UFPR – UNIVERSIDADE FEDERAL DO PARANÁ
DEPARTAMENTO DE MATEMÁTICA
PET – PROGRAMA DE EDUCAÇÃO TUTORIAL

Tutor:	Prof. Alexandre Kirilov
Estudantes:	André Ferrando Arthur Rezende Alves Neto Bruno de Lessa Victor Carlos Henrique Venturi Ronchi Diogo Ubaldino Jaqueline Aline Iensen Jean Carlo Baena Vicente Lucas Lamy Luciano Luzzi Junior Nilmara de Jesus Biscaia Pinto Rodrigo Zeni Stocco Wagner Augusto Almeida de Moraes Wesley dos Santos Villela Batista
Site:	www.petmatematica.ufpr.br facebook.com/petmatematicaufpr
Telefone:	(41) 3361-3672
Data do Curso:	07 a 10 de Julho de 2014
Horários:	das 8h30 às 12h00 (turma da manhã) das 13h30 às 17h00 (turma da tarde)
Local de Realização:	PC - Bloco de Exatas, Centro Politécnico - UFPR

Curitiba, 2014.

Sumário

Capítulo 1

Criptografia

1.1 Um pouco de História

A criptografia é geralmente descrita como a arte e a ciência de criar códigos secretos. Criada a partir da necessidade de buscar sigilo no envio e recebimento de informações, algo que é muito antigo, na Roma antiga o imperador César a usava para enviar mensagens codificadas que apenas seus generais conseguiam ler, mais recentemente, durante a segunda guerra mundial, o exército alemão possuia artefatos mecânicos bastante sofisticados projetados para codificar as mensagens enviadas.

O termo criptografia deriva da fusão das palavras gregas *kryptós* (oculto) e *egráphein* (escrever) e atualmente existe uma área de pesquisa em matemática dedicada o estudo de técnicas e algoritmos que garantam a confidencialidade da informação e a integridade dos dados transmitidos.

Acredita-se que as primeiras informações criptografadas tenham sido registradas por escribas do faraó Khnumhotep II, por volta de 1900 a.C, no antigo Egito, que resolveu trocar trechos das escritas em argila que indicavam os caminhos para os tesouros guardados nas pirâmides, de forma que só os sacerdotes poderiam decifrá-los.

A criptografia também proliferou na Mesopotamia, onde os "integlios" (peças de pedra com símbolos de identificação) funcionavam como certificados rudimentares. Os hebreus, por volta de 600 a 500 a.C, valiam-se das cifras ATBASH, ALBAM ATBAH, que consistiam da substituição simples de uma letra por outra (substituição monoalfabétia). O ATBASH foi utilizado para escrever o "Livro do Profeta Jeremias" e correspondia a trocar a primeira letra (Aleph) do alfabeto pela última (Taw) e assim sucessivamente. No alfabeto latino tal correspondência seria:

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

Assim, a palavra cifrada XIRKGLTIZURZ, corresponde ao texto CRIPTOGRAFIA.

Outro exemplo famoso do uso da criptografia é o bastão de Licurgo, utilizado pelo general espartano Panasius, por volta de 475 a.C, que consistia em escrever a mensagem em uma fita enrolada em um bastão padrão. Ao término, a fita era desenrolada e entregue ao mensageiro

que a usava como cinto. Para decifrar o código, o destinatário simplesmente enrolava a fita no seu bastão e lia o conteúdo.

Também devemos citar o código de Políbio, que se trata de um exemplo de cifra de substituição que troca letras pela combinação de dois números referentes a sua posição em uma tabela. Por exemplo, em relação a tabela

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

a palavra CRIPTOGRAFIA seria criptografada como: 13422441443522421121241 1.

Na Idade Média, a contribuição maior foi dada pelos árabes, principalmente pelo temor da Inquisição, que assolava o mundo ocidental. Nos anos 700, al-Khalil apresenta o método da "palavra provável" utilizado para decifrar mensagens. Nos anos 800, al-Kindi, filósofo árabe e autor de mais de 290 livros, escreve um tratado sobre a utilização da "análise de frequência" para decifrar mensagens. O método consiste em analisar a repetição de uma letra na mensagem e substituí-la pelas letras que são normalmente mais usadas, como 'a', 'e', 'o', etc.

Com a chegada da Renascença, encerrando o período de trevas da Idade Média, o estudo e aperfeiçoamento da criptografia ganham força, incentivados principalmente pelos governos, cientes de que informação era poder.

No final dos anos 1400, Leon Battista Alberti apresenta a substituição polialfabética, uma nova técnica que permitia que diferentes símbolos cifrados pudessem representar o mesmo símbolo do texto claro, dificultando a aplicação da análise de frequência. Nos anos 1500, Heinrich Cornelius Agrippa apresenta a cifra de Pig Pen (Porco no chiqueiro), que substitui letras por símbolos. Aperfeiçoando as ideias de Alberti, Blaise de Vigenère, em 1549, apresenta a cifra de Vigenère, um dos marcos da criptografia e que resistiu a todas as técnicas da criptoanálise por três séculos, até ser quebrada por Babagge e Kasiski já nos anos 1800.

1.2 Código de César

Júlio César por volta de 50 a.C foi o criador da cifra mais famosa da Antiguidade, o código de César, que consistia na substituição de uma letra pela que lhe sucedia em três posições.

Normal	a	b	c	d	e	f	g	h	i	j	k	l	m
Código	D	E	F	G	H	I	J	K	L	M	N	O	P

Normal	n	o	p	q	r	s	t	u	v	w	x	y	z
Código	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

A palavra CRIPTOGRAFIA seria transmitida como FULSWRJUDILD.

O código de César ainda é bastante utilizado nos dias de hoje, para garantir que textos eletrônicos não sejam lidos por acidente ou distração. Os mais famosos são o ROT13 e o ROT47. No ROT13 altera-se o valor do deslocamento para 13 letras.

Normal	a	b	c	d	e	f	g	h	i	j	k	l	m
Código	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Normal	n	o	p	q	r	s	t	u	v	w	x	y	z
Código	A	B	C	D	E	F	G	H	I	J	K	L	M

A vantagem desse método é que não há qualquer diferença entre o procedimento para codificar um texto em ROT-13 e o procedimento para decodificá-lo; basta aplicar o mesmo procedimento uma segunda vez. Já o ROT47 permite incluir pontuação e espaços em branco na codificação, trazendo um resultado final aparentemente mais difícil de ser decifrado.

Faça uma pesquisa na internet sobre esses dois métodos, temos certeza que você ficará impressionado com a quantidade de sites e grupos de discussão que usam esse método e com os programinhas desenvolvidos pelos usuários para facilitar o uso desses métodos.

1.3 Quebrando o Código de César

Como descrito acima, a criptografia de César é bastante simples, e por esse motivo torna-se fácil "quebrá-la", ou seja, é fácil descriptografar uma mensagem interceptada.

Na realidade, qualquer código que envolva a substituição sistematica de letras por outros símbolos sofrerá do mesmo problema, isso ocorre porque a frequência média com que cada letra aparece em um texto é, de certa forma, constante.

A porcentagem com que cada letra aparece em um texto (frequência) varia muito, depende do assunto do texto, do seu autor e do idioma em que foi escrito. Entretanto, de forma mais genérica, podemos considerar essa a seguinte tabela de frequências para textos escritos em português:

Letra	%	Letra	%	Letra	%	Letra	%
A	14.63	H	1.28	O	10.73	V	1.67
B	1.04	I	6.18	P	2.52	W	0.01
C	3.88	J	0.40	Q	1.20	X	0.21
D	4.99	K	0.02	R	6.53	Y	0.01
E	12.57	L	2.78	S	7.81	Z	0.47
F	1.02	M	4.74	T	4.74		
G	1.30	N	5.05	U	4.63		

Assim, tendo uma mensagem criptografada pelo método de substituição de símbolos, podemos usar a tabela acima para descriptografar tal mensagem, como pode ser visto no exemplo abaixo.

Exemplo 1. Usando a frequência de letras vamos decifrar a mensagem abaixo.

DGKV TGO IQHBZ VZ TCQHUVHBZ BG OVJGOVJQUZ HGDDG VHZ IVOZD VECGDGHJVC EVCV IZUG LO EZLUZ BV UCQEJZYCVPQV GDEGCVOZD WLG IZUG YZDJG

Primeiro criamos uma tabela com o percentual aproximado de ocorrência de cada símbolo.

Letra	%	Letra	%	Letra	%	Letra	%
A	0	H	6	O	6	V	15
B	3	I	4	P	1	W	1
C	7	J	5	Q	5	X	0
D	8	K	1	R	0	Y	2
E	5	L	2	S	0	Z	13
F	0	M	0	T	2		
G	13	N	0	U	6		

Usando a frequência de letras e a tabela acima podemos chegar em algumas conclusões, tal como é muito provável que o símbolo V represente a letra a na mensagem original, e podemos ver que os símbolos G e Z aparecem com a mesma frequência e perdem na quantidade de vezes apenas para o V, sabendo que a segunda e terceira letra mais frequentes no alfabeto são e e o, respectivamente, podemos fazer uma breve análise da palavra VZ. Vamos assumir que V represente a, sabendo que Z pode assumir o valor de e ou de o, então, restam duas opções para a tradução da palavra, ae, ao, mas sabemos que a palavra ae não faz parte do vocabulario formal então concluimos que o valor de Z é o e G é e.

Agora substituimos esses valores na mensagem criptografada:

DeKa TeO IQHBo ao TCQHUaHBo Be OaJeOaJQUo HeDDe aHo IaOoD aECeDeHJaC EaCa IoUe LO EoLUo Ba UCQEJoYCaPQa eDEeCaOoD WLe IoUe YoDJe

Ainda não podemos tirar nenhuma conclusão, então vamos analisar o símbolo D que seria o próximo a aparecer com mais frequência na mensagem, seguindo a tabela de porcentagem, D poderia significar r ou s, então vamos substituir na mensagem e ver o que ocorre.

Primeiro vamos testar o D como r.

reKa TeO IQHBo ao TCQHUaHBo Be OaJeOaJQUe Herre aHo IaOor aECereHJaC EaCa IoUe LO EoLUo Ba UCQEJoYCaPQa erEeCaOor WLe IoUe YorJe

Agora testamos o D como s.

seKa TeO IQHBo ao TCQHUaHBo Be OaJeOaJQUo Hesse aHo IaOos aECeseHJaC EaCa IoUe LO EoLUo Ba UCQEJoYCaPQa esEeCaOos WLe IoUe YosJe

Agora vamos analisar a palavra "HeDDe". Veremos alguns valores que o H pode assumir, sabendo que a frequência dele é de aproximadamente 5%. Segundo a tabela, as letras mais prováveis são d, n, m e t, mas sabemos os valores possíveis de D, ou seja, a palavra poderia ser "Hesse" ou "Herre", mas a palavra Herre com os valores de H não faz sentido para o português, então, se D vale s, temos duas possibilidades plausíveis, para "HeDDe", "desse" ou "nesse", entretanto temos a palavra "aHo", se H vale d temos "ado", o que não faz sentido, então associamos o valor de D a s e de H a n, então, mais uma vez substituímos os valores na frase original.

seKa TeO IQnBo ao TCQnUanBo Be OaJeOaJQUo nesse ano IaOos aECesenJaC EaCa IoUe LO EoLUo Ba UCQEJoYCaPQa esEeCaOos WLe IoUe YosJe

Agora vamos analisar a palavra "IoUe", ela é uma palavra de tamanho médio, e aparece duas vezes no texto, o que, nesse caso, é uma frequência alta, então ela tende a ser uma palavra comum, pelas suas letras provavelmente seria "voce", então vamos associar o valor de I a v e de U a c, logo, da palavra "vaOos" temos que o valor de O é m, em frequência, O estava empatada no topo com o símbolo C, tiramos que o valor de C tem que ser r, dada sua porcentagem na tabela de porcentagens. Então substituímos os valores na frase criptografada.

seKa Tem vQnBo ao TrQncanBo Be maJemaJQco nesse ano vamos aEresenJar Eara voce Lm EoLUo Ba UrQEJoYraPQa esEeramos WLe voce YosJe

Nesse ponto é facil ver que a primeira frase é "seja bem vindo ao brincando de matematico", com isso traduzimos o resto da frase, que fica:

Seja bem vindo ao Brincando de Matemático! Nesse ano vamos apresentar para você um pouco da criptografia. Esperamos que você goste.

1.4 Problema de Chave Pública

Os tipos de criptografia citados até o momento, chamados criptografia de chave simétrica ou secreta, parecem de fácil decodificação, basta saber o código utilizado para imediatamente serem decifrados. Tendo isso em mente, podemos encontrar um método de criptografar que seja fácil de fazer, porém muito difícil de desfazer, que mesmo sabendo como foi codificada, fosse extremamente trabalhoso a sua decodificação.

A metodologia da criptografia com chave pública surgiu em 1976, inovando com a utilização de pares de chaves distintas e complementares: uma chave para a codificação e outra para a decodificação. Os algoritmos de chave assimétrica também são chamados como algoritmos de chave pública e privada, onde a chave pública pode ser divulgada e a outra chave, a privada (secreta), só é conhecida pelo legítimo detentor.

A chave pública é disponibilizada a qualquer pessoa que deseja se comunicar com outra de forma segura, já a chave privada só é conhecida pelo seu titular específico. O destinatário de uma informação pode decodificar uma mensagem criptografada com sua chave pública, utilizando a chave privada correspondente. O mecanismo de distribuição pelo qual as chaves

públicas são transportadas aos usuários é um certificado. Normalmente, esses certificados são assinados por uma autoridade de codificação.

As chaves públicas e privadas são implementadas por meio de algoritmos que exploram as propriedades específicas dos números grandes, aumentando a segurança pela dificuldade da fatoração desses números, mesmo em rápidos e modernos computadores. Quanto maior a chave, mais difícil será decifrá-la. Mais a frente voltaremos a este tópico.

1.5 Código em Blocos

Código em blocos é uma maneira de criptografar uma mensagem que basicamente consiste em separar a mensagem em blocos e embaralhar esses blocos. Quando você deseja criptografar uma mensagem dessa forma o algoritmo para embaralhar os blocos consiste em:

1. Eliminar os espaços entre as palavras e completar a mensagem com um A no final caso tenha uma quantidade ímpar de letras;
2. Subdividir a mensagem em blocos de duas letras;
3. Refletir cada bloco;
4. Permutar os blocos trocando o primeiro com o último, o terceiro com o antepenúltimo, e assim por diante, mas deixando os outros como estão.

Como esse tipo de criptografia não consiste em trocar letras por símbolos ele torna inviável a aplicação de uma contagem por frequência, porém ele ainda sofre do problema da "chave pública", o que o torna inutilizável em situações como transições via web e em transições bancárias.

Exemplo 2. Vamos criptografar a mensagem "TREZE É UM NÚMERO PRIMO"

Primeiro eliminamos os espaços da mensagem e completamos ela,

TREZEEUMNUMEROPRIMOA

dividimos a mensagem em blocos,

TR-EZ-EE-UM-NU-ME-RO-PR-IM-OA

então refletimos os blocos,

RT-ZE-EE-MU-UN-EM-OR-RP-MI-AO

finalmente, permutamos os blocos,

AO-ZE-RP-MU-EM-UN-OR-EE-MI-RT

então a mensagem codificada fica 'AOZERPMUEMUNOREEMIRT'.

1.6 Criptografia com Matrizes

Sejam A e B matrizes 2×2, onde B é a matriz inversa de A. [Dúvidas sobre matrizes? Este capítulo tem um apêndice que pode lhe ajudar! Veja na página 13]

$$A = \begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix} \text{ e } B = \begin{bmatrix} 1 & -1 \\ -2 & 3 \end{bmatrix}$$

Vamos utilizar essas duas matrizes como "chaves" para codificar e decodificar a mensagem. O remetente vai usar a matriz A para codificar a mensagem e o destinatário vai usar a matriz B para decodificar a mensagem. O primeiro passo para codificar uma mensagem é convertê-la da forma alfabética para uma forma numérica. Então vamos utilizar a tabela abaixo:

Valores para as letras

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P	Q	R	S	T	U	V	X	W	Y	Z	.	!	#	
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

O remetente e o destinatário devem conhecer essa tabela de valores. Lembramos que esses valores são arbitrários e, desde que sejam combinados entre o remetente e o destinatário, podem assumir quaisquer valores. Vamos fazer um exemplo com a frase:"Eu acredito na educação."

1º Passo: Vamos fazer a correspondência entre as letras e os números usando a tabela dada.

E	U	#	A	C	R	E	D	I	T	O	#	N	A	#	E	D	U	C	A	Ç	A	O	.
5	21	29	1	3	18	5	4	9	20	15	29	14	1	29	5	4	21	3	1	3	1	15	27

Usamos o símbolo # entre as palavras para não gerar confusão. Como temos a matriz decodificadora A de ordem 2×2, vamos colocar a sequência de números dispostos em uma matriz de duas linhas. Se o número de elementos da mensagem for ímpar, podemos acrescentar um caracter vazio (não vai alterar a mensagem). No caso o número 30.

$$M = \begin{bmatrix} 5 & 21 & 29 & 1 & 3 & 18 & 5 & 4 & 9 & 20 & 15 & 29 \\ 14 & 1 & 29 & 5 & 4 & 21 & 3 & 1 & 3 & 1 & 15 & 27 \end{bmatrix}$$

2º Passo: Agora temos que codificar a mensagem, para que possamos enviá-la. Para fazer isso basta multiplicar a matriz A pela M tal que A.M=N.

$$\begin{aligned} N &= \begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 5 & 21 & 29 & 1 & 3 & 18 & 5 & 4 & 9 & 20 & 15 & 29 \\ 14 & 1 & 29 & 5 & 4 & 21 & 3 & 1 & 3 & 1 & 15 & 27 \end{bmatrix} \\ &= \begin{bmatrix} 29 & 64 & 116 & 8 & 13 & 75 & 18 & 13 & 30 & 61 & 60 & 114 \\ 24 & 43 & 87 & 7 & 10 & 57 & 13 & 9 & 21 & 41 & 45 & 85 \end{bmatrix} \end{aligned}$$

Assim temos os elementos de N que constituem a mensagem criptografada.

3º Passo: Quando o destinatário receber a mensagem N codificada ele terá que usar a matriz B para decodificar e obter a matriz original, e então poder ler a mensagem. Multiplicando a matriz B por N:

$$\begin{aligned} B.N &= \begin{bmatrix} 1 & -1 \\ -2 & 3 \end{bmatrix} . \begin{bmatrix} 29 & 64 & 116 & 8 & 13 & 75 & 18 & 13 & 30 & 61 & 60 & 114 \\ 24 & 43 & 87 & 7 & 10 & 57 & 13 & 9 & 21 & 41 & 45 & 85 \end{bmatrix} \\ &= \begin{bmatrix} 5 & 21 & 29 & 1 & 3 & 18 & 5 & 4 & 9 & 20 & 15 & 29 \\ 14 & 1 & 29 & 5 & 4 & 21 & 3 & 1 & 3 & 1 & 15 & 27 \end{bmatrix} = M \end{aligned}$$

Agora é só reverter os números da matriz B.N para conseguir a sua mensagem:

5	21	29	1	3	18	5	4	9	20	15	29	14	1	29	5	4	21	2	1	3	1	15	27
E	U	#	A	C	R	E	D	I	T	O	#	N	A	#	E	D	U	C	A	Ç	A	O	.

Note que na mensagem inicial revertida em números tem várias repetições de números, enquanto que a mensagem codificada não contém números repetidos, tornando-a mais difícil de ser desvendada. O que precisa ser escondido são apenas as matrizes A e B.

A seguir faremos mais um exemplo, dessa vez com uma matriz A 3×3. Vamos usar a matriz A e a inversa dela B como:

$$A = \begin{bmatrix} 3 & 1 & 2 \\ 2 & 1 & -1 \\ 3 & 1 & 3 \end{bmatrix} \text{ e } B = \begin{bmatrix} 4 & -1 & -3 \\ -9 & 3 & 7 \\ -1 & 0 & 1 \end{bmatrix}$$

Vamos usar a frase "The plot thickens" que em português significa "Entrou areia". Agora seguiremos o mesmo processo da frase anterior.

1º Passo: Consultando a tabela "Valores para as letras" podemos converter a nossa frase em números e arranjá-la em uma matriz 6×3.

$$M = \begin{bmatrix} 20 & 8 & 5 & 29 & 16 & 12 \\ 15 & 20 & 29 & 20 & 8 & 9 \\ 3 & 11 & 5 & 14 & 19 & 30 \end{bmatrix}$$

2º Passo: Para codificar a mensagem multiplicaremos a matriz M pela A, assim temos N = A.M

$$\begin{aligned} N &= \begin{bmatrix} 3 & 1 & 2 \\ 2 & 1 & -1 \\ 3 & 1 & 3 \end{bmatrix} . \begin{bmatrix} 20 & 8 & 5 & 29 & 16 & 12 \\ 15 & 20 & 29 & 20 & 8 & 9 \\ 3 & 11 & 5 & 14 & 19 & 30 \end{bmatrix} \\ &= \begin{bmatrix} 81 & 66 & 54 & 135 & 94 & 105 \\ 52 & 25 & 34 & 64 & 21 & 3 \\ 84 & 77 & 59 & 149 & 113 & 135 \end{bmatrix} \end{aligned}$$

Assim temos a nossa matriz N com a mensagem criptografada.

3º Passo: Para decodificar vamos multiplicar a nossa matriz B com a matriz N para conseguirmos a matriz M com a mensagem original.

$$\begin{aligned} B.N &= \begin{bmatrix} 4 & -1 & -3 \\ -9 & 3 & 7 \\ -1 & 0 & 1 \end{bmatrix} . \begin{bmatrix} 81 & 66 & 54 & 135 & 94 & 105 \\ 52 & 25 & 34 & 64 & 21 & 3 \\ 84 & 77 & 59 & 149 & 113 & 135 \end{bmatrix} \\ &= \begin{bmatrix} 20 & 8 & 5 & 29 & 16 & 12 \\ 15 & 20 & 29 & 20 & 8 & 9 \\ 3 & 11 & 5 & 14 & 19 & 30 \end{bmatrix} = M \end{aligned}$$

1.7 Apêndice: Matrizes

Definição 1. Denomina-se **matriz** a toda tabela formada por números dispostos em linhas e colunas.

Se uma matriz possui m linhas e n colunas, então dizemos que ela é de ordem $m \times n$, mais que isso, podemos dizer que se $m \neq n$ ela é uma matriz retangular e se $m = n$ ela é uma matriz quadrada.

Forma geral da matriz:

$$A = [a_{ij}]_{m \times n}$$

Em que a é o elemento localizado na linha i e na coluna j.

No caso $A_{3\times3}$ temos:

$$A_{3\times3} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

Exemplo 3. $A_{3\times3} = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$

Operações com Matrizes

Adição

Considere as matrizes A e B do tipo $m \times n$.
Para somá-las basta somar os elementos de mesma linha e mesma coluna:

$$A + B = [a_{ij} + b_{ij}]_{m \times n}$$

Exemplo 4. $A_{3\times3} = \begin{bmatrix} 0 & -1 \\ 2 & 1/2 \end{bmatrix} + \begin{bmatrix} 2 & 7 \\ 23 & 3/2 \end{bmatrix} = \begin{bmatrix} 0+2 & -1+7 \\ 2+23 & 1/2+3/2 \end{bmatrix} = \begin{bmatrix} 2 & 6 \\ 25 & 2 \end{bmatrix}$

Matriz nula: Aquela em que todas as entrada são iguais a 0. Sendo, portanto, o elemento neutro da soma.

Exemplo 5.

$$A_{2\times2} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0_{2\times2}$$

Propriedade 1. *Sejam A, B e C do tipo $m \times n$, seguem as seguintes propriedades:*

1) Comutativa: $A + B = B + A$

2) Associativa: $(A + B) + C = A + (B + C)$

3) Elemento Neutro: $A + 0 = 0 + A = A$

Multiplicação de matriz por um número

Para fazer o produto de um número por uma matriz basta multiplicar o número por cada elemento:

$$\lambda A_{m\times n} = [\lambda a_{ij}]_{m\times n}$$

Exemplo 6. $\lambda.\begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} \lambda x & \lambda y \\ \lambda z & \lambda w \end{bmatrix}$

Quando $\lambda = -1$ temos $(-1).A = -A$. Note que $A - A = 0$, logo $-A$ é o **elemento oposto** da adição.

Produto de matrizes

O produto de matrizes pode ser efetuado somente se o número de colunas da primeira matriz é igual ao número de linhas da segunda.

Sejam $A = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$ e $B = \begin{bmatrix} j & k & l \\ m & n & o \\ p & q & r \end{bmatrix}$,

então $A.B = \begin{bmatrix} aj+bm+cp & ak+bn+cq & al+bo+cr \\ dj+em+fp & dk+en+fq & dl+eo+fr \\ gj+hm+ip & gk+hn+iq & gl+ho+ir \end{bmatrix}$.

Exemplo 7. $A = \begin{bmatrix} 1 & 5 \\ 1 & 2 \\ 2 & 1 \end{bmatrix}$ e $B = \begin{bmatrix} 1 & 2 & 1 \\ 4 & 2 & 1 \end{bmatrix}$, então $A.B = \begin{bmatrix} 21 & 12 & 6 \\ 9 & 6 & 3 \\ 6 & 6 & 3 \end{bmatrix}$.

Perceba que $B.A = \begin{bmatrix} 5 & 10 \\ 8 & 25 \end{bmatrix}$. Assim, temos que, na maioria dos casos, $A.B \neq B.A$.

Matriz Identidade: É a matriz quadrada na qual os elementos da diagonal são iguais a 1 e os demais iguais a 0.

Exemplo 8. No caso em que a ordem da matriz é 3×3:

$$I_{3\times 3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Verifica-se que $I.A = A = A.I$, por isso ela é o **elemento neutro** da multiplicação.

Propriedade 2 (do produto de matrizes). *O produto de matrizes A, B e C de ordens compatíveis, satisfaz:*

1) Associativa: $(A.B).C = A.(B.C)$

2) Distributiva a direita: $(A + B).C = A.C + B.C$

3) Distributiva a esquerda: $C.(A + B) = C.A + C.B$

4) Número real λ: $(\lambda.B).A = B.(\lambda.A) = \lambda(B.A)$

Determinante

É o número associado a uma matriz quadrada.
Determinante de 1^a ordem:

$$A = [7] \Rightarrow det(A) = 7$$

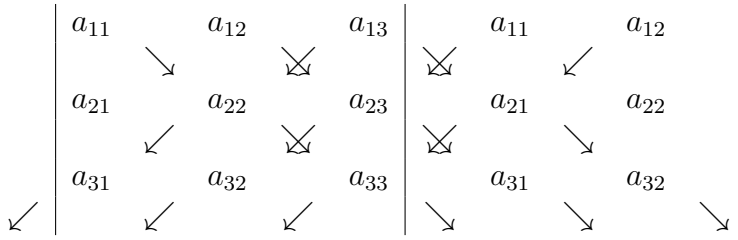
Determinante 2^a ordem:

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \Rightarrow \det A = \begin{vmatrix} a_{11} & & a_{12} \\ & \diagdown\!\!\diagup & \\ a_{21} & & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

Determinante 3^a ordem:

Seja $A_{3\times 3} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$.

Então, o determinante de A é:



$$-(a_{13}a_{22}a_{31} + a_{11}a_{23}a_{32} + a_{12}a_{21}a_{33}) + (a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32})$$

$$det(A) = -(a_{13}a_{22}a_{31} + a_{11}a_{23}a_{32} + a_{12}a_{21}a_{33}) + (a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32})$$

Proposição 1. *Sejam A e B matrizes tais que o produto $A.B$ seja uma matriz quadrada, então vale que:*

$$det(A.B) = det(A).det(B)$$

Matriz Inversa

Se $A.B = I = B.A$, então $B = A^{-1}$ é a matriz inversa de A, e A é a matriz inversa de B.

Em particular, vale que

$$det(A^{-1}) = \frac{1}{det(A)}$$

A matriz quadrada admite inversa se $det(A) \neq 0$.

Matriz quadrada que não é inversível é dita singular.

1.8 Exercícios

Exercício 1. Utilizando a Cifra de ATBASH decifre a mensagem VHHV VCVIXRXRL V UZXRO.

Exercício 2. Utilize o código de Políbio para codificar a mensagem "Pensar é um privilégio para poucos".

Exercício 3. Codifique a mesma mensagem do exercício anterior, porém utilizando o Código de César e depois o Rot13.

Exercício 4. Usando a frequência das letras em português decifre a mensagem:

MP CAE PWRADHE CHEWQRAE CHIKDA CW VDRFKAZDWQRW H CW PWKHPWKRVW H WVBWD MP WGZADRKRPA FWDW VWGVMGWD FDRPAE CH ZDWICHE JWGADHE.

Exercício 5. Na criptografia por blocos, por que escolhemos acrescentar exatamente a letra A quando a mensagem tem quantidade ímpar de letras?

Exercício 6. Por que a código em blocos tem o problema de “Chave Pública”?

Exercício 7. Descriptografe a mensagem

ASGALAADDSETATITACSEAMONAMTEAIEHMA.

Utilizando a codificação de letras feita acima resolva:

Exercício 8. Usando a matriz $A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ codifique a palavra SHERLOCK.

Exercício 9. Usando a matriz B$= \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix}$ codifique a palavra WATSON.

Exercício 10. Utilizando a matriz C$= \begin{bmatrix} 1 & -1 \\ -2 & 3 \end{bmatrix}$ decodifique a mensagem 52, 64, 40, 43.

Exercício 11. Utilizando a matriz C$= \begin{bmatrix} 1 & -1 \\ -2 & 3 \end{bmatrix}$ decodifique a mensagem 44, 45, 66, 75, 31, 36, 47, 55.

Exercício 12. $\begin{bmatrix} 3 & 0 & 4 \\ 0 & -2 & 2 \\ 0 & -6 & 3 \end{bmatrix} + \begin{bmatrix} 1 & 2 & 3 \\ -5 & 0 & 6 \\ -7 & 1 & 13 \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$

Exercício 13. $\begin{bmatrix} 3 & 2 & 4 \\ 0 & -2 & 5 \\ 1 & -6 & 8 \end{bmatrix} + \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = \begin{bmatrix} 4 & 4 & 7 \\ 4 & -6 & 11 \\ 8 & -5 & 17 \end{bmatrix}$

Exercício 14. $\begin{bmatrix} 0 & 0 & -5 \\ 2 & -2 & 12 \\ 9 & -6 & 6 \end{bmatrix} - \begin{bmatrix} 10 & -2 & 3 \\ 5 & 0 & -6 \\ -7 & 11 & 3 \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$

Exercício 15. $\begin{bmatrix} 0 & 9 & 2 \\ 0 & -2 & 5 \\ -1 & -1 & 5 \end{bmatrix} - \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = \begin{bmatrix} 1 & -4 & 0 \\ -4 & -6 & 11 \\ 2 & -4 & 16 \end{bmatrix}$

Exercício 16. Calcule:

a) $2.\begin{bmatrix} 1 & -9 \\ 7 & 2 \end{bmatrix} + 3.\begin{bmatrix} 1 & -9 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

b) $-5.\begin{bmatrix} 1 & 0 \\ 6 & 2 \end{bmatrix} - 3.\begin{bmatrix} 2 & -9 \\ 0 & -2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

Exercício 17. Dados $A = \begin{bmatrix} 1 & 5 \\ 1 & 2 \\ 2 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 2 & 1 \\ 3 & 2 & 1 \end{bmatrix}$, $C = \begin{bmatrix} 2 & 5 \\ 5 & 2 \end{bmatrix}$, e $D = \begin{bmatrix} 1 & 2 \\ 4 & 2 \end{bmatrix}$, calcule:

a) $A.B$
b) $B.A$
c) $C.D$
d) $B.C$

Exercício 18. Encontre o determinante:

a) $\begin{bmatrix} -11 \end{bmatrix}$

b) $\begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix}$

c) $\begin{bmatrix} 3 & 1 & 2 \\ 5 & 1 & 1 \\ 0 & 2 & -1 \end{bmatrix}$

Capítulo 2

Trabalhando com restos - aritmética modular

Definição 2. Dados dois números a e b, ambos *inteiros*, dizemos que a **divide** b e escrevemos $a|b$ se existe um número inteiro c tal que $b = a.c$. Isto é, ao dividir b por a o resto da divisão é zero.

Se $a|b$, então temos que a é um **divisor** de b, a é um **fator** de b, ou ainda, b é **múltiplo** de a.

Dizemos que a não divide b se o resto da divisão de b por a é diferente de zero.

Em outras palavras...
Vamos recordar os termos de uma divisão:

$$\text{Dividendo} = \text{Divisor} \times \text{Quociente} + \text{Resto}$$

Quando o resto for zero, dizemos que o dividendo é divisível pelo divisor.

Exemplo 9. $6 = 3 \times 2 + 0$
Portanto, 6 é divisível por 3. Também podemos dizer que 3 é divisor de 6. Além disso, 6 é multiplo de 3.

2.1 Critérios de divisibilidade

Já sabemos que um número é divisível por outro quando o resto da divisão é igual a zero. Observando esses casos é possível chegar a alguns critérios de divisibilidade:

Por 1:
Todo número é divisível por 1, pois $a.1 = 1.a = a$.

Por 2:
Todos os números terminados em 0, 2, 4, 6 e 8 são divisíveis por 2.

Exemplo 10. $12 \div 2 = 6$
$1024 \div 2 = 512$

Por 3:
Um número inteiro é divisível por 3, se a soma dos seus algarismos é divisível por 3.

Exemplo 11. $66 \div 3$, pois $6 + 6 = 12$
$81 \div 3$, pois $8 + 1 = 9$
$558 \div 3$, pois $5 + 5 + 8 = 18$

Por 5:
Para um número ser divisível por 5 basta que seu último algarismo seja 0 ou 5.

Exemplo 12. $25 \div 5 = 5$
$200 \div 5 = 40$

Por 7:
Para saber se um número é divisível por 7, duplicamos o algarismo das unidades e subtraimos o resultado do número inicial sem o algarismo final. Se o resultado for divisível por 7, o número é divisível por 7.

Exemplo 13. $203 \div 7$, pois $2 \times 3 = 6$ e 20 - 6 = 14
$294 \div 7$, pois $2 \times 4 = 8$ e 29 - 8 = 21
$840 \div 7$, pois $2 \times 0 = 0$ e 84 - 0 = 84

Por 9:
Se a soma dos algarismo de um número é um múltiplo de 9, então o número também o é.

Exemplo 14. 324 é múltiplo de 9, pois $3 + 2 + 4 = 9$, e de fato $324 = 36 \times 9$.

2.2 Número primo

Definição 3. Números primos são números pertencentes ao conjunto dos números naturais não nulos, que possuem exatamente apenas dois divisores naturais distintos, o número 1 e o próprio número.

Perceba que segundo esta definição o número 1 não é um número primo, pois o mesmo não apresenta dois divisores distintos.

O número 2 é o único número primo par, já que todos os demais números pares possuem ao menos 3 divisores, dentre eles a unidade, o próprio número e o número 2.

Os dez primeiros primos são $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$. Não é possível apresentar todos, pois o conjunto dos números primos é infinito.

Dizemos, por exemplo, que 4 e 9 são **compostos**, visto que $1, 2$ e 4 dividem o primeiro, enquanto que $1, 3$ e 9 dividem o segundo.

A qualidade de ser primo é algo que também afeta os números negativos. Para os negativos, dizemos que um número é primo negativo quando pode ser dividido por -1 e por ele mesmo.

Exemplo 15. O número -3, que também pode ser dividido pelos negativos -1 por ele mesmo, também é primo.

2.3 Fatoração em números primos

Fatorar em números primos é achar uma multiplicação de números primos que resulta no número que se deseja fatorar.

Para fatorar um número em fatores primos é possível usar o método que foi ensinado a vocês nas primeiras séries do colégio.

Começamos escrevendo o número a fatorar com uma barra vertical ao lado. Em seguida, procura-se o menor primo que divida o número, o resultado da divisão é escrito a esquerda da linha vertical, e repete-se este processo até chegar ao número 1. Vejam estes exemplos:

81	3
27	3
9	3
3	3
1	

126	2
63	3
21	3
7	7
1	

147	3
49	7
7	7
1	

Logo, achamos a fatoração em primos destes números:

Número	Fatoração em primos	Fatoração utilizando potências
81	$3 \cdot 3 \cdot 3 \cdot 3$	3^4
126	$2 \cdot 3 \cdot 3 \cdot 7$	$2 \cdot 3^2 \cdot 7$
147	$3 \cdot 7 \cdot 7$	$3 \cdot 7^2$

2.4 Relações de Equivalência

Uma **relação de equivalência** é uma relação binária entre elementos de um dado conjunto X que satisfaz estas propriedades:

1. $\forall a \in X$, vale que a R a. (*Reflexividade*)
2. $\forall a, b \in X$, se a R b, então b R a. (*Simetria*)
3. $\forall a, b, c \in X$, se a R b e b R c, então a R c. (*Transitividade*)

Nota: $\forall$ é o símbolo que substitui a expressão "para todo".

2.5 Congruências

O conceito e a técnica das congruências foi desenvolvido inicialmente por Karl Gauss em 1801.

Definição 4. Sejam $a, b \in \mathbb{Z}$ e $m \geq 0$. Dizemos que a e b são **congruentes** módulo m quando $(a - b)$ é divisível por m, isto é, quando $a - b = m \cdot k$, com $k \in \mathbb{Z}$.

Caso contrário, dizemos que a não é congruente a b módulo m.

Notação 1. $a \equiv b \pmod{m} \Leftrightarrow m|(a - b)$

Congruência é uma relação de equivalência em $\mathbb{Z}$, pois obedece a todas as propriedades:

1. Reflexiva: $\forall a \in \mathbb{Z}, a \equiv a \pmod{m}$, pois $a - a = 0 = 0 \cdot m$.

   Exemplo 16. $10 \equiv 10 \pmod{5}$, pois $5|(10 - 10)$, ou ainda $10 - 10 = 0 = 0 \cdot 5$.

2. Simétrica:

   Perceba que para quaisquer $a, b \in \mathbb{Z}$ com $a \equiv b \pmod{m}$ significa que existe $k \in \mathbb{Z}$ tal que $a - b = m \cdot k$, mas $a - b = -(b - a) = mk \Rightarrow b - a = m(-k)$, logo $m|b - a$. Portanto $b \equiv a \pmod{m}$.

   Exemplo 17. $7 \equiv 3 \pmod{2}$, pois $2|(7 - 3)$, ou ainda, $7 - 3 = 4 = 2 \cdot 2$.

3. Transitiva: $\forall a, b, c \in \mathbb{Z}, a \equiv b \pmod{m}$ e $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

   Veja o Exercício 22.

   Exemplo 18. $8 \equiv 2 \ (mod\ 2)$ e $2 \equiv 0 \ (mod\ 2) \Rightarrow 8 \equiv 0 \ (mod\ 2)$

Proposição 2. *Seja $m \geq 0$, então, $a \equiv b \pmod{m}$ se, e somente se, a e b têm mesmo resto quando divididos por m.*

Exemplo 19. Para $m = 2$, temos que $5 \equiv 3 \pmod{2}$, pois $5 = 2.2 + 1$ e $3 = 2.1 + 1$, ou seja, 5 e 3 possuem resto igual a 1.

Proposição 3. *Seja $m \geq 0$ e $a \in \mathbb{Z}$. Se o resto da divisão de a por m é r, então, $a \equiv r \pmod{m}$. Em outras palavras, todo número quando dividido por m é congruente ao resto da divisão módulo m.*

Exemplo 20. 9 dividido por 4 é igual a 2 mais o resto 1, então $9 \equiv 1 \pmod{4}$

2.6 Aritmética modular

Vejamos que a aritmética modular respeita algumas boas propriedades.

Propriedade 3. *$\forall a, b, c, , d, k \in \mathbb{Z}$ vale que:*

1. $a \equiv b \pmod{m} \Rightarrow a + c \equiv b + c \pmod{m}$

   Exemplo 21. $4 \equiv 1 \pmod{3} \Rightarrow (4 - 1) \equiv (1 - 1) \pmod{3}$

   Exemplo 22. $8 \equiv 3 \pmod{5} \Rightarrow (8 - 2) \equiv (3 - 2) \pmod{5}$

2. $a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{m}$

   Exemplo 23. $7 \equiv 1 \pmod{6} \Rightarrow 7.2 \equiv 1.2 \pmod{6}$

   Exemplo 24. $9 \equiv 3 \pmod{6} \Rightarrow -9 \equiv -3 \pmod{3}$

3. $a \equiv b \pmod{m}$ *e* $c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$

Exemplo 25. $10 \equiv 2 \pmod 4$ e $7 \equiv 3 \pmod 4 \Rightarrow 10.7 \equiv 2.3 \pmod 4$

4. $a \equiv b \pmod{m} \Rightarrow a^k \equiv b^k \pmod{m}, \forall k \geq 0$

Exemplo 26. $4 \equiv 2 \pmod 2$ e $4^4 \equiv 2^4 \pmod 2$

Exemplo 27. Utilizando essas propriedades, prove que $233|2^{29} - 1$, ou seja, que $2^{29} \equiv 1 \pmod{233}$.

Sabemos que todo número inteiro é congruente com seu resto, vamos tomar a menor potência de 2, que é maior que 233, e aplicar o algoritmo da divisão;

$$2^8 = 256 \Rightarrow 256 = 233 \cdot 1 + 23 \Rightarrow 2^8 \equiv 23 \pmod{233}$$

Utilizando a propriedade *4*,

$$(2^8)^2 \equiv 23^2 \pmod{233} \Rightarrow 2^{16} \equiv 529 \pmod{233}$$

$$529 = 233 \cdot 2 + 63 \Rightarrow 2^{16} \equiv 63 \pmod{223}$$

Utilizando a propriedade *3*,

$$2^{16} \cdot 2^8 \equiv 63 \cdot 23 \pmod{233} \Rightarrow 2^{24} \equiv 1449 \pmod{233}$$

$$1449 = 233 \cdot 6 + 51 \Rightarrow 2^{24} \equiv 51 \pmod{233}$$

$$2^{24} \cdot 2^5 \equiv 51 \cdot 32 \pmod{233} \Rightarrow 2^{29} \equiv 1632 \pmod{233}$$

$$1632 = 233 \cdot 7 + 1 \rightarrow 2^{29} \equiv 1 \pmod{233}$$

Exemplo 28. Vamos justificar o critério de divisibilidade por 3 usando congruência módulo 3.

Seja a um número inteiro qualquer composto pelos algarismos $a_n a_{n-1} \cdots a_1 a_0$. Ao decompor ele usando unidades, dezenas, centenas, milhares, obtém-se

$$a = a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10 + a_0$$

Veja para $1551 = 1 \cdot 10^3 + 5 \cdot 10^2 + 5 \cdot 10 + 1$.

Tendo que $a_n + a_{n-1} + ... + a_1 + a_0 \equiv 0 \pmod 3$ e que $10 \equiv 1 \pmod 3$, logo $10^k \equiv 1^k \pmod 3$. Usando as propriedades temos:

$$\begin{array}{c} a_n 10^n \equiv a_n \pmod 3 \\ a_{n-1}10^{n-1} \equiv a_{n-1} \pmod 3 \\ \vdots \\ a_1 10 \equiv a_1 \pmod 3 \\ +a_0 \equiv a_0 \pmod 3 \\ \hline (a_n 10^n + a_{n-1}10^{n-1} + ... + a_1 10 + a_0) \equiv (a_n + a_{n-1} + ... + a_1 + a_0) \equiv 0 \pmod 3 \end{array}$$

Ou seja, a é múltiplo de 3.

2.7 Teorema de Bézout

Para tratar do Teorema de Bézout precisamos das seguinte noções:

Definição 5. O **Conjunto D(a,b)** contém os números que dividem tanto a quanto b, sendo $a, b \in \mathbb{Z}$.

Definição 6. O **máximo divisor comum** entre dois números inteiros a e b, em que pelo menos um deles não é zero, é o maior elemento do conjunto D(a,b) e será denotado por $mdc(a, b)$.

Teorema 1. *O máximo divisor comum sempre existe, já que* 1 *é divisor de qualquer elemento de* $\mathbb{N}$,

Exemplo 29. $mdc(36, 18) = ?$
$D(36) = 2, 3, 4, 6, 9, 12, 18, 36$ e $D(18) = 2, 3, 6, 9, 18$, logo $D(36, 18) = 2, 3, 6, 9, 18$.
Portanto $mdc(36, 18) = 18$

Definição 7. Dois números a e b são chamados **primos entre si** se $mdc(a, b) = 1$.

Proposição 4. *Sejam* $a, b, c, d \in \mathbb{Z}$. *Se* $ac \equiv bc \pmod m$ *e* $mdc(c, m) = 1$, *então* $a \equiv b \pmod m$

Exemplo 30. $12 \equiv 6 \pmod 2$, pois $4.3 \equiv 2.3 \pmod 2$, $(3, 2) = 1$ e $4 \equiv 2 \pmod 2$

Porém se quiséssemos o $mdc(1551, 366)$ ficaria complicado achar todos os divisores comuns entre 1551 e 336. Então usaremos o seguinte teorema para encontrar o máximo divisor comum entre quaisquer inteiros.

Teorema 2 (de Bézout). *Seja* $d = mdc(a, b)$, *então existem* $r, s \in \mathbb{Z}$ *tais que*

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

Mas como achar tais $r, s \in \mathbb{Z}$?
Basta usar o algoritmo da divisão!

Sejam $a, b \in \mathbb{Z}$ com $b < a$.

1º passo: Dividimos o maior pelo menor.

$a = b \times k_1 + r_1$, com $k_1, r_1 \in \mathbb{Z}$ e $r_1 < b$.

2º passo: Dividimos o dividendo b pelo resto r_1.
$b = r_1 \times k_2 + r_2$ com $k_2, r_2 \in \mathbb{Z}$ e $r_2 < r_1$.

Passos Restantes: Dividimos o dividendo pelo resto, até que o resto seja igual a 0.
O último resto diferente de zero é o máximo divisor comum entre a e b.

Para achar os tais r e s, já sabendo o valor do mdc, basta "voltar" nos passos, isolando os restos.

Exemplo 31. $mdc(30, 18) = ?$

1º passo: dividimos o maior pelo menor

$$30 = 18 \cdot 1 + 12$$

2º passo: dividimos o dividendo pelo seu resto

$$18 = 12 \cdot 1 + 6$$

Como o resto ainda não é igual a zero, dividimos novamente o dividendo pelo resto:

$$12 = 6 \cdot 2 + 0$$

Como o resto é zero, $mdc(30, 18) = 6$.
Isolando os restos nas equações acima encontramos r e s satisfazendo $30 \cdot r + 18 \cdot s = 6$:

$$18 = 12 \cdot 1 + 6 \Rightarrow 6 = 18 - 12$$
$$30 = 18 \cdot 1 + 12 \Rightarrow 12 = 30 - 18$$

Então

$$6 = 18 - 12 \Rightarrow 6 = 18 - (30 - 18)$$
$$6 = -1 \cdot 30 + 2 \cdot 18 \Rightarrow r = -1, s = 2$$

Exemplo 32. $mdc(128, 72) = ?$

$$128 = 72 \cdot 1 + 56$$
$$72 = 56 \cdot 1 + 16$$
$$56 = 16 \cdot 3 + 8$$
$$16 = 8 \cdot 2 + 0$$

Logo $mdc(128, 72) = 8$. Para encontrar r e s tais que $128 \cdot r + 72 \cdot s = 8$ fazemos o caminho inverso:

$$8 = 56 - 3 \cdot 16$$

$$16 = 72 - 56$$

$$56 = 128 - 72$$

$$8 = 56 - 3 \cdot (72 - 56) = -3 \cdot 72 + 4 \cdot 56$$

$$8 = -3 \cdot 72 + 4 \cdot (128 - 72) = 4 \cdot 128 - 7 \cdot 72 \Rightarrow r = 4, s = -7$$

Exemplo 33. $mdc(187, 91) =?$

$$187 = 91 \cdot 2 + 5$$

$$91 = 5 \cdot 18 + 1$$

$$5 = 5 \cdot 1 + 0$$

$$mdc(187, 91) = 1$$

Isto é, 187 e 91 são primos entre si. Encontremos agora r, s de tal modo que $187 \cdot r + 91 \cdot s = 1$.

$$1 = 91 - 5 \cdot 18$$

$$5 = 187 - 91 \cdot 2$$

$$1 = 91 - 18 \cdot (187 - 2 \cdot 91)$$

$$1 = 91 - 18 \cdot 187 + 36 \cdot 91 = 37 \cdot 91 - 18 \cdot 187 \Rightarrow r = 37, s = 18$$

Exemplo 34. $mdc(391, 247) =?$

$$391 = 247 \cdot 1 + 144$$

$$247 = 144 \cdot 1 + 103$$

$$144 = 103 \cdot 1 + 41$$

$$103 = 41 \cdot 2 + 21$$

$$41 = 21 \cdot 1 + 20$$

$$21 = 20 \cdot 1 + 1$$

$$20 = 20 \cdot 1 + 0$$

391 e 247 são primos entre si, porque $mdc(391, 247) = 1$.

$$1 = 21 - 20, \text{ mas } 20 = 41 - 21$$

$$1 = 21 - (41 - 21) = 21 - 41 + 21 = 2 \cdot 21 - 41$$

$$1 = 2 \cdot 21 - 41, \text{ mas } 21 = 103 - 2 \cdot 41$$

$$1 = 2 \cdot (103 - 2 \cdot 41) - 41 = 2 \cdot 103 - 5 \cdot 41$$

$$1 = 2 \cdot 103 - 5 \cdot 41, \text{ mas } 41 = 144 - 103$$
$$1 = 2 \cdot 103 - 5 \cdot (144 - 103) = 7 \cdot 103 - 5 \cdot 144$$
$$1 = 7 \cdot 103 - 5 \cdot 144, \text{ mas } 103 = 247 - 144$$
$$1 = 7 \cdot (247 - 144) - 5 \cdot 144 = 7 \cdot 247 - 12 \cdot 144$$
$$1 = 7 \cdot 247 - 12 \cdot 144, \text{ mas } 144 = 391 - 247$$
$$1 = 7 \cdot 247 - 12 \cdot (391 - 247) = 19 \cdot 247 - 12 \cdot 391 \Rightarrow r = 19, s = 12$$

2.8 Exercícios

Exercício 19. Encontre a fatoração em primos de: $56, 94, 260, 78$ e 196.

Exercício 20. Encontre o mdc dos seguintes pares: $(45, 33), (584, 276), (384, 175)$ e $(96, 224)$.

Exercício 21. Qual é o menor número que devemos adicionar a 25013 para que a soma seja divisível ao mesmo tempo por 3 e por 7?

Exercício 22. Se um número n for dividido por 27, o resto da divisão será igual a 7. Se dividirmos o número n+50 também por 27, qual será o resto obtido?

Exercício 23. Fatore em números primos, os números a seguir:
a) 28
b) 247
c) 1024
d) 363

Exercício 24. Justifique por que vale a propriedade de transitividade para congruências.

Exercício 25. Sabendo que $k \equiv 1 \pmod 4$, mostre que $6k + 5 \equiv 3 \pmod 4$.

Exercício 26. Utilizando as propriedades de cogruência módulo m, determine o resto da divisão de $2^{2014} + 3^{2014}$ por 13.
Sugestão: observe que $2^2 + 3^2 \equiv 0 \pmod{13}$.

Exercício 27. (Provão 2003) Se o resto da divisão de um inteiro n por 5 é igual a 3, o resto da divisão de n^2 por 5 é, necessariamente, igual a:
a) 0
b) 1
c) 2
d) 3
e) 4

Exercício 28. Determine o resto da divisão de 5^{60} por 26;

Exercício 29. Determine o resto da divisão 2^{50} por 7

Exercício 30. Determine o $mdc(231, 130)$ e encontre os respectivos r e s.

Exercício 31. Determine o $mdc(150, 91)$ e encontre os respectivos r e s.

Capítulo 3

Base Teórica para a Criptografia de Alto Nível

Os números naturais $1, 2, 3, 4, ...$ foram os primeiros a surgir na história da humanidade. Eles apareceram de maneira espontânea, pela necessidade de contar e ordenar objetos. Denotamos o conjunto de naturais pelo símbolo $\mathbb{N}$. Associadas a ele, nasceram duas operações: a soma e a multiplicação. Representamos em geral a operação de produto pelo símbolo $(\cdot)$, enquanto que a adição é representada por $(+)$.

Duas perguntas interessantes que podem ser feitas são as seguintes:

I) Qual o menor subconjunto de $\mathbb{N}$ que munido apenas da operação de **soma**, gera o conjunto dos naturais?

II) Qual o menor subconjunto de $\mathbb{N}$ que munido apenas da operação de **produto**, gera o conjunto dos naturais?

A resposta para o caso **I)** é extremamente simples. Considere $\{1\}$, ou seja, o conjunto que contém apenas o número 1. Dado qualquer n natural, basta somar o número 1 exatamente n vezes. Por exemplo, $3 = 1 + 1 + 1$.

Já a resposta da questão **II)** não é tão imediata, pois precisamos do conceito de número primo e de um dos mais famosos teoremas da história da matemática, publicado pela primeira vez na obra *Elementos* de Euclides, há mais de 2300 anos.

Teorema 3 (**Fundamental da Aritmética**). *Todo número natural diferente de* 1 *pode ser decomposto como produto de primos, com tal decomposição sendo única.*

Não iremos demonstrar este teorema, pois não é este o propósito desta apostila. Para ilustrar, vamos decompor 36. Sabemos que este número é par, pois termina em 6. Podemos então dividí-lo por 2, obtendo 18 como quociente, que é novamente par. Fazendo a divisão

por 2, o resultado é 9, que é múltiplo de 3. Dividimos por 3 duas vezes e chegamos em 1. Assim, $36 = 2 \cdot 2 \cdot 3 \cdot 3 = 2^2 \cdot 3^2$.

Lembremos agora o que foi visto no capítulo 2:

Para checarmos se dois números quaisquer são primos entre si, basta decompor ambos em produto de primos. Se existir qualquer fator em comum entre eles, o máximo divisor comum será maior que 1 e portanto os números não serão primos entre si. A fatoração na verdade nos dá muito mais do que isso. Podemos obter exatamente o máximo divisor comum dos dois números. Façamos alguns exemplos:

1) $48 = 2^4 \cdot 3$ e $27 = 3^3$. Logo, $\text{mdc}(48, 27) = 3$.

2) $54 = 2 \cdot 3^3$ e $77 = 7.11$. Assim os dois números são primos entre si.

3) $108 = 2^2 \cdot 3^3$ e $180 = 2^2 \cdot 3^2 \cdot 5$. Então ambos são múltiplos de $2^2 \cdot 3^2 = 36$.
Portanto, $\text{mdc}(108, 180) = 36$.

3.1 Divisão Modular

Quando estudamos divisão de frações, aprendemos que

$$\frac{1}{2} \div \frac{5}{4} = \frac{1}{2} \cdot \frac{4}{5},$$

ou seja, conservamos a primeira fração e invertemos a segunda. Porque fazemos isto?

Para começar, perceba que

$$\frac{5}{4} \cdot \frac{4}{5} = 1.$$

De maneira mais geral,

$$\frac{x}{y} \cdot \frac{y}{x} = 1, \text{ se } x \neq 0 \text{ e } y \neq 0.$$

Dado $x \in \mathbb{R}$, se existe $y \in \mathbb{R}$ tal que $x \cdot y = 1$, dizemos que y é o inverso da multiplicação de x. Em $\mathbb{R}$, todo elemento diferente de 0 possui inverso, e este é único.

Na escola, vemos as operações de multiplicação e divisão como coisas separadas. Mas, de fato, **só há a operação de produto**. Quando dividimos 4 por 2, o que fazemos é **multiplicar** 4 **pelo inverso de** 2. É isso que explica o método adotado para divisão de frações que citamos anteriormente.

Voltemos agora à aritmética modular. Já sabemos que podemos multiplicar e somar as classes de maneira totalmente análoga ao que fazemos com os inteiros. Será que podemos "dividir"? Isto é, quando um número possui inverso?

Definição 8. Seja n um número natural diferente de 1, e $a \in \mathbb{Z}$. Dizemos que a é **inversível módulo** n se existe $b \in \mathbb{Z}$ de forma que $a \cdot b \equiv 1 \pmod{n}$.

Façamos algumas contas para ver o que ocorre.

- 8 claramente não é inversível módulo 8, pois para todo m natural $8m \equiv 0 \pmod{n}$;
- 3 é inversível módulo 8, pois $3 \cdot 3 = 9$, e $9 \equiv 1 \pmod{8}$.
- 2 não é inversível módulo 8. Vamos provar isso:

  Suponha que existe $a \in \mathbb{Z}$ tal que $2 \cdot a \equiv 1 \pmod{8}$. Pela definição de congruência, temos que $2 \cdot a - 8 \cdot b = 1$, para algum b inteiro.
  Mas perceba que do lado esquerdo temos um inteiro par, enquanto que 1 é ímpar. Temos assim uma contradição. Concluímos então que 2 não é inversível módulo 8.

Agora vamos generalizar esta ideia.

Teorema 4. *Se $mdc(m, n) \neq 1$, então m não é inversível módulo n.*

Demonstração 1. Cosidere $mdc(m, n) = d$. Logo, $m = a \cdot d$ e $n = b \cdot d$. Suponhamos por contradição que existe $r \in \mathbb{Z}$ de maneira que $r \cdot m \equiv 1 \pmod{n}$. Então, também existe $s \in \mathbb{Z}$ tal que $(r \cdot m - s \cdot n) = 1$. Escrevendo m e n em função de d, temos: $r \cdot (a \cdot d) - s \cdot (b \cdot d) = 1 \Rightarrow d \cdot (r \cdot a - s \cdot b) = 1 \Rightarrow d|1$. Mas d é maior que 1!! Temos uma contradição.

Portanto, a afirmação está provada.

Estudemos agora o caso onde m e n são primos entre si. Será que existe algum caso onde m possui inverso módulo n?

Tomemos $m = 2$ e $n = 3$. Multiplicando 2 por 2, obtemos $2 \cdot 2 = 4 = 1 \cdot 3 + 1 \Rightarrow 4 \equiv 1 \pmod{3}$. Podemos ver assim que a resposta é afirmativa.

Escolhendo $m = 7, n = 9$, temos $4 \cdot 7 = 28 = 3.9 + 1 \Rightarrow 4 \cdot 7 \equiv 1 \pmod{9}$. A questão que surge neste momento é: será que isto sempre ocorre?

Teorema 5. *Se $mdc(m, n) = 1$, então m é inversível módulo n.*

Demonstração 2. Basta aplicar o Teorema de Bézout, já visto anteriormente. Pelo teorema, como $mdc(m, n) = 1$, existem r, $s \in \mathbb{Z}$ tal que $r \cdot m - s \cdot n = 1$. Logo, $r \cdot m = 1 + s \cdot n \Rightarrow r \cdot m \equiv 1 \pmod{n}$.

Corolário 1. *Seja p um número primo e n um número inteiro que não é divísivel por p. Então n é inversível módulo p.*

Demonstração 3. Se p é primo, seus únicos divisores são 1 e p. Como p não divide n, temos que $mdc(n, p) = 1$. Basta agora aplicar o teorema anterior.

Para encontrarmos um inverso módulo n, é suficiente repetirmos as contas já feitas quando vimos o Teorema de Bézout. No entanto, este inverso **não é único**. Na verdade, a única coisa que importa é o **resto** da divisão por n.

Para ilustrar o que queremos dizer, façamos um exemplo.

Exemplo 35. Encontre um inverso de 5 módulo 7.

Pelo algoritmo da divisão, $7 = 5 \cdot 1 + 2$ e $5 = 2 \cdot 2 + 1$. Então, temos:

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 = \\ &= 5 - 2 \cdot (7 - 1 \cdot 5) = \\ &= 3 \cdot 5 - 2 \cdot 7 \end{aligned}$$

Concluimos então que 3 é um inverso de 5 módulo 7. No entanto, fazendo $10 \cdot 5 = 50 = 7^2+1$ e $50 \equiv 1 \pmod 7$, temos que 10 também é inverso de 5 módulo 7. Na verdade, isto vale para todo número da forma $3+(7 \cdot n)$, com $n \in \mathbb{Z}$, pois $5 \cdot (3+7 \cdot n) = 15+7 \cdot (5 \cdot n) \equiv 1+0 \equiv 1 \pmod 7$.

Por outro lado, todos os inversos de 5 módulo 7 são desta forma. Se $5 \cdot a \equiv 1 \pmod 7$, então $5 \cdot a \equiv 5 \cdot 3 \pmod 7$. Multiplicando por 3 em ambos os lados, temos: $(5 \cdot 3) \cdot a \equiv (5 \cdot 3) \cdot 3 \pmod 7$. Mas $15 \equiv 1 \pmod 7$. Finalizando, $(5 \cdot 3) \cdot a \equiv 1 \cdot a \equiv (5 \cdot 3) \cdot 3 \equiv 1 \cdot 3 \pmod 7 \Rightarrow a \equiv 3 \pmod 7 \Rightarrow a = 3 + (7 \cdot n)$, para algum n inteiro.

Com tal raciocínio, é possível provar que sempre que m possui inverso módulo n, existem infinitos números diferentes que fazem o papel, mas todos possuem o mesmo resto na divisão por n.

3.2 Potências Modulares

Uma importante aplicação das congruências é o cálculo de restos da divisão de uma potência por um número qualquer. O problema é que quando nos deparamos com alguma potência cujo expoente não é um número relativamente pequeno, então essa potência se torna um número muito grande ficando assim inviável calcularmos o resto dessa divisão apenas utilizando os métodos tradicionais.

Exemplo 36. Calcule o resto da divisão de 2^{90} por 13. Mesmo que o número 2 seja uma base pequena para calcularmos suas potências, o expoente 90 faz esse número possuir um valor absurdamente alto:

$$2^{90} = 1237940039285380274899124224$$

Esse número possui 28 digitos, como, em geral, nossas calculadoras nos permitem fazer cálculos com no máximo 8 dígitos, esse tipo de conta se torna impossível de ser realizada por uma calculadora normal usando apenas as propriedades do Algoritmo da Divisão.

3.3 Algumas propriedades a respeito do Resto de uma Divisão

Relembrando alguns conceitos dos capítulos anteriores: Dados dois inteiros a e m, sabemos pelo Algoritmo da Divisão que existem inteiros q e r denominados respectivamente, de quociente e resto (da divisão de a por m), tais que:

$$a = q.m + r$$

onde $0 \leq r < m$, logo

$$a - r = q.m$$

ou seja, $a - r$ é múltiplo de m, em outras palavras, m divide $a - r$.

Portanto, pela definição de congruência modular, temos:

$$a \equiv r \pmod{m}$$

Observação 1. O resto r, da divisão de a por m, pode assumir qualquer valor entre 0 e $m-1$.

Exemplo 37. Temos que, 17 dividido por 5 é igual a 3, e sobra resto 2. Então podemos dizer que:

$$17 \equiv 2 \pmod{5}$$

Definição 9. O conjunto $\{0, 1, 2, \ldots, m-1\}$ dos inteiros menores que m, forma um sistema completo de resíduos módulo m.

Exemplo 38. Se fixarmos $m = 7$, então a classe de resíduos – restos – módulo 7 possui exatamente 7 elementos, são eles: $0, 1, 2, 3, 4, 5, 6$.

Proposição 5. *Todo número inteiro a é congruente módulo m a exatamente um dos valores entre:*

$$0, 1, 2, \ldots, m-1$$

Demonstração 4. Vamos pegar dois números x e y, tais que $x, y \in \{0, 1, 2, \ldots, m-1\}$ e $x \leq y$. Vamos supor que a é congruente a x módulo m, ou seja:

$$a \equiv x \pmod{m}$$

então temos que existe $q \in \mathbb{Z}$ tal que:

$$a - x = q.m \implies a = q.m + x \tag{3.1}$$

Agora vamos supor que a é congruente a y módulo m, ou seja:

$$a \equiv y \pmod{m}$$

então temos que existe $t \in \mathbb{Z}$ tal que:

$$a - y = t.m \implies a = t.m + y \tag{3.2}$$

Como $a = a$, podemos igualar as duas equações anteriores (3.1) e (3.2):

$$q.m + x = t.m + y$$

$$q.m - t.m = y - x$$

$$(q - t).m = y - x$$

Portanto $(y - x)$ é múltiplo de m, ou seja, $(y - x) = k.m$. Porém $x, y \in \{0, 1, 2, \ldots, m-1\}$, então $(y - x) < m$. Com isso podemos concluir que $(y - x) = 0.m = 0$, ou seja $x = y$.

Em outras palavras, a proposição anterior nos diz que o resto da divisão entre dois números inteiros é único.

Exemplo 39. Vamos encontrar a solução para a seguinte equação modular:

$$25 \equiv x \pmod 7$$

Sabemos que para x satisfazer essa equação, x dividido por 7 deve ter o mesmo resto que a divisão de 25 por 7, ou seja, deve ter resto igual a 4. Com isso temos que qualquer x que seja da forma $7n+4$, com n inteiro, é solução dessa equação. Sabemos então que temos infinitas soluções e que o conjunto solução é $\{4, 11, 18, 25, 32, \ldots\}$. Porém só existe uma solução para x em que ele pertence ao conjunto da classe de resíduos módulo 7, ou seja $\{0, 1, 2, 3, 4, 5, 6\}$, e essa solução é justamente o resto da divisão de 25 por 7. Portanto, se $x \in \{0, 1, 2, 3, 4, 5, 6\}$, então essa equação possui uma única solução que é $x = 4$.

3.4 Calculando restos de potências

Suponha que queiramos calcular o resto da divisão de 10^{135} por 7.

Você saberia fazer este cálculo?

Para resolvermos este desafio devemos utilizar as propriedades da aritmética modular. A primeira coisa a fazer é calcular as potências de 10 módulo 7:

$$\begin{array}{ll} 10 & \equiv 3 \pmod 7 \\ 10^2 & \equiv 10.10 \equiv 3.3 \equiv 9 \equiv 2 \pmod 7 \\ 10^3 & \equiv 10^2.10 \equiv 2.3 \equiv 6 \pmod 7 \\ 10^4 & \equiv 10^3.10 \equiv 6.3 \equiv 18 \equiv 4 \pmod 7 \\ 10^5 & \equiv 10^4.10 \equiv 4.3 \equiv 12 \equiv 5 \pmod 7 \\ 10^6 & \equiv 10^5.10 \equiv 5.3 \equiv 15 \equiv 1 \pmod 7 \end{array} \Longrightarrow \left[\begin{array}{ll} 10 & \equiv 3 \pmod 7 \\ 10^2 & \equiv 2 \pmod 7 \\ 10^3 & \equiv 6 \pmod 7 \\ 10^4 & \equiv 4 \pmod 7 \\ 10^5 & \equiv 5 \pmod 7 \\ 10^6 & \equiv 1 \pmod 7 \end{array}\right]$$

Portanto sabemos que $10^6 \equiv 1 \pmod 7$, vamos aproveitar essa informação para facilitar nossos cálculos:

$$10^{135} \equiv x \pmod 7$$

sabemos que $135 = 6.22 + 3$, então podemos reescrever a equação acima da seguinte maneira:

$$10^{135} \equiv 10^{6.(22)+3} \equiv 10^{6.(22)}.10^3 \equiv (10^6)^{22}.10^3 \equiv (1)^{22}.6 \equiv 6 \pmod 7$$

$$10^{135} \equiv 6 \pmod 7$$

ou seja, o "truque" para resolvermos esse problema foi encontrar uma potência de 10 que fosse congruente a 1 módulo 7.

Exemplo 40. Qual o resto da divisão de 2^{124512} por 31?

Calculando as potências de 2 módulo 31, vemos que:

$$\begin{array}{ll} 2^2 & \equiv 4 \pmod{31} \\ 2^3 & \equiv 8 \pmod{31} \\ 2^4 & \equiv 16 \pmod{31} \\ 2^5 & \equiv 32 \equiv 1 \pmod{31} \end{array}$$

também temos que $124512 = 5.(24902) + 2$, então

$$2^{124512} \equiv 2^{5.(24902)+2} \equiv 2^{5.(24902)}.2^2 \equiv (2^5)^{24902}.2^2 \equiv (1)^{24902}.2^2 \equiv 4 \pmod{31}$$

$$2^{124512} \equiv 4 \pmod{31}$$

Trabalhando com potências de potências

Agora que já sabemos encontrar os restos de divisões de potências, iremos, de maneira análoga, resolver problemas envolvendo potências de potências.

Exemplo 41. Vamos encontrar o resto da divisão de $2^{11^{98765}}$ por 31?

Pelo *Exemplo 40* sabemos que $2^5 \equiv 1 \pmod{31}$, portanto parte do cálculo já está resolvido. A segunda parte seria escrever o expoente na forma de um múltiplo de 5 mais algum resto qualquer. A única diferença entre este problema e os anteriores é que o expoente aqui também é uma potência, portanto temos que encontrar algum r tal que:

$$11^{98765} = 5.q + r$$

mas isso é o mesmo que calcular $11^{98765} \equiv r \pmod{5}$ e isso nós já sabemos fazer.

$$11 \equiv 1 \pmod{5} \Longrightarrow 11^{98765} \equiv 1^{98765} \equiv 1 \pmod{5}$$

com isso temos que:

$$11^{98765} = 5.q + 1$$

onde q seria o quociente da divisão de 11^{98765} por 5, porém nós não precisamos saber qual o valor de q para resolver nosso problema original.

$$2^{11^{98765}} \equiv 2^{5.q+1} \equiv (2^5)^q.2 \equiv (1)^q.2 \equiv 2 \pmod{31}$$

$$2^{11^{98765}} \equiv 2 \pmod{31}$$

3.5 Ordem de um Inteiro Modular

Os cálculos com potências feitos acima só foram facilmente resolvidos porque, em cada caso, descobrimos um expoente positivo para o qual a potência envolvida era congruente a 1 no módulo tomado, como por exempo:

$$10^6 \equiv 1 \pmod{7} \text{ e } 3^4 \equiv 1 \pmod{31}$$

Porém será que isto sempre é possível? Isto é, será que dados dois inteiros positivos a e m sempre existe um inteiro positivo $k \neq 0$ tal que $a^k \equiv 1 \pmod{m}$?

Definição 10. Sejam a e m dois inteiros positivos, diremos que a **ordem** de a módulo m é o menor inteiro positivo k tal que:

$$a^k \equiv 1 \pmod{m}$$

Exemplo 42. Sempre que falamos de ordem, devemos lembrar que é o *menor* k tal que $a^k \equiv 1 \pmod{m}$. Isso porque ele não é o único expoente que tem essa propriedade, por exemplo:

$$\begin{aligned} 2^5 &\equiv 1 \pmod{31} \\ 2^{10} &\equiv 1 \pmod{31} \\ 2^{105} &\equiv 1 \pmod{31} \end{aligned}$$

aqui temos que a ordem de 2 módulo 31 é igual a 5. É fácil ver que para qualquer expoente múltiplo de 5 (ou seja, da ordem) teremos a congruência igual a 1, isto é:

$$2^{5.n} \equiv (2^5)^n \equiv (1)^n \equiv 1 \pmod{31}$$

Reformulando a pergunta anterior:

Dados dois inteiros a e m, tal que $a < m$, será que a sempre terá alguma ordem módulo m?

A resposta é **NÃO**. Isso só será possível se a e m forem números primos entre si, isto é, $mdc(a, m) = 1$. Pois, como visto anteriormente, se $mdc(a, m) \neq 1$ então a não possui um inverso módulo m.

Exemplo 43. Vamos verificar se 2 possui alguma ordem módulo 6:

$$\begin{aligned} 2^1 &\equiv 2 \pmod{6} \\ 2^2 &\equiv 4 \pmod{6} \\ 2^3 &\equiv 8 \equiv 2 \pmod{6} \\ 2^4 &\equiv 16 \equiv 4 \pmod{6} \end{aligned}$$

os valores das potências de 2 módulo 6 vão se alternar entre 2 e 4. Assim, podemos concluir que nenhuma potência de 2 será congruente a 1 módulo 6, isso ocorre porque $mdc(2, 6) = 2 \neq 1$.

3.6 Sistemas de Resíduos

Definição 11. Seja $m \in \mathbb{N}$. Um **sistema completo de resíduos** módulo m é um conjunto de m inteiros que se obtém escolhendo um, e somente um, elemento em cada classe de congruencia módulo m.

Em outras palavras, o conjunto $\{r_1, r_2, \ldots, r_m\}$ é um sistema completo de resíduos módulo m se:

$$\forall a \in \mathbb{Z},\ \exists r_i,\ \text{para } i = 1, 2, \ldots, m,\ \text{tal que } a \equiv r_i \pmod{m}$$

Nota: O símbolo $\exists$ significa "existe pelo menos um".

Observação 2. Sendo $\{r_1, r_2, \ldots, r_m\}$ um sistema completo de resíduos módulo m tem-se que, se $i \neq j$, então r_i não é congruente com r_j módulo m.

Definição 12. Seja $m \in \mathbb{N}$. Um **sistema reduzido de resíduos** módulo m é um conjunto $\{r_1, r_2, \ldots, r_k\}$ de inteiros satisfazendo:

(i) $\forall a \in \mathbb{Z},\ \exists r_i,\ \text{para } i = 1, 2, \ldots, m,\ \text{tal que } a \equiv r_i \pmod{m}$

(ii) $mdc(r_i, m) = 1$ para todo $i = 1, 2, \ldots, k$

Observação 3. Da definição conclui-se imediatamente que um sistema reduzido de resíduos módulo m se obtém tomando um sistema completo de resíduos módulo m e retirando-lhe os elementos que não são relativamente primos com m.

Teorema 6. *Dado $m \in \mathbb{N}$, todos os sistemas reduzidos de resíduos módulo m têm o mesmo número de elementos.*

Demonstração 5. Sejam $\{r_1, r_2, \ldots, r_k\}$ e $\{s_1, s_2, \ldots, s_t\}$ dois sistemas reduzidos de resíduos módulo m. Vamos provar que $k = t$.

Seja r_i um elemento qualquer do primeiro sistema reduzido de resíduos módulo m. Como $mdc(r_i, m) = 1$, existe somente um elemento, digamos s_j, do segundo sistema reduzido tal que $r_i \equiv s_j \pmod{m}$. E claro que a dois elementos diferentes do primeiro sistema não pode corresponder o mesmo elemento do segundo sistema, porque se isso acontecesse eles seriam congruentes módulo m, o que não pode ocorrer. Logo, conseguimos definir uma função injetiva do primeiro sistema para o segundo, pelo que $k \leq t$. Trocando os papéis dos dois sistemas e repetindo o raciocínio concluímos que $t \leq k$. Logo, $k = t$.□

Proposição 6. *Seja $\{r_1, r_2, \ldots, r_k\}$ um sistema reduzido de resíduos módulo m e seja a um inteiro tal que $mdc(a, m) = 1$. Então $\{ar_1, ar_2, \ldots, ar_k\}$ é também um sistema reduzido de resíduos módulo m.*

Demonstração 6. Começamos por observar que $mdc(ar_i, m) = 1$ para $i = 1, 2, \ldots, k$. Vejamos que no conjunto $\{ar_1, ar_2, \ldots, ar_k\}$, não há dois elementos congruentes módulo m. De fato, se $ar_i \equiv ar_j \pmod{m}$ pelo fato de a ser relativamente primo com m, teríamos $r_i \equiv r_j \pmod{m}$, que é uma contradição. Temos então k inteiros, primos com m e não congruentes dois a dois módulo m, pois contém representantes de todas as classes de congruência módulo m cujos elementos são primos com m.□

3.7 A Função ϕ de Euler

Definição 13. Seja n um número inteiro positivo, a **função ϕ de Euler**, denotada por $\phi(n)$, é definida como sendo o número de inteiros positivos menores ou iguais a n e que são relativamente primos com n.

Exemplo 44. Na tabela abaixo apresentamos o valor de $\phi(n)$ para $n = 1, 2, \cdots, 15$.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8

Teorema 7. *Para p primo e a um inteiro positivo, temos:*

$$\phi(p^a) = p^a - p^{a-1}$$

Em particular

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

Demonstração 7. Pela definição de $\phi(n)$ sabemos que $\phi(p^a)$ é o número de inteiros positivos menores ou iguais a p^a e relativamente primos com p^a. Mas os únicos números não primos com p^a e menores ou iguais a p^a são aqueles divisíveis por p. Seja m um inteiro positivo tal que $1 \leq m \leq p^{a-1}$, então, $p \leq mp \leq p^a$, portanto $m = 1, \cdots, p^{a-1}$. Com isso temos que os múltiplos de p não-superiores a p^a são, em número, p^{a-1}. □

Exemplo 45. Vamos calcular $\phi(9)$:

$$\phi(9) = \phi(3^2) = 3^2 - 3^1 = 9 - 3 = 6$$

Definição 14. Uma **função multiplicativa** é uma função aritmética (não-nula) tal que

$$f(mn) = f(m)f(n)$$

para todo par de inteiros positivos m e n relativamente primos.

Teorema 8. *A função ϕ de Euler é multiplicativa, isto é, para $mdc(m,n) = 1$ temos:*

$$\phi(mn) = \phi(m)\phi(n)$$

Demonstração 8. Vamos distribuir os números de 1 até mn em uma matriz da seguinte maneira:

$$\begin{bmatrix} 1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ m & 2m & 3m & \cdots & nm \end{bmatrix}$$

Se na r-ésima linha, onde estão os termos $r, m+r, 2m+r, \cdots, (n-1)m+r$, tivermos $mdc(m,r) = d > 1$, então nenhum termo desta linha será primo com mn, já que esses termos são divisíveis por d. Logo, para encontrarmos os termos dessa matriz que são relativamente primos com mn, devemos olhar na linha r somente se $mdc(m,r) = 1$. Portanto teremos $\phi(m)$ linhas onde todos os elementos são coprimos com m. Agora devemos procurar entre essas $\phi(m)$ linhas, quantos elementos são coprimos com n, uma vez que todos já são coprimos com m. Como $mdc(m,n) = 1$ os elementos $r, m+r, 2m+r, \cdots, (n-1)m+r$ formam um sistema completo de resíduos módulo n, portanto a quantidade de elementos coprimos com n em cada linha é $\phi(n)$. Com isto temos que a quantidade de números coprimos com mn é igual $\phi(m)$, o números de linhas em que os elementos são primos com m, multiplicado por $\phi(n)$, o número de elementos primos com n em cada uma dessas linhas. Disto sai que:

$$\phi(mn) = \phi(m)\phi(n). \square$$

Teorema 9. *Se p e q são números primos então*

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

Basta aplicar usar os resultados dos teoremas 7 e 8 para obter:

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

Exemplo 46. Vamos calcular quanto vale $\phi(30)$. Como 30 não é uma potência de um único primo, então não basta apenas usarmos o teorema7, para isso precisamos também do teorema 8:

$$\phi(30) = \phi(2.3.5) = \phi(2)\phi(3)\phi(5) = (2-1)(3-1)(5-1) = 1.2.4 = 8$$

3.8 Teoremas de Euler e Fermat

Teorema 10. */***Teorema de Euler***/** *Seja m um número natural. Se a for um inteiro relativamente primo com m, então:*

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

Demonstração 9. Seja $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ um sistema reduzido de resíduos módulo m. Pela proposição 6, $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ é também um sistema reduzido de resíduos módulo m. Para cada elemento ar_i do segundo sistema existe apenas um elemento r_j do primeiro tal que $ar_i \equiv r_j \pmod{m}$. Multiplicando membro a membro todas estas $\phi(m)$ congruências, obtemos:

$$ar_1.ar_2.\ldots.ar_{\phi(m)} \equiv r_1.r_2.\ldots.r_{\phi(m)} \pmod{m}$$

o que é o mesmo que

$$a^{\phi(m)}.r_1.r_2.\ldots.r_{\phi(m)} \equiv r_1.r_2.\ldots.r_{\phi(m)} \pmod{m}$$

Como todos os r_i são primos com m, o seu produto também é primo com m. Então existe um inverso modular para $r_1.r_2.\ldots.r_{\phi(m)}$, multiplicando por esse inverso nos dois lados, temos:

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

Corolário 2. (Pequeno Teorema de Fermat) *Seja a um inteiro e seja p um número primo. Então se p não divide a, temos:*

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

Demonstração 10. Basta observar que se p não divide a, então $mdc(a,p) = 1$ e também temos que por p ser primo, $\phi(p) = p - 1.\square$

Exemplo 47. Agora que conhecemos esses dois teoremas vamos calcular o resto da divisão de 3^{64} por 31.

Pelo teorema de Fermat temos que $3^{30} \equiv 1 \pmod{31}$ e portanto:

$$3^{64} \equiv (3^{30})^2.3^4 \equiv 1.81 \equiv 19 \pmod{31}$$

Exemplo 48. Vejamos o que acontece quando usamos o teorema anterior para calcularmos o valor de $\phi(p)$, onde p é um número primo:

$$\phi(p) = \phi(p^1) = p^1 - p^0 = p - 1$$

3.9 Exercícios

Exercício 32. Encontre inversos módulo 11 dos seguintes valores: 122, 37, 52, 65, 86, 79, 102, 16, 117, 215.

Exercício 33. Resolva a congruência $4x \equiv 9 \ mod\ 13$.

Exercício 34. Encontre o conjunto solução das seguintes equações modulares. Dentre as soluções encontradas, qual delas está no sistema completo de resíduos apresentado na *Definição 9* na página 33?

a) $17 \equiv x \pmod 3$

b) $30 \equiv x \pmod 4$

c) $12 \equiv x \pmod 5$

Exercício 35. Calcule o resto das divisões abaixo, assim como o conjunto solução de suas respectivas equações modulares.

a) $10^{65} \div 7$, equação: $10^{65} \equiv x \pmod 7$.

b) $3^{78} \div 7$, equação: $3^{78} \equiv x \pmod 7$.

c) $2^{7987668} \div 7$, equação: $2^{7987668} \equiv x \pmod 7$.

d) $2^{90} \div 13$, equação: $2^{90} \equiv x \pmod{13}$.

Exercício 36. Calcule o resto da divisão por 31 das seguintes potências:

a) $2^{13^{98765}}$

b) $64^{3^{9876}}$

c) $2^{14^{45231}}$

Exercício 37. Calcule a ordem de:

a) 3 módulo 7.

b) 2 módulo 11.

c) 5 módulo 31.

d) 7 módulo 43.

Exercício 38. Mostre que se a e m são inteiros positivos pares, então nenhuma potência de a é congruente a 1 módulo m.

Exercício 39. Determine a ordem de cada um dos inteiros a, tal que $1 \leq a \leq 10$, módulo 11

Exercício 40. Determine a ordem de cada um dos inteiros a, tal que $1 \leq a \leq 11$, módulo 12. Lembre-se que alguns destes inteiros nem sequer admitem uma ordem módulo 12. Você pode começar por descobrir quais são e assim nem sequer precisará calcular suas potências.

Exercício 41. Seja p um primo positivo e a um inteiro que não é divisível por p. Digamos que k é a ordem de a módulo p.

a) Explique porque $k \leq p - 1$

b) Seja r o resto da divisão de $p - 1$ por k. Mostre que, como $a^{p-1} \equiv a^k \equiv 1 \pmod{p}$, então:

$$a^r \equiv 1 \pmod{p}$$

c) Lembrando que $0 \leq r \leq k - 1$, mostre que $r = 0$

d) Conclua que a ordem de a é um divisor de $p - 1$

Exercício 42. Encontre o valor da função ϕ para os seguintes números: 21, 35 e 55.

Exercício 43. Calcule o resto das seguintes divisões utilizando o Teorema de Fermat

a) 3^{98745} por 43

b) 3^{1034^2} por 1033

c) 2^{41048^2} por 41047

d) $3^{19!}$ por 307

Exercício 44. Calcule o resto das seguintes divisões utilizando o Teorema de Euler

a) 2^{495} por 15841

b) 2^{41045} por 41041

c) 2^{77} por 2465

Capítulo 4

Criptografia RSA

4.1 Introdução

A partir da década de 70 foi desenvolvida uma nova ideia de criptografia, a criptografia assimétrica. Diffie e Hellman a criaram e depois outros 3 cientistas as colocaram em prática, Ronald L. Rivest, Adi Shamir, e Leonard Adleman em 1977. Tal sistema se chama RSA. Esse método é diferente de outros, pois assume chave pública e chave confidencial, ou seja, quando se criptografa algo uma parte da mensagem é de conhecimento de todos e outra parte é de conhecimento de quem recebe. Estudaremos aqui todos os passos da criptografia RSA. A motivação do estudo da aritmética modular nos dias anteriores é a aplicação que se encontra no RSA. Tal conhecimento é fundamental para o desenvolvimento deste sistema.

Resumindo o processo utilizado:

- Primeiramente escolhemos dois primos distintos muito grandes p e q e calculamos o produto $n = p \cdot q$;
- codificamos a mensagem usando n;
- para decodificar uma mensagem usamos p e q;
- n pode ser tornado público;
- p e q devem ser mantidos em segredo;
- quebrar o RSA consiste em fatorar n, algo que pode levar muito tempo se n for grande.

4.2 Pré-Codificação

Nosso objetivo é enviar uma mensagem de modo que apenas as pessoas que queremos que recebam a entendam. Como nossas mensagens são formadas essencialmente por letras e nós estamos trabalhando com números, nosso primeiro passo é transformar os caracteres em números. Este processo é chamado de pré-codificação e abaixo apresentamos um exemplo que será usado no decorrer do capítulo.

Pré-codificação do alfabeto ou **Mapa de caracteres**

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

Geralmente as mensagens não incluem apenas letras e, portanto, outros caracteres também precisam ser pré-codificados, como, por exemplo, números e símbolos como $*$, (,), $+$, $-$, /, \$, @, !, ?, &, etc., porém quanto mais caracteres pré-codificados, maiores serão as contas que precisaremos fazer. Por esta razão, utilizaremos apenas a tabela acima daqui em diante.

Exemplo 49. Pré-codifique a palavra **BRINCANDO** utilizando a tabela acima.

Fazendo a associação mostrada no mapa de caracteres, temos que a palavra BRINCANDO transforma-se em

$$12281924131124 1425$$

Cuidados

A pré-codificação mostrada na tabela acima é apenas um exemplo. Você mesmo pode criar uma pré-codificação, porém precisa tomar alguns cuidados:

1. É preciso garantir que a sua mensagem em forma numérica não abra margens para mensagens distintas na sua forma alfabética. Por exemplo, suponha que $A \mapsto 1$ e $S \mapsto 11$ e temos a pré-codificação 1111. A mensagem era $AAAA$, ASA, SAA, SS ou AAS? No nosso caso, o fato de cada caractere ser representado por um número de dois algarismos garante que situações como esta não ocorrerão. Contudo existem muitas formas de garantir que isto não ocorra, é uma questão de usar a imaginação!

2. Uma alternativa para consertar o problema anterior seria fazer $A \mapsto 01$ e $S \mapsto 11$. Ao pré-codificar a palavra ASA obteríamos 011101. Como iremos fazer contas com esse número, o primeiro 0 deixaria de fazer sentido e trabalharíamos apenas com 11101. Logo, os números não podem começar com o algarismo 0.

4.3 Codificação

Escolhendo o n

Como foi visto na seção anterior, a nossa mensagem foi transformada em números. Agora vamos analisar como será feito o envio dessa mensagem de uma maneira segura. Precisamos escolher um número n que será a nossa chave pública. E esse n deve ser tal que $n = p \cdot q$, em que p e q são números primos.

Exemplo 50. Seja $n = 221$, então $p = 17$ e $q = 13$; $n = 899$, $p = 29$, $q = 31$

Agora vamos tomar um n para criptografar nossa palavra em questão. Seja $n = 55$ tal que $p = 5$ e $q = 11$. A escolha de valores pequenos para p e q foi feita de modo a simplificar as nossas contas, mas o que faremos vale para n tão grande quanto você consiga imaginar.

Sobre o p e q

Eles são chamados de parâmetros. Nossos números p e q geralmente são números primos. Estes são escolhidos de forma que facilite os cálculos do $\phi(n)$ que veremos a seguir.

A separação em blocos

Agora, já que relacionamos o nosso alfabeto com certos números, vamos separar algumas palavras em blocos. Mas o que isso significa? Dado uma correspondência de letras com os números, nossas palavras ficam definidas através de números. Como foi mostrado na seção de Pré Codificação, BRINCANDO se escreve como:

$$122819241311241425.$$

E separando em blocos obtemos:

$$1-22-8-19-2-4-1-31-12-4-14-2-5.$$

Vamos fazer mais alguns exemplos usando a correspondência letras-números dada na seção anterior:

1. MATEMÁTICO:

$$23113015231112191325.$$

Separando em blocos, obtemos:

$$2-31-1-30-15-2-3-11-1-21-9-13-1-1.$$

2. CRIPTOGRAFIA:

$$13281926302517281116191 1.$$

Separando em blocos, obtemos:

$$1-32-8-19-2-6-30-25-1-7-28-1-11-6-19-1-1.$$

Conseguem observar um certo padrão nos nossos blocos?

Cuidados:

Este padrão que foi observado é o tamanho dos blocos que separamos, pode-se observar que cada bloco não passa de 55. Generalizando, isto nos indica que o número do bloco não pode passar do n escolhido. Além do mais, nenhum bloco pode começar com 0, pois isso pode nos complicar mais para frente.

Lembrando que a separação em blocos não é única, podemos fazê-la da maneira que quisermos, desde que esteja de acordo com o que foi dito anteriormente.

Transformando a mensagem

Agora nós iremos pôr a mão na massa e transformar os blocos obtidos anteriormente em outros blocos nos quais apenas quem queremos que receba a mensagem consiga decifrar.

Na seção anterior, nossa mensagem inicial separada em blocos ficou

$$1 - 22 - 8 - 19 - 2 - 4 - 31 - 12 - 14 - 5.$$

Precisamos criptografar estes blocos antes de enviar e, para isto, precisaremos da chave pública $n = 55$, escolhida na seção anterior.

Para construir a chave pública n, escolhemos dois primos distintos p e q e fizemos $n = p \cdot q$. Assim, pelo Teorema 9, página 38, temos que

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

Quanto maior o valor de n mais difícil é calcular $\phi(n)$, pois para isto precisamos da fatoração de n em números primos.

Exemplo 51. Calcule $\phi(55)$.

$$\phi(55) = \phi(5 \cdot 11) = 4 \cdot 10 = 40.$$

Nosso próximo passo é escolher um número d que seja inversível $\pmod{\phi(n)}$. Vimos que uma condição para que d seja inversível $\pmod{\phi(n)}$ é que seja coprimo com $\phi(n)$, isto é, que

$$mdc(d, \phi(n)) = 1.$$

Após esta escolha, elevamos cada bloco da mensagem à potência d e utilizamos o resto da divisão por n para ser o bloco criptografado. Note que o d deve ser o mesmo para TODOS os blocos. À primeira vista, parece ser muito complicado, mas vejamos como isso acontece com um exemplo.

Exemplo 52. Vamos criptografar o terceiro bloco de nossa mensagem: 8.

Já temos que $\phi(55) = 40$. Assim, resta escolhermos um d tal que $mdc(d, 40) = 1$. Vamos escolher

$$d = 7.$$

Verifique que, de fato, 7 e 40 são coprimos. Agora precisamos do resto da divisão de 8^7 por $n = 55$, ou seja, calcular $0 < r < 55$ tal que

$$8^7 \equiv r \pmod{55}.$$

Existem diversas maneiras de fazer isto e algumas delas estão no apêndice na página 51. Fazendo as contas, concluímos que

$$r = 2.$$

Portanto, 8, que era o terceiro bloco, se transforma em 2. Indicaremos isto por

$$C(8) = 2.$$

Veja o Exercício 48.

Pela notação introduzida anteriormente, podemos sintetizar o que foi discutido da seguinte maneira:

Definição 15. Fixados a chave pública n e o número d tal que $mdc(d, \phi(n)) = 1$. Seja b um bloco da mensagem. O **bloco criptografado** $C(b)$ é tal que $0 < C(b) < n$ e

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

Cuidados:
Na hora de enviar a mensagem, ela deve estar divida em blocos, caso contrário, a pessoa que receber a mensagem não conseguirá fazer o processo inverso para ler a mensagem original.

4.4 Decodificação

Após codificar a mensagem o destinatário deverá receber o par (m, d), onde "m" é a mensagem e "d" o valor utilizado anteriormente na codificação. Resta agora decodificar esta mensagem, se você fez corretamente a codificação dos blocos anteriormente propostos obteve a seguinte mensagem:

$$1 - 33 - 2 - 24 - 18 - 49 - 1 - 26 - 23 - 49 - 9 - 18 - 25$$

Talvez você consiga arriscar qual o cálculo utilizado para decodificar a mensagem, basta tomar "e", o inverso multiplicativo de d módulo $\phi(n)$, e elevar cada um dos blocos da mensagem transmitida a esta potência. No nosso caso devemos calcular o número que satisfaça

$$7e \equiv 1 \pmod{40}$$

Note que 23 satisfaz a relação acima, pois:

$$7 \cdot 23 \equiv 161 \equiv 1 \pmod{40}$$

Falta agora calcular cada uma das potências dos blocos codificados.

$$\begin{array}{rlrl} 1^{23} \equiv & (\text{mod } 55) & 33^{23} \equiv & (\text{mod } 55) \\ 2^{23} \equiv & (\text{mod } 55) & 24^{23} \equiv & (\text{mod } 55) \\ 18^{23} \equiv & (\text{mod } 55) & 49^{23} \equiv & (\text{mod } 55) \\ 26^{23} \equiv & (\text{mod } 55) & 23^{23} \equiv & (\text{mod } 55) \\ 9^{23} \equiv & (\text{mod } 55) & 25^{23} \equiv & (\text{mod } 55) \end{array}$$

Ao fazer os cálculos acima e substituir os respectivos blocos da mensagem enviada retornaremos justamente aos blocos que separamos, antes mesmo de realizar a codificação. Para decifrar a mensagem falta juntar os blocos e utilizar o mapa de caracteres que definimos ao início deste processo.

4.5 Por que funciona?

Note que estamos fazendo todas estas contas acreditando que o processo inverso (decodificação) irá nos levar novamente a mensagem numérica, para então utilizarmos o "mapa de caracteres", mas em nenhum momento mostramos que isto funciona. Mas o que significa mostrar que o processo funciona?

Denotemos novamente cada bloco com a letra "b", sejam também "C" e "D" os processos de codificação e decodificação respectivamente. Primeiramente codificamos os blocos ($C(b)$), em seguida os decodificamos ($D(C(b))$) e para que tudo o que fizemos dê certo o resultado final destes cálculos deve ser o mesmo bloco b, matematicamente falando:

$$D(C(b)) \equiv b \pmod{n}$$

Mostrar que a relação acima é verdadeira para quaisquer b é o mesmo que mostrar que o RSA funciona. Note que

$$D(C(b)) = b^{de},$$

além disto, d e e são inversíveis módulo $\phi(n)$, ou seja

$$de = k\phi(n) + 1.$$

Isto seria facilmente provado se soubessemos que $mdc(b, n) = 1$, bastaria utilizar o Teorema de Euler visto na página 39, porém em nenhum momento tomamos este cuidado. Sabemos quanto vale $\phi(n)$, então podemos escrever

$$de = k(p-1)(q-1) + 1.$$

Observe agora as seguintes relações.

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

Estas relações são verdadeiras, pois nos casos em que b é comprimo com p ou q basta usar o pequeno teorema de Fermat (corolário 2, página 39) caso não sejam coprimos, b é um múltiplo de p ou q e sendo assim ambos os lados da relação serão nulos, portanto a equivalência ainda é válida.

Utilizando a definição de congruência modular nas relações acima podemos facilmente verificar que:

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

Portanto o método de criptografia RSA funciona!

4.6 Segurança

Imagine que, de alguma forma, você foi capaz de interceptar uma mensagem da sua namorada, cujo destinatário é o ex-namorado dela. Como todo bom namorado, nestas horas

o ciúmes fala mais alto e o único objetivo da sua vida, no momento, é descobrir o que está escrito nesta mensagem.

Você sabe que o método de criptografia empregado foi o RSA e agora agradece por ter sacrificado uns dias das suas férias pelo "Brincando de Matemático".

Ao lembrar do que lhe foi ensinado naquela época, pôde diferenciar claramente a mensagem e o valor "d" empregado na codificação. Se você descobrir quem é o "e" poderá, sem grandes dificuldades, decifrar a mensagem.

Lembrando que o número e pode ser calculado, pois este é o inverso de d módulo $\phi(n)$, também que $\phi(n) = (p-1)(q-1)$, e, além disto, que o valor de n pode ser obtido, pois o RSA é um método de criptografia de chave pública, você percebe que todas as suas preocupações se resumem a fatorar n.

Agora você se sente muito mais motivado e sem perder tempo vai descobrir qual a chave pública. Após alguns minutos de pesquisa, você descobre que a chave pública é:

$$3107418240490043721350750035888567930037346022842727545720161948$$
$$8232064405180815045563468296717232867824379162728380334154710731 0$$
$$8501919548529007337724822783525742386454014691736602477652346609$$

Então você logo percebe que é mais fácil aprender a confiar na sua namorada do que decifrar a mensagem que ela enviou para o "ex".

Na história acima podemos perceber que a maior parte da segurança no método RSA está relacionada à fatoração da chave pública. Apenas falando pode parecer uma tarefa simples, principalmente considerando o auxílio de computadores, mas na realidade isto pode vir a ser uma grande complicação e isto só depende da escolha da chave pública.

Não existe nenhum algoritmo de fatoração que seja útil para um número qualquer, normalmente, o tempo tomado para o algoritmo decompor o número depende dos fatores deste, se são grandes ou pequenos, próximos ou distantes um do outro. É possível tomar primos que tornem a maioria dos métodos de fatoração existentes ineficazes.

Na fatoração do número disposto logo acima, foram necessários 8 computadores trabalhando simultaneamente durante 5 meses para encontrar quais os dois primos que o compõe. Atualmente são utilizados números com 3, 4 ou 5 vezes mais casas decimais do que este, ou seja, algo em torno de 1000 casas decimais, uma boa escolha do valor de n pode garantir que a criptografia será segura durante alguns anos.

4.7 Exercícios

Exercício 45. Utilizando o mapa de caracteres, pré-codifique **seu nome** e a palavra **MATEMATICO**.

Exercício 46. Crie seu próprio sistema de pré-codificação e pré-codifique **seu nome** e as palavras **BRINCANDO** e **MATEMATICO**.

Exercício 47. Agora, pegue o **seu nome** que foi convertido em números no exercício anterior e separe-o em blocos.

Exercício 48. Criptografe os blocos da mensagem, ou seja, transfome nossa mensagem

$$1 - 22 - 8 - 19 - 2 - 4 - 31 - 12 - 14 - 5$$

em

$$C(1) - C(22) - 2 - C(19) - C(2) - C(4) - C(31) - C(12) - C(14) - C(5).$$

Note que já calculamos que C(8)=2 no Exemplo 51.

Exercício 49. Criptografe agora os blocos de **seu nome**. Se quiser, escolha outro d que seja invertível mod 40.

Capítulo 5

Apêndice

5.1 Como calcular restos na calculadora?

Vamos, a partir de alguns exemplos, mostrar como calcular o resto da divisão de dois números utilizando a calculadora.

Exemplo 53. Calcule o resto da divisão de 8^7 por 55.

Este cálculo foi utilizado no capítulo 4 para determinar $C(8)$. Para fazer 8^7 na calculadora basta apertar os botões

$$8\,\hat{}\,7\,=$$

e obterá 2097152. Ao fazer a divisão de 2097152 por 55, você obterá

$$2097152 \div 55 = 38130,03636.$$

Para obter o resto, subtraia a parte inteira deste número, ou seja, subtraia o número que vem antes da vírgula,

$$38130,03636 - 38130 = 0,0363636.$$

Agora multiplique o resultado pelo divisor, ou seja, multiplique por 55,

$$0,0363636 \times 55 = 1,999998.$$

Como a calculadora trabalha com aproximações, concluímos que o resto da divisão de 2097152 por 55 é 2.

Exemplo 54. Calcule o resto da divisão de 31^7 por 55.

Este resto é o $C(31)$ na mensagem codificada no capítulo 4. Ao fazer na calculadora 31^7 obtemos

$$2.751261411 \times 10^{10},$$

ou seja, o número é tão grande que precisou ser transformado em notação científica. Neste caso, estamos impossibilitados de continuar, pois desconhecemos a parte inteira deste número. Para contornar esta situação, faremos o cálculo do resto utilizando propriedades da congruência.

Uma maneira que envolve poucas contas é escrever o expoente na base 2, ou seja, como soma de potências de 2. Em nosso caso,

$$7 = 2^0 + 2^1 + 2^2.$$

Assim, queremos $0 \leq r < 55$ tal que

$$31^7 \equiv r \pmod{55}.$$

$$31^7 \equiv 31^{2^0+2^1+2^2} \equiv 31^{2^0} \cdot 31^{2^1} \cdot 31^{2^2} \equiv 31 \cdot 31^2 \cdot 31^4 \pmod{55}.$$

Agora sim, utilizando as técnicas do exemplo anterior, obtemos

- $31 \equiv 31 \pmod{55}$,
- $31^2 \equiv 26 \pmod{55}$,
- $31^4 \equiv (31^2)^2 \equiv 26^2 \equiv 16 \pmod{55}$.

Portanto,

$$31^7 \equiv 31 \cdot 26 \cdot 16 \equiv 12896 \equiv 26 \pmod{55}.$$

Logo, o resto da divisão de 31^7 por 55 é 26.

A vantagem de utilizar a base 2 está no fato de conseguir as potências de forma fácil, uma vez que se é sabido que

$$31^{2^m} \equiv q \pmod{55}.$$

Para descobrir 31^{2^k}, com $k > m$, basta fazer $q^{2^{k-m}}$, pois

$$31^{2^k} \equiv \left(31^{2^m}\right)^{2^{k-m}} \equiv q^{2^{k-m}} \pmod{55}.$$

Referências Bibliográficas

[1] ALVES, E. *Teoria dos números: exercícios de congruência linear*. Disponível em: <http://ellalves.net.br/textos/conteudo/21/teoria_dos_numeros_exercicios_de_congruencia_linear>. Acesso em: 19 mai. 2014.

[2] BIGGS, N. L. *Codes: An Introduction to Information Communication and Cryptography*, Londres: Springer, 2008

[3] COUTINHO, S. C. . *Criptografia*. OBMEP, 2008.

[4] DIAS, J. L. Desenvolvimento Histórico da Criptografia. *Revista do Centro Universitário Planalto do Distrito Federal*, Distrito Federal, v. 3, n. 3, 2006. Disponível em: <www.cesubra.edu.br/revista/vol3n3.pdf#page=12>. Acesso em: 01 mai. 2014.

[5] Fernando. *Matrizes e Criptografia*. Vitória da Conquista, 2001. Disponível em: <educacaomatematica2010.blogspot.com.br/2011/01/matrizes-e-criptografia.html>. Acesso em: 20 abr. 2014.

[6] HEFEZ, Á. *Elementos de Aritmética*. 2. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2005.

[7] MALAGUTTI, P. *Atividades de Contagem a partir da Criptografia*. OBMEP, 2009.

[8] MILIES, C. P.; COELHO, S. P. *Números Uma Introdução á Matemática*. São Paulo: Editora da Universidade de São Paulo, 2006.

[9] NASCIMENTO, R. do. Criptografia tradicional simétrica e criptografia de chave pública: Análise das vantagens e desvantagens. *Revista do Centro Universitário Planalto do Distrito Federal*, Distrito Federal, v. 2, n. 4, 2005. Disponível em: <www.cesubra.edu.br/revista/vol2n4.pdf#page=67>. Acesso em: 29 abr. 2014.

[10] RODRIGUES, R. *3ª lista de exercícios: Congruência*. Disponível em: <http://www.robson.mat.br/UNISUZ/%C3%81lgebra_I/3%C2%AA%20Lista%20de%20Exerc%C3%ADcios%20-%20Congru%C3%AAncia.pdf>. Acesso em: 19 de mai. de 2014.

[11] RUSSO, W. Satélite brasileiro geoestacionário de defesa e comunicações. *Ciência e Cultura*, São Paulo, v. 65, n. 4, 2013. Disponível em: <cienciaecultura.bvs.br/scielo.php?pid=S0009-67252013000400002&script=sci_arttext>. Acesso em: 04 mai. 2014.

[12] SILVEIRA, A. S.; FALEIROS, A. C. Criptografia de Chave Pública – O Papel da Aritmética em Precisão Múltipla. In: ENCONTRO DE INICIAÇÃO CIENTÍFICA E PÓS-GRADUAÇÃO DO ITA, 11, 2005, São José dos Campos, *Anais...* Disponível em: <www.bibl.ita.br/xiencita/Artigos/Fund05.pdf>. Acesso em: 30 abr. 2014.

[13] SILVEIRA, F.; WINTERLEWW, P. *Matrizes e Criptografia*. Porto Alegre, 2012. Disponível em: <pucrs.br/famat/demat/facin/algainf/criptografia.pdf>. Acesso em: 20 abr. 2014.

[14] SIQUEIRA, L. *Matemática discreta*. Disponível em: <http://www.ptmat.fc.ul.pt/∼lsequeir/md/2004-2005/teoricas/Mar02print.pdf>. Acesso em: 19 de mai. 2014.