História ocidental; métodos estes que se caracterizam pela utilização, ora de letras do alfabeto latino, ora de números, como símbolos para transmitir mensagens codificadas. Conseguintemente, o objetivo aqui proposto é o de estabelecer uma base de pesquisa para professores que queiram abordar o tema da criptografia em suas aulas.

Neste trabalho, analisaremos também a Teoria dos Números, ramo da Matemática que contribuiu para o desenvolvimento do mecanismo criptográfico que tornou mais seguras as transações comerciais via Internet: o método RSA.

No Capítulo 1, destacaremos alguns processos de codificar mensagens usados antes do surgimento do computador. Para cada método apresentado, elaboramos um exemplo de codificação, seguido da respectiva decodificação – tudo isso, com modelos simples, de fácil entendimento.

No Capítulo 2, veremos alguns tópicos da Teoria dos Números. Focamos a nossa atenção no estudo de números primos e congruências, apresentando as principais proposições e teoremas que envolvem tais tópicos. Objetivamos, com esse capítulo, formar uma base para o entendimento de um sistema de criptografar muito empregado nos tempos atuais: o RSA.

No Capítulo 3, trabalharemos o funcionamento do método RSA. Para tanto, destacaremos um exemplo de cifragem de palavra com o uso do mesmo.

No Capítulo 4, apresentaremos sugestões de atividades – desafios ou exercícios de aplicação – para serem trabalhadas em aulas de Matemática. Isso envolverá conteúdos como funções, matrizes, análise de frequência, propriedades das potências e outros que, porventura, o leitor julgar exequível.

Capítulo 1

Códigos Secretos Notáveis

Neste capítulo, veremos as quatro maneiras mais comuns de criptografar – segundo[7] – da era pré-computador.

i) substituição monoalfabética: cada letra do alfabeto é representada por um símbolo diferente, que pode ser um número, uma letra ou uma figura qualquer;

ii) substituição polialfabética: cada símbolo representa uma letra diferente de acordo com sua posição na mensagem;

iii) transposição: a mensagem é transformada em uma matriz e criptografada pela matriz transposta

iv) combinação de substituição e transposição

1.1 Um pouco de História

No decorrer da História da humanidade, a criptografia sempre esteve presente. Tal prática persiste até os tempos atuais, seja em situações de caráter pessoal – como, por exemplo, nos diários de adolescentes que não querem que seus segredos sejam revelados –, seja numa conjuntura mais ampla, como a que envolve informações sobre pessoas, empresas, nações, táticas de guerra etc.

Um dos primeiros povos ocidentais a registrar uma maneira de codificar mensagens em guerras foi os gregos – mais precisamente, o exército espartano, há mais de 2500 anos – (ver[5]).

A troca de mensagens se dava da seguinte forma: o remetente escrevia a mensagem em uma faixa de pergaminho enrolada em espiral, ao longo de um cilindro, chamado cítala – o texto deveria ser escrito no sentido do comprimento desse objeto. Consequentemente, a mensagem tornar-se-ia clara se o pergaminho fosse enrolado em outra cítala, de mesmo diâmetro.

No caso dos espartanos, a cítala era como a "chave"do código, pois servia tanto para ocultar a mensagem como para revelá-la. A chave, no caso citado, era um objeto. No entanto, com o passar do tempo, ela foi, aos poucos, substituída por outros elementos, tais como números, mudança de posição de letras, símbolos associados a letras, entre outros.

Veremos agora algumas maneiras de codificação conhecidas na História ocidental.

1.2 Quadrado de Polybius

De origem grega, esta cifra consiste em um quadrado 5x5 onde são distribuídas as letras do alfabeto, estando as letras I e J na mesma posição.

Para criptografar por esse método associamos a cada letra um número de dois dígitos formado pela linha e coluna, nessa ordem, onde estava a letra, conforme ilustra a Figura 1.1 abaixo.

Figura 1.1

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

Fonte: o autor

Por exemplo a letra L é representada pelo número 31. O L está situado no encontro da terceira linha com a primeira coluna. Continuando dessa maneira ciframos a palavra

LÁPIS pelo número 3111352443

e

LÁPIS PRETO por 31113524433542154434.

O quadrado de Polybius apresentava uma maneira de associar letras e números, mas não era fixo, senão não teria utilidade visto que todos que o usassem uma vez sempre saberiam como decifrar as mensagens. As letras

poderiam ser colocadas no interior do quadro de maneira aleatória o que daria inúmeras possibilidades de variação da cifra.

1.3 Troca de César

Os romanos, naturalmente, também fizeram uso de mensagens secretas . O imperador romano Julio César, utilizava um artifício que consistia em se trocar a letra original pela letra que se encontra a algumas posições a frente pela ordem do alfabeto.

Por exemplo se ele deslocasse as letras da mensagem original duas unidades teríamos a cifra ilustrada na Figura 1.2.

Figura 1.2

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

Fonte: o autor

Nessa configuração a letra B seria representada por D, a palavra

GUERRA ficaria IWGTTC

e a frase

VIM, VI, VENCI fica XKO XK XGPEK.

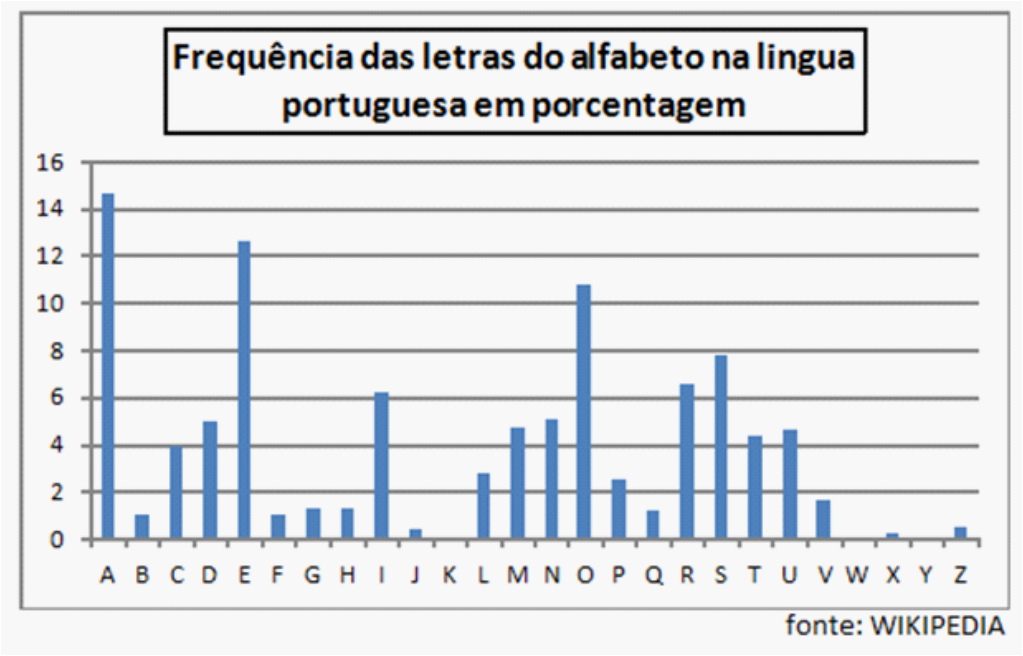
Com algumas variações, usando qualquer um desses sistemas podemos criar muitas maneiras de cifrar uma mensagem. Independente da escolha, só estamos mudando o símbolo que representa a letra. Esse procedimento faz com que a frequência do símbolo associado a letra permaneça a mesma. Na prática, continuamos com um alfabeto de 26 símbolos . Por exemplo, em um texto criptografado pelo quadrado de Polyibius, configurado da maneira como dispusemos, sempre que aparecer o número 31 ele vai representar a letra L.

Códigos como estes são chamados de Códigos de Substituição Alfabética e eram muito utilizados até o século IX. Neste século o cientista árabe Al-Kindi

descreveu uma maneira de decifrar mensagens de acordo com a frequência em que os símbolos apareciam nas mesmas, (ver[7]). Esse método é conhecido, hoje, como "análise de frequência". Ele realiza uma contagem de símbolos da mensagem e associa a quantidade deles com a frequência de cada letra nos textos escritos na língua em que a mensagem foi, supostamente, escrita.

A Figura 1.3 mostra qual é a porcentagem de frequência das letras num texto em português.

Figura 1.3



Com o uso das informações contidas nele, podemos concluir que o símbolo com maior frequência em um texto tem uma grande possibilidade de ser um A, se o texto estiver em português.

Como o objetivo da criptografia é ocultar informações, uma simples substituição alfabética, com o passar do tempo, deixou de ser segura tornando necessária a criação de novas maneiras de ocultar mensagens.

1.4 O Quadrado de Trithemius

Os textos criptografados por substituição monoalfabéticas se tornaram vulneráveis após Al-Kindi. Mesmo assim, perduraram por algum tempo pois a troca de informações era muito lenta nessa época. No século XV, Leon Battista Alberti escreveu um manuscrito propondo uma nova forma de criptografia, a substituição polialfabética, ou seja, um código que possui mais de

um alfabeto em sua estrutura de codificação. O método de criptografia apresentado faz uso de um quadro formado por 26 linhas e 26 colunas contendo todas as letras do alfabeto. Cada linha do quadro representa uma troca de César em relação à primeira linha.

O primeiro livro impresso que continha a descrição dessa forma de criptografar foi: «*Polygraphiae libri sex, Ioannis Trithemii abbatis Peapolitani, quondam Spanheimensis, ad Maximilianum Ceasarem*», traduzido, "Poligrafia em seis livros por João Trithemius, abade de Würzburg, anteriormente de Sponheim, dedicados ao Imperador Maximiliano". Devido a isso o quadro usado por Alberti ficou conhecido como Qaudrado de Trithemius, (ver[7],[8]).

A Figura1.4 representa o Quadrado de Trithemius.

Figura 1.4

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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Fonte: o autor

Cifrar uma mensagem usando esse sistema é simples. Deslocamos e substituímos as letras de acordo com a posição na mensagem. Sendo o deslocamento igual a uma unidade a menos que a posição. Consideramos o alfabeto um ciclo e a ordem alfabética das letras como o sentido positivo de deslocamento.

A Figura 1.5 mostra como codificar a palavra POLIGRAFIA.

Figura 1.5

Letra	P	O	L	I	G	R	A	F	I	A
Deslocamento	0	1	2	3	4	5	6	7	8	9
Cifra	P	P	N	L	K	W	G	M	Q	J

Fonte: o autor

Assim: POLIGRAFIA torna-se PPNLKWGMQJ

Note que, o primeiro I é cifrado por L e o segundo I por Q. Apenas a análise de frequência não é suficiente para quebrar esse tipo de código.

Para decodificar, basta fazer o deslocamento oposto ao da codificação, como está apresentado na Figura 1.6.

Figura 1.6

Cifra	P	P	N	L	K	W	G	M	Q	J
Deslocamento	0	-1	-2	-3	-4	-5	-6	-7	-8	-9
Letra	P	O	L	I	G	R	A	F	I	A

Fonte: o autor

O Quadrado de Trithemius serviu de base para outros tipos de substituição polialfabética, como veremos a seguir.

1.5 A cifra de Vigenère

Ao estudar Trithemius e outros autores, no final do século XVI, Blaise de Vigenère escreveu *Traité des chiffres ou secrètes manières d'écrire*: em que descreve os modos de encriptação usados na época. Um dos método descrito por Vigenère, no qual se utiliza o Quadrado de Trithemius e uma palavra chave para cifrar mensagens, foi originalmente proposto por Giovan Batista Belaso em seu livro "*La cifra del. Sig. Giovan Batista Belaso*", (ver[7], [8]).

Acompanhe, passo a passo, como codificar a palavra LEITURA, utilizando como chave a palavra: PRIMO.

Conforme a Figura 1.7, escrevemos a palavra chave sobre o texto a ser cifrado, letra sobre letra e repetindo a mesma palavra até que este termine.

Figura 1.7

Chave	P	R	I	M	O	P	R
Texto	L	E	I	T	U	R	A

Fonte: o autor

Para cifrar, devemos ter nas mãos o Quadrado de Trithemius. Cada letra da cifra é obtida pela interseção da linha iniciada pela letra da palavra chave com a coluna iniciada pela letra do texto.

Na mensagem que estamos codificando a primeira letra é obtida pela interseção da linha que inicia com "P"com a coluna que inicia com "L"que é a letra "A". A segunda letra é obtida pela interceção da linha que começa com "R"com a coluna que começa com "E"que é "V".Seguindo esse procedimento obtemos a cifra ilustrada na figura 1.8.

Figura 1.8

Chave	P	R	I	M	O	P	R
Texto	L	E	I	T	U	R	A
Cifra	A	V	Q	F	I	G	R

Fonte: o autor

Dessa maneira: LEITURA é cifrada como AVQFIGR.

Para decifrar o receptor deve escrever o texto cifrado sob a chave, letra com letra e deve utilizar o Quadrado de Trithemius. A Figura 1.9 ilustra esse procedimento no caso da mensagem ser AVQFIGR.

Figura 1.9

Chave	P	R	I	M	O	P	R
Cifra	A	V	Q	F	I	G	R

Fonte: o autor

Para obter a primeira letra da mensagem original, seguimos a linha que inicia com "P"até encontrarmos a letra "A". A primeira letra da coluna que contém esse "A"que, no caso é "L", é a primeira letra da mensagem. Para a segunda letra, seguimos a linha que inicia em "R"até a coluna que contém "V", a letra do topo dessa coluna, no caso "E"é a segunda letra da mensagem. Procedendo dessa maneira para cada par de letras Chave/Cifra encontramos o texto original.(Figura 1.10)

Figura 1.10

Chave	P	R	I	M	O	P	R
Cifra	A	V	Q	F	I	G	R
Texto	L	E	I	T	U	R	A

Fonte: o autor

Apesar de ter sido elaborada por Belaso essa cifra é chamada de Cifra de Vigenère.

Além desse sistema, Vigenere propôs um esquema chamado cifra de auto chave, onde a chave era a própria mensagem iniciada por uma letra, chamada letra primária, previamente combinada entre remetente e receptor. As Figuras 1.11 e 1.12 mostram como ficaria a nossa mensagem usando como letra primária o "S".

Figura 1.11

Chave	S	L	E	I	T	U	R
Texto	L	E	I	T	U	R	A

Fonte: o autor

Como a maneira de codificar é a mesma:

Figura 1.12

Chave	S	L	E	I	T	U	R
Texto	L	E	I	T	U	R	A
Cifra	D	P	M	B	N	L	R

Fonte: o autor

A mensagem codificada é : "DPMBNLR".

Para decifrar a mensagem, visto que não temos uma palavra chave, procedemos do seguinte modo:

Tabelamos a mensagem e a letra primária como mostra a Figura 1.13.

Figura 1.13

Chave	S						
Cifra	D	P	M	B	N	L	R

Fonte: o autor

Como a letra primária é "S"e a primeira letra da mensagem é "D", devemos determinar a primeira letra da coluna que cruza a linha que inicia com "S"em "D". Dessa forma encontraremos o "L". Então "L"é a primeira letra da mensagem e também a segunda letra da chave.(Figura 1.14)

Figura 1.14

Chave	S	L					
Cifra	D	P	M	B	N	L	R
Texto	L						

Fonte: o autor

Agora repetimos esse procedimento com o "L"e o "P"para encontrar o "E", que é a segunda letra da mensagem e a terceira letra da chave. Repetimos o processo até o término da mensagem ilustrado na Figura 1.15.

Figura 1.15

Chave	S	L	E	I	T	U	R
Cifra	D	P	M	B	N	L	R
Texto	L	E	I	T	U	R	A

Fonte: o autor

A cifra de Vigenère foi uma campeã em segurança. Foram precisos 300 anos para que, em meados do século XIX, Charles Babbage (na Inglaterra) e Friedrich Kasiski (na Alemanha) quebrassem a cifra, (ver[8]).

1.6 Criptografia por Transposição

A quebra da Cifra de Vigenère mostrou a vulnerabilidade das cifras de substituição voltando a atenção dos criptoanalistas para outras formas de encriptação. Uma dessas formas é embaralhar o terxto, ao invés de subtituir as letras. Uma das maneiras de fazer isso é criptografar a mensagem por transposição. A mais simples é a transposição geométrica, assim chamadas por usar como base uma matriz retangular. O texto original é escrito dentro da matriz no sentido das linhas, completando com X os espaços que sobram. Feito isso, é feita a transposição da matriz. A mensagem criptografada é obtida pelo conjunto de blocos de letras formados pelas linhas.

Observe como isto é feito com o comando:

ATACAREMOS AO NASCER DO SOL

Como a ordem é formada por 23 letras, vamos escrevê-la em uma matriz de 4 por 6, conforme a Figura 1.16.

Figura 1.16

A	T	A	C	A	R
E	M	O	S	A	O
N	A	S	C	E	R
D	O	S	O	L	X

Fonte: o autor

A transposta desta matriz é dada na Figura 1.17.

Figura 1.17

A	E	N	D
T	M	A	O
A	O	S	S
C	S	C	O
A	A	E	L
R	O	R	X

Fonte: o autor

Assim:

ATACAREMOS AO NASCER DO SOL

torna-se

AEND TMAO AOSS CSCO AAEL RORX

Para decodificar a mensagem, os blocos são escritos em uma matriz de 6 por 4, cuja transposta é a mensagem original.

1.7 A cifra ADFGX

Apesar de muito simples, criptografia por transposição serviu de base para outro algoritmo, que foi utilizado durante a Primeira Guerra Mundial

No século XIX, foi inventado o telégrafo trazendo um grande avanço nas comunicações. Agora as mensagens viajariam grandes distâncias sem a necessidade de um mensageiro o que, teoricamente, era uma garantia maior de sigilo entre remetente e receptor da mensagem.

A utilização do telégrafo para envio de mensagens trazia também alguns inconvenientes, tais como: eram necessários operadores nos postos e estes teriam acesso a mensagem enviada, a linha telegráfica poderia ser "grampeada"por alguém com o equipamento correto e assim a mensagem seria interceptada. Isso representaria um perigo em tempos de guerra

Para contornar essa situação os alemães criaram uma nova cifra utilizando o tabuleiro de Polybius, substituindo os números 12345 pelas letras ADFGX, uma palavra chave e uma transposição.

Acompanhe como codificar uma mensagem usando este sistema:

Inicialmente, criamos uma matriz parecida com o tabuleiro de Polybius.(Figura 1.18)

Figura 1.18

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

Fonte: o autor

A maneira de cifrar a mensagem segue, de início, da forma já vista, apenas trocando o par de números pelo par de letras. Se a mensagem fosse

CHEGAREI SÁBADO,

teríamos:

C=AF,H=DF,E=AX,G=DD,A=AA,R=GD,E=AX,I=DG,
S=GF,A=AA,B=AD,A=AA,D=AG,O=FG

que, agrupado, fica

AFDFAXDDAAGDAXDGGFAAADAAAGFG

A próxima etapa é escolher uma palavra-chave, que pode ter qualquer tamanho mas não ter letras repetidas. Neste caso vamos utilizar a palavra CIFRA.

Montamos uma tabela com as letras da palavra-chave na primeira linha e completamos a tabela com a mensagem cifrada, uma letra para cada célula da tabela, conforme ilustra a Figura 1.19.

Figura 1.19

C	I	F	R	A
A	F	D	F	A
X	D	D	A	A
G	D	A	X	D
G	G	F	A	A
A	D	A	A	A
G	F	G		

Fonte: o autor

A tabela deve ser reorganizada de forma que as letras da palavra-chave fiquem em ordem alfabética, alterando nas colunas correspondentes as letras de forma apropriada:(Figura 1.20)

Figura 1.20

A	C	F	I	R
A	A	D	F	F
A	X	D	D	A
D	G	A	D	X
A	G	F	G	A
A	A	A	D	A
	G	G	F	

Fonte: o autor

A mensagem cifrada é formada pelos grupos de cada coluna, excetuando a linha da palavra-chave. Em nosso caso, a mensagem enviada pelo telégrafo se torna:

AADAA AXGGAG DDAFAG FDDGDF FAXAA.

O código ADFGX, por sua vez, deu origem a outro, o ADFGVX, que incluía os algarismos de 0 a 9 e foi utilizado pelo exército alemão no final primeira guerra mundial.

Embora o número de grupamentos nos dão a quantidade de letras da palavra chave, esse código foi difícil de ser quebrado, feito realizado por Georges-Jean Painvin sem o auxílio de computadores. Estes são capazes de realizar várias simulações por segundo, podendo "quebrar"a mensagem pelo que é chamado "força bruta"que significa testar todos os casos.

Mas se o método da "força bruta"pode "quebrar códigos"e decodificar mensagens, surge a necessidade de criar uma maneira de codificação que mesmo os computadores não possam decifrar.

Um método usado atualmente que vem conseguindo realizar essa proeza é o RSA. Para apresentá-lo vamos revisar alguns conceitos de Teoria dos Números que servem como base para o mesmo.

Capítulo 2

Números Inteiros

Neste capítulo trataremos de alguns pontos da Teoria dos Números sem os quais não poderemos entender o método RSA. Nossa atenção será focada nas proposições e teoremas necessários para a compreensão do mesmo. Ao final do capítulo utilizaremos um de seus tópicos para cifrar e decifrar de maneira mais rápida alguns métodos de criptografia vistos no Capítulo 1. Pautamos este capítulo nos trabalhos: [1], [3] e [4] .

2.1 Indução Matemática

As ciências naturais baseiam suas conclusões a respeito de determinados fenômenos por meio de um grande número de observações e posterior análise de resultados semelhantes. Dessa maneira, se um fenômeno, observado várias vezes, produz o mesmo resultado, é possível fazer conclusões sobre ele. Tal fenômeno conduz a tal resultado.

Fazendo uma analogia com a matemática, os fenômenos são as proposições. Lembrando que proposições são sentenças declarativas afirmativas que podem ser verdadeiras ou falsas. O fato de uma proposição ser verdadeira num grande número de casos particulares não nos permitirá concluir que ela é válida. Uma afirmação sobre números só é valida se for verdadeira para todos os números aos quais ela se refere. Como não podemos verificar a veracida de uma proposição com todos os números, usamos testes que se baseiam nas características dos conjuntos numéricos envolvidos. Um teste para afirmações sobre números inteiros, que veremos a seguir, é o chamado método de recorrência ou indução matemática([3]).

2.1.1 Elemento mínimo de um conjunto de inteiros

Definição 2.1. *Seja A um conjunto de inteiros. Chama-se* ***elemento mínimo*** *de A um elemento de A tal que $a \leq x$ para todo $x \in A$.*

Notação: $minA$, se lê: mínimo de A.

Teorema 2.2. *Se a é elemento mínimo de A, então esse elemento é único.*

Demonstração: Com efeito, se existisse um outro elemento mínimo b de A, teríamos: $a \leq b$, porque $a = minA$ e $b \leq a$, porque $b = minA$ o que implica em $a = b$. □

O elemento mínimo de A, se existe, denomina-se também primeiro elemento de A ou menor elemento de A.

2.1.2 Princípio da Indução Finita

O Princípio da Indução é um importante instrumento para provar teoremas que envolvam números inteiros. Para demonstrá-lo, no entanto, precisamos do seguinte axioma.

Axioma 1. *Seja $\mathbb{N}$ o conjunto dos números inteiros positivos e S um subconjunto de $\mathbb{N}$ tal que*

i) $0 \in S$

ii) S é fechado com respeito à operação de "somar 1"a seus elementos, ou seja, para todo elemento $n \in S$ implicar $(n + 1) \in S$.

Então $S = \mathbb{N}$.

Se $A \subset \mathbb{N}$ e $a \in \mathbb{N}$, usaremo a seguinte notação: $a + A = \{a + x;\ x \in A\}$. É imediato verificar que: $a + \mathbb{N} = \{m \in \mathbb{N};\ m \geq a\}$

Teorema 2.3. *(**Princípio da Indução**) Seja $\mathbb{N}$ o conjunto dos números inteiros positivos e P(n) uma proposição associada a cada inteiro positivo n e que satisfaz às duas seguintes condições:*

i) P(1) é verdadeira;

ii) para todo inteiro positivo k, se P(k) é verdadeira, então P(k + 1) também é verdadeira.

Nestas condições, a proposição P(n) é verdadeira para todo inteiro positivo n.

Demonstração: Seja V o subconjunto dos elementos de $\mathbb{N}$ para os quais $P(n)$ é verdade. Considere o conjunto

$$S = \{m \in \mathbb{N}; a + m \in V\},$$

que verifica trivialmente $a+S \subset V$.Como, pela primeira condição, temos que $a+0=a \in V$, segue que $0 \in S$.Por outro lado, se $m \in S$, então $a+m \in V$, e por (ii), temos que $a+m+1 \in V$, logo $m+1 \in S$. Assim, pelo Axioma de Indução, temos $S=\mathbb{N}$. Portanto,

$$\{m \in \mathbb{N}; m \geq a\} = a+\mathbb{N} \subset V,$$

o que prova o resultado. □

2.1.3 Propriedade da Boa Ordem

A Propriedade ou Princípio da Boa Ordem é uma maneira de dispor os elementos de um subconjunto, não vazio, de números inteiros como se estes formassem uma fila. Assim como o Princípio da Indução, é de grande relevância nas demonstrações de teoremas que envolvem Números Inteiros.

Teorema 2.4. *Sendo* $\mathbb{N}$ *o conjunto dos números inteiros positivos todo subconjunto não vazio de* $\mathbb{N}$ *possui um menor elemento.*

Demonstração: Seja S um subconjunto não vazio de $\mathbb{N}$ e suponha, por absurdo, que S não possui um menor elemento. Queremos mostrar que S é vazio, conduzindo a uma contradição. Considere o conjunto T, complementar de S em $\mathbb{N}$.Queremos, portanto, mostrar que $T=\mathbb{N}$. Defina o conjunto

$$I_n = \{k \in \mathbb{N}; k \leq n\},$$

e considere a sentença aberta

$$p(n) : I_n \subset T.$$

Como $0 \leq n$ para todo n,segue que $0 \in T$, pois, caso contrário, 0 seria um menor elemento de S. Logo $p(0)$ é verdade. Supomha agora que $p(n)$ seja verdade. Se $n+1 \in S$, como nenhum elemento de I_n está em S, teríamos que $n+1$ é um menor elemento de S, o que não é permitido. Logo,

$$I_{n+1} = I_n \cup \{n+1\} \subset T,$$

o que prova que para todo n, $In \subset T$; portanto $\mathbb{N} \subset T \subset \mathbb{N}$ e, consequentemente, $T=\mathbb{N}$. □

2.2 Fatores e Números Primos

Nesta seção apresentamos algumas propriedades relativas à divisão de números inteiros, os números primos e teoremas envolvendo números primos e divisibilidade. Citamos, também, algumas fórmulas de obtenção de números primos e o Método de Fatoração de Fermat.

2.2.1 Divisibilidade e propriedades

Definição 2.5. *: Sejam a e b números inteiros, com a diferente de zero. Dizemos que a divide b, e notamos $a|b$, se existe um único inteiro c tal que $b = ac$.*

Nos termos da definição2.5, podemos dizer que b é múltiplo de a, que a é fator ou divisor de b e, ainda, se $1<a<b$, a é um fator próprio de b. O número c na definição acima é chamado de cofator de a em b.

Proposição 2.6. *Sejam $a, b, c \in \mathbb{Z}^*$.*

i) $1|c$, $a|a$ e $a|0$.
ii) Se $a|b$ e $b|c$, então $a|c$.
iii) Se $a|b$ e $a|c$, então $a|(b \pm c)$.
iv) Se $a|b$, então $a|bc$.
v) Se $a|b$ e $a|(b \pm c)$, então $a|c$.

Demonstração: **i)** Vem das igualdades $c = 1 \cdot c, a = 1 \cdot a$ e $0 = a \cdot 0$.

ii) Como $a|b$ e $b|c$,então, por definição, existem d e $f \in \mathbb{Z}$ tais que $b = a \cdot d$ e $c = b \cdot f$. Subtituindo o valor de b da primeira equação na outra temos:

$$c = b \cdot f = (a \cdot d) \cdot f = a \cdot (d \cdot f),$$

o que mostra que $a|c$.

iii) Como $a|b$ e $a|c$, então, por definição, existem d e $f \in \mathbb{Z}$ tais que $b = a \cdot d$ e $c = a \cdot f$. De modo que:

$$b \pm c = (a \cdot d) \pm (a \cdot f) = a(d \pm f)$$

Logo $a|(b \pm c)$.

iv) Sendo que $a|b$,por definição existe $d \in \mathbb{Z}$ tal que $b = a \cdot d$, logo:

$$bc = (a \cdot d) \cdot c = a \cdot (d \cdot c).$$

Portanto, $a|bc$.

v) Vamos considerar o caso $(b + c)$. Como $a|b$ e $a|(b + c)$,então, por definição, existem d e $f \in \mathbb{Z}$ tais que $b = a \cdot d$ e $(b+c) = a \cdot f$. Substituindo b na segunda igualdade, temos:

$$b + c = (a \cdot d) + c = a \cdot f.$$

Subtraindo $a \cdot d$ de ambos os lados da igualdade temos:

$$c = a \cdot f - a \cdot d = a(f - d),$$

o que mostra que $a|c$. □

2.2.2 Algorítmo da Divisão ou Divisão Euclidiana

Proposição 2.7. ***(Algorítmo da Divisão)*** *Dados $a, b \in \mathbb{Z}$; com $b > 1$, existem únicos $q, r \in \mathbb{Z}$ tais que*

$$a = bq + r \ \ e \ 0 \leq r < b$$

onde q é o quociente e r é o resto da divisão de a por b.

Demonstração: Seja $b \in \mathbb{Z}$, com $b > 1$. Dado um número $a \in \mathbb{Z}$, temos duas possibilidades:

i) a é múltiplo de b, ou seja, existe $q \in \mathbb{Z}$ tal que $a = bq$.

ii) a está entre dois múltiplos de b, ou seja, existe $q \in \mathbb{Z}$ tal que $bq < a < b(q + 1)$. (Essas possibilidades são chamadas de *Propriedades de Arquimedes*).

Subtraindo bq na igualdade (ii), esta torna-se:

$$0 < a - bq < b.$$

Seja $r \in \mathbb{Z}$, tal que $r = a - bq$ e

$$0 < r < b,$$

é claro que se $r = 0$, então $a = bq$. Caso (i). Resta saber se r e q são únicos. Para isso supomos que $a = bq + r$ e $a = bq_1 + r_1$ com $0 \leq r, r_1 < b$. Consideremos $r \neq r_1$ com $r > r_1$. Assim

$$bq + r = bq_1 + r_1 \Longrightarrow b(q_1 - q) = r - r_1,$$

donde, concluímos que $q_1 > q$ e $r = r_1 + b(q_1 - q)$. Como $r_1 > 0$ e $q_1 - q > 1$, temos, pela última igualdade, que $r > b$ o que é um absurdo. Então $r = r_1$ e $q_1 = q$. □

Exemplo 2.1. *Na expressão* $17 = 3 \cdot 5 + 2$ *temos que na divisão de 17 por 5 o quociente* $q = 3$ *e o resto* $r = 2$.

2.2.3 Máximo Divisor Comum e Mínimo Múltiplo Comum

Definição 2.8. *Sejam os números* $a, b \in \mathbb{Z}$. *Um número inteiro* d *é chamado de* ***Máximo Divisor Comum*** *de* a *e* b *(denota-se* $d = mdc(a, b)$*) se:*

i) $d|a$ e $d|b$
ii) Se, para algum $c \in \mathbb{Z}$, temos $c|a$ e $c|b$, então $c|d$.

Por (i) temos que d é divisor tanto de a quanto de b e por (ii) temos que d é o maior divisor com a caraterística (i).

Definição 2.9. *Sejam os números* $a, b \in \mathbb{Z}$. *Um número inteiro* m *é chamado de* ***Mínimo Múltiplo Comum*** *de* a *e* b *(denota-se* $m = mmc(a, b)$*) se:*

i) $a|m$ e $b|m$
ii) Se, para algum $c \in \mathbb{Z}$, temos $a|c$ e $b|c$, então $m|c$.

Enfim m é o menor dos múltiplos comuns de a e b.

Teorema 2.10. *(**Teorema de Bachet-Bézout**)Dados dois inteiros* a *e* b*, não conjuntamente nulos. Seja* $d = mdc(a, b)$*, então existem* x *e* y *inteiros tais que:* $d = ax + by$*, ou seja,* d *é uma combinação linear de* a *e* b.

Demonstração: Considere o conjunto $L = \{\ ax + by$, todas as combinações lineares de a e $b\}$ e $n = ax_0 + by_0$ onde n é o menor elemento natural de L. Suponha, por absurdo, que $n \nmid a$, então: $a = nq + r \qquad (i)$, para q e r inteiros com $0 < r < n$. Subtraindo nq de ambos os lados, a igualdade (i) se torna $r = a - nq$. Substituindo o valor de n, temos:

$$r = a - (ax_0 + by_0)q = a - ax_0q + by_0q = a(1 - x_0q) + b(y_0q).$$

Isto implica em $r \in L$, o que é um absurdo, pois $r > 0$ e $r < n$ e n é o menor elemento de L. Portanto $n|a$. Analogamente $n|b$. Assim n é divisor comum de a e b. Resta mostrar que n é o maior divisor comum de a e b, ou seja, $n = d$. Como $d = mdc(a, b)$, então:

$$d|a \text{ implica que existe } q_1 \in \mathbb{Z} \text{ tal que } a = dq_1 \qquad (ii)$$
$$d|b \text{ implica que existe } q_2 \in \mathbb{Z} \text{ tal que } b = dq_2 \qquad (iii)$$

Sendo $n = ax_0 + by_0$, de (ii) e (iii), $n = dq_1x_0 + dq_2y_0$. Isolamos d e temos $n = d(q_1x_0 + q_2y_0)$, donde concluímos que $d|n$. Do fato n ser divisor comum de a e b e $d = mdc(a, b)$, vem $n \leq d$ e de $d|n$ temos $d \leq n$, logo $d = n$, consequentemente $d = ax_0 + by_0$. □

Uma consequência direta do *Teorema de Bachet-Bézout* é que se $mdc(a, b) = 1$ exitem inteiros s e r tais que:

$$a \cdot r + b \cdot s = 1.$$

Definição 2.11. *Dados $a, b \in \mathbb{Z} - \{-1, 0, 1\}$ se $mdc(a, b) = 1$ dizemos que os números a e b são **coprimos** ou **primos entre si**.*

2.2.4 Números Primos

Definição 2.12. *Um número inteiro $p \geq 2$ é dito **primo** se seus únicos divisores positivos são 1 e p, caso contrário p é um número **composto**.*

Exemplo 2.2. *O número 7 é primo, pois tem como divisores apenas o 1 e o 7 enquanto que o número 6 é composto pois seus divisores são 1, 2, 3 e 6.*

Proposição 2.13. *Sejam a, b e $p \in \mathbb{Z}$, com p primo. Se $p|ab$ então $p|a$ ou $p|b$.*

Demonstração: Supõe-se que $p \nmid a$. Então os divisores comuns de p e a são apenas 1 e -1.Daí o $mdc(a; p) = 1$.Logo, existem x, $y \in \mathbb{Z}$ de maneira que

$$1 = ax + py$$

Portanto, multiplicando ambos os membros da igualdade por b, temos $b = (ab)x + p(by)$.Como $p|(ab)$ existe um $k \in \mathbb{Z}$ tal que $ab = kp$. Dado que $p|p$, então

$$b = (kp)x + p(by) = p(kx + by).$$

Logo, $p|b$. □

Corolário 2.14. *Se p é um primo tal que $p|p_1 \cdots p_n$, então $p|p_i$ para algum $i = 1, ..., n$.*

Demonstração: Usando Indução, a proposição é verdadeira para $n = 1$(imediato) e para $n = 2$ (pela Proposição 2.13). Supondo, pois, $n > 2$ e que, se p divide um produto com menos de n fatores, então p divide pelo

menos um dos fatores (hipótese de indução). Pela proposição..., se $p|p_1 \cdots p_n$, então $p|p_n$ ou $p|p_1 \cdots p_{n-1}$. Se $p|p_n$, a proposição está demonstrada, e se, ao invés, $p|p_1 \cdots p_{n-1}$, então a hipótese de indução assegura que $p|p_k$, com $1 < k < n-1$. Em qualquer dos casos, p divide um dos inteiros $p_1, p_2, ..., p_n$. □

Corolário 2.15. *Se $p, p_1, ..., p_n$ são números primos e se $p|p_1 \cdots p_n$, então $p = p_i$ para algum $i = 1, ..., n$.*

Demonstração: De fato, pelo Corolário 2.14, existe um índice k, com $1 < k < n$, tal que $p|p_k$, como os únicos divisores positivos de p_k são 1 e p_k, porque p_k é primo, segue-se que $p = 1$ ou $p = p_k$. Mas, $p > 1$, porque p é primo. Logo, $p = p_k$. □

Teorema 2.16. ***(Teorema Fundamental da Aritmética)*** *Todo inteiro maior do que 1 é primo ou pode ser representado de maneira única (a menos da ordem dos fatores) como um produto de fatores primos.*

Demonstração: Usaremos o Princípio da Indução. Se $n = 2$, o resultado é óbvio pois 2 é primo. Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, não há o que demonstrar. No caso de n ser composto, existem números inteiros positivos n_1 e n_2 tais que $n = n_1 \cdot n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem primos $p_1, p_2, ..., p_r$ e $q_1, q_2, ..., q_s$ tais que $n_1 = p_1, p_2, ..., p_r$ e $n_2 = q_1, q_2, ..., q_s$. Portanto,

$$n = p_1 \cdot p_2 \cdots p_r \cdot q_1 \cdot q_2 \cdots q_s.$$

Suponha, agora, que $n = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s$, onde os p_i e os q_j são números primos. Como $p_1|q_1 \cdot q_2 \cdots q_s$ pelo corolário 2.14, temos que $p_1 = q_j$ para algum $j \leq s$, que, ao reordenarmos os fatores $q_1, q_2, ..., q_s$ podemos chamar de q_1.Portanto,

$$p_2 \cdots p_r = q_2 \cdots q_s$$

Como $p_2 \cdots p_r < n$, a hipótese de indução implica em $r = s$ e os p_i e q_j são iguais aos pares. Isso mostra a unicidade da fatoração de n. □

Teorema 2.17. *Existem infinitos números primos.*

Demonstração: Consideremos que a quantidade de números primos seja finita e $P = \{p_1, p_2, p_3, , p_n\}$ o conjunto de todos os primos. Seja $R = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1$; notemos que R é maior que qualquer $p_i \in P$ e nenhum elemento de P é fator de R. Como, pelo Teorema Fundamental da Aritmética, ou R é primo ou possui algum fator primo, isto implica na existência de um primo que não pertence P. Portanto P não pode ser um conjunto finito. □

2.2.5 Como saber se um número é primo

Como sabemos, um número primo p não possui divisores positivos diferentes de 1 e ele mesmo. Quando precisamos verificar se um dado número n é primo ou não devemos tentar encontrar divisores primos de n efetuando as divisões até obtermos um resto zero. Caso isto não ocorra: n é primo. Por sorte, de acordo com a seguinte proposição, não precisamos efetuar todas as divisões.

Proposição 2.18. *Se p é o menor fator primo de n então $p \leq \sqrt{n}$.*

Demonstração: Denotaremos por $D(n)$ o conjunto dos divisores positivos de n diferentes de 1 ou n. Como n não é primo, temos que $D(n) \neq \varnothing$. Pelo Princípio da Boa Ordem, existe um elemento $p \in D(n)$ tal que, para todo $q \in D(n)$ tem-se $p \leq q$. Supondo que $p > \sqrt{n}$ e que q seja cofator de p em relação a n temos $q > p > \sqrt{n}$. Disto $n = (\sqrt{n})^2 < p \cdot q = n$, isto é um absurdo. Sendo assim $p \leq \sqrt{n}$. □

Exemplo 2.3. *Para determinar se o número 173 é primo basta tentarmos dividí-lo pelos primos menores ou igual a 13 que é, aproximadamente, sua raiz quadrada:*

$$\begin{array}{lll} 173 = 86 \cdot 2 + 1 & resto & 1 \\ 173 = 57 \cdot 3 + 2 & resto & 2 \\ 173 = 34 \cdot 5 + 3 & resto & 3 \\ 173 = 24 \cdot 7 + 5 & resto & 5 \\ 173 = 15 \cdot 11 + 8 & resto & 8 \\ 173 = 13 \cdot 13 + 4 & resto & 4 \end{array}$$

Logo, 173 é primo.

Esta proposição diminui a quantidade de cálculos necessário para determinar se um número dado é primo. Mesmo assim o processo é pouco prático e demorado. Por isso o método RSA baseia sua segurança no processo de fatoração de números extremamente grandes. pois sua chave pública é formada por um número composto n que é produto de primos p e q com mais

de 60 algarismos cada. Fatorar um número como esse, usando testes de divisibilidade toma muito tempo, questão de anos para os computadores mais avançados.

2.2.6 Método da Fatoração de Fermat

Pierre de Fermat (1601-1665) foi um dos poucos matemáticos amadores famosos. Filho de um rico comerciante de couro, pôde se dedicar completamente aos estudos. Por influência de sua mãe, descendente de uma família de juristas, estudou leis na Universidade de Orleans e formou-se em advocacia. Trabalhou durante toda sua vida na corte de justiça de Toulouse. Foi nomeado juiz e ocupava os seus momentos de folga em diversos lazeres, entre os quais a poesia e a Matemática.

Seu interesse na teoria dos números surgiu após ler o livro Aritmética de Diofanto (matemático grego, 200 A.C.) e alguns dos problemas propostos por Fermat, nesta área, eram tão difíceis que somente muitos anos mais tarde foram provados. Seu resultado mais famoso resistiu por mais de 350 anos e inspirou a publicação, em 1996, do bestseller *O Último Teorema de Fermat.* Este teorema diz que "se n é um natural maior que 2, então não existem números inteiros x, y e z que satisfaçam a equação $x^n + y^n = z^n$". Isto foi provado definitivamente, em 1994, pelo matemático inglês Andrew Wiles (repare que no caso n = 2 o teorema é satisfeito por todos os ternos pitagóricos, isto é, por inteiros que satisfaçam o Teorema de Pitágoras)[8].

Apresentamos, agora, uma idéia de reduzir a quantidade necessária de cálculos para a fatoração de um número: o Método da fatoração de Fermat.

Proposição 2.19. *Seja $n > 1$ um inteiro ímpar. Há uma correspondência biunívoca entre a fatoração de n e a representação de n como diferença de dois quadrados.*

Demonstração: Se $n = a \cdot b$, e n ímpar, então a e b são ímpares. Logo $a + b$ e $a - b$ são pares, e $\frac{a-b}{2}$ e $\frac{a+b}{2}$ são inteiros.Então,

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

expressa n como a diferença de dois quadrados. Reciprocamente, suponha n escrito como a diferença de dois quadrados: $n = s^2 - t^2$, então $n = (s-t) \cdot (s+t)$ é a forma fatorada de n. Você pode ver que esses dois procedimentos – da fatoração para a diferença e da diferença para a fatoração – determinam uma relação biunívoca. □

Algorítmo de Fermat

A proposição 2.19 nos permite descrever um algorítmo, que é muito eficiente nos casos em que n tem um fator primo próximo de $\sqrt{n}$. A ideia é tentar achar números inteiros positivos x e y tais que $n = x^2 - y^2$. Caso estes números sejam encontrados, temos que:

$$n = x^2 - y^2 = (x + y) \cdot (x - y).$$

Logo $x - y$ e $x + y$ são fatores de n.

O caso mais fácil ocorre quando n é um quadrado perfeito; isto é, quando existe algum inteiro r tal que $n = r^2$. Neste caso temos que $x = r$ e $y = 0$. Observe que se $y > 0$ então

$$x = \sqrt{n + y^2} > \sqrt{n}$$

Tentamos encontrar x e y, onde $(x - y)$ e $(x + y)$ são fatores de n, com o seguinte procedimento:

Passo 1: Fazemos $x = \lfloor \sqrt{n} \rfloor$ (parte inteira de $\sqrt{n}$); se $n = x^2$ então x é fator de n e podemos parar.

Passo 2: Caso contrário incrementamos x de uma unidade e calculamos $y = \sqrt{x^2 - n}$. Se y for inteiro, paramos.

Passo 3: Repetimos o Passo 2 até encontrarmos y inteiro ou até que x seja igual a $\frac{n+1}{2}$, neste caso n é primo.

Exemplo 2.4. *Vamos usar o Algorítmo de Fermat para encontrar dois fatores do número* $n = 1297603$. *Iniciamos fazendo* $x = \lfloor \sqrt{1297603} \rfloor = 1139$. *Como* $1139^2 = 1297321 < 1297603$, *passamos a incrementar* x *de um em um e calculamos* y. *Vamos dispor os cálculos em uma tabela.(Tabela 2.1)*

Tabela 2.1

x	$\sqrt{x^2 - n}$
1140	44,69
1141	65,41
1142	81

Fonte: o autor

Obtivemos, assim um inteiro no terceiro laço. Portanto $x = 1142$ *e* $y = 81$ *são os valores desejados. Os fatores correspondentes são* $(x + y) = 1223$ *e* $(x - y) = 1061$.*Logo, 1061 e 1223 são fatores de* 1297603.

Essa maneira de encontrar fatores de um número inteiro n é prática quando, pelo menos um deles estiver próximo de $\sqrt{n}$.Também não é muito útil para números inteiros muito grandes. Uma saída para agilizar a fatoração de números, seria encontrar uma fórmula simples que fornecesse todos os números primos.

Ainda não existe uma fórmula aritmética simples e eficaz que forneça somente primos. As seções seguintes fornecem algumas fórmulas, elaboradas por grandes matemáticos, que geram uma certa quantidade deles.

2.2.7 Formula de Fermat

Fermat conjecturou que números da forma

$$F_n = 2^{2^n} + 1$$

são primos.

Para $n = 0, 1, 2, 3, 4$ os números:

$$\begin{aligned} F_0 &= 2^{2^0} + 1 = 3 \\ F_1 &= 2^2 + 1 = 5 \\ F_2 &= 2^{2^2} + 1 = 17 \\ F_3 &= 2^{2^3} + 1 = 257 \\ F_4 &= 2^{2^4} + 1 = 65.537 \end{aligned}$$

são todos primos. Porém, Euler mostrou que:

$$F_5 = 2^{2^5} + 1 = 4.294.967.297 = 641 \cdot 6700417.$$

Portanto F_5 não é primo.

Até o momento só são conhecidos estes cinco primos de Fermat, (ver[8]).

2.2.8 Fórmula de Euler

Leonhard Euler (1707 -1783) foi um matemático e físico de origem suíça. Nasceu na Basiléia, filho do pastor calvinista Paul Euler que, desprezando seu prodigioso talento matemático, determinou que ele estudasse Teologia e seguiria a carreira religiosa. Daniel e Nikolaus Bernoulli convenceram o pai de Euler a permitir que seu filho trocasse o hábito pelos números.

Durante sua vida resolveu enorme quantidade de problemas, da navegação às finanças, da acústica à irrigação. A solução de tais problemas, que atendiam aos reclamos do mundo prático, não o entediava, principalmente

porque cada novo trabalho inspirava-o para criar uma Matemática nova e engenhosa. Era capaz de escrever vários trabalhos em um único dia com os cálculos completos e prontos para serem publicados, (ver[3][8]).

Em 1772 Euler descobriu um polinômio tendo uma longa sucessão de valores primos, dado por

$$F(n) = n^2 + n + 41$$

que fornece primos para n = 1, 2, ..., 39. Entretanto, para n = 40 o valor é composto. De fato:

$$F(40) = 40^2 + 40 + 41 = 40.(40 + 1) + 41$$

$$= 40.41 + 41 = 41.(40 + 1) = 41.41.$$

2.2.9 Fórmula de Mersenne:

Marin Mersenne (1588 - 1648) em 1644 fez a seguinte afirmação: "Todo natural

$$M_p = 2^p - 1$$

é primo para os primos p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 e 257, e é composto para todos os outros primos menores que 257".

A formula de Mersene fornece uma série de números primos e os números primos que são obtidos pela sua fórmula recebem o nome de primos de Mersene.

Estudos posteriores mostraram que Mersene havia se equivocado ao fazer a sua lista: Incluiu M_{67} e M_{257} na sua lista de primos e excluiu dessa lista M_{61}, M_{89}, M_{107}.. Nos meados do século XX, 300 anos depois, a lista correta p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 e 127 onde p $<$ 257, ficou pronta, (ver[3]).

Segundo o site http://www.mersenne.org/ prime.htm, até janeiro de 2014 já eram conhecidos, 48 primos de Mersene, para os primos p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 1213 ,19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, 20996011, 24036583, 30402457, 32582657, 37156667, 42643801, 43112609 e 57885161. Esse último primo foi descoberto em janeiro de 2013 e tem 17.425.170 de dígitos, (ver[3] e [8]).

2.3 Congruências

A codificação e decodificação pelo método RSA é baseada em cálculos que envolvem congruências. Nessa parte de nosso estudo veremos algumas definições e proposições a repeito da mesma.

Definição 2.20. *Seja m um número natural diferente de zero. Diremos que dois números a e b são congruentes módulo m se os restos das divisões euclidianas de a por m e de b por m forem iguais.*

A representação de a e b são congruentes módulo m é

$$a \equiv b(\mathrm{mod}\, m).$$

Exemplo 2.5. $23 \equiv 31(\mathrm{mod}\, 4)$, *já que os restos das divisões de 23 e de 31 por 4 são iguais a 3.*

Proposição 2.21. *Dados três inteiros a, b e m, com $m > 0$, temos que $a \equiv b(\mathrm{mod}\, m)$ se, e somente se, $m|(b-a)$.*

Demonstração: Sejam $a = mq + r$, com $|r| < |m|$ e $b = mq\prime + r\prime$, com $|r\prime| < |m|$ as divisões euclidianas de a e b por m, respectivamente. Logo, $b - a = m(q' - q) + (r' - r)$ onde $|r' - r| < |m|$. Portanto, $a \equiv b(\mathrm{mod}\, m)$ se, e somente se, $r' = r$, o que equivale a dizer que $m|b - a$. □

Proposição 2.22. *Sejam $m \in \mathbb{Z}$ com $m > 1$. Para todo $a, b, c, d \in \mathbb{Z}$,tem-se que*

i) $a \equiv a(\mathrm{mod}\, m)$
ii) se $a \equiv b(\mathrm{mod}\, m)$,então $b \equiv a(\mathrm{mod}\, m)$,
iii) se $a \equiv b(\mathrm{mod}\, m)$ e $b \equiv c(\mathrm{mod}\, m)$, então $a \equiv c(\mathrm{mod}\, m)$
iv) se $a \equiv b(\mathrm{mod}\, m)$ e $c \equiv d(\mathrm{mod}\, m)$, então $a + c \equiv b + d(\mathrm{mod}\, m)$
v) se $a \equiv b(\mathrm{mod}\, m)$ e $c \equiv d(\mathrm{mod}\, m)$, então $a \cdot c \equiv b \cdot d(\mathrm{mod}\, m)$
vi) se $a \equiv b(\mathrm{mod}\, m)$,então $a^n \equiv b^n(\mathrm{mod}\, m)$.

Demonstração: i) $a \equiv a(\mathrm{mod}\, m)$ pois $m|(a - a) = 0$.

ii) Se $a \equiv b(\mathrm{mod}\, m)$, pela proposição2.22 que $m|(b - a)$ sendo assim, existe um inteiro x tal que $(b - a) = xm$, por outro lado, existe o inteiro $-x$, simétrico de x, tal que $-xm = -(b - a) = (a - b)$. Donde concluímos que $m|(a - b)$, ou seja $b \equiv a(\mathrm{mod}\, m)$.

iii) Se $a \equiv b(\mathrm{mod}\, m)$ e $b \equiv c(\mathrm{mod}\, m)$,então $m|(b - a)$ e $m|(c - b)$. Pela proposição2.6 (iii) $m|(b - a) + (c - b)$ que equivale a $m|(b - a + c - b)$, ou $m|(-a + c)$.Portanto $a \equiv c(\mathrm{mod}\, m)$.

iv) Se $a \equiv b(\mathrm{mod}\, m)$ e $c \equiv d(\mathrm{mod}\, m)$, então $m|(b-a)$ e $m|(d-c)$.Pela proposição2.6 (iii) $m|(b-a)+(d-c)$ que é o mesmo que $m|(b-a+d-c)$, ou $m|(b+d-a-c)$ ou, ainda, $m|((b+d)-(a+c))$.Portanto $a+c \equiv b+d(\mathrm{mod}\, m)$.

v) Se $a \equiv b(\mathrm{mod}\, m)$ e $c \equiv d(\mathrm{mod}\, m)$, logo $m|(b-a)$ e $m|(d-c)$.Faça $bd-ac = d(b-a)+a(d-c)$.Como $m|d(b-a)+a(d-c)$ concluímos que $m|bd-ac$, portanto $a \cdot c \equiv b \cdot d(\mathrm{mod}\, m)$.

vi) Usando o Princípio da Indução, temos que para $n = 1$ é verdadeira. Supondo que $a^n \equiv b^n(\mathrm{mod}\, m)$ como verdadeira, temos, usando a propriedade (v) $a \equiv b(\mathrm{mod}\, m)$ e $a^n \equiv b^n(\mathrm{mod}\, m)$, então $a \cdot a^n \equiv b \cdot b^n(\mathrm{mod}\, m) \Longrightarrow a^{n+1} \equiv b^{n+1}(\mathrm{mod}\, m)$.O que mostra que a propriedade é verdadeira. □

Proposição 2.23. *Sejam $a, b, c, m \in \mathbb{Z}$, com $c \neq 0$ e $m > 1$. Temos que*

$$a + c \equiv b + c(\mathrm{mod}\, m) \text{ se, e somente se, } a \equiv b(\mathrm{mod}\, m)$$

.

Demonstração: Suponhamos que $a + c \equiv b + c(\mathrm{mod}\, m)$. A propriedade (i) nos garante que $c \equiv c(\mathrm{mod}\, m)$ isto impílica que $(c-c) \equiv (c+(-c)) \equiv 0(\mathrm{mod}\, m)$. Somando $-c$ a ambos os lados da igualdade temos:

$$a + c + (-c) \equiv b + c + (-c)(\mathrm{mod}\, m) \text{ que implica } a + 0 \equiv b + 0(\mathrm{mod}\, m)$$

logo

$$a \equiv b(\mathrm{mod}\, m).$$

Partindo de $a \equiv b(\mathrm{mod}\, m)$. Temos, por (i), $c \equiv c(\mathrm{mod}\, m)$. Usando a propriedade (iv) temos $a + c \equiv b + c(\mathrm{mod}\, m)$. □

Proposição 2.24. *Sejam $a, b, c, m \in \mathbb{Z}$, com $c \neq 0$ e $m > 1$. Então*

$$ac \equiv bc(\mathrm{mod}\, m) \text{ se, e somente se } a \equiv b(\mathrm{mod}\, \frac{m}{mdc(c,m)}).$$

Demonstração: Note que $\frac{m}{mdc(c,m)}$ e $\frac{c}{mdc(c,m)}$ são coprimos. Temos, então, que $ac \equiv bc(\mathrm{mod}\, m)$ se, e somente se, $m|c(b-a)$, dividimos ambos os termos por $mdc(c,m)$

$$\frac{m}{mdc(c,m)} | \frac{c}{mdc(c,m)}(b-a)$$

que é equivalente a

$$\frac{m}{mdc(c,m)} | (b-a)$$

ou seja

$$a \equiv b(\mathrm{mod}\, \frac{m}{mdc(c,m)}).$$

□

Da Proposição 2.24 decorre que:

Sejam a, b, c e m números inteiros, com $c \neq 0$, $m > 1$ e $mdc(c, m) = 1$. Temos que: $ac \equiv bc(\mathrm{mod}\, m)$ se, e somente se, $a \equiv b(\mathrm{mod}\, m)$ e existe um inteiro c' tal que $c \cdot c' \equiv 1(\mathrm{mod}\, m)$. Sendo c' chamado de **inverso** de c módulo m.

Exemplo 2.6. *a)* $36 \equiv 21(\mathrm{mod}\, 5)$ *como 36 e 21 são múltiplos de 3, podemos escrever* $12 \cdot 3 \equiv 7 \cdot 3(\mathrm{mod}\, 5)$ *que, pela proposição2.24 se torna* $12 \equiv 7(\mathrm{mod}\, 5)$ *pois* $mdc(3, 5) = 1$.*Note, também que* $3 \cdot 2 \equiv 1(\mathrm{mod}\, 5)$. *Logo 2 é o inverso de 3 módulo 5.*

Proposição 2.25. *Se existir um fator primo comum entre a e m, então a não admite inverso módulo m.*

Demonstração: Digamos que m e a são inteiros positivos tais que $1 < a < m$ e existe um inteiro p, tal que $1 < p$, $p|a$ e $p|m$.Suponha que existe um inteiro b tal que $ab \equiv 1(\mathrm{mod}\, m)$. Assim teremos um q inteiro tal que $ab - 1 = qm$ ou $1 = qm - ab$.Por hipótese

$$\left.\begin{array}{c} p|a, \text{ logo } p|ab \\ p|m, \text{ então } p|qm \end{array}\right\}$$

pela Proposição 2.6 (iii) $p|qm - ab$ o que implica em $p|1$ que é um absurdo pois $1 < p$. Logo, nestas condições , não existe tal b. □

Exemplo 2.7. $16 \equiv 10(\mathrm{mod}\, 6)$ *como 16 e 10 são múltiplos de 2, podemos escrever* $8 \cdot 2 \equiv 5 \cdot 2(\mathrm{mod}\, 6)$ *que não implica* $8 \equiv 5(\mathrm{mod}\, 6)$ *pois* $8 \equiv 2(\mathrm{mod}\, 6)$. *Isto está de acordo com a proposição pois* $mdc(2, 6) \neq 1$.

A Proposição 2.25 pode ser visualizada nas Tabelas 2.2 e 2.3 nos casos de $m = 7$ e $m = 6$, respectivamente.

Tabela 2.2

Resto	Inverso	Justificativa
1	1	1x1≡ 1(mod 7)
2	4	2x4≡8≡ 1(mod 7)
3	5	3x5≡15≡ 1(mod 7)
4	2	4x2≡8≡ 1(mod 7)
5	3	3x5≡15≡ 1(mod 7)
6	6	6x6≡36≡ 1(mod 7)

Fonte: o autor

Tabela 2.3

Resto	Inverso	Justificativa
1	1	1x1≡ 1(mod 6)
2	não existe	mdc(6,3)=3
3	não existe	mdc(6,2)=2
4	não existe	mdc(6,4)=2
5	5	5x5≡25≡ 1(mod 6)

Fonte: o autor

Em termos de congruência, podemos dizer que sendo p primo e a e b pertencem ao conjunto $\{0, 1, 2, ...p-1\}$ com $mdc(a, p) = 1$ a congruência $ax \equiv b(\mathrm{mod}\, p)$ tem solução única.

Os teoremas que serão vistos a seguir confirmam essa afirmação.

2.3.1 Teorema de Fermat

Pequeno Teorema de Fermat

Teorema 2.26. *Se p é primo e se o $mdc(p, a) = 1$ então:*

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

Demonstração: Consideremos os $(p-1)$ primeiros positivos do conjunto $S = \{a, 2a, 3a, 4a, ...(p-1)a\}$. Certamente, nenhum desses $(p-1)$ inteiros é divisível por p e, além disso, dois quaisquer deles são incongruentes módulo p, pois, se fosse teríamos r e s tais que: $ra \equiv sa(\mathrm{mod}\, p)$, *com* $1 \leq r \leq s \leq (p-1)$. Então, o fator comum a poderia ser cancelado, visto que o $mdc(a, p) = 1$. Teríamos: $r \equiv s(\mathrm{mod}\, p)$, isto é $p|(s-r)$ o que é impossível, porque $0 < s-r < p$. Assim sendo, dois quaisquer dos $(p-1)$ inteiros $a, 2a, 3a, ..., (p-1)a$ divididos por p deixam restos distintos e, por conseguinte, cada um desses $p-1$ inteiros é congruente módulo p a um único dos inteiros $1, 2, 3, ..., p-1$. Naturalmente numa certa ordem. Multiplicando ordenadamente essas $p-1$ congruências, teremos:

$$a \cdot 2a \cdot 3a \cdot ... \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1)(\mathrm{mod}\, p),$$

ou seja:

$$a^{p-1} \cdot (1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) \equiv 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1)(\mathrm{mod}\, p),$$

Como o $mdc(p, (p-1)!) = 1$, porque p é primo e p não divide $(p-1)!$, podemos cancelar o fator $(p-1)!$, concluindo o argumento de Fermat:

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

□

Exemplo 2.8. *Um exemplo para verificação numérica deste teorema pode ser dado considerando* $p = 7$, $a = 5$ *e* $(p-1) = 6$. *Teríamos, então:*

$$S = \{5, 10, 15, 20, 25, 30\}$$

Todos os elementos de S *são incongruentes módulo* 7, *pois:*

$$5 \equiv 5(\mathrm{mod}\, 7), 10 \equiv 3(\mathrm{mod}\, 7), 15 \equiv 1(\mathrm{mod}\, 7),$$

$$20 \equiv 6(\mathrm{mod}\, 7), 25 \equiv 4(\mathrm{mod}\, 7) e 30 \equiv 2(\mathrm{mod}\, 7),$$

Pela Proposição 2.22 (v), temos:

$$(5 \cdot 10 \cdot 15 \cdot 20 \cdot 25 \cdot 30) \equiv (5 \cdot 3 \cdot 1 \cdot 6 \cdot 4 \cdot 2)(\mathrm{mod}\, 7)$$

ordenando os fatores do primeiro termo

$$(5 \cdot 10 \cdot 15 \cdot 20 \cdot 25 \cdot 30) \equiv (1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6)(\mathrm{mod}\, 7)$$

isolando 5 *nos fatores do primeiro termo*

$$((5\cdot 1)\cdot(5\cdot 2)\cdot(5\cdot 3)\cdot(5\cdot 4)\cdot(5\cdot 5)\cdot(5\cdot 6)) \equiv (1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6)(\mathrm{mod}\, 7)$$

separando os fatores 5

$$5^6(\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6) \equiv (1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6)(\mathrm{mod}\, 7)$$

escrevendo como fatorial

$$5^6\cdot 6! \equiv 6!(\mathrm{mod}\, 7).$$

como $mdc(6!, 7) = 1$, *pela proposição2.24, podemos cancelar* $6!$ *e teremos*

$$5^6 \equiv 1(\mathrm{mod}\, 7).$$

O Teorema de Fermat é utilizado para determinar restos de divisões de potências como as dos exemplos que segue:

Exemplo 2.9. *Determine o resto da divisão de* 5^{234} *por 11.Como 11 é primo e* $mdc(11, 5) = 1$, *temos que* $5^{10} \equiv 1(\mathrm{mod}\, 11)$ *aplicando o Teorema de Fermat na questão dada, temos:*

$$5^{234} \equiv 5^{10\cdot 23+4} \equiv (5^{10})^{23}\cdot 5^4 \equiv 1^{23}\cdot 5^4 \equiv 5^4 \equiv 625(\mathrm{mod}\, 11) \equiv 9(\mathrm{mod}\, 11)$$

Exemplo 2.10. *Determine o resto da divisão de* 33^{458} *por 7. Inicialmente, temos:*$33^{458} \equiv (4\cdot 7+5)^{458} \equiv (0+5)^{458} \equiv 5^{458}(\mathrm{mod}\, 7)$. *Como 7 é primo e* $mdc(7, 5) = 1$, *temos que* $5^6 \equiv 1(\mathrm{mod}\, 7)$ *aplicando o Teorema de Fermat na questão dada, temos:*

$$33^{458} \equiv 5^{458}(\mathrm{mod}\, 7) \equiv 5^{6\cdot 76+2}(\mathrm{mod}\, 7) \equiv (5^6)^{76}\cdot 5^2(\mathrm{mod}\, 7)$$

$$(5^6)^{76}\cdot 5^2 \equiv 1^{76}\cdot 5^2(\mathrm{mod}\, 7) \equiv 5^2(\mathrm{mod}\, 7) \equiv 25(\mathrm{mod}\, 7) \equiv 4(\mathrm{mod}\, 7)$$

2.3.2 Teorema de Euler

Função Totiente ϕ(n)

Definição 2.27. *Chama-se função aritmética toda função* f *definida no conjunto* $\mathbb{N}$ *dos naturais e com valores no conjunto* $\mathbb{Z}$ *dos inteiros, i.e., toda função* f *de* $\mathbb{N}$ *em* $\mathbb{Z}$ *(*$f : \mathbb{N} \longrightarrow \mathbb{Z}$*) .*

Definição 2.28. *Chama-se Função Totiente a função aritmética* $\phi(n)$ *que denota a quantidade de inteiros* $k \in [1, 2, 3, ..., n]$ *,tais que* $mdc(k, n) = 1$.

Exemplo 2.11.

$\phi(1) = 1$, *pois* $mdc(1,1) = 1$
$\phi(3) = 2$, *pois* $mdc(3,1) = 1, mdc(3,2) = 1$
$\phi(4) = 2$, *pois* $mdc(4,1) = 1, mdc(4,2) = 2, mdc(4,3) = 1$
$\phi(5) = 4$, *pois* $mdc(5,1) = 1, mdc(5,2) = 1, mdc(5,3) = 1, mdc(5,4) = 1$

Proposição 2.29. *i) Se p é primo, então $\phi(p) = p - 1$.*

ii) Sejam m e n inteiros positivos, ambos maiores que 1, e $mdc(m,n) = 1$ então $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.

Demonstração: i) De fato, seja o conjunto $Q = \{1, 2, 3, .., p-1\}$ dos números inteiros menores que p. Como p é primo nenhum elemento de Q é fator de p, Logo para todo $k \in Q$, $mdc(k,p) = 1$. Como há $p-1$ elementos Q o resultado segue.□

ii) Se considerarmos que m e n são ambos primos para podermos fazer uso da propriedade (i), temos que $\phi(m) = m - 1$ e $\phi(n) = n - 1$ e o produto $\phi(m) \cdot \phi(n) = mn - m - n + 1$. O conjunto $P = \{1, 2, 3, m, ..n, .., mn\}$ possui $m - 1$ elementos $k_1, k_2, ..., k_{m-1}$ tais que $mdc(k_i, mn) = n$ e $n - 1$ elementos $l_1, l_2, l_3, \ \ , l_{n-1}$ tais que $mdc(l_i, mn) = m$ e o próprio mn. Para o restante dos elementos $p_i \in P$, temos: $mdc(p_i, mn) = 1$ então a quantidade de elementos p_i de P é dada por $mn - (m-1) - (n-1) - 1$ logo $\phi(mn) = mn - m - n + 1$ o que confirma a propriedade. □

A propriedade (ii) nos garante que se n é o produto de dois números primos p e q temos que $\phi(n) = (p-1)(q-1)$.

Teorema de Euler

Antes de enunciarmos o Teorema de Euler, vamos considerar o seguinte lema.

Lema 2.30. *Sejam a e $n > 1$ inteiros tais que o $mdc(a,n) = 1$. Se $a_1, a_2, ..., a_n$ são inteiros positivos menores que n e cada um deles coprimo com n, então cada um dos inteiros $a.a_1, a.a_2, ..., a.a_n$ é congruente módulo n a um dos inteiros $a_1, a_2, ..., a_n$ (não necessariamente nesta ordem em que aparecem).*

O argumento usado para a demonstração deste lema é o mesmo utilizado na prova do Pequeno Teorema de Fermat.

Teorema 2.31. *(**Teorema de Euler**) Se n é um inteiro positivo e se $mdc(a, n) = 1$, então:*

$$a^{\phi(n)} \equiv 1(\mathrm{mod}\, n).$$

Demonstração: A proposição é verdadeira para $n = 1$, pois $a^{\phi(1)} \equiv 1(\mathrm{mod}\, 1)$. Suponhamos, pois, $n > 1$, e sejam $a_1, a_2, ..., a_{\phi(n)}$ os inteiros positivos menores que n e relativamente primos a n. Como o $mdc(a, n) = 1$, então, pelo Lema 2.30, os inteiros $a.a_1, a.a_2, ..., a.a_{\phi(n)}$ são congruentes módulo n aos inteiros $a_1, a_2, ..., a_{\phi(n)}$, em uma certa ordem:

$$a.a_1 \equiv a_{1'}(\mathrm{mod}\, n), a.a_{2\equiv}a_{2'}(\mathrm{mod}\, n), ..., a.a_{\phi(n)} \equiv a_{\phi(n')}(\mathrm{mod}\, n)$$

onde $a_{1'}, a_{2'}, ..., a_{\phi(n')}$ denotam os inteiros $a_1, a_2, ..., a_{\phi(n)}$ em uma certa ordem. Multiplicando ordenadamente todas essas $\phi(n)$ congruências, obtemos:

$$(a.a_1) \cdot (a.a_2).....(a.a_{\phi(n)}) \equiv a_{1'} \cdot a_{2'} \cdot ... \cdot a_{\phi(n')}(\mathrm{mod}\, n)$$

ou seja,

$$a^{\phi(n)} \cdot (a_1, a_2, ..., a_{\phi(n)}) \equiv a_1, a_2, ..., a_{\phi(n)}(\mathrm{mod}\, n).$$

Cada um dos inteiros $a_1, a_2, ..., a_{\phi(n)}$ é coprimo com n, de modo que podem ser sucessivamente cancelados, o que dá a congruência de Euler:

$$a^{\phi(n)} \equiv 1(\mathrm{mod}\, n).$$

□

Nota: se p é um primo, $\phi(p) = p - 1$, e se o $mdc(a, p) = 1$, então:

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

que nada mais é que uma generalização do Teorema de Fermat.

Corolário 2.32. *Se $m > 1$, $k \geq 0$, $n \geq 0$ e a um inteiro qualquer são tais que, $mdc(a, m) = 1$ e $k \equiv n(\mathrm{mod}\, \phi(m))$ então, $a^k \equiv a^n(\mathrm{mod}\, m)$.*

Demonstração: Consideremos o caso em que $k > n$. Como $k \equiv n(\mathrm{mod}\, \phi(m))$ existe $q \geq 1$ tal que $k - n = q \cdot \phi(m)$ e, portanto,

$$a^k = a^{k-n} \cdot a^n = a^{q \cdot \phi(n)} \cdot a^n = (a^{\phi(n)})^q \cdot a^n \equiv a^n(\mathrm{mod}\, m).$$

□

Exemplo 2.12. *Sejam $a = 5$, $m = 6$, $k = 8$ e $n = 2$. Temos $\phi(6) = 2$, e $8 \equiv 2(\mathrm{mod}\, 2)$. Como $5^2 \equiv 1(\mathrm{mod}\, 6)$, então $5^8 \equiv 1(\mathrm{mod}\, 6)$ e desta forma, $5^8 \equiv 5^2(\mathrm{mod}\, 6)$.*

O Teorema de Euler aplicado em resoluções de congruências lineares A congruência linear $a \cdot x \equiv b(\mathrm{mod}\, m)$ no caso em que o $mdc(a, m) = 1$, admite uma única solução módulo m, que se pode facilmente obter usando o Teorema de Euler. Com efeito, a partir da expressão

$$a \cdot x \equiv b(\mathrm{mod}\, m)$$

obtemos

$$a \cdot x \equiv b \cdot a^{\phi(m)}(\mathrm{mod}\, m).$$

Como $mdc(a, m) = 1$, podemos cancelar o fator comum a, que resulta em

$$x \equiv b \cdot a^{\phi(m)-1}(\mathrm{mod}\, m).$$

Nas congruências abaixo encontramos a solução com a aplicação do Teorema de Euler.

Exemplo 2.13. *Determinar x na congruência $5 \cdot x \equiv 7(\mathrm{mod}\, 8)$. Como $mdc(5, 8) = 1$, uma aplicação do argumento acima fica:*

$$x \equiv 7 \cdot 5^{\phi(8)-1} \equiv 7 \cdot 5^{4-1} \equiv 7 \cdot 5^3 \equiv 7 \cdot 125(\mathrm{mod}\, 8)$$

$$x \equiv 7 \cdot (120 + 5) \equiv 7 \cdot (\underline{8 \cdot 15} + 5) \equiv 7 \cdot (\underline{0} + 5)(\mathrm{mod}\, 8)$$

$$x \equiv 7 \cdot 5 \equiv 35 \equiv 3(\mathrm{mod}\, 8)$$

Note que 3 é o valor procurado , pois $5 \cdot 3 = 15 \equiv 7(\mathrm{mod}\, 8)$.

Em particular, $a \cdot x \equiv 1(\mathrm{mod}\, n)$ implica em $x \equiv a^{\phi(n)-1}(\mathrm{mod}\, n)$ o que nos leva a concluir que $a^{\phi(n)-1}$ é o inverso multiplicativo de a módulo n.

Exemplo 2.14. *Determine um inverso multiplicativo de 7 módulo 11. Aplicando o teorema de Euler e o fato de $mdc(7, 11) = 1$, temos $x \equiv 7^{\phi(11)-1} \equiv 7^{10-1} \equiv 7^9 \equiv 40.353.607 \equiv 8(\mathrm{mod}\, 11)$ assim, $x = 8$ é o menor inverso multiplicativo de 7 módulo 11.*

2.4 Sistemas de Congruências Lineares

No livro "Manual Aritmético do Mestre Sol" escrito por Sun Zi Suanjing (ou Sun Tzu Suan Ching), nos primeiros séculos de nossa era, aparece o seguinte problema:

"Temos coisas, mas não sabemos quantas; se as contarmos de três em três, o resto é 2; se as contarmos de cinco em cinco, o resto é 3; se as contarmos de sete em sete, o resto é 2.

Quantas coisas temos?"

Utilizando congruências para resumir o problema, sendo X a quantidade de coisas procuradas, temos:

$$\begin{cases} X \equiv 2(\mathrm{mod}\, 3) \\ X \equiv 3(\mathrm{mod}\, 5) \\ X \equiv 2(\mathrm{mod}\, 7) \end{cases}$$

Uma maneira de resolução para este sistema será mostrada logo após o seguinte teorema:

Teorema 2.33. ***Teorema Chinês do Resto(TCR)*** *. (Restrito a duas congruências com módulos primos entre si). Sejam m e n inteiros positivos* primos entre si. *Se a e b são inteiros quaisquer, então o sistema*

$$\begin{cases} x \equiv a(\mathrm{mod}\, m) \\ x \equiv b(\mathrm{mod}\, n) \end{cases}$$

sempre tem solução e qualquer uma de suas soluções pode ser escrita na forma $a + m \cdot (m\prime \cdot (b - a) + n \cdot t)$; onde t é um inteiro qualquer e $m\prime$ é o inverso de m módulo n.

Demonstração: Considere o sistema

$$\begin{cases} x \equiv a(\mathrm{mod}\, m) \\ x \equiv b(\mathrm{mod}\, n) \end{cases}$$

onde m e n são inteiros positivos distintos e digamos que o número inteiro x_0 é uma solução desta congruência. Isto significa que x_0 satisfaz a ambas as congruências:

$$\begin{cases} x_0 \equiv a(\mathrm{mod}\, m) \\ x_0 \equiv b(\mathrm{mod}\, n) \end{cases}$$

Como os módulos são diferentes, só podemos combinar as duas congruências se convertermos uma delas em uma igualdade de inteiros.Fazendo isto com a primeira equação, verificamos que

$$x_0 = a + m \cdot k \qquad (i)$$

onde k é um inteiro qualquer, de forma que podemos concluir que

$$a + m \cdot k \equiv b(\mathrm{mod}\, n)$$

ou ainda

$$m \cdot k \equiv (b - a)(\mathrm{mod}\, n) \qquad (ii)$$

Supondo que m e n sejam primos entre si, temos pela Proposição 2.1.2 que m é inversível módulo n . Digamos que $m\prime$ é o inverso de m módulo n ou $m \cdot m' \equiv 1(\mathrm{mod}\, n)$. Multiplicando (ii) por $m\prime$, obtemos

$$k \equiv m' \cdot (b-a)(\mathrm{mod}\, n)$$

em outras palavras,

$$k = m\prime \cdot (b-a) + n \cdot t$$

para algum inteiro t. Substituindo esta expressão para k em (i), vemos que

$$x_0 = a + m \cdot (m\prime \cdot (b-a) + n \cdot t).$$

Resumindo, provamos que x_0 é uma solução do sistema. □

Exemplo 2.15. *Determinar o menor número inteiro que dividido por 3 tem resto 2 e dividido por 7 tem resto 3. Devemos determinar um valor x que satisfaça o sistema de congruências:*

$$\begin{cases} x \equiv 2(\mathrm{mod}\, 3) \\ x \equiv 3(\mathrm{mod}\, 7) \end{cases}$$

Chamando m' o inverso de 3 módulo 7, temos que $m\prime = 5$, visto que $3 \cdot 5 \equiv 15 \equiv 1(\mathrm{mod}\, 7)$.Pela fórmula do TCR, temos que x_0 é uma solução:

$$\begin{aligned} x_0 &= 2 + 3(5(3-2) + 7t) \\ x_0 &= 2 + 15 + 21t \\ x_0 &= 17 + 21t \end{aligned}$$

Logo x=17 é a menor solução positiva para o problema dado.

Embora tenha sido usado uma parte restrita do TCR o procedimento usado para encontrarmos uma fórmula para x pode ser estendido para sistemas com mais de duas congruências.

No momento só nos interessa um caso particular de sistemas, vamos resolvê-los por substituição e utilizando os Teoremas de Fermat e Euler.

Estudaremos apenas sistemas do tipo:

$$\begin{cases} X \equiv a_1(\mathrm{mod}\, b_1) \\ X \equiv a_2(\mathrm{mod}\, b_2) \\ \qquad ... \\ X \equiv a_n(\mathrm{mod}\, b_n) \end{cases}$$

onde $mdc(b_i, b_j) = 1$, com $i = 1, 2, ...n$ e $j = 1, 2, ...n$.

Exemplo 2.16. *Resolveremos o problema proposto no "Manual Aritmético do Mestre Sol"*

$$\begin{cases} X \equiv 2(\mathrm{mod}\,3) \\ X \equiv 3(\mathrm{mod}\,5) \\ X \equiv 2(\mathrm{mod}\,7) \end{cases}$$

pois $mdc(3,5) = 1$, $mdc(3,7) = 1$ *e* $mdc(5,7) = 1$, *temos da primeira equação que existe um inteiro* y *tal que:* $X = 3y + 2$. *Substituindo na segunda congruência, temos:* $3y + 2 \equiv 3(\mathrm{mod}\,5)$, *que implica em* $3y \equiv 1(\mathrm{mod}\,5)$, *donde* $y \equiv 3^{\phi(5)-1} \equiv 3^3 \equiv 27 \equiv 2(\mathrm{mod}\,5)$, *que significa que existe um* K, *inteiro, tal que* $y = 5K + 2$.*Agora temos:* $X = 3(5K + 2) + 2$ *onde* $X = 15K + 8$.*Substituindo na terceira congruência, temos:* $15K + 8 \equiv 2(\mathrm{mod}\,7)$, *que implica em* $15K \equiv -6(\mathrm{mod}\,7)$, *sendo* $K \equiv -6 \equiv 1(\mathrm{mod}\,7)$ *que significa que existe um* U, *inteiro, tal que* $K = 7U + 1$. *Finalmente:* $X = 15(7U + 1) + 8 \Longrightarrow X = 105U + 23$. *Então* $X = 23$ *é a menor solução positiva para este sistema de congruências.*

2.5 Congruência e Criptografia

Podemos usar congruências, de maneira direta, para codificar e decodificar mensagens. Vamos usar como exemplo a Cifra de César, a Cifra de Trithemius e a Cifra de Vigenere.

Para todas elas iniciamos com uma troca de letra por número de acordo com a Tabela 2.4.

Tabela 2.4

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

Fonte: o autor

2.5.1 Cifra de César

Codificação

Sendo i o índice que indica a posição da letra na mensagem, L_i o valor da letra que queremos cifrar e C_i o valor da letra cifrada, temos:

$$C_i \equiv L_i + d(\mathrm{mod}\,26)$$

onde d é o deslocamento utilizado. Usamos mod 26 por ser este o número de letras do alfabeto latino.

A tabela 2.5 mostra como codificar a palavra CODIGO com $d = 15$.

Tabela 2.5

i	mensagem	L_i	L_i+d	$C_i=L_i+d(\text{mod}26)$	cifra
1	C	2	17	17	R
2	O	14	29	3	D
3	D	3	18	18	S
4	I	8	23	23	X
5	G	6	21	21	V
6	O	14	29	3	D

Fonte: o autor

Assim:

CODIGO por está Cifra de César é RDSXVD

Decodificação

Para decodificar, partimos da fórmula inicial $C_i \equiv L_i+d(\text{mod}\,26)$, subtraímos d de ambos os lados da congruência e teremos:

$$L_i = C_i - d(\text{mod}\,26).$$

Assim a decodificação de RDSXVD com $d = 15$, fica:

Tabela 2.6

i	cifra	C_i	C_i-d	$L_i=C_i$-d(mod26)	mensagem
1	R	17	2	2	C
2	D	3	-12	14	O
3	S	18	3	3	D
4	X	23	8	8	I
5	V	21	6	6	G
6	D	3	-12	14	O

Fonte: o autor

Temos, então:

RDSXVD decodificação CODIGO

2.5.2 Cifra de Trithemius

Codificação

Na Cifra de César usamos $C_i \equiv L_i + d (\mathrm{mod}\, 26)$, com d fixo. Na cifra de Trithemius, como visto no Capítulo 1, o deslocamento não é fixo e sim atrelado a posição da letra. Para a primeira letra o deslocamento é zero, para a segunda é um e assim por diante. Como o deslocamento vale uma unidade a menos que a posição, temos $d = i - 1$.A fórmula para a cifragem se torna:

$$C_i \equiv L_i + i - 1 (\mathrm{mod}\, 26)$$

Observe na Tabela 2.7 a codificação da expressão: CEU AZUL

Tabela 2.7

i	mensagem	L_i	L_i+i-1	$C_i=L_i+i-1(\mathrm{mod}26)$	cifra
1	C	2	2	2	C
2	E	4	5	5	F
3	U	20	22	22	W
4	A	0	3	3	D
5	Z	25	29	3	D
6	U	20	25	25	Z
7	L	11	17	17	R

Fonte: o autor

Assim:

CEUAZUL por Trithemius CFWDDZR.

Decodificação

Usando as propriedades das congruências e somando $i-1$ a ambos os termos da expressão temos a fórmula de decodificação:

$$L_i = C_i - i + 1 (\mathrm{mod}\, 26)$$

Caso a mensagem cifrada fosse CFWDDZR, teríamos:

Tabela 2.8

i	cifra	C_i	C_i-i+1	L_i=Ci-i+1(mod26)	mensagem
1	C	2	2	2	C
2	F	5	4	4	E
3	W	22	20	20	U
4	D	3	0	0	A
5	D	3	-1	25	Z
6	Z	25	20	20	U
7	R	17	11	11	L

Fonte: o autor

Assim, temos:

CFWDDZR decodificação CEUAZUL.

2.5.3 Cifra de Vigenère

Codificação

Vamos codificar, usando a Cifra de Vigenère, a palavra LEITURA, tendo como chave a palavra PRIMO. No Capítulo 1 mostramos como fazê-lo usando o Quadrado de Trithemius. As letras do texto codificado são obtidas pelo cruzamento da linha que inicia com a letra da palavra chave, com a coluna que inicia com a letra do texto. Este modelo pode ser entendido como uma Cifra de César com deslocamento variado. Para a Cífra de César temos: $C_i \equiv L_i + d (\mathrm{mod}\, 26)$, com d fixo. Podemos afirmar que o deslocamento de cada letra da mensagem é dado pelo valor associado à letra da palavra chave. Sendo K_i o valor da $i-$ésima letra da chave e L_i o valor da $i-$ésima letra do texto, temos que o valor C_i da letra codificada é dado por:

$$C_i \equiv L_i + K_i (\mathrm{mod}\, 26).$$

Este método requer uma pré-codificação que consiste em substituir as letras, tanto da mensagem como da palavra chave, por seus respectivos valores de acordo com a Tabela 2.4.

A Tabela 2.9 mostra a maneira como devemos dispor as letras da chave com a mensagem

Tabela 2.9

Chave	P	R	I	M	O	P	R
Texto	L	E	I	T	U	R	A

Fonte: o autor

enquanto a Tabela 2.10 mostra as letras já substituídas pelos valores da Tabela 2.4

Tabela 2.10

K_i	15	17	8	12	14	15	17
L_i	11	4	8	19	20	17	0

Fonte: o autor

Neste ponto, utilizamos a Tabela 2.11para codificar a mensagem

Tabela 2.11

i	Texto	L_i	K_i	L_i+K_i	$C_i=L_i+K_i(mod26)$	Cifra
1	L	11	15	26	0	A
2	E	4	17	21	21	V
3	I	8	8	16	16	Q
4	T	19	12	31	5	F
5	U	20	14	34	8	I
6	R	17	15	32	6	G
7	A	0	17	17	17	R

Fonte: o autor

obtendo
LEITURA por Vigenère AVQFIGR.

Decodificação

Neste método a decodificação também necessita de uma fase preparatória da mesmo forma que foi feita na codificação. Agora usamos C_i para $i-$ésima letra cifrada e K_i para a $i-$ésima letra da chave. Na Tabela 2.12, temos a pré decodificação.

Tabela 2.12

Chave	P	R	I	M	O	P	R
Ki	15	17	8	12	14	15	17
Cifra	A	V	Q	F	I	G	R
Ci	0	21	16	5	8	6	17

Fonte: o autor

Para decodificarmos, devemos determinar o valor de L_i a partir de $C_i \equiv L_i + K_i (\mathrm{mod}\, 26)$ que foi a fórmula utilizada para codificar. Se subtrairmos K_i de ambos os membros da congruência temos, como equação de decodificação: $C_i - K_i \equiv L_i (\mathrm{mod}\, 26)$ ou $L_i \equiv C_i - K_i (\mathrm{mod}\, 26)$. Para evitarmos valores negativos para L_i, incrementamos em 26 o segundo termo da congruência. Note que esse incremento não altera em nada a expressão visto que $26 \equiv 0 (\mathrm{mod}\, 26)$. Assim:

$$L_i = 26 + C_i - K_i (\mathrm{mod}\, 26).$$

Na Tabela 2.13, temos a decodificação de AVQFIGR

Tabela 2.13

i	Cifra	Ci	Ki	26+Ci-Ki	Li= 26+Ci-Ki(mod26)	Texto
1	A	0	15	26	11	L
2	V	21	17	30	4	E
3	Q	16	8	34	8	I
4	F	5	12	19	19	T
5	I	8	14	20	20	U
6	G	6	15	17	17	R
7	R	17	17	26	0	A

Fonte: o autor

Dessa forma

AVQFIGR decodificação LEITURA.

O capítulo a seguir mostra como podemos utilizar congruências para aplicar um método mais complexo de cifragem.

Capítulo 3

A Teoria dos Números e a Criptografia RSA

Neste capítulo trataremos, exclusivamente, da criptografia RSA, seu surgimento, a maneira como codificar e decodificar mensagens e um exemplo de cifragem simples utilizando o método, tendo como base[1]

3.1 O método de criptografia RSA

A procura por uma forma de criptografia que consiga sobrepujar a capacidade de cálculo do computador ocupou – e ainda ocupa – o tempo de muitos cientistas, que, mediante isso, anelam pela criação de um sistema criptográfico perfeito.

Antes do surgimento dos computadores propriamente ditos, os alemães, pouco tempo depois da Primeira Guerra Mundial, desenvolveram uma máquina de criptografia que consideravam infalível: a ENIGMA. De fato, ela possuía um sistema de encriptação dificílimo de ser decifrado. Isso fez com que os governos francês, inglês e polonês reunissem esforços para conseguir desvendar o processo semiótico do referido aparelho. Tal feito foi alcançado graças, em parte, ao fato de os aliados terem acesso a algumas máquinas obtidas antes ou no decorrer da guerra. A equipe de cientistas envolvida no projeto de decodificação era chefiada por Alan Turing, na Inglaterra. Na ocasião, esse cientista projetou o que hoje é chamado de "Máquina de Turing", um dispositivo de tal sofisticação que pode ser considerado um precursor dos computadores atuais.

Os computadores trouxeram grande avanço à ciência, à comunicação, ao comércio etc. Porém, embora mais modernos, estavam vulneráveis aos mesmos perigos verificados no uso do telégrafo, ou seja, alguma pessoa mal-

intencionada, com o equipamento certo, poderia interceptar mensagens e, agora, com uma agravante: tinha a seu dispor uma poderosa máquina de calcular com o potencial de decifrar as mensagens criptografadas.

Essa insegurança perdurou até o final do século passado, quando Ronald Rivest, Adi Shamir e Leonard Adleman criaram a RSA, um dos métodos de criptografia mais seguros de todos os tempos, utilizado por governos e empresas do mundo inteiro.

Fazendo uma retrospectiva, é interessante observar que, desde as cítalas, usadas pelos gregos, passando pelos demais sistemas criptográficos surgidos posteriormente, havia, entre todos esses mecanismos, como ponto em comum, uma chave secreta, na qual residiria a segurança na troca de correspondências. Entretanto, nos tempos atuais, com a Internet, processos semióticos dessa natureza seriam inviáveis. Por exemplo, no ato de efetuar uma compra via computador, o usuário teria que receber, da empresa que organiza a página virtual, cartas confidenciais que o orientassem acerca de como codificar os seus dados. Isto tornaria o comércio eletrônico inviável ou muito restrito, pois como confiar na segurança de uma operação mediante a emissão de cartas?

A novidade trazida pelo método RSA é que ele configura um sistema de chave pública, ou seja, opera como uma porta de duas chaves diferentes: a chave A tranca a porta, mas uma chave diferente (B) a destranca. Então, a chave A não precisa ser secreta, e a distribuição de cópias dela não compromete a segurança. Na hipótese de esta porta guardar a entrada da seção segura da página virtual de uma empresa, esta poderia distribuir livremente a chave A para qualquer visitante virtual que quisesse enviar uma mensagem segura, como, por exemplo, o número do cartão de crédito. Embora todos possam codificar seus dados usando a mesma chave, ninguém pode ler as mensagens codificadas dos outros.

A chave A é composta por um par de números (n, e), no qual "n" é o produto de dois números primos muito grandes, e "e" não tem fator comum com "n"; a chave B é um número "d", que aprenderemos a encontrar no decorrer do processo.

A segurança deste método tem suas bases na teoria dos números e é garantida pela dificuldade de fatoração dos números inteiros quando estes são muito grandes. Lembremos que, de acordo com o que se estuda no Ensino Fundamental, fatorar um número é escrevê-lo como um produto de números primos. Por exemplo: $10 = 2 \cdot 5$ e $42 = 2 \cdot 3 \cdot 7$. É claro que fatorar números pequenos é fácil, mas, à medida que eles aumentam, a fatoração vai-se tornando uma tarefa demorada, visto que não há uma fórmula específica para fazê-la diretamente.

O processo manual para fatorar um número "n", dividindo o por números primos até encontrar um divisor, exige uma quantidade de tentativas que en-

volvem os primos "p" de 2 até "$p \leq \sqrt{n}$". Os números utilizados pelo RSA são números com mais de 200 algarismos. Como o processo de fatoração com o uso de computador segue, praticamente, o mesmo princípio do processo manual – tentativas de divisão –, e os números usados são muito grandes, seriam necessários alguns anos de cálculo para o melhor computador do mundo fatorar um desses números, o que torna o esforço de fazê-lo uma tarefa impraticável.

Obviamente, para trabalharmos um exemplo de como criptografar usando o RSA, não poderemos usar um número absurdamente grande. Então, vamos utilizar números que podemos manusear com calculadora de bolso.

3.1.1 Descrição do método RSA

Consideramos, para esta explanação, n, e, p e q números inteiros, sendo p e q primos, $n = p \cdot q$ e $mdc(n, e) = 1$.

Pré-Codificação

As mensagens enviadas, geralmente, são textos e o método trabalha com números. Assim, para podermos utilizá-lo cada letra do alfabeto é colocada em correspondência biunívoca com um número de dois algarismos. Escolhemos um número, também de dois algarismos, diferente dos demais para representar o espaço entre as palavras. Feito isso, a mensagem se transforma em um número. Para tanto, podemos substituir as letras de acordo com a Tabela 3.1.

Tabela 3.1

A	B	C	D	E	F	G	H	I
11	12	13	14	15	16	17	18	19
J	K	L	M	N	O	P	Q	R
20	21	22	23	24	25	26	27	28
S	T	U	V	W	X	Y	Z	[ ]
29	30	31	32	33	34	35	36	55

Fonte: o autor

Esse processo é chamado de pré-codificação.

Fazemos cada letra corresponder a um número de, pelo menos, dois algarismos para evitarmos confusões. Veja que, se fizéssemos A corresponder ao número 1, B ao 2, e assim por diante, não teríamos como saber se 12 representa AB ou L, já que esta última é a décima segunda letra do alfabeto.

Codificação

Feita a pré-codificação, obtemos uma sequência de números. Separamos este número em uma sequência em blocos menores, de forma que o número formado por cada bloco seja menor que n. Denotamos esses blocos por b_i, onde $i = 1; 2; ...; k$.

O bloco codificado, que chamaremos de $C(b_i)$, é o resto da divisão b_i^e por n, ou $C(b_i)$ é a menor solução positiva da congruência:

$$b_i^e \equiv C(b_i) (\mathrm{mod}\, n) \qquad \text{(i)}$$

Doravante chamaremos os blocos codificados de x_i, ou seja $x_i = C(b_i)$ para $i = 1; 2; ...; k$.

Decodificação

Para decodificar a mensagem precisamos encontrar uma relação, ora chamada $D(x_i)$, tal que $D(x_i) \equiv b_i (\mathrm{mod}\, n)$. Para tanto, recordemos alguns conceitos já estudados.

Sendo b_i um inteiro , relativamente primo com n, o Teorema de Euler nos diz que:

$$b_i^{\phi(n)} \equiv 1 (\mathrm{mod}\, n) \qquad \text{(ii)}$$

Como p e q são primos. Segue, das propriedades da função Totiente de Euler, que:

$$\phi(p) = p - 1 \text{ e } \phi(q) = q - 1$$

e, ainda

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

Para decifrar a mensagem é necessário encontrar um inteiro d tal que:

$$e \cdot d \equiv 1 (\mathrm{mod}\, \phi(n)) \quad \text{(iii)}$$

o que implica em

$$e \cdot d \equiv 1 (\mathrm{mod}(p - 1)(q - 1)) \quad \text{(iv)}$$

que, pelo teorema de Euler, tem como resultado

$$d \equiv e^{\phi((p-1)(q-1))-1} (\mathrm{mod}(p - 1)(q - 1)).$$

Assim, de $e \cdot d \equiv 1 (\mathrm{mod}\, \phi(n))$ concluímos que existe um inteiro t tal que $e \cdot d \equiv t \cdot \phi(n) + 1$ de onde segue que:

$$b_i \equiv b_i \cdot 1 \equiv b_i(1)^t \equiv b_i(b_i^{\phi(n)})^t \equiv b_i^{t \cdot \phi(n)+1} (\mathrm{mod}\, n)$$

e

$$b_i^{t\cdot\phi(n)+1} \equiv b_i^{ed} \equiv (b_i^e)^d \equiv (C(b_i))^d \equiv (C(b_i))^d \equiv x_i^d (\mathrm{mod}\, n).$$

Portanto

$$D(x_i) \equiv x_i^d (\mathrm{mod}\, n)$$

Observe que $D(x_i)$ é a relação inversa de $C(b_i)$.

3.1.2 Um exemplo de mensagem criptografada de acordo com o método RSA

Vamos codificar e decodificar a mensagem SAIA JÁ de acordo com o RSA. Usaremos como chave pública o par $(n; e) = (253; 3)$.

Pré Codificação

Como dito anteriormente as mensagens, geralmente, são textos devemos, então, achar uma maneira de converter a mensagem em uma sequência de números.

Faremos isso, desconsiderando o acento agudo, de acordo com a Tabela 3.1, segundo a qual:

SAIA JÁ

torna-se

29111911552011.

Agora quebramos o grande bloco, formado inicialmente, em blocos menores que n. Para escolher os blocos em que vamos dividir a mensagem devemos tomar alguns cuidados. Como já foi dito: nenhum bloco deve ser maior que n e, também, não devemos iniciar um bloco com zero. A explicação para essa condição será dada após a codificação e decodificação da mensagem na qual estamos trabalhando. A mensagem atual pode ser quebrada assim:

$$29 - 111 - 91 - 155 - 201 - 1.$$

Encerrada a fase de pré-codificação podemos passar à etapa de codificação propriamente dita.

Codificação A partir dos blocos

Tabela 3.2

b_1	b_2	b_3	b_4	b_5	b_6
29	111	91	155	201	1

Fonte: o autor

vamos denotar o bloco codificado por $C(b_i)$.

Como $e = 3$ a receita que vamos utilizar para calcular $C(b_i)$ é a seguinte:

$$C(b_i) = \text{resto da divisão de } b_i^3 \text{ por } 253$$

ou

$$C(b_i) \equiv b_i^3 (\text{mod}\, 253).$$

Assim, o bloco 29 da mensagem anterior deve ser codificado como o resto da divisão de 29^3 por 253.

Fazendo as contas, temos:

$C(b_1) \equiv 29^3 \equiv 24389 \equiv 101 (\text{mod}\, 253) \Longrightarrow C(29) = 101$

$C(b_2) \equiv 111^3 \equiv 1367631 \equiv 166 (\text{mod}\, 253) \Longrightarrow C(111) = 166$

$C(b_3) \equiv 91^3 \equiv 753571 \equiv 137 (\text{mod}\, 253) \Longrightarrow C(91) = 137$

$C(b_4) \equiv 155^3 \equiv 3723875 \equiv 221 (\text{mod}\, 253) \Longrightarrow C(155) = 221$

$C(b_5) \equiv 201^3 \equiv 8120601 \equiv 60 (\text{mod}\, 253) \Longrightarrow C(201) = 60$

$C(b_6) \equiv 1^3 \equiv 1 \equiv 1 (\text{mod}\, 253) \Longrightarrow C(1) = 1$

Reunindo os blocos temos a seguinte mensagem codificada:

$$101 - 166 - 137 - 221 - 60 - 1$$

e os blocos codificados conforme a Tabela 3.3.

Tabela 3.3

x_1	x_2	x_3	x_4	x_5	x_6
101	166	137	221	60	1

Fonte: o autor

onde $x_i = C(b_i)$.

Uma observação importante a ser feita é que não podemos agrupar novamente os números formando um só bloco, pois a decodificação da mensagem está vinculada a cada resto, se eles forem agrupados haveria confusão. Por exemplo três blocos que originalmente seriam $12 - 32 - 25$, agrupados, formariam o número 123225 que poderia ser interpretado pelos blocos $132 - 225$ que também são restos possíveis para $n = 253$.

Decodificação Agora vamos decodificar um bloco da mensagem codificada. Veremos de que forma, possuindo a mensagem codificada e a chave secreta, podemos reconstruir a mensagem original.

A informação necessária para decodificar consiste de dois números: n e o inverso $d > 0$ de 3 módulo $(p-1)(q-1)$, onde q e p são os únicos fatores primos de n. Neste caso: $p = 11$ e $q = 23$, visto que $11 \cdot 23 = 253$.

Isto significa que devemos ter;

$$\begin{aligned} &3 \cdot d \equiv 1(\mathrm{mod}(p-1)(q-1)) \\ &3 \cdot d \equiv 1(\mathrm{mod}(11-1) \cdot (23-1)) \\ &3 \cdot d \equiv 1(\mathrm{mod}\, 220) \end{aligned}$$

aplicando o resultado

$$d \equiv e^{\phi((p-1)(q-1))-1}(\mathrm{mod}(p-1)(q-1))$$

temos

$$d \equiv 3^{\phi(220)-1}(\mathrm{mod}\, 220).$$

Como $\phi(220) = \phi(10) \cdot \phi(22) = 4 \cdot 10 = 40$, segue que.

$$d \equiv 3^{40-1} \equiv 3^{39} \equiv 147(\mathrm{mod}\, 220)$$

Temos, então, que $d = 147$ é o menor inteiro positivo que é solução da congruência dada.

Chamaremos o par $(n; d)$ de chave de decodificação. O segredo para a decodificação da mensagem se encontra nestes dois números, portanto, apenas quem tem a função de receber a mensagem deve possuí-los.

De posse do par $(n; d)$, calculamos $D(x_i)$, onde:

$$D(x_i) = \text{resto da divisão de } x_i^d \text{por } n$$

em cada bloco para retornarmos ao bloco original.

Aplicando esta fórmula no primeiro bloco da mensagem codificada, temos que $\mathbf{D}(\mathbf{x}_1) = \mathbf{D}(\mathbf{101})$ é igual ao resto da divisão de 101^{147} por $n = 253$. Efetuamos este cálculo com a ajuda dos Teorema de Fermat e da resolução de sistemas de congruências.

Calculamos 101^{147} módulo 11 e 101^{147} módulo 23 que são os primos em que n se fatora. Inicialmente, temos:

$$\begin{aligned} &101 \equiv 2(\mathrm{mod}\, 11) \quad (i) \\ &101 \equiv 9(\mathrm{mod}\, 23) \quad (ii). \end{aligned}$$

De (i), temos:

$$101^{147} \equiv 2^{147}(\mathrm{mod}\, 11).$$

Pelo teorema de Fermat

$$2^{10} \equiv 1 (\mathrm{mod}\, 11).$$

Como

$$147 = 10 \cdot 14 + 7$$

segue que

$$101^{147} \equiv 2^{10 \cdot 14 + 7} \equiv (2^{10})^{14} \cdot 2^7 \equiv 1^{14} \cdot 2^7 \equiv 2^7 \equiv 7 (\mathrm{mod}\, 11) \quad (1)$$

Da equação (ii), resulta

$$101^{147} \equiv 9^{147} (\mathrm{mod}\, 23)$$

ou, sendo $9^{147} = 3^{294}$,

$$101^{147} \equiv 3^{294} (\mathrm{mod}\, 23).$$

Pelo teorema de Fermat

$$3^{22} \equiv 1 (\mathrm{mod}\, 23).$$

Como

$$294 = 22 \cdot 13 + 8$$

segue que

$$101^{147} \equiv 3^{22 \cdot 13 + 8} \equiv (3^{22})^{13} \cdot 3^8 \equiv 1^{13} \cdot 3^8 \equiv 3^8 \equiv 6 (\mathrm{mod}\, 23) \quad (2)$$

Chamando 101^{147} de X, temos, por(1) e (2):

$$X \equiv 7 (\mathrm{mod}\, 11)$$
$$X \equiv 6 (\mathrm{mod}\, 23).$$

Resolvemos este sistema de equações utilizando o algoritmo Chinês dos Restos, da primeira equação temos que, existe $Y \in \mathbb{Z}$, tal que:

$$X = 11Y + 7.$$

Substituindo X na segunda equação, temos:

$$11Y + 7 \equiv 6 (\mathrm{mod}\, 23) \text{ que resulta em } Y \equiv 2 (\mathrm{mod}\, 23).$$

Logo, existe $K \in \mathbb{Z}$, tal que:

$$Y = 23K + 2.$$

Voltamos à primeira equação e substituímos o valor de Y

$$X = 11(23K + 2) + 7 \Longrightarrow X = 253K + 29$$

onde 29 é a menor solução positiva para o sistema e também o bloco inicial procurado.

Procedendo da mesma maneira podemos decifrar os blocos restantes, reagrupá-los novamente e assim obter a mensagem inicial.

$\mathbf{D}(\mathbf{x}_2) = \mathbf{D}(\mathbf{166})$

Calculamos 166^{147} módulo 11 e 166^{147} módulo 23 que são os primos em que n se fatora. Inicialmente, temos:

$$\begin{array}{l} 166 \equiv 1(\mathrm{mod}\, 11) \quad (i) \\ 166 \equiv 5(\mathrm{mod}\, 23) \quad (ii). \end{array}$$

De (i), temos:

$$166^{147} \equiv 1^{147} \equiv 1(\mathrm{mod}\, 11) \qquad (1)$$

Da equação (ii):

$$166^{147} \equiv 5^{147}(\mathrm{mod}\, 23).$$

Pelo teorema de Fermat

$$5^{22} \equiv 1(\mathrm{mod}\, 23)$$

Como

$$147 = 22 \cdot 6 + 15$$

segue que

$$166^{147} \equiv 5^{22\cdot 6+15} \equiv (5^{22})^6 \cdot 5^{15} \equiv 5^8 \cdot 5^7 \equiv 16 \cdot 17 \equiv 19(\mathrm{mod}\, 23) \quad (2)$$

Chamando 166^{147} de X, temos, por(1) e (2):

$$\begin{array}{l} X \equiv 1(\mathrm{mod}\, 11) \\ X \equiv 19(\mathrm{mod}\, 23) \end{array}$$

Resolvemos este sistema de equações utilizando o algoritmo Chinês dos Restos: Da primeira equação temos que, existe $Y \in \mathbb{Z}$, tal que:

$$X = 11Y + 1$$

substituindo X na segunda equação, temos:

$$11Y + 1 \equiv 19(\mathrm{mod}\, 23) \text{ que resulta em } Y \equiv 10(\mathrm{mod}\, 23)$$

logo, existe $K \in \mathbb{Z}$, tal que:

$$Y = 23K + 10$$

voltamos à primeira equação e substituímos o valor de Y

$$X = 11(23K + 10) + 1 \Longrightarrow X = 253K + 111$$

onde 111 é a menor solução positiva para o sistema e também o bloco inicial procurado.

$\mathbf{D(x_3) = D(137)}$

Calculamos 137^{147} módulo 11 e 137^{147} módulo 23 que são os primos em que n se fatora. Inicialmente, temos:

$$\begin{array}{l} 137 \equiv 5 (\mathrm{mod}\, 11) \quad (i) \\ 137 \equiv -1 (\mathrm{mod}\, 23) \quad (ii). \end{array}$$

De (i), temos:

$$137^{147} \equiv 5^{147} (\mathrm{mod}\, 11).$$

Pelo teorema de Fermat

$$5^{10} \equiv 1 (\mathrm{mod}\, 11).$$

Como

$$147 = 10 \cdot 14 + 7$$

segue que

$$137^{147} \equiv 5^{10 \cdot 14 + 7} \equiv (5^{10})^{14} \cdot 5^7 \equiv 1^{14} \cdot 5^7 \equiv 5^7 \equiv 3 (\mathrm{mod}\, 11) \ (1)$$

Da equação (ii):

$$137^{147} \equiv -1^{147} (\mathrm{mod}\, 23)$$

segue que

$$137^{147} \equiv -1 (\mathrm{mod}\, 23) \quad (2)$$

Disto, chamando 137^{147} de X, temos, por(1) e (2):

$$\begin{array}{l} X \equiv 3 (\mathrm{mod}\, 11) \\ X \equiv -1 (\mathrm{mod}\, 23) \end{array}$$

Resolvemos este sistema de equações utilizando o algoritmo Chinês dos Restos: Da primeira equação temos que, existe $Y \in \mathbb{Z}$, tal que:

$$X = 11Y + 3.$$

Substituindo X na segunda equação, temos:

$$11Y + 7 \equiv -1 (\mathrm{mod}\, 23) \text{ que resulta em } Y \equiv 8 (\mathrm{mod}\, 23)$$

Logo, existe $K \in \mathbb{Z}$, tal que:

$$Y = 23K + 8$$

voltamos à primeira equação e substituímos o valor de Y

$$X = 11(23K + 8) + 3 \Longrightarrow X = 253K + 91$$

onde 91 é a menor solução positiva para o sistema e também o bloco inicial procurado.

$\mathbf{D}(\mathbf{x}_4) = \mathbf{D}(\mathbf{221})$

Calculamos 221^{147} módulo 11 e 221^{147} módulo 23 que são os primos em que n se fatora. Inicialmente, temos:

$$\begin{array}{ll} 221 \equiv 1 (\mathrm{mod}\, 11) & (i) \\ 221 \equiv 14 (\mathrm{mod}\, 23) & (ii) \end{array}$$

De (i), temos:

$$221^{147} \equiv 1^{147} \equiv 1 (\mathrm{mod}\, 11) \qquad (1)$$

Da equação (ii):

$$221^{147} \equiv 14^{147} (\mathrm{mod}\, 23)$$

ou, sendo $14 \equiv -9 (\mathrm{mod}\, 23)$ e $-9^{147} = -3^{294}$

$$221^{147} \equiv -3^{294} (\mathrm{mod}\, 23).$$

Pelo teorema de Fermat

$$3^{22} \equiv 1 (\mathrm{mod}\, 23).$$

Como

$$294 = 22 \cdot 13 + 8$$

segue que

$$221^{147} \equiv -3^{22 \cdot 13 + 8} \equiv -(3^{22 \cdot 13} \cdot 3^8) - (1^{13} \cdot 3^8) \equiv -3^8 \equiv -6 (\mathrm{mod}\, 23) \quad (2)$$

Disto, chamando 221^{147} de X, temos, por(1) e (2):

$$X \equiv 1(\mathrm{mod}\, 11)$$
$$X \equiv -6(\mathrm{mod}\, 23)$$

Resolvemos este sistema de equações utilizando o algoritmo Chinês dos Restos: Da primeira equação temos que, existe $Y \in \mathbb{Z}$, tal que:

$$X = 11Y + 1.$$

Substituindo X na segunda equação, temos:

$$11Y + 1 \equiv -6(\mathrm{mod}\, 23) \text{ que resulta em } Y \equiv 14(\mathrm{mod}\, 23).$$

Logo, existe $K \in \mathbb{Z}$, tal que:

$$Y = 23K + 14$$

voltamos à primeira equação e substituímos o valor de Y

$$X = 11(23K + 14) + 1 \Longrightarrow X = 253K + 155$$

onde 155 é a menor solução positiva para o sistema e também o bloco inicial procurado.

$\mathbf{D}(\mathbf{x}_5) = \mathbf{D}(\mathbf{60})$

Calculamos 60^{147} módulo 11 e 60^{147} módulo 23 que são os primos em que n se fatora. Inicialmente, temos:

$$60 \equiv 5(\mathrm{mod}\, 11) \quad (i)$$
$$60 \equiv 14(\mathrm{mod}\, 23) \quad (ii).$$

De (i), temos:

$$60^{147} \equiv 5^{147}(\mathrm{mod}\, 11).$$

Pelo teorema de Fermat

$$5^{10} \equiv 1(\mathrm{mod}\, 11).$$

Como

$$147 = 10 \cdot 14 + 7$$

segue que

$$60^{147} \equiv 5^{10 \cdot 14 + 7} \equiv (5^{10})^{14} \cdot 5^7 \equiv 1^{14} \cdot 5^7 \equiv 5^7 \equiv 3(\mathrm{mod}\, 11) \ (1)$$

Da equação (ii), resulta:

$$60^{147} \equiv 14^{147} (\mathrm{mod}\, 23)$$

sendo $14 \equiv -9 (\mathrm{mod}\, 23)$ e $-9^{147} = -3^{294}$

$$60^{147} \equiv -3^{294} (\mathrm{mod}\, 23).$$

Pelo teorema de Fermat

$$3^{22} \equiv 1 (\mathrm{mod}\, 23).$$

Como

$$294 = 22 \cdot 13 + 8$$

segue que

$$60^{147} \equiv -3^{22 \cdot 13 + 8} \equiv -(1^{13} \cdot 3^8) \equiv -3^8 \equiv -6 (\mathrm{mod}\, 23) \quad (2)$$

Disto, chamando 101^{147} de X, temos, por(1) e (2):

$$X \equiv 3 (\mathrm{mod}\, 11)$$
$$X \equiv -6 (\mathrm{mod}\, 23)$$

Resolvemos este sistema de equações utilizando o algoritmo Chinês dos Restos: Da primeira equação temos que, existe $Y \in \mathbb{Z}$, tal que:

$$X = 11Y + 3.$$

Substituindo X na segunda equação, temos:

$$11Y + 3 \equiv -6 (\mathrm{mod}\, 23) \text{ que resulta em } Y \equiv 18 (\mathrm{mod}\, 23)$$

Logo, existe $K \in \mathbb{Z}$, tal que:

$$Y = 23K + 18$$

voltamos à primeira equação e substituímos o valor de Y

$$X = 11(23K + 18) + 3 \Longrightarrow X = 253K + 201$$

onde 201 é a menor solução positiva para o sistema e também o bloco inicial procurado.

$\mathbf{D}(\mathbf{x}_6) = \mathbf{D}(\mathbf{1})$
Calculamos:

$$1^{147} = 1 \equiv 1 (\mathrm{mod}\, 253)$$

onde 1 é a menor solução positiva para o sistema e também o bloco inicial procurado.

A Tabela 3.4 resume os resultados da decodificação

Tabela 3.4

$D(x_1)$	$D(x_2)$	$D(x_3)$	$D(x_4)$	$D(x_5)$	$D(x_6)$
29	111	91	155	201	1

Fonte: o autor

Agrupando os blocos, formamos novamente o número 29111911552011, que, de acordo com a convenção da Tabela 3.1, significa SAIA JÁ.

Afirmamos, antes de codificarmos a mensagem, que um bloco não poderia iniciar com zero, vamos ver o porquê.

Supondo que "...MAU USO..."seja parte de uma mensagem, codificada segundo as normas da Tabela 3.5.

Tabela 3.5

A	B	C	D	E	F	G	H	I
10	11	12	13	14	15	16	17	18
J	K	L	M	N	O	P	Q	R
19	20	21	22	23	24	25	26	27
S	T	U	V	W	X	Y	Z	[ ]
28	29	30	31	32	33	34	35	55

Fonte: o autor

A pré-codificação seria:

$$...221030553028245...$$

sendo $n = 2173$, pode ser separada nos seguintes blocos:

$$... - 221 - 030 - 553 - 028 - 245 - ...$$

codificada com $e = 3$,

$$... - 567 - 924 - 825 - 222 - 1434 - ...$$

ao ser decodificada, ficaria

$$... - 221 - 30 - 553 - 28 - 245 - ...$$

quando agrupamos novamente, temos:

...2213055328245...

que, convertido em texto se torna

MD? W?O...

que, é claro, não corresponde à mensagem original.

Assim encerramos nosso capítulo sobre RSA.

Capítulo 4

Sugestão de Atividade

Os métodos de criptografia apresentados neste trabalho possibilitam uma série de aplicações em aulas de matemática.

A Cifra de César, ou qualquer outro método de substituição monoalfabética, pode ser usada como base para estudo de análise de frequência com uso de gráficos em Estatística, bem como em exercícios de probabilidade.

A criptografia por transposição, como o próprio nome sugere, pode ser trabalhado como modelo no estudo de transposição de matrizes.

A criptografia RSA, pela filosofia utilizada, fornece um bom exemplo de aplicação de relação inversa.

Este capítulo apresenta uma sugestão de atividade, apresentado aqui como Plano de Aula, a ser desenvolvida no estudo de funções, particularmente, no estudo de função inversa. Sugerimos, num primeiro momento, a revisão do conceito de função inversa., e também das condições necessárias para que uma função possa ser inversivel.

O Plano de Aula aqui apresentado segue um roteiro semelhante ao método de criptografia RSA, apresentado no Capítulo 3 deste trabalho.

Num primeiro momento, criamos uma tabela, Tabela 4.1, de conversão onde damos valores numéricos às letras do alfabeto e ao espaço entre palavras. Utilizamos essa tabela para uma transformação da mensagem escrita em uma mensagem numérica. A maneira de realizar essa etapa é semelhante à pré codificação feita em RSA, com a diferença que devemos separar cada número com um espaço. Na prática a pré codificação já é uma forma simples de cifragem.

Realizada a primeira etapa, escolhemos uma função para codificar a mensagem. No RSA utilizamos congruência para realizar o processo. Como congruência não é tópico de estudo do Ensino Médio, devemos utilizar funções conhecidas dos estudantes. Sugerimos funções de primeiro grau pela facilidade do manuseio. A codificação é feita calculando a imagem da função em

cada valor da mensagem. Podemos fazer isso com o auxílio de uma tabela, Tabela 4.2.

Para decodificar, encontramos a função inversa da função usada para codificar e calculamos o valor da mesma em cada valor da cifra (Tabela 4.3). A sequência dos valores da imagem relativos aos valores do código deve ser a sequência numérica da mensagem original. Isto feito trocamos os números pelas letras correspondentes da Tabela 4.1.

4.1 Plano de Aula

Dados de Identificação:

Escola:
Professor:
Disciplina: Matemática
Série: 1° Ano do Ensino Médio
Turma:
Período:

Tema:

Criptografia e uso de Relação Inversa

Objetivo geral:

Aplicar o conceito de função inversa.

Objetivos específicos:

- Calcular o valor de uma função em um ponto dado;
- Definir a função inversa de uma função dada;
- Utilizar uma função e sua inversa como recurso para troca de mensagens criptografadas.

Conteúdo:

- Função inversa;
- Criptografia.

Desenvolvimento do tema:Criptografia e uso da função inversa

A arte de usar símbolos diferenciados para representar mensagens é quase tão antiga quanto a própria escrita. Atualmente, esse procedimento recebe o nome de criptografia, termo cuja origem vem do grego kryptós (escondido) e gráphein (escrita). De modo geral, essa técnica pode ser entendida como o ato de aplicar um determinado código a fim de manter secreto o conteúdo de certas informações.

O processo de codificar e decifrar uma mensagem pode ser entendido como uma transformação. E é justamente a palavra transformação, de um ponto de vista intuitivo, que caracteriza o estudo das funções.

Do ponto de vista matemático, veremos a aplicação de uma função – para cifrar uma mensagem – e sua inversa – para decifrar a mensagem cifrada. Para tanto é necessário que a função escolhida, seja uma função bijetora, uma vez que somente estas possibilitam a construção de funções inversas.

Utilizando números e deslocamento podemos criar uma maneira própria de codificação e decodificação de mensagens.

Inicialmente faremos algo chamado pré-codificação, que consiste em associar a cada letra do alfabeto um número, de preferência de dois algarismos, como mostra a Tabela 4.1.

Tabela 4.1

A	B	C	D	E	F	G	H	I
11	12	13	14	15	16	17	18	19
J	K	L	M	N	O	P	Q	R
20	21	22	23	24	25	26	27	28
S	T	U	V	W	X	Y	Z	[ ]
29	30	31	32	33	34	35	36	55

Fonte: o autor

Por exemplo: Pré codificamos o texto

O LAPIS

que fica

25 55 22 11 26 19 29

A partir desta tabela criamos uma relação de substituição que associe a cada número x, da palavra pré-codificada um outro número y, por exemplo

$$y = 2x - 3,$$

esta relação é a chave de codificação pois com ela codificamos a mensagem.

Com essa chave a mensagem O LAPIS é codificada da seguinte forma:

Tabela 4.2

Letra	valor(x)	cifragem(2x-3)	cifra(y)
O	25	$2 \cdot 25 - 3$	47
[ ]	55	$2 \cdot 55 - 3$	107
L	22	$2 \cdot 22 - 3$	41
A	11	$2 \cdot 11 - 3$	19
P	26	$2 \cdot 26 - 3$	49
I	19	$2 \cdot 19 - 3$	35
S	29	$2 \cdot 29 - 3$	55

agora

O LAPIS

se escreve como

47 107 41 19 49 35 55.

Conhecendo a maneira de cifrar podemos então decifrar ou retornar as letras para a posição original. Para isso usamos uma relação inversa à usada inicialmente, ou seja, trocamos x e y de posição, assim teremos

$$x = 2y - 3.$$

Agora o x passa a ser o valor da cifra e o y o valor da letra. Isolando o y teremos o cálculo que decifra que é

$$y = \frac{(x+3)}{2}$$

e é chamado de chave de decodificação.

Tabela 4.3

cifra(x)	decodificação($\frac{(x+3)}{2}$)	valor(y)	Letra
47	$(47+3) \div 2$	25	O
107	$(107+3) \div 2$	55	[ ]
41	$(41+3) \div 2$	22	L
19	$(19+3) \div 2$	11	A
49	$(49+3) \div 2$	26	P
35	$(35+3) \div 2$	19	I
55	$(55+3) \div 2$	29	S

Exercícios

1) Considerando que cada uma das sentenças a seguir é a lei de associação de uma função bijetora, obtenha a lei de associação da inversa de cada função.

a) $y = 3x - 5$

b) $y = \frac{3x-2}{4}$

c) $y = \frac{3x-2}{x+1}$

2)Combine com um colega uma mensagem a ser codificada, a expressão de codificação e, a partir dela, determinem a chave de decodificação.

3)Interceptem, de maneira pacífica, a mensagem de outra dupla e vejam se é fácil decodificar.

4)Faça alguma observação sobre esse tipo de cifragem.

Recursos didáticos:

- Quadro;
- Giz;
- Projetor Multimídia.

Avaliação:

A avaliação será feita mediante relatório de aula, participação nas atividades e apresentação da resolução dos exercícios.

Conclusão

No desenvolvimento deste estudo tivemos a certeza de que os códigos secretos tem prazo de validade, pois sua criação sempre dá origem a uma força contrária que visa quebrá-los.

Geralmente essa força é formada por cientistas a serviço de países que estão, de alguma forma, sendo "atacados"pela complexidade do código. Essa batalha mental entre criptoanalistas, como são chamados os cientistas que estudam as diferentes formas de criptografia, faz com que os métodos devam ser melhorados a cada instante.

Infelizmente, ou felizmente, a criptologia é uma ciência que desconhece a paz, visto que não há como garantir por quanto tempo um método criptográfico será seguro, pois são constantemente atacados, mesmo em tempos de paz. Governos buscam vigiar pessoas, empresas e também nações por motivo de segurança e o ataque pode vir de onde menos se espera, prova disso é o recente escândalo da espionagem dos Estados Unidos sobre as nações amigas.

No texto, citamos que o RSA é um modelo de criptografia usado para manter a segurança das pessoas que realizam transações comerciais pela internet e falamos também sobre sua segurança. Convém ressaltar, porém que, embora o método seja seguro, só a criptografia dos dados não garante que uma pessoa não possa ter seus dados expostos na rede, não por falha na cifragem dos mesmos e sim por descuido próprio. Atualmente não há necessidade de se subir em postes, com aparelhos de escuta, para interceptar uma mensagem e interceptá-la criptografada também não é um bom negócio para a espionagem. Hoje os ataques são mais sutis, os usuários de internet são atacados em suas próprias casas, mais especificamente em seus computadores, por programas que roubam senhas, embutidos em mensagens, enviadas por e-mails chamativos, que fazem com que suas senhas sejam lidas antes mesmo de serem criptografadas. Podemos analisar a criptografia como uma chave para a segurança de nossos dados pessoais, mas não adianta termos a chave se deixamos a porta aberta.

Convém ressaltar que o método RSA tem uma importância significativa para a matemática, pois deu uma nova dimensão à Teoria dos Números, que possuía, antes dele , pouca aplicação prática, mostrando que em matemática, em alguns casos, podemos ter a solução antes mesmo do problema.

Embora apresente uma série de possibilidades, a criptografia é pouco explorada em atividades escolares, geralmente aparece como desafios. Isso é justificável pela sua natureza instigadora que desperta a curiosidade do aluno. Então por que não explorá-la mais?

Mostramos neste trabalho que isto é possível, sem que seja necessário o uso de cálculos mirabolantes que desestimulam nosso educando. O exemplo sugerido pode ser aplicado sem que seja necessário abrir um espaço no currículo só para tratar de criptografia, podemos utilizá-la no estudo de funções, como sugerido, além de matrizes, probabilidade, estatística, propriedade das potências entre outros.

Devido ao tempo em que foi elaborado, férias escolares, não temos resultado de aplicação em sala de aula. Distribuímos e discutimos as questões com alguns professores que se mostraram otimistas em relação aos resultados que podem ser obtidos, tais como: um interesse maior pela disciplina e esclarecimentos sobre a aplicação da mesma

Como a criptografia está atrelada à tecnologia e é cada vez maior o número de estudantes que tem acesso a ela, boa parte de nossos alunos já possuem, celulares, smartphones ou tablets, é justificável que devam também ter acesso ao modo como suas mensagens são protegidas.

Referências Bibliográficas

[1] Coutinho, S. C., **Números Inteiros e Criptografia RSA**, Série de Computação e Matemática, IMPA, Segunda Edição, 2003.

[2] Fabossi, Tomas Edson Barros, **Números Inteiros e Criptografia RSA**.Disponível em: http://www.dm.ufscar.br/dm/attachments/article/5/359335_B.pdf. Acesso em:07/12/2013

[3] Fonseca, Rubens Vilhena: **Teoria dos Números** - Disponível em: http://pt.scribd.com/doc/71606082/Introducao-a-Teoria-dos-Numeros-UEPA. Acesso: 05/12/2013.

[4] Hefez, Abramo, **Elementos de Aritmética**, 2.ed. Rio de Janeiro: SBM, 2011.

[5] Sautoy, Marcus Du, **A música dos números primos: a história de um problema não resolvido da matemática**; tradução, Diego Alfaro. Rio de Janeiro: Zahar, 2007.

[6] Silva, Elen Viviani Pereira da, **Introdução à Criptografia RSA**. Disponível em: http://www.impa.br/opencms/pt/eventos/downloads/jornadas_2006/trabalhos/. Acesso em:07/12/2013

[7] Tkotz, Viktoria. **Iintroduçao à criptografia numaboa**.Disponível em http://www.numaboa.com.br/criptografia/gerais/153-introducao, acessado em 20/11/2013

[8] WIKIPÉDIA. **Wikipedia, the free encyclopedia**. Wikimedia Foundation, Inc. Disponível em: http://es.wikipedia.org/. Acesso: dez. 2013.

[9] Paiva, Manoel Rodrigues.**Matemática: Paiva**/ Manoel Rodrigues Paiva - 2. ed.- São Paulo: Moderna, 2010.