Universidade de Lisboa

Faculdade de Ciências

Departamento de Matemática

Criptografia e Matemática

Victor Manuel Calhabrês Fiarresga

Mestrado em Matemática para Professores

Setembro de 2010

Universidade de Lisboa

Faculdade de Ciências

Departamento de Matemática

Criptografia e Matemática

Victor Manuel Calhabrês Fiarresga

Dissertação realizada sob a supervisão do

Professor Doutor Jorge Nuno Monteiro de Oliveira e Silva,

Professor Auxiliar da

Faculdade de Ciências da Universidade de Lisboa

Mestrado em Matemática para Professores

Setembro de 2010

Aos meus pais,

à Berta e Isabel

Agradecimentos

Agradeço:

Ao meu orientador, Professor Doutor Jorge Nuno Silva, todo o apoio na elaboração desta tese.

À Isabel Fiarresga, minha mulher, pela paciência e por não ter deixado, na parte não científica, que algumas gralhas grasnassem.

À escola básica 2, 3 Sophia de Mello Breyner Andresen pelo facto de ter proporcionado a frequência da parte curricular deste mestrado.

Aos meus pais e sogra por todo o apoio prestado.

Victor Manuel Calhabrês Fiarresga

Belas, Setembro 2010

Criptografia e Matemática

Resumo

Neste trabalho, fazemos um pequeno estudo sobre as origens da criptografia e alguns criptossistemas.

No primeiro capítulo, definimos criptografia e introduzimos alguns conceitos que lhe estão inerentes, a saber: alfabeto de cifra e cifras de substituição, transposição, monoalfabéticas e polialfabéticas.

No segundo capítulo, fazemos uma breve história da criptografia, em que procuramos abordar as suas origens, bem como, os seus momentos mais marcantes ao longo do tempo.

A principal ferramenta da criptografia é a Matemática, assim no terceiro capítulo, são estudados alguns resultados da Matemática, que são de extrema importância para o funcionamento da criptografia. Aqui não podemos deixar de salientar a importância actual da Teoria dos Números.

No quarto capítulo, estudamos os criptossistemas simétricos e assimétricos. Definimos cada uma das cifras e através de exemplos simples mostramos como elas são aplicadas.

No quinto capítulo, abordamos as assinaturas digitais. Aqui são estudados três esquemas de assinaturas digitais: RSA, ELGamal e Digital Standard. Mais uma vez, recorremos a exemplos simples para mostrar a sua aplicabilidade.

Por último, no sexto capítulo, fazemos a conclusão deste trabalho, onde referimos que a criptografia pode ser utilizada para criar gosto, hábitos de trabalho e persistência nos alunos dos Ensinos Básico e Secundário, de uma forma diferente.

Cryptography and Mathematics

Abstract

In this work, we do a small study on the origins of some cryptography and cryptosystems.

In the first chapter, we define encryption and introduce some concepts that would arise, namely, alphabet cipher and substitution, transposition, and monoalphabetic and polyalphabetic ciphers.

In the second chapter, we present a brief history of cryptography; we seek to address its origins, as well as their most memorable moments over time.

The main tool of cryptography is the mathematics, so in the third chapter, are studied some results of mathematics, which are of extreme importance for the purpose of cryptography. Here we can not fail to emphasize the current importance of the Theory of Numbers.

In the fourth chapter, we study the symmetric and asymmetric cryptosystems. We define each one of the ciphers and through simple examples show how they are applied.

In the fifth chapter we discuss the digital signatures. Here we study three schemes of digital signatures: RSA, ElGamal and Digital Standard. Again, we resort to simple examples to show its applicability.

Finally, in chapter six, we conclude this work, where we mentioned that cryptography can be used to create enjoyment, work habits and persistence in students of basic and secondary school in a different way.

Índice

Lista de Tabelas

Lista de Figuras

Introdução

Quando, em 1940, G. H. Hardy declarou que a melhor matemática é, em grande parte, inútil, acrescentou logo que isso não é necessariamente uma má coisa: «As matemáticas a sério não têm qualquer efeito na guerra. Ninguém ainda descobriu que qualquer aplicação guerreira fosse servida pela Teoria dos Números».

Singh, S. *A Solução do Último Teorema* de Fermat, 1997.

Hoje podemos dizer que Hardy estava errado? Não! O que Hardy afirmou, só prova uma coisa: que a Matemática tem estado muitas vezes à frente do Tempo – umas vezes mais longe, outras mais perto! No entanto, quando menos se espera, pode entrar nas nossas vidas sem pedir licença, para o Bem e para o Mal. Foi o que aconteceu com a Teoria dos Números a partir do último quartel do século passado.

Quando da abordagem do tema da criptografia e o seu relacionamento com a Matemática, havia alguma noção da riqueza do tema, no entanto este relacionamento ultrapassou as expectativas pela tamanha grandeza que evidenciou. Devido ao secretismo que o tema envolve por parte de estados e empresas a noção dos seus limites continua a não estar ao nosso alcance. Contudo a aprendizagem efectuada aquando do desenvolvimento destes assuntos contribuiu para um enriquecimento quer pessoal quer profissional.

Ao longo do texto, são dados exemplos que ajudam numa melhor compreensão dos diversos métodos de encriptar e desencriptar mensagens, para tal utilizamos números primos com o máximo de dois dígitos; pois o objectivo, não é transcrever a realidade do mundo da criptografia, onde se utilizam números primos com centenas de algarismos, mas dar uma simples visão desse mundo.

No capítulo um, damos a noção de criptografia e fazemos a distinção entre criptografia e esteganografia, a qual muitas vezes não é clara! Abordamos alguns tipos de criptografia, simétrica e assimétrica. Dentro da criptografia

simétrica, fazemos a distinção entre cifra de substituição e cifra de transposição. Falamos também das distinções entre o trabalho do criptógrafo e do criptanalista. Serão dadas, como exemplo, algumas cifras para nos familiarizarmos com o verdadeiro papel da criptografia – ocultar a informação! Esclarecemos ainda quais os objectivos da criptografia.

No capítulo dois, fazemos uma breve, mas esclarecedora, História da Criptografia. A compreensão da evolução histórica de um tema, ajuda-nos não só a entender a sua importância para a Humanidade; como também, o seu desenvolvimento ao longo do tempo. E neste caso, a criptografia adaptou-se sempre ao sucesso dos criptanalistas.

No terceiro capítulo, expomos algumas partes da Matemática, que contribuíram para o desenvolvimento da Criptografia: estruturas algébricas, teoria dos números, problema do logaritmo discreto, testes de primalidade, algoritmos de factorização, etc. Embora a maior parte da Matemática, não fosse criada para esse efeito; a Criptografia viu nela e continua a ver, uma aliada insubstituível!

No quarto capítulo, falamos de alguns criptosistemas que nos pareceram ser os mais importantes; não só pela sua importância histórica, como também, alguns, pela segurança revelada ao longo do tempo.

No capítulo cinco, as assinaturas digitais são abordadas, de modo, a explicar um futuro para todos, que está já ao virar da esquina! Assinar um contrato, com números e não com a nossa querida assinatura que era reconhecida pelo notário, será motivo de desconfiança mesmo para quem ensina Matemática, quanto mais, para o cidadão comum!

Por último, fazemos um balanço do que foram estes dois anos de trabalho e tecemos algumas considerações sobre o Ensino da Matemática, neste momento, no nosso país. Lançamos ainda um desafio, por analogia com um outro, que a criptografia, embora pareça de enorme complexidade, tem muitos assuntos, que com as devidas adaptações podem ser abordados quer no Ensino Básico quer no Secundário, o que permitiria desenvolver nos nossos jovens, não só o gosto pela matemática, como ajudar a estimular a capacidade de resiliência.

Capítulo 1

Criptografia

A necessidade de sigilo na comunicação escrita deve ser tão velha como a própria escrita.

Ao longo dos tempos, com a evolução da tecnologia e consequentemente dos meios de comunicação, a complexidade de ocultar a mensagem escrita tem vindo a aumentar de uma forma exponencial. Se há necessidade de guardar um segredo, então, em princípio, existe alguém que o quer saber. É este jogo do gato e do rato que a humanidade vem praticando desde há muito tempo.

A ocultação de uma mensagem pode ser feita através da esteganografia, nome que deriva de duas palavras gregas: *steganos* que significa coberto e *graphien* que significa escrever. Ou seja, como a origem do próprio nome indica, esta técnica consiste em ocultar a existência de uma mensagem. Esta técnica já era praticada no século V a. C. e continua a sê-lo nos nossos dias. No entanto, padece de uma enorme fragilidade – se for interceptada, o seu conteúdo, logo no momento, fica claro como água.

Um dos exemplos mais caricatos da esteganografia, foi relatado por Heródoto que registou o modo como Histieu transmitiu uma mensagem a Aristágoras de Mileto. Histieu rapou a cabeça de um indivíduo, escreveu no seu couro cabeludo a mensagem que queria enviar, esperou que o cabelo voltasse a crescer e, enviou-o em viagem até ao seu destinatário. Este quando chegou, rapou novamente a cabeça e mostrou a mensagem a Aristágoras de Mileto.

Tão velha, mas com o mesmo objectivo primordial, ocultar a mensagem, – a criptografia - que também deriva de dois vocábulos gregos: *kryptos*, que significa oculto e *graphien* cujo significado já é conhecido, não esconde a existência da mensagem, apenas oculta o seu significado. De um modo geral, se a mensagem cair nas mãos de um intruso, este ao lê-la, não a compreenderá. Só o remetente e o destinatário, em princípio, através de um acordo pré-estabelecido, é que têm acesso ao significado da mensagem. O termo criptografia é usado muitas vezes como sinónimo de criptologia,

abrangendo, desta forma, a criptanálise que tem por função descobrir os segredos, quebrar a confidencialidade entre emissor e receptor.

O trabalho do criptógrafo consiste em transformar um texto simples (mensagem original antes da criptação) num texto em cifra (mensagem após ser criptada), o criptanalista tenta fazer o inverso. Foram estes homens que colocaram as suas inteligências ao serviço de reis, de nações, do Bem e do Mal. Alguns tiveram uma importância fulcral no percurso da História da Humanidade, mas trabalharam no anonimato e alguns permaneceram anónimos.

Até à década de 70, do século passado, as cifras eram todas simétricas; isto é, a chave para encriptar e desencriptar uma mensagem era a mesma e o seu uso era mais político e militar. Só há trinta e três anos, é que se começou a utilizar a cifra assimétrica, para a qual existem duas chaves: uma pública, que serve para encriptar a mensagem; e uma outra, a privada que serve para a desencriptar.

Com a utilização generalizada do computador pelo cidadão comum, a criptografia assume um papel fundamental na nossa vida diária: o código do multibanco e a assinatura digital no cartão do cidadão, são apenas dois, dos muitos exemplos que poderíamos dar. Neste momento, os objectivos da criptografia são:

- Confidencialidade – mantém o conteúdo da informação secreto para todos excepto para as pessoas que tenham acesso à mesma.
- Integridade da informação – assegura que não há alteração, intencional ou não, da informação por pessoas não autorizadas**.**
- Autenticação de informação – serve para identificar pessoas ou processos com quem se estabelece comunicação.
- Não repudiação – evita que qualquer das partes envolvidas na comunicação negue o envio ou a recepção de uma informação.

A criptografia tem utilizado diferentes cifras ao longo do tempo. Existem cifras de transposição e cifras de substituição. Enquanto na cifra de transposição cada letra conserva a sua identidade, mas muda de posição dentro da

mensagem; na cifra de substituição, cada letra conserva a sua posição, mas é substituída por uma outra letra ou símbolo.

Quando utilizamos a criptografia por transposição, a mensagem original é transformada num anagrama. Por exemplo, a palavra **SER**, pode ser cifrada em 5 (3! -1) anagramas distintos: **RES, RSE, ERS, ESR** e **SRE.** Já a palavra **TEORIA** pode originar 719 (6! – 1) anagramas diferentes. Se considerarmos a frase: **RONALDO REGRESSA AO SPORTING**, existem mais de $1{,}87 \times 10^{20}$ formas de combinar as letras desta curta frase ($\frac{25!}{4! \times 4! \times 2 \times 3! \times 2 \times 3!}$). À medida que o número de letras aumenta no texto, o número de combinações das letras trocadas de uma forma aleatória aumenta de uma forma exponencial, o que dificulta a recuperação da mensagem original por qualquer intruso. Mais adiante apresentaremos outros exemplos da utilização da cifra de transposição.

Para cifrarmos uma mensagem por substituição, um dos primeiros passos é fazer corresponder o alfabeto comum a um alfabeto em cifra. Nas cifras de substituição monoalfabéticas, que foram bastante eficientes durante séculos, o alfabeto simples é: reordenado, substituído por números ou outros caracteres; criando desta forma uma função bijectiva. Após escrevermos o texto original, substituímos cada letra, pela letra ou símbolo correspondente do alfabeto em cifra; criando, desta forma, um texto em cifra que, em princípio, só será entendido pelo seu verdadeiro destinatário. Dizemos em princípio, porque ao longo da História muitas foram as mensagens que foram interceptadas e o curso dos acontecimentos alterados.

A quebra das chaves das cifras de substituição monoalfabéticas, através da análise de frequências – método que será exposto mais à frente -, levou ao aparecimento das cifras de substituição polialfabéticas; neste tipo de cifras utilizam-se diversos alfabetos de cifra; ou seja, na passagem do texto original para o texto em cifra, cada uma das letras pode ser substituída ao longo da mensagem por diversas letras ou símbolos, dificultando, desta forma, a quebra da chave pela análise de frequências.

Capítulo 2

UMA BREVE HISTÓRIA DA CRIPTOGRAFIA

Há 4000 anos, no Antigo Egipto, numa vila chamada Menet Khufu, no túmulo de Khnumhotep II, um membro da nobreza egípcia, foram usados hieróglifos que não eram compreendidos pelo resto da população. O seu objectivo foi ocultar o significado de mensagens, ou seja, usou-se a criptografia. Embora, este seja o registo de criptografia mais antigo, segundo Kahn, a criptografia não apareceu só num determinado local. Foi aparecendo em diferentes civilizações e de diferentes modos; todas com o mesmo objectivo - guardar o significado da mensagem.

Na Palestina foram usadas as cifras hebraicas. Os hebreus, desde a Antiguidade que sempre tiveram interesse em ocultar informações, para tal utilizavam as cifras atbash, albam e atbah.

Na cifra atbash, a primeira letra do alfabeto é substituída pela última, a segunda letra pela penúltima e assim sucessivamente, como se pode observar na tabela em baixo.

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	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b	a

Tabela 2.1 – Cifra atbash.

A cifra albam, é também uma cifra de substituição. Neste caso, considerando novamente o nosso alfabeto que tem 26 letras, a substituição é feita da seguinte forma: a primeira letra é substituída pela que ocupa 14ª posição, a segunda letra pela que ocupa a 15ª, até a 13ª letra ser substituída pela 26ª.

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
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

Tabela 2.2 – Cifra albam.

A cifra atbah, tal e qual como as anteriores, consiste em substituir umas letras pelas outras. Esta substituição é feita da seguinte forma:

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

Tabela 2.3 – Cifra atbah.

O nome Atbah tem a seguinte origem: a primeira letra do alfabeto hebreu (Aleph) é trocada por Teth e a segunda (Beth) é trocada por Heth. Logo, Aleph Teth Beth Heth originou ATBAH.

Os espartanos usavam o scytale ou bastão de Licurgo, uma cifra de transposição, para transmitir mensagens confidenciais.

Figura 2.1 – Scytale ou bastão de Licurgo

Este engenho militar, que podemos observar na figura 2.1, remonta ao século V a.C.. A sua referência encontra-se descrita no tomo III de *As Vidas Paralelas de Plutarco*. Neste cilindro, era enrolada uma tira de couro ou papiro, onde era escrita uma mensagem no sentido do seu comprimento, em seguida desenrolava-se a tira e era transportada como um cinto, com as letras voltadas para dentro, por um mensageiro até ao destinatário. Este enrolava a tira num bastão de igual diâmetro e ficava conhecedor de tão importante informação. Desta forma, os governantes e generais de Esparta trocavam, com segurança, as suas mensagens secretas.

Em 200 a.C. Políbio descreve pela primeira vez, uma cifra que ficará conhecida com o seu nome. O seu funcionamento baseia-se na seguinte tabela:

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

Tabela 2.4 - Cifra de Políbio.

Utilizando esta tabela, substituímos o A por AA, o B por AB e assim sucessivamente. As letras I e J, têm a mesma cifração, assim, quando se proceder à decifração da mensagem codificada, escolhe-se a que dá significado ao texto.

Vamos dar o seguinte exemplo desta cifra:

Texto simples: **JESUS É A SALVAÇÃO DO BENFICA**

Texto em cifra:

BDAEDCDEDCAEAADCAACAEAAAACAACDADCDABAECCBABDACAA

A cifra de Políbio utiliza somente cinco letras, mas o texto em cifra tem o dobro do comprimento do texto original.

Se na tabela de Políbio substituirmos as letras A, B, C, D e E pelos primeiros cinco algarismos, cada letra pode ser representada por um número.

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

Tabela 2.5 – Cifra de Políbio, usando números.

Políbio sugeriu que se aproveitasse esta tabela para transmitir mensagens, utilizando tochas de fogo. A mensagem era transmitida letra a letra, por exemplo: para transmitir a letra h, que corresponde ao número 12, um mensageiro segurava na mão direita um tocha e na esquerda duas.

Por volta de 60 a.C., o imperador Júlio César trocava as suas mensagens secretas com os seus generais, usando uma cifra de substituição, em que as letras do alfabeto em cifra resultam do avanço da ordem das letras do alfabeto simples três posições para a direita. A tabela seguinte, mostra a conversão do alfabeto simples no alfabeto em cifra.

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
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

Tabela 2.6 - Cifra de César.

Para proceder à decifragem, deslocam-se as ordens das letras do texto em cifra três posições para a esquerda, obtendo-se desta forma o texto original.

Na Índia, no ano 400, o brâmane Vatsyayana escreveu o *Kama-sutra*. Este livro recomenda às senhoras que estudem 64 artes, uma delas, a 45ª era mlecchita--vikalpa, a arte da escrita secreta, que lhes permitia guardar os seus segredos.

A idade das trevas na Europa, também o foi para a criptografia. Durante a Idade Média, a criptografia era vista como magia negra o que levou à perda de grande parte do conhecimento que existia.

Em, 855 d. C., Abū Yūsūf Ya 'qūb ibn Is-hāq ibn as-Sabbāh ibn' Omrān ibn Ismail al-Kindi mais conhecido por al-Kindi, escreveu vários livros sobre diferentes matérias. Num dos seus tratados, intitulado *Um Manuscrito sobre a Decifração de Mensagens Criptográficas*, descreve o método para decifrar mensagens encriptadas, utilizando a análise de frequências.

As cifras utilizadas até esta altura, eram cifras monoalfabéticas. Em cada língua, quando se faz a contagem do número de vezes que cada letra aparece em textos longos, observamos que cada letra tem uma determinada frequência relativa. Através deste facto, os árabes abriram as portas para a criptanálise. Por exemplo, na Língua Portuguesa, a frequência relativa de cada uma das letras do alfabeto português é a seguinte:

Letra	%	Letra	%	Letra	%	Letra	%
A	12,71%	H	0,74%	O	11,32%	V	1,36%
B	0,81%	I	7,18%	P	3,07%	W	0,02%
C	4,16%	J	0,21%	Q	1,41%	X	0,28%
D	5,52%	K	0,00%	R	6,47%	Y	0,02%
E	11,99%	L	3,23%	S	7,99%	Z	0,37%
F	1,34%	M	4,48%	T	5,31%		
G	1,32%	N	5,24%	U	3,44%		

Tabela 2.7 – Frequência relativa de cada uma das letras, na Língua Portuguesa.

Analisando a tabela, podemos agrupar as letras consoante o nível das suas frequências:

1º A, E, O

2º S, R, I

3º N, D, M, U, T, C

4º L, P, V, G, H, Q, B, F

5º Z, J, X, K, W, Y.

Um criptanalista para decifrar uma mensagem, em que foi utilizada uma cifra monoalfabética e cujo texto original foi escrito em português, começa por fazer uma tabela de frequências das letras ou símbolos do texto em cifra. E comparando o valor das frequências relativas das diferentes letras ou símbolos, com os valores da tabela anterior, pode ir substituindo as letras ou símbolos pelas letras que têm percentagens semelhantes até a mensagem fazer sentido.

A hierarquia superior da Ordem do Templo, os Templários, utilizou a criptografia para comunicar entre si e para cifrar letras de câmbio e outros documentos financeiros e comerciais da Ordem. Deste modo, os seus membros não transportavam riquezas. O seu funcionamento era análogo a um banco, onde os documentos circulavam protegidos e eram reconhecidos nos diferentes templos.

A sua cifra foi retirada da Cruz das Oito Beatitudes, que era o emblema da Ordem. É uma cifra monoalfabética, que se encontra na figura abaixo.

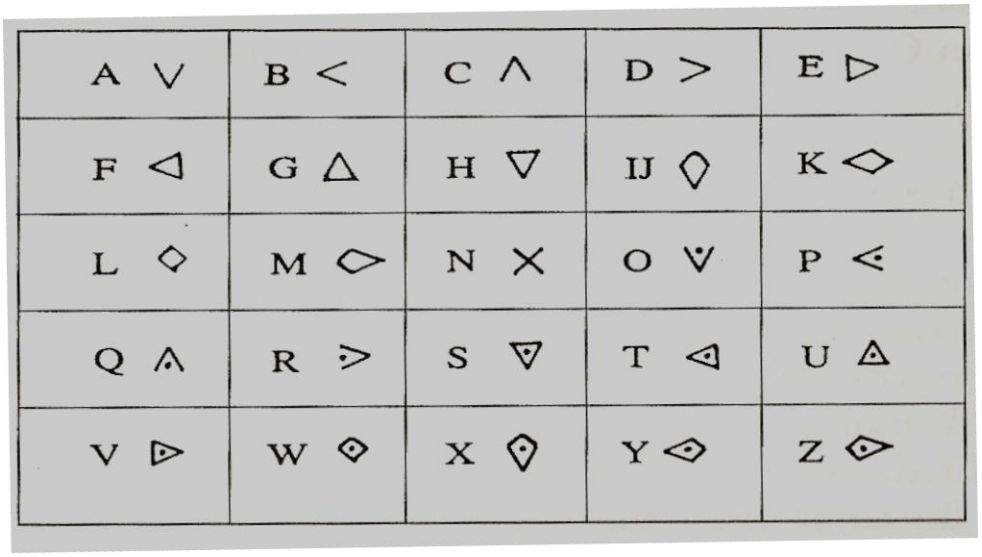


Figura 2.2 – Cifra dos templários.

No século XIII, o monge franciscano, Roger Bacon, escreveu o livro *A Epístola sobre as obras de Arte Secretas e a Nulidade da Magia*; o primeiro livro europeu que descreve o uso da criptografia.

Em 1379, Clemente VII, o antipapa, pediu ao seu secretário Gabrieli di Lavinde para unificar o sistema de cifras da Itália Setentrional. Este coligiu várias cifras num manual, do qual o Vaticano guarda uma cópia de 1379.

Lavinde criou o nomenclator que é constituído pela junção de uma cifra de substituição com um código de listas de palavras, sílabas e nomes equivalentes.

Em 1411, aparecem as primeiras cifras homofónicas. Nesta época, com o objectivo de combater a análise de frequências, são introduzidos os homófonos e os nulos. Estes últimos, não estavam ligados a nenhuma letra, eram colocados aleatoriamente ao longo do texto cifrado para confundir qualquer criptoanalista que fizesse uma análise de frequências do texto cifrado. Os homófonos funcionavam da seguinte forma: na tabela 2.7, a letra “e” aparece num texto cerca de 12%, se fizermos corresponder a esta letra três símbolos distintos e por cada “e” que for substituído, utilizarmos um dos três símbolos alternadamente, a letra “e” será mais difícil de ser detectada através da análise de frequências.

No início do século XV, Qalqashandi, Shihab al-Din abu `l-`Abbas Ahamad Àli bem Ahmad `AbdAllah al- Qalqashandi escreveu uma enciclopédia de 14 volumes, onde se encontra uma secção de Criptologia, aí refere-se o nome de Taj ad-Din Àli ibn ad- Duraihim bem Muhammad ath-Tha`álibi al-Mausili como o autor das informações desta secção. Nela é apresentada uma lista de cifras de substituição, transposição e uma cifra com várias substituições para cada letra do texto original.

Durante o século XV, assistiu-se a um grande desenvolvimento da criptografia em Itália, devido à grande actividade diplomática.

Uma das grandes figuras do Renascimento, Leon Battista Alberti publicou, em 1466, o livro *Modus scribendi in ziferas*, onde fala do disco de cifra (figura 2.3), o primeiro sistema polialfabético conhecido. O disco de cifra era constituído por dois discos concêntricos e de raios diferentes. O disco maior era fixo, e o menor móvel. Alberti dividiu cada uma das circunferências em vinte e quatro sectores; em cada um dos sectores do disco maior escreveu o alfabeto em

letras maiúsculas pela sua ordem normal, mas não continha as letras H, J, K, U, W e Y; nos quatro sectores que sobraram colocou os algarismos 1, 2, 3 e 4.

No disco móvel, colocou de uma forma aleatória, em cada um dos sectores, as letras do alfabeto, que eram 24, sendo a vigésima quarta o & (et).

No disco pequeno – que representa o alfabeto de cifra - escolhe-se uma letra chave, por exemplo a k, alinha-se esta letra alternadamente com as letras de uma palavra-chave no disco maior, e podemos começar a encriptar o texto. Se utilizarmos a palavra-chave LEON, alinhamos a posição da letra k do disco menor com a letra L e ciframos a primeira letra do texto simples; em seguida, alinhamos a letra k do disco menor com a letra E do disco maior e ciframos a segunda letra; após ciframos a quarta letra, repetimos o processo de alinhamento até cifrarmos a mensagem toda. Neste caso, temos uma cifra polialfabética, onde se utilizaram quatro alfabetos de cifra. Os intervenientes têm que ter conhecimento da letra-chave e da palavra-chave.

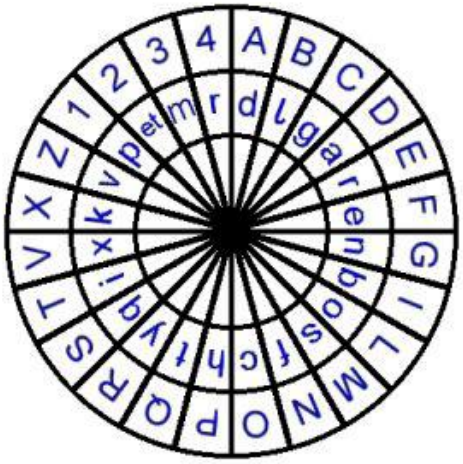


Figura 2.3 – Disco de Alberti.

Vamos dar um exemplo, utilizando o disco, a letra-chave e a palavra-chave anteriormente referidas, para ilustrar o funcionamento desta cifra:

Texto simples: **Neda, símbolo de coragem.**

Texto em cifra:**1SVZ4CS43OBTZ2B1VP3R.**

Uma das desvantagens deste método, é que emissor e receptor têm que ter dois discos iguais e muito bem guardados; pois a segurança deste sistema depende de ocultar os discos de olhos indiscretos.

O abade Johannes Trithemius escreveu o livro *Polygraphia libri sex*, onde são descritas várias cifras polialfabéticas, sendo uma delas, uma tabela de substituição denominada Tabula recta Caesar. Nesta tabela encontram-se, como mostra a figura abaixo, todos os alfabetos de deslocação possíveis.


Recta transpositionis tabula.

a b c d e f g h i k l m n o p q r s t u x y z w
b c d e f g h i k l m n o p q r s t u x y z w a
c d e f g h i k l m n o p q r s t u x y z w a b
d e f g h i k l m n o p q r s t u x y z w a b c
e f g h i k l m n o p q r s t u x y z w a b c d
f g h i k l m n o p q r s t u x y z w a b c d e
g h i k l m n o p q r s t u x y z w a b c d e f
h i k l m n o p q r s t u x y z w a b c d e f g
i k l m n o p q r s t u x y z w a b c d e f g h
k l m n o p q r s t u x y z w a b c d e f g h i
l m n o p q r s t u x y z w a b c d e f g h i k
m n o p q r s t u x y z w a b c d e f g h i k l
n o p q r s t u x y z w a b c d e f g h i k l m
o p q r s t u x y z w a b c d e f g h i k l m n
p q r s t u x y z w a b c d e f g h i k l m n o
q r s t u x y z w a b c d e f g h i k l m n o p
r s t u x y z w a b c d e f g h i k l m n o p q
s t u x y z w a b c d e f g h i k l m n o p q r
t u x y z w a b c d e f g h i k l m n o p q r s
u x y z w a b c d e f g h i k l m n o p q r s t
x y z w a b c d e f g h i k l m n o p q r s t u
y z w a b c d e f g h i k l m n o p q r s t u x
z w a b c d e f g h i k l m n o p q r s t u x y
w a b c d e f g h i k l m n o p q r s t u x y z

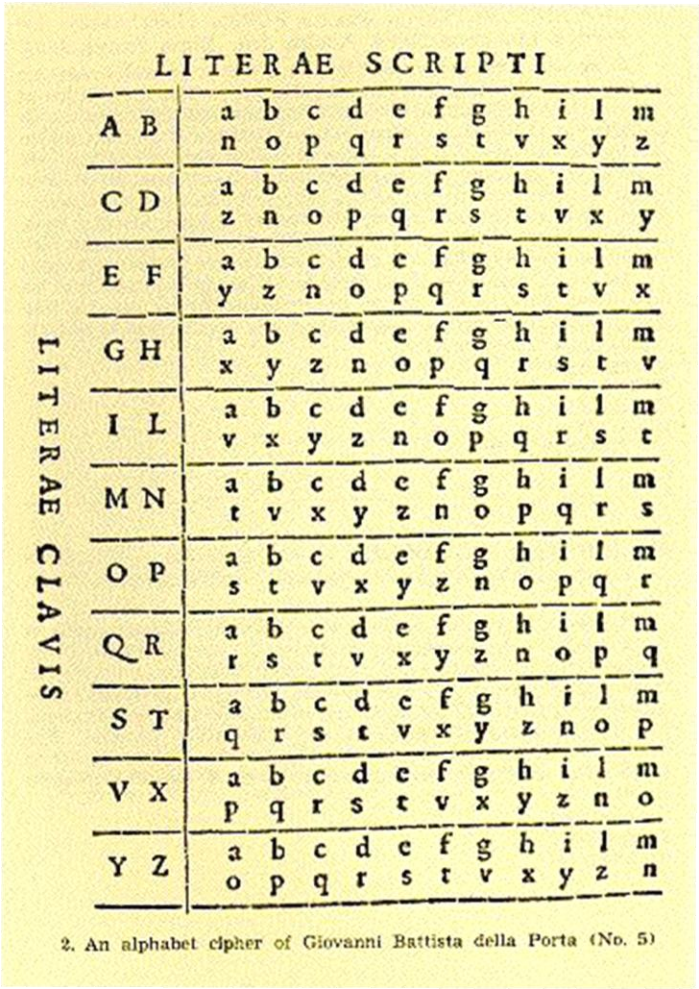
In hac tabula literarũ canonica siue recta tot ex uno & usuali nostrc
latinarum literarum ipsarum per mutationem seu transpositionẽ habe:
alphabeta, quot in ea per totum sunt monogrammata, uidelicet quate
& uigesies quatuor & uiginti, quæ faciunt in numero D.lxxvi. acper
tidẽ multiplicata, paulo efficiunt minus q̃ quatuordecẽ milia.

o ñj

Figura 2.4 – Tabula recta Caesar.

Em 1563, Giovanni Battista Della Porta escreveu a obra *De Furtivis Literarum Notis* constituída por quatro volumes, a sua obra mais importante sobre criptografia. Nesta obra, Della Porta estudou as cifras clássicas e respectivas criptoanálises e também criou uma cifra nova – a cifra de Della Porta. Sugeriu, ainda, o uso de sinónimos e erros ortográficos para escapar à análise de frequências.

Na sua cifra, Della Porta utilizou onze alfabetos distintos. Como mostra a figura abaixo.



2. An alphabet cipher of Giovanni Battista della Porta (No. 5)

Figura 2.5 – Alfabetos de cifra utilizados por Della Porta.

Como o nosso alfabeto é constituído por vinte e seis letras, para utilizarmos esta cifra de forma análoga devemos utilizar treze alfabetos.

Nesta cifra é uma palavra-chave que nos indica qual dos onze alfabetos é que devemos utilizar. Por exemplo, se utilizarmos a palavra-chave PORTA e o quadro em cima, para cifrar a letra S, utilizamos o alfabeto OP da tabela e substituímos a letra S pela letra A e assim sucessivamente até percorrermos as letras da palavra-chave, se por acaso a mensagem for mais comprida que a palavra-chave, reutilizamos novamente a mesma palavra-chave. Deste modo, podemos encriptar a seguinte mensagem:

Texto simples: **Sophie Germain traída por M. Le Blanc.**

Texto em cifra: **AHLZXYNXBZSPHDESPVQCHMQORTQRIP.**

O diplomata francês, Blaise de Vigenère, depois de ter lido os textos dos três últimos autores citados, publica, em 1586, o livro *Traicté des Chiffres*, onde é apresentada pela primeira vez a cifra indecifrável, que trataremos num dos próximos capítulos.

Em 1586, Mary Stuart, rainha da Escócia, é condenada à morte, depois de ser descoberta a sua conspiração contra a vida de sua prima, Elizabeth I, rainha de Inglaterra. Apesar da comunicação entre Mary Stuart e os restantes conspiradores ter sido feita através de mensagens cifradas, através do uso de um nomenclator, Thomas Phelippes, um criptoanalista ao serviço do secretário-mor da rainha Elisabeth I, Sir Francis Walsingham, conseguiu através da análise de frequências descobrir a respectiva correspondência entre caracteres e letras e identificar os nulos; as palavras em código foram deduzidas pelo contexto. Verificamos com este exemplo, que a criptografia ou a criptoanálise podem mudar o destino de um reino.

No século XVI, o filósofo inglês Francis Bacon criou uma cifra em que cada letra é substituída por uma sequência de cinco letras, esta sequência é formada unicamente pelas letras A e B. Neste caso, a = AAAAA, b = AAAAB, c = AAABA, d = AAABB e assim sucessivamente até chegarmos ao z = BABBB. Se substituirmos o A por zero e o B por um, podemos escrever cada uma das letras do alfabeto em código binário. Como $2^5 = 32$, ainda sobram sequências para outros símbolos.

Em 1626, Antoine Rossignol e o seu filho Bonaparte criaram a Grande Cifra ao serviço do rei Luís XIV. Esta cifra era tão forte, que só foi quebrada passados duzentos anos por Bazeries.

O franciscano Athanasius Kircher transformou as cifras polialfabéticas em cifras numéricas (1663).

O grande matemático alemão, Gottfried Wilhelm Von Leibniz inventou a máquina de calcular e descreveu o sistema binário.

Em 1795, Thomas Jefferson inventou a cifra de roda, que é utilizada com bastante eficácia na cifra de substituição polialfabética. Para tal, Jefferson criou o cilindro que pode ser observado na figura 2.6.

Figura 2.6 – Cilindro de Jefferson.

Charles Babbage, em 1854, quebra a cifra de Vigenère, mas não publica o feito, pelo que, este é atribuído a Friedrich Wilhelm Kasiski, que publicou a criptanálise desta cifra em *Die Geheimschriften und die Dechiffrir-Kunst*, em 1863.

Sir Charles Wheatstone inventou a cifra de Playfair, que foi publicada por Lyon Playfair. Esta cifra faz parte das cifras de substituição, substitui cada par de letras do texto simples por um outro par de letras. Neste caso, o emissor e o receptor combinam uma palavra-chave e a partir dessa palavra é construído um quadrado 5×5, com as letras do alfabeto, começando pela palavra-chave.

A mensagem do texto simples é dividida em conjuntos de duas letras cada. As duas letras de cada um dos conjuntos têm de ser diferentes, quando tal não suceder separam-se acrescentando uma outra letra entre elas.

Cada um dos conjuntos está numa de três categorias, a saber:

1) As letras estão na mesma linha;
2) As letras estão na mesma coluna;
3) As letras não estão na mesma linha nem na mesma coluna.

Se ocorrer 1), então cada letra é substituída pela letra imediatamente à direita, se uma das letras estiver no final da linha, então é substituída pela letra que está no início da linha; se ocorrer 2), cada uma das letras é substituída pela letra que se encontra por baixo dela, se uma das letras estiver no final da coluna, será substituída pela primeira letra da coluna; no caso 3), para

substituir a primeira letra seguimos pela linha até encontrar a coluna onde se encontra a segunda letra, a segunda é trocada de forma análoga.

Exemplo:

TEXTO SIMPLES: **DOPINGAPRAGADOCICLISMO**

PALAVRA-CHAVE: **JARDEL**

Com a palavra-chave vamos construir uma tabela 5 × 5:

J A R D E

L B C F G

H I/K M N O

P Q S T U

V W X Y Z

TEXTO SIMPLES EM CONJUNTOS DE DUAS LETRAS: **DO PI NG AP RA GA DO CI CL IS MO**

TEXTO EM CIFRA: **ENQHOFJQDRBEENBMFBMQNH.**

Marconi descobre a rádio. A comunicação começa a ser feita sem o uso de fios. O canal é aberto, a comunicação mais do que nunca está dependente do uso da criptografia.

William Frederick foi o homem que utilizou o termo “criptoanálise” pela primeira vez.

Gilbert Sandford Vernam inventou uma máquina de cifragem polialfabética que utiliza uma chave totalmente aleatória que nunca se repete. Mais tarde deu origem ao One-Time Pad.

No final da Primeira Guerra Mundial, em Março de 1918 o exército alemão inventou e usou a cifra ADFGVX, que era simultaneamente de substituição e transposição; que foi quebrada a dois de Junho do mesmo ano, pelo tenente francês Georges Painvin.

A primeira parte da construção desta cifra era algo semelhante à cifra de Políbio; pois consistia numa tabela de 7 x 7, onde na primeira linha e na primeira coluna desta tabela colocamos, pela ordem indicada, as seguintes letras: A, D, F, G, V e X, nos restantes espaços colocamos, de forma aleatória, as 26 letras e os 10 algarismos, o que nos dá 36! chaves diferentes para construir a matriz; é claro que, emissor e receptor tinham que partilhar a mesma tabela. As letras A, D, F, G, V e X foram escolhidas, visto que as mensagens eram transmitidas em Código Morse, e estas letras neste código são bastante diferentes o que minimizava os erros quando a mensagem era transmitida.

Tal como em exemplos anteriores, cada letra ou algarismo era substituído por duas letras, consoante a posição que ocupasse na tabela. Depois de substituirmos todas as letras e números, passava-se à parte da transposição; para tal, escolhia-se uma palavra-chave, por baixo desta palavra escrevia-se a mensagem que já estava cifrada, em seguida ordenavam-se as letras da palavra-chave por ordem alfabética e consequentemente as letras da mensagem mudavam de posição e seria por esta ordem que eram enviadas em código morse.

Vamos exemplificar esta cifra, que numa primeira leitura pode parecer de difícil compreensão por utilizar dois métodos de cifração: substituição e transposição. Para tal consideremos a seguinte tabela:

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

Tabela 2. 8 – Cifra ADFGVX.

Texto simples: **Desastre no Ensino da Matemática, 6V**

Texto em cifra:

VAAVGVGFGVDFDAAVXDFVAVXDGVFFXDFVVAGFXGGFDFAVXG GFDFFFVDGFDXVG

Até aqui utilizamos a cifra de substituição. De seguida, utilizava-se uma palavra-chave **CRATO** para aplicar a cifra de transposição, do seguinte modo:

C	R	A	T	O
V	A	A	V	G
V	G	F	G	V
D	F	D	A	A
V	X	D	F	V
A	V	X	D	G
V	F	F	X	D
F	V	V	A	G
F	X	G	G	F
D	F	A	V	X
G	G	F	D	F
F	F	V	D	G
F	D	X	V	G

Tabela 2.9 – Mensagem escrita utilizando a palavra-chave.

Agora, ordeno a tabela com a palavra-chave escrita por ordem alfabética, que ficará do seguinte modo:

A	C	O	R	T
A	V	G	A	V
F	V	V	G	G
D	D	A	F	A
D	V	V	X	F
X	A	G	V	D
F	V	D	F	X
V	F	G	V	A
G	F	F	X	G
A	D	X	F	V
F	G	F	G	D
V	F	G	F	D
X	F	G	D	V

Tabela 2.10 – Mensagem escrita depois da palavra-chave ser ordenada por ordem alfabética.

E a mensagem a ser enviada neste caso será a seguinte:

AVGAVFVVGGDDAFADVVXFXAGVDFVDFXVFGVAGFFXGADXFVFGFGDV FGFDXFGDV.

Em 1929, Lester S. Hill descreve como cifra um texto codificado através de uma operação de matrizes, que será explorado mais adiante.

Após a Primeira Guerra Mundial, o alemão Scherbuis criou a máquina Enigma (figura 2.7), que revolucionou o mundo da criptografia. Esta máquina de cifra, devido ao elevado número de chaves que pode utilizar e à sua complexidade foi usada para fins militares pelos alemães, pois estavam convictos da sua segurança.

Figura 2.7 – Máquina Enigma.

A máquina Enigma utilizada pelos alemães, era formada pelas seguintes componentes: um teclado, uma unidade de cifragem e um painel de visionamento.

O operador para cifrar uma mensagem, utilizava o teclado para introduzir as letras do texto simples uma a uma; na unidade de cifragem, cada letra era transformada numa outra; a letra transformada era então comunicada ao

operador através do painel de visionamento, onde era acesa a lâmpada correspondente.

A unidade de cifragem era composta por três cilindros móveis, que podiam alternar a sua posição dentro da máquina, e um fixo, que se chamava espelho. Cada um dos cilindros contem as vinte e seis letras do alfabeto.

Entre o teclado e o primeiro cilindro existe um painel de ligação, que permite a troca de seis pares de letras das vinte e seis do alfabeto. O que eleva bastante o número de chaves que se pode utilizar.

Por cada letra cifrada, o primeiro cilindro roda um sexto sempre no sentido directo, quando dá uma volta completa, o segundo cilindro roda também um sexto, após seis voltas do primeiro cilindro, o segundo dá uma volta completa e o terceiro roda um sexto. Ou seja, por cada seis letras cifradas, o segundo cilindro move-se e por cada 36 letras move-se o terceiro, o que permite o uso de 17576 alfabetos de cifra diferentes.

Mas não é só no número de alfabetos de cifra que esta máquina é forte, o número de chaves é muito grande. O seu verdadeiro número pode ser calculado da seguinte maneira:

1) Para começar, os cilindros podem permutar entre si, como são três, temos 3! = 6;

2) Cada um dos três cilindros pode ser regulado de vinte e seis maneiras diferentes, o que dá $26^3 = 17576$;

3) No painel de ligação podem-se trocar seis pares de letras a partir das vinte e seis do alfabeto, o que pode ser feito de

$$\frac{(26\times25)\times(24\times23)\times(22\times21)\times(21\times19)\times(18\times17)\times(16\times15)}{2^6\times6!} = 100391791500$$ maneiras diferentes

4) Por fim, o número de chaves é dado por:

17576 × 6 × 100391791500 = 1058691676442400.

A colocação dos cilindros, a sua regulação inicial e o conhecimento da troca dos seis pares de letras determinam a chave a usar.

Na 2.8, podemos ver um diagrama simplificado da máquina enigma.

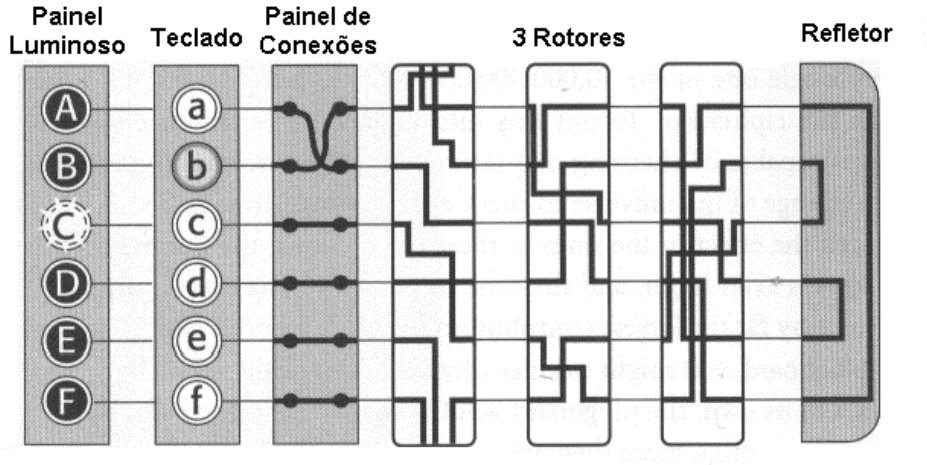


Figura 2.8 – Maqueta da máquina Enigma.

Neste diagrama, a letra **B**, está trocada com a letra **A,** no painel das ligações. Quando se tecla **B,** esta é logo trocada por **A** e vai, nos cilindros seguir o caminho que estava destinado para o **A,** até aparecer cifrada por **C**, no painel luminoso.

Durante a Segunda Guerra Mundial, em Blethcheley Park, travou-se uma batalha silenciosa, cujo alvo era quebrar a chave da Enigma. Uma vasta equipa que incluía não só matemáticos, mas pessoas de várias áreas, levou a melhor e deu um grande contributo para a vitória dos Aliados, da qual, podemos distinguir: Alan Turing, pois foi graças a ele que a Enigma foi vencida!

Em meados do século XX, o aparecimento do computador veio revolucionar o mundo da criptografia. A grande capacidade do computador em cifrar mensagens, aliado ao facto do computador modificar números e não letras do alfabeto, trouxe vários problemas ao mundo da criptografia. Com a utilização crescente de computadores por parte das empresas e a necessidade do uso da criptografia como medida de segurança, teve que se proceder a uma estandardização, de modo, a que as empresas pudessem trocar mensagens de uma forma segura e eficiente.

A conversão de letras em números, pode ser feita através do American Sandard Code For Information Interchange, que é conhecida pela sigla ASCII. Utilizando números binários de sete dígitos, o ASCII permite converter as letras

do alfabeto (minúsculas e maiúsculas), pontuação e algarismos em números binários.

Na tabela seguinte, cada letra maiúscula é convertida em código binário:

A	1000001	N	1001110
B	1000010	O	1001111
C	1000011	P	1010000
D	1000100	Q	1010001
E	1000101	R	1010010
F	1000110	S	1010011
G	1000111	T	1010100
H	1001000	U	1010101
I	1001001	V	1010110
J	1001010	W	1010111
K	1001011	X	1011000
L	1001100	Y	1011001
M	1001101	Z	1011010

Tabela 2.11 – Números binários ASCII para as letras maiúsculas.

Com a crescente capacidade dos computadores houve necessidade de criar algoritmos de cifra mais complexos. Um desses algoritmos ficou conhecido como Lúcifer.

O Lúcifer codifica as mensagens do seguinte modo:

1) A mensagem é traduzida para uma longa fila de dígitos binários;

2) A fila é dividida em blocos de 64 dígitos;

3) Cada um dos blocos de 64 dígitos é baralhado;

4) Cada bloco de 64 dígitos é dividido em 2 blocos de 32 dígitos, designados por Esquerdo^0 e Direito^0;

5) Os dígitos do bloco Direito^0 são submetidos a uma função complexa que os altera;

6) O bloco Direito^0 é adicionado ao bloco Esquerdo^0, originando um bloco de 32 dígitos que passará a ser designado por Direito^1. No entanto, o Direito^0 passa a ser designado por Esquerdo^1.

7) Repetem-se os passos 5) e 6) 16 vezes;

8) O texto cifrado é então enviado e para decifrar a mensagem o processo é invertido.

As chaves usadas por computadores são números. A cifra de Lúcifer era bastante potente devido ao elevado número de chaves que podiam ser utilizadas.

Devido a problemas, ditos de "segurança de Estado", o número de chaves foi limitado a 10^{17} (este número escrito em sistema binário tem 56 dígitos). No dia 23 de Novembro de 1976, a versão 56 bits da cifra de Lúcifer foi adoptada como padrão oficial americano para a encriptação, que ficou conhecido como Data Encryption Standard (DES). A DES resolveu o problema da estandardização da criptografia, e fomentou o seu uso por parte das empresas.

Apesar da cifração e decifração de mensagens se ter tornado mais rápida e complexa, existia um velho problema que se agudizava com a generalização do uso da criptografia – **a distribuição da chave.**

O problema da distribuição da chave continuava em aberto. A melhor forma de emissor e receptor trocarem uma chave, continuava a ser na base da confiança, o que originava grandes encargos para governos, empresas e bancos. Em 1976, a dupla Whitfied Diffie e Martin Hellman encontraram uma forma de poder haver uma troca segura de chaves, sem as pessoas se encontrarem. Até então, as chaves utilizadas eram funções matemáticas injectivas – uma determinada função servia para cifrar uma mensagem, a sua inversa para decifrar.

Hellman colocou a aritmética modular ao serviço da criptografia.

Diffie continuou a trabalhar no problema da distribuição da chave e teve uma ideia brilhante – a cifra assimétrica. A ideia de Diffie era usar uma chave para cifrar uma mensagem e usar uma diferente para a decifrar. Até então, em criptografia só se tinham usado cifras simétricas – usam a mesma chave para cifrar e decifrar uma mensagem. Ou seja, Diffie teve uma ideia que iria revolucionar o mundo da criptografia, o seu problema era não saber como pô-la em prática.

Não sabia ele e não sabia mais ninguém. Ronald Rivest, Adi Shamir, cientistas informáticos, e Leonard Adleman, matemático, resolveram formar uma equipa para pôr a ideia de Diffie em prática.

Durante um ano, os dois cientistas informáticos desenvolveram ideias para criar uma cifra assimétrica. Estas eram submetidas ao crivo matemático de Adleman, que as deitava fora devido às suas falhas. Até que, em Abril de 1977, numa noite de inspiração de Rivest, este resolveu de vez, o problema da distribuição da chave. No final do artigo que escreveu nessa noite colocou os nomes dos elementos da equipa por ordem alfabética. Os seus colegas concordaram em colocar o nome no seu artigo, mas o nome dele tinha que vir em primeiro lugar. E desta forma, se deu nome à cifra assimétrica **RSA** (Rivest, Shamir e Adleman).

Em 1984, Taher ELGamal, baseado no Problema do Logaritmo Discreto, criou uma cifra assimétrica que foi baptizada com o seu nome.

Em 1986, Miller introduz na criptografia as curvas elípticas.

Durante os anos 90, aparecem alguns trabalhos com computadores quânticos e criptografia quântica. A biometria é aplicada na autenticação.

Xuejia Lai e James Massey publicam uma proposta para um novo Padrão de Encriptação de Bloco, que viria a substituir o DES. O IDEA, como ficou conhecido, utiliza uma chave de 128 bits e emprega operações adequadas para a maioria dos computadores, tornando as implementações do software mais eficientes.

São publicados por Charles H. Bennett e Gilles Brassard os primeiros resultados sobre Criptografia Quântica. Esta usa fotões únicos para transmitir um fluxo de bits chave para uma posterior comunicação usando a cifra de Vernam. Na Criptografia Quântica surge a indicação, se ocorrer uma intercepção de um certo número máximo de bits. Uma desvantagem desta criptografia é a necessidade de existirem fios de fibra óptica entre as partes que se comunicam.

Phil Zimmermann publica a primeira versão de PGP (Pretty Good Privacy), que oferece uma boa segurança para o cidadão comum trocar informação. O PGP é disponibilizado como freeware, o que fez dele um padrão mundial. O PGP5.0 Freeware é amplamente distribuído para uso não comercial.

O governo dos Estados Unidos da América adopta o SHA-1 (Secure Hash Algorithm) para a autenticação de documentos digitais pelos departamentos e agências federais.

As bases da criptografia nos EUA sofrem um abanão; pois o padrão de encriptação DES de 56 bits, base da sua criptografia, é quebrado por uma rede de 14 000 computadores. Mais tarde volta a ser quebrado por pesquisadores da Electronic Frontier Foundation em apenas 56 horas. O golpe final foi dado em 1999, quando este padrão de encriptação é quebrado em apenas 22 horas e 15 minutos. O governo vê-se obrigado a abandonar o DES de 56 bits e a adoptar o Triple-DES.

No ano 2000, o algoritmo Rijndael é seleccionado para substituir o DES e é denominado AES – Advanced Encryption Standard.

Capítulo 3

MATEMÁTICA

Hoje em dia, a criptografia tem como principal aliada a Matemática. A criptografia explora as virtudes e as fraquezas desta disciplina para seu próprio proveito. Embora utilize vários ramos da Matemática, é da Teoria dos Números que mais vezes se serve; caindo por terra, desta forma, a percepção de Hardy de que a Teoria dos Números não tinha nenhuma aplicação no dia-a-dia.

Nas próximas linhas serão expostos alguns conceitos matemáticos indispensáveis para a compreensão do modo como a criptografia tem evoluído ao longo dos tempos, especialmente desde 1977. Procuraremos dar: definições, teoremas, algumas demonstrações e alguns exemplos, de modo a ilustrar as suas aplicações.

3.1 Grupos, anéis e corpos

3.1.1 Definição. Seja G um conjunto munido de uma operação binária $\star : G \times G \rightarrow G$. Dizemos que $(G, \star)$ é grupo com respeito à operação $\star$ se nele se verificarem as propriedades:

- $\star$ é associativa, ou seja, $g \star (h \star k) = (g \star h) \star k$ sempre que $g, h, k \in G$;

- existe $e \in G$ tal que $e \star g = g \star e = g$ sempre que $g \in G$: e é a identidade ou elemento neutro de G;

- se $g \in G$, então existe $g^{-1} \in G$ tal que $g \star g^{-1} = g^{-1} \star g = e$.

Quando o grupo G verifica a propriedade $g \star h = h \star g$ sempre que $g, h \in G$, dizemos que G é grupo comutativo ou abeliano.

Por exemplo, $(\mathbb{Z}, +)$, sendo que $\mathbb{Z}$ é o conjunto dos números inteiros relativos, com a adição usual é um grupo abeliano.

3.1.2 Definição. Se o conjunto G for finito, dizemos que G é um grupo finito e escrevemos |G| para designar a ordem de G, ou seja, o seu número de elementos.

3.1.3 Definição. Um grupo G diz-se cíclico se existe algum elemento $g \in G$ tal que $\langle g \rangle = G$. Neste caso, g diz-se o gerador de G.

3.1.4 Definição. Seja $S \subseteq G$, $S \neq \emptyset$. Dizemos que $(S, *)$é um subgrupo do grupo $(G, *)$ se $ab \in S$ e $a^{-1} \in S$ com $a, b \in S$.

3.1.5 Definição. Um anel é um conjunto $R \neq \emptyset$ munido de duas operações binárias, + e $\times$, tal que:

- R é grupo abeliano para +, com elemento neutro 0;

- $\times$ é associativa;

- as duas operações estão ligadas pelas leis distributivas:

  - $(a + b) \times c = (a \times c) + (b \times c)$ $(a, b, c \in R)$ e
  - $a \times (b + c) = (a \times b) + (a \times c)$ $(a, b, c \in R)$.

Se a multiplicação é comutativa, o anel diz-se comutativo.

Um anel tem identidade quando existe um elemento, designado por 1, que é o elemento neutro para a multiplicação.

Por exemplo, $(\mathbb{R}, +, \times)$, em que $\mathbb{R}$ é o conjunto dos números reais, é um anel comutativo.

3.1.6 Definição. Um corpo é um anel K tal que $K \setminus \{0\}$ é um grupo abeliano para a multiplicação: a identidade deste grupo é designada por $1 = 1_k$.

Consideremos o seguinte exemplo, $(\mathbb{C}, +, \times)$, o conjunto dos números complexos, com a adição e a multiplicação definidas de forma habitual, é um corpo.

3.2 Divisibilidade e algoritmo de Euclides

3.2.1 Definição. Dados a e $b \in \mathbb{Z}$, com $a \neq 0$, diz-se que a divide b, e escreve-se $a \mid b$, se existe $q \in \mathbb{Z}$ tal que $b = aq$ $(a \times q)$.

3.2.2 Propriedades. Sejam a, b, c, x e y números inteiros.

a) Se $a \mid b$, então $ac \mid bc$, qualquer que seja c.

b) Se a | b e b | c, então a | c.

c) Se a | b e b ≠ 0, então $|a| \leq |b|$.

d) Se a | b e a | c, então a | (xb + yc).

Na demonstração que se segue utilizaremos o facto de $(\mathbb{Z}, +, \times)$ ser um anel comutativo.

Demonstração:

a) Se a | b, então existe um f ∈ $\mathbb{Z}$ tal que b = af. Pelo que, bc = (af)c = f(ac).

b) Se a | b e b | c, então existem f e g ∈ $\mathbb{Z}$, tais que b = af e c = bg. O que implica que c = bg = (af)g = a(fg).

c) Se a | b e b ≠ 0, então existe f ∈ $\mathbb{Z}$ e f ≠ 0 tal que b = af. Logo

$|b| = |af| \geq |a|$.

d) Se a | b e a | c, então existem f e g ∈ $\mathbb{Z}$ tais que b = fa e c = ga. O que implica que xb + yc = xfa + yga = (xf + yg)a.

■

3.2.3 Teorema. Dados a e b ∈ $\mathbb{Z}$, com a > 0, existem números inteiros q e r, com 0 ≤ r < a, tais que b = qa + r.

Os números inteiros q e r, designados, respectivamente, por quociente e resto da divisão de b por a, são unicamente determinados por a e b.

Demonstração: Consideremos o conjunto

{…, b – 3a, b – 2a, b – a, b, b + a, b + 2a, b + 3a,…}.

Este conjunto tem de certeza números inteiros não negativos. Designemos por r o menor deles. Então r é da forma b – qa para certo número inteiro q, donde b = qa + r. Pela sua própria definição, tem-se que r ≥ 0. Vamos provar agora que r < a. Suponhamos que r ≥ a, temos então que

r – a = b – qa – a = b – (q + 1)a,

donde podemos concluir que r – a pertence ao conjunto acima referido. O que é absurdo, visto que, por definição, r é o menor elemento não negativo que pertence ao conjunto.

Vamos agora provar a unicidade de q e r. Suponhamos que $b = qa + r$, com $0 \leq r < a$ e $b = q_1a + r_1$, com $0 \leq r_1 < a$. Se $r_1 > r$ (no caso $r_1 < r$ o raciocínio seria análogo), então $r_1 – r > 0$ e $r_1 – r < a$, visto que $r_1 < a$ e $r < a$. Mas, por outro lado, temos que $r_1 – r = b – q_1a – (b – qa) = (q – q_1)\, a$, donde se conclui que $a|(r_1 – r)$, como $r_1 – r < a$, sai que $r_1 – r = 0$, ou seja, $r_1 = r$.

Uma vez que $r_1 = r$, então $q_1a = qa$, logo $q_1 = q$.

■

3.2.4 Observação: Sejam b e c dois números inteiros. Quando um número inteiro a divide b e c, dizemos que a é um divisor comum de b e c. Se b e c não forem ambos nulos, o número de divisores comuns de b e c é finito. O conjunto dos divisores comuns de dois números inteiros é não vazio, pois 1 pertence a esse conjunto e nenhum dos divisores pode ser maior que o maior desses números.

3.2.5 Definição. Sejam b e c números inteiros não nulos. Ao maior dos divisores comuns de b e c chama-se máximo divisor comum de b e c. A notação é (b, c) ou m.d.c. (b, c).

Por exemplo m.d.c. (12,18) = 6.

3.2.6 Observação: O máximo divisor comum de dois números inteiros não ambos nulos existe e é um número inteiro positivo.

3.2.7 Definição. Dizemos que um número inteiro positivo p é primo se $p \neq 1$ e os únicos divisores de p são p e 1.

Os primeiros vinte números primos são: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67 e 71.

3.2.8 Definição. Se um número inteiro positivo (diferente de 1) não é primo, então diz-se composto.

O número 20 é um número composto, pois tem mais de dois divisores, a saber: 1, 2, 4, 5, 10 e 20.

3.2.9 Definição. Se m.d.c. (a , b) = 1, com a ≠ b, a e b dizem-se primos entre si.

O m.d.c. (20 , 33) = 1, logo 20 e 33 são primos entre si.

3.2.10 Teorema. Qualquer número natural a > 1 é um produto de números primos.

Demonstração: Seja a ∈ ℕ, a > 1. Se a for primo, então temos um produto com um só factor. Vamos supor que a é composto. Por definição, a tem divisores entre 1 e a. Se m é o menor dos divisores de a então é primo, pois se não for primo, existem divisores de m que também seriam divisores de a. Designemos m por p_1. Então temos $a = p_1a_1$ com p_1 primo e $1 < a_1 < a$. Se a_1 for primo, está provado. Se a_1 for composto, de forma análoga concluímos que a_1 tem um divisor primo p_2 satisfazendo $1 < p_2 < a_1$, donde $a = p_1p_2a_2$ com p_1 e p_2 primos e $1 < a_2 < a_1 < a$.

Continuando desta forma, obtemos números naturais $a > a_1 > a_2 >$…. Qualquer sucessão de números naturais não pode decrescer indefinidamente, pelo que, há-de chegar o momento em que um destes números é primo, digamos p_r, pelo que $a = p_1p_2...p_r$.

■

3.2.11 Algoritmo de Euclides - Sejam b e c números inteiros não ambos nulos. Sem perda de generalidade, podemos supor c > 0. Proceda-se à seguinte sequência de divisões inteiras:

$$b = q_1c + r_1,\ 0 < r_1 < c$$

$$c = q_2r_1 + r_2,\ 0 < r_2 < r_1$$

$$r_1 = q_3r_2 + r_3,\ 0 < r_3 < r_2$$

…

$$r_{k-2} = q_kr_{k-1} + r_k,\ 0 < r_k < r_{k-1}$$

$$r_{k-1} = q_{k+1}r_k.$$

Então r_k (o último resto não nulo) é o máximo divisor comum de b e c.

Demonstração: Sabemos que, na sequência de divisões, os restos não podem permanecer sempre positivos, porque cada um é menor que o anterior.

Seja d o máximo divisor comum de b e c. Vamos provar que $r_k = d$.

Das igualdades acima indicadas, concluímos que $r_k \mid r_{k-1}$. Assim sendo, da penúltima igualdade concluímos que $r_k \mid r_{k-2}$. Da anterior, que $r_k \mid r_{k-3}$. E assim sucessivamente, podemos concluir que $r_k \mid c$ e, por fim, $r_k \mid b$. Pelo que r_k é um divisor comum de b e c , logo $r_k \mid d$.

Como d | b e d | c, partindo das igualdades anteriores, e desta vez fazendo o percurso inverso, chegamos à conclusão que $d \mid r_k$.

Como $r_k \mid d$ e $d \mid r_k$ e ambos positivos, tem-se que $r_k = d$.

■

Para determinar o m.d.c. (245, 135), podemos fazê-lo da seguinte forma:

$$245 = 1 \times 135 + 110$$

$$135 = 1 \times 110 + 25$$

$$110 = 4 \times 25 + 10$$

$$25 = 2 \times 10 + 5$$

$$10 = 2 \times 5 + 0$$

E, pelo algoritmo de Euclides, concluímos que o m.d.c. (245, 135) = 5.

3.2.12 Teorema. (Identidade de Bezout) - Se a e b são números inteiros não ambos nulos, então existem números inteiros m e n tais que m.d.c. (a, b) = = ma + nb.

Demonstração: Sejam a e b dois números inteiros positivos. Como cada combinação linear de a e b é um múltiplo de d = m.d.c. (a, b), se d for escrito nesta forma, então é o menor número inteiro positivo com esta propriedade.

Consideremos o conjunto de todas as combinações lineares

$$S = \{ma + nb: m, n \in \mathbb{Z}\}.$$

Seja c o menor número inteiro positivo em S, e $c = m_1a + n_1b$, com $m_1, n_1 \in \mathbb{Z}$. Sabemos que $c \leq a$ e $c \leq b$. Usando o algoritmo da divisão podemos escrever $a = qc + r$, $0 \leq r < c$.

Por conseguinte, $r = a - qc = a - q(m_1a + n_1b) = (1 - qm_1)a - qn_1b$.

Se $r \neq 0$, r está escrito como uma combinação linear de a e b e é menor que c; o que é absurdo visto que c é o menor positivo que verifica esta condição.

Logo r = 0; isto é a = qc, ou seja, c divide a. Analogamente, c divide b. Pelo que, c = d, visto que d | c e c é um divisor comum de a e b.

■

Pegando no exemplo anterior, podemos escrever o 5 como combinação linear de 135 e 245, ou seja:

$$5 = 25 - 2 \times 10$$

$$5 = 25 - 2 \times (110 - 4 \times 25)$$

$$5 = 9 \times 25 - 2 \times 110$$

$$5 = 9 \times (135 - 110) - 2 \times 110$$

$$5 = 9 \times 135 - 11 \times 110$$

$$5 = -11 \times 245 + 20 \times 135$$

Temos que m = -11 e n = 20.

3.2.13 Teorema. Seja p um número primo e a e b dois números inteiros quaisquer. Então:

1. ou p divide a , ou a e p são números primos entre si;
2. se p | ab, então p | a ou p | b;

Demonstração: 1. Por definição m.d.c. (a , p) é um divisor positivo de p, uma vez que p é primo, ou é 1 ou é p. Se m.d.c. (a , p) = p, então como m.d.c. (a , p)

divide a, temos que p divide a; se m.d.c. (a , p) = 1 então a e p são primos entre si.

2. Seja p um divisor de ab. Se p não divide a, então por 1. implica que m.d.c. (a, p) = 1. Pela identidade de Bezout temos que 1 = au + pv para os números inteiros u e v, logo b = aub + pvb. Por hipótese, temos que p | ab, logo divide aub; como p é um dos factores de pvb é claro que p divide pvb, pelo que p divide b.

■

3.2.14 Corolário. Se p é primo e p | $a_1a_2\ldots a_n$, então p | a_k para algum k, onde $1 \leq k \leq n$.

Demonstração: Pelo método de indução, temos que para n = 1 a conclusão é óbvia, enquanto para n = 2 estamos nas condições do teorema anterior. Para n > 2, tomemos para hipótese de indução que se p divide um produto com menos de n factores, então divide um desses factores. Consideremos agora que p | $a_1a_2\ldots a_n$. Pelo teorema anterior, ou p | a_n, ou p | $a_1a_2\ldots a_{n-1}$. Se p | a_n, está provado. Se p | $a_1a_2\ldots a_{n-1}$, por hipótese de indução p | a_k, para algum k, com $1 \leq k \leq n-1$. Assim, podemos concluir que p divide um dos factores $a_1a_2\ldots a_n$.

3.2.15 Teorema. (Teorema Fundamental da Aritmética) Qualquer número natural a > 1 escreve-se de forma única como um produto de números primos.

Demonstração: Seja a > 1 qualquer. Pelo teorema 3.2.10, temos que a se escreve como um produto de números primos. Vamos demonstrar a unicidade por absurdo. Suponhamos que a pode ser escrito como produto de números primos de duas maneiras diferentes: $a = p_1p_2\ldots p_r = q_1q_2\ldots q_t$.

Como p_1 divide $p_1p_2\ldots p_r$, também divide $q_1q_2\ldots q_t$, isto é, $p_1 | q_1q_2\ldots q_t$. Como p_1 divide um produto de factores, tem que dividir um dos seus factores, seja $p_1 | q_j$, com $j \in \{1, 2, \ldots, t\}$. Como ambos os números são primos, então $p_1 = q_j$, logo a factorização é única.

■

Por exemplo o número 100, escreve-se como um produto de números primos: $100 = 2^2 \times 5^2$.

3.2.16 Teorema. Existem uma infinidade de números primos.

Demonstração: Vamos demonstrar por absurdo.

Suponhamos que havia um número finito de números primos, digamos p_1, p_2, …, p_r. Seja $n \in \mathbb{N}$, tal que $n = p_1p_2...p_r + 1$. Logo n é maior que todos os primos p_1, p_2, …, p_r, n é múltiplo de pelo menos um deles, pelo Teorema Fundamental da Aritmética. Sem perda de generalização, suponhamos que p_1 é divisor de n (se for por qualquer outro, o raciocínio é análogo). Temos então que $n = qp_1$, para $q \in \mathbb{Z}$, e podemos concluir que $p_1(q – p_2…p_r) = 1$, ou seja, $p_1 \mid 1$. O que é absurdo, porque p_1 é número primo.

■

3.3 CONGRUÊNCIAS

3.3.1 Definição. Seja m um número inteiro positivo e a e b números inteiros. Dizemos que a é congruente com b módulo m, se a diferença entre a e b for divisível por m, e representa-se por $a \equiv b \pmod m$. Se $m \nmid (a – b)$, escrevemos $a \not\equiv b \pmod m$ e dizemos que a não é congruente com b módulo m.

Pelo exposto, temos que $23 \equiv 5 \pmod 9$, pois 23 – 5 = 18 e 18 é divisível por 9.

$\mathbb{Z}_n$ – este conjunto dos números inteiros 0, 1, 2,…, (n-1) é um anel com a adição + e a multiplicação × efectuadas em módulo n.

3.3.2 Proposição. Seja $n \in \mathbb{N}$. Então $\mathbb{Z}_n$ é um corpo se e só se n é número primo.

Demonstração: Suponhamos que $n = p \in \mathbb{p}$ (onde $\mathbb{p}$ é o conjunto dos números primos). Como $\mathbb{Z}_p$ é anel comutativo, resta mostrar que $\mathbb{Z}_p\backslash\{0\}$ é grupo para multiplicação. Primeiro, mostramos que todos os elementos de $\mathbb{Z}_p\backslash\{0\}$ têm inverso multiplicativo. Se $a \in \mathbb{Z}$ é tal que m.d.c. (a , p) = 1, então pelo teorema 3.2.12. existem $u, v \in \mathbb{Z}$ tais que $ua + vp = 1$. Logo, $u + p\mathbb{Z} \in \mathbb{Z}_p\backslash\{0\}$ é o inverso de $a + p\mathbb{Z} \in \mathbb{Z}_p\backslash\{0\}$. Falta mostrar que $\mathbb{Z}_p\backslash\{0\}$ é fechado para a multiplicação.

Suponhamos que $\alpha, \beta \in \mathbb{Z}_p \backslash \{0\}$ são tais que $\alpha\beta \notin \mathbb{Z}_p \backslash \{0\}$. Logo, $\alpha\beta = 0$ e, pela existência dos inversos,

$$1 = \alpha^{-1}\alpha\beta\beta^{-1} = \alpha^{-1}0\beta^{-1} = 0,$$

o que é falso. Está provado que $\mathbb{Z}_p$ é corpo.

Inversamente, suponhamos que $n \notin \mathbb{p}$. Se n = 1 em $\mathbb{Z}_n$ então 1 = 0 em $\mathbb{Z}_n$ e $\mathbb{Z}_n$ não é corpo. Logo, n > 1 e podemos escrever n = ab com a , b $\in \mathbb{N}$ e 1 < a , b < n. Então $(a + n\mathbb{Z})(b + n\mathbb{Z}) = (ab + n\mathbb{Z}) = n + n\mathbb{Z} = 0 + n\mathbb{Z}$, enquanto

$$(a + n\mathbb{Z}),(b + n\mathbb{Z}) \neq 0 + n\mathbb{Z};$$

logo, $\mathbb{Z}_n$ não pode ser corpo.

■

3.3.3 Teorema. Seja F um corpo. Então qualquer subgrupo multiplicativo e finito de F é cíclico.

Para $\mathbb{Z}_7$, definimos as operações + e $\times$, do seguinte modo:

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

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

3.3.4 Observação: $\mathbb{Z}^*_n$ é o grupo multiplicativo formado por todos os elementos invertíveis de $\mathbb{Z}_n$, ou seja, por todos os elementos $a \in \mathbb{Z}_n$ tais que existe $b \in \mathbb{Z}_n$ onde $a \times b \equiv 1 \pmod{n}$.

3.3.5 Teorema. A congruência módulo m é uma relação de equivalência, pois verifica as seguintes propriedades:

1. $a \equiv a \pmod{m}$;
2. Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$;
3. Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

Demonstração:

1. $a \equiv a \pmod{m}$, pois $a - a = 0$ e 0 é múltiplo de m.

2. Se $a \equiv b \pmod{m}$, então $a - b$ é múltiplo de m. Como $b - a = -(a - b)$, então $b - a$ também é múltiplo de m. Logo $b \equiv a \pmod{m}$.

3. Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então existem números inteiros k e n tais que $a - b = km$ e $b - c = nm$. Logo,

$$a - c = (a - b) + (b - c) = km + nm = (k + n)m, \text{ pelo que } a \equiv c \pmod{m}.$$

■

3.3.6 Proposição:

1. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $(a \pm c) \equiv (b \pm d) \pmod{m}$.

2. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a \times c \equiv b \times d \pmod{m}$.

3. Se $a \equiv b \pmod{m}$ e $d \mid m$, $d > 0$, então $a \equiv b \pmod{d}$.

4. Se $a \equiv b \pmod{m}$, então $a \times c \equiv b \times c \pmod{m}$, com $c \in \mathbb{Z}$.

5. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então

$$(ax + cy) \equiv (bx + dy) \pmod{m}, \forall\, x, y \in \mathbb{Z}.$$

6. Se $a \equiv b \pmod{m}$, então $a^k \equiv b^k \pmod{m}$, $\forall\, k \in \mathbb{N}$.

Demonstração:

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

$$\Rightarrow a = b + mx,\ c = d + my$$

$$\Rightarrow a \pm c = b \pm d + m(x \pm y)$$

$$\Rightarrow (a \pm c) \equiv (b \pm d) \pmod{m}$$

2. $a \equiv b \pmod{m}$, $c \equiv d \pmod{m} \Rightarrow$

$$\Rightarrow a = b + mx \text{ e } c = d + my$$

$$\Rightarrow a \times c = (b + mx)(d + my) = b \times d + m(by + xd + mxy)$$

$$\Rightarrow a \times c \equiv b \times d \pmod{m}.$$

3. Se $m \mid (a - b)$ e $d \mid m$, então d divide todos os múltiplos de m, ou seja, $d \mid (a - b)$, logo $a \equiv b \pmod{d}$.

4. Temos que $m \mid (a - b)$ e $(a - b)c$ é um múltiplo de $(a - b)$, pelo que concluímos que $m \mid (ac - bc)$, ou seja, $ac \equiv bc \pmod{m}$.

5. Temos que (a – b) = km e (c – d) = lm, com k,l ∈ $\mathbb{Z}$. Logo (a – b)x = (kx)m e (c – d)y = (ly)m, ou seja, (ax + cy) – (bx + dy) = (kx + ly)m e daqui concluímos que (ax + cy) ≡ (bx + dy) (mod m), ∀ x, y ∈ $\mathbb{Z}$.

6. Vamos provar esta afirmação pelo método de indução.

Por hipótese, temos que a afirmação é válida para k = 1.

Para hipótese de indução, consideremos a afirmação verdadeira para k = n. Temos então que $a^n \equiv b^n \pmod m$, como $a^1 \equiv b^1 \pmod m$, pela propriedade 2 desta proposição, concluímos que $a^n \times a^1 \equiv b^n \times b^1 \pmod m$; ou seja, $a^{n+1} \equiv b^{n+1} \pmod m$, pelo que está provada a tese de indução.

■

3.3.7 Teorema. Para a, x, y e m números inteiros tal que m > 0:

1. $ax \equiv ay \pmod m \Leftrightarrow x \equiv y \left(\mod \frac{m}{m.d.c(a, m)}\right)$.
2. Se $x \equiv y \bmod (m_i)$, i = 1,…,r, então $x \equiv y \pmod{[m_1,\ldots, m_r]}$, onde m_1, m_2,…, m_r são números inteiros positivos.

3.3.8 Teorema. (Teorema da inversão) A classe $\bar{a}$ tem inverso em $\mathbb{Z}_n$ se e só se a e n são primos entre si.

Demonstração:

(⇒) Suponhamos que $\bar{a}$ tem inverso. Então existe $\bar{b}$ tal que $\bar{a}\bar{b} \equiv 1 \pmod n$. Logo, ab + kn = 1 e portanto m.d.c. (a, n) = 1.

(⇐) Suponhamos m.d.c. (a, n) = 1. Logo existem α e β tais que α a + βn = 1. Logo α a = - βn + 1, ou seja, $\alpha a \equiv 1 \pmod n$ e portanto $\bar{a}$ tem inverso em $\mathbb{Z}_n$.

■

3.3.9 Teorema. A congruência linear $ax \equiv b \pmod m$ tem exactamente d = m.d.c. (a, m) soluções se d | b, e não tem soluções se d ∤ b.

Se d | b e x_0 é uma solução, então as d soluções distintas módulo m são $x_0 + \frac{m}{d} \times i \pmod m$ para i = 0, 1,…, d – 1.

Demonstração:

Se d = 1, a equação tem uma solução, pois a tem um inverso módulo m. A solução é única módulo m porque $ax_1 \equiv b \pmod m$ e $ax_2 \equiv b \pmod m$ implica que $ax_1 \equiv ax_2 \pmod m$. Podemos cortar a, porque m.d.c. (a, m) = 1, obtendo desta forma $x_1 \equiv x_2 \pmod m$.

Se d > 1 e d ł b, então a congruência linear não tem solução, visto que m ł (ax – b) para algum x. Se d | b, então resolvemos $\frac{a}{d} x \equiv \frac{b}{d} \left(\text{mod } \frac{m}{d}\right)$.

Esta última equação tem uma única solução x_0 módulo $\frac{m}{d}$ porque $\frac{a}{d}$ tem um inverso módulo $\frac{m}{d}$. Ao escrevermos $\frac{a}{d} x_0 - \frac{b}{d} = k \frac{m}{d}$ para algum número inteiro k, podemos eliminar d e obtemos $ax_0 – b = km$. Então x_0 é uma solução para $ax \equiv b \pmod m$. Uma outra solução x precisa de satisfazer a equação $x \equiv x_0 \pmod{\frac{m}{d}}$, ou seja $x – x_0 = i\left(\frac{m}{d}\right)$. As soluções x_i e x_j são distintas módulo m se e só se $i \not\equiv j \pmod m$. Demonstremos esta última afirmação. Se $x_i \not\equiv x_j \pmod m$, então $i\left(\frac{m}{d}\right) \not\equiv j\left(\frac{m}{d}\right) \pmod m$. Como $\frac{m}{d}$ é um divisor de m, podemos dividir todos os termos por $\frac{m}{d}$ e obtemos $i \not\equiv j \pmod d$. Se $i \not\equiv j \pmod d$, então $x_i \not\equiv x_j \pmod m$. O que mostra que existem exactamente d soluções distintas.

■

3.3.10 Observação: resolver a congruência linear $ax \equiv b \pmod m$ é equivalente a resolver a equação ax – my = b. Pois

$ax \equiv b \pmod m \Leftrightarrow m \mid (ax-b) \Leftrightarrow ax – b = my \Leftrightarrow ax – my = b$, para algum $y \in \mathbb{Z}$.

Exemplo: consideremos a congruência linear $18x \equiv 30 \pmod{42}$. Como m.d.c. (18, 42) = 6, e 6 é um divisor de 30, podemos concluir que esta equação tem seis soluções distintas, que são congruentes módulo 42. Esta congruência linear é equivalente a 18x – 42y = 30, que é uma equação Diofantina.

Comecemos por escrever 6 = m.d.c. (18 , 42) como uma combinação linear de 18 e 42, ou seja, $42 - 2 \times 18 = 6$. Se multiplicarmos ambos os membros por 5, obtemos $18 \times (-10) - 42 \times (-5) = 30$, donde $x = -10$ e $y = -5$ satisfazem a equação Diofantina e consequentemente, todas as soluções de $18x \equiv 30 \pmod{42}$ são dadas pela fórmula $x = -10 + \frac{42}{6} \times t = -10 + 7 \times t$, em que $t = 0, 1, 2, 3, 4, 5$. Daqui podemos concluir que

$x \equiv -10 \pmod{42}$, $x \equiv -3 \pmod{42}$, $x \equiv 4 \pmod{42}$, $x \equiv 11 \pmod{42}$

$x \equiv 18 \pmod{42}$, $x \equiv 25 \pmod{42}$ são as soluções da congruência linear. Se quisermos só as soluções positivas temos $x \equiv 4, 11, 17, 25, 32, 39 \pmod{42}$.

3.3.11 Corolário. Se m.d.c. (a, n) = 1, então a congruência linear $ax \equiv b \pmod{n}$ tem uma única solução módulo n.

3.3.12 Teorema. (Teorema Chinês dos Restos) – Sejam $m_1, m_2, \ldots, m_k$ números primos relativos dois a dois, ou seja, tal que m.d.c. $(m_i, m_j) = 1$ para $i \neq j$, e sejam $a_1, a_2, \ldots, a_k$ números inteiros. Então, o sistema de congruências

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \ldots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

tem solução. Quaisquer duas soluções são congruentes módulo $m_1 m_2 \ldots m_k$.

Demonstração:

Seja $m = m_1 m_2 \ldots m_k$. Para cada $j \in \{1, 2, \ldots, k\}$, tem-se $\frac{m}{m_j} \in \mathbb{Z}$ e m.d.c. $\left(\frac{m}{m_j}, m_j\right) = 1$. Então, para cada j, a congruência $\frac{m}{m_j} x \equiv 1 \pmod{m_j}$ tem solução. Seja b_j uma solução dessa congruência. Tem-se, para cada

$j \in \{1, 2, \ldots, k\}$, por um lado $\frac{m}{m_j} b_j \equiv 1 \pmod{m_j}$ e por outro $\frac{m}{m_j} b_j \equiv 0 \pmod{m_i}$ se $i \neq j$ porque, se $i \neq j$, o número inteiro $\frac{m}{m_j}$ é múltiplo de m_i.

Seja $x_0 = \frac{m}{m_1} b_1 a_1 + \frac{m}{m_2} b_2 a_2 + \ldots + \frac{m}{m_k} b_k a_k$.

Então, para cada $j \in \{1, 2, \ldots, k\}$, tem-se $x_0 \equiv \frac{m}{m_j} b_j a_j \equiv a_j \pmod{m_j}$ ou seja x_0 é uma solução do sistema de congruências.

Como $m_1, m_2, \ldots, m_k$ são números primos dois a dois, tem-se $[m_1, m_2, \ldots, m_k] = m_1 m_2 \ldots m_k$, logo a segunda afirmação do teorema resulta de algumas propriedades da relação de congruência, pois se x' e x'' forem duas soluções do sistema acima indicado, então tem-se $x' \equiv x'' \pmod{m_1}$, $x' \equiv x'' \pmod{m_2}$, $\ldots$, $x' \equiv x'' \pmod{m_k}$.

O conjunto completo das soluções é então $[x_0]_m$.

■

Exemplo: Consideremos o sistema

$$x \equiv 2 \pmod 3$$

$$x \equiv 3 \pmod 5$$

$$x \equiv 2 \pmod 7.$$

Vamos utilizar o Teorema Chinês dos Restos, para resolver este sistema.

Sejam $m_1 = 3$, $m_2 = 5$ e $m_3 = 7$, logo $m = 3 \times 5 \times 7 = 105$, $c_1 = 35$, $c_2 = 21$ e $c_3 = 15$. Primeiro precisamos de encontrar uma solução $y = d_1$ de $c_1 y \equiv 1 \pmod{m_1}$, ou seja, $35y \equiv 1 \pmod 3$; o que é equivalente a: $-y \equiv 1 \pmod 3$; assim $y = d_1 = -1$, por exemplo. De forma análoga, $c_2 y \equiv 1 \pmod{m_2}$, feitas as devidas substituições, temos $21y \equiv 1 \pmod 5$, logo uma solução é $y = d_2 = 1$. Para $c_3 y \equiv 1 \pmod{m_3}$, temos $15y \equiv 1 \pmod 7$, podemos tomar para solução $y = d_3 = 1$. Finalmente, temos

$$x_0 = a_1 c_1 d_1 + a_2 c_2 d_2 + a_3 c_3 d_3 = 2 \times 35 \times (-1) + 3 \times 21 \times 1 + 2 \times 15 \times 1 = 23,$$

logo as soluções para o sistema são dadas por $x = 23 + 105t$ ($t \in \mathbb{Z}$).

3.4 Matrizes

Vamos abordar as matrizes de modo a compreendermos a cifra de Hill, que será estudada no próximo capítulo. Deste modo, não abordaremos o estudo

das matrizes de uma forma generalizada, mas apenas com o intuito de compreendermos o funcionamento desta cifra, no que respeita ao exemplo apresentado.

Considerando o parágrafo anterior, definimos a multiplicação de uma matriz quadrada 3×3 com uma matriz coluna 3×1. Para o efeito consideremos as matrizes: $A = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$ e $B = \begin{bmatrix} j \\ k \\ l \end{bmatrix}$, então

$A \times B = \begin{bmatrix} a \times j + b \times k + c \times l \\ d \times j + e \times k + f \times l \\ g \times j + h \times k + i \times l \end{bmatrix}$. A multiplicação de matrizes não é comutativa.

Vamos agora calcular o determinante da matriz A, utilizando a regra de Sarrus:

$\det A = |A| = (a \times e \times i + c \times d \times h + b \times f \times g) -$

$- (c \times e \times g + a \times f \times h + d \times b \times i).$

Com o cálculo do determinante de uma matriz quadrada, podemos saber se existe inversa para essa matriz, ou não!

Neste caso, se o determinante e 26 forem números primos entre si, então a matriz quadrada tem inversa; ou seja, existe uma matriz quadrada A^{-1}, tal que $A \times A^{-1} = A^{-1} \times A = I$, em que $I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, I é a matriz identidade módulo 26.

3.5 Teorema de Euler

3.5.1 Definição. Seja $m \in \mathbb{N}$. Um sistema reduzido de resíduos módulo m é um conjunto $\{r_1, r_2, \ldots, r_k\}$ de números inteiros satisfazendo m.d.c. $(r_i, m) = 1$, $i = 1, \ldots, k$; tal que, $i \neq j \Rightarrow r_i$ não é congruente com r_j módulo m e para todo $a \in \mathbb{Z}$, com m.d.c. $(a, m) = 1$, existe um r_i, para o qual $a \equiv r_i \pmod m$.

3.5.2 Definição. Seja m um número inteiro positivo. A função φ de Euler é uma função natural de variável natural onde $\varphi(m)$ é definida como o número de números naturais menores que m que são primos relativos a m.

Por exemplo $\varphi(15) = 8$. Pois 1, 2, 4, 7, 8, 11, 13 e 14 são primos relativos a 15.

3.5.3 Proposição. Sendo p um número primo e α um número natural, tem-se $\varphi\ (p^{\alpha}) = \ p^{\alpha} - \ p^{\alpha-1}$.

Demonstração:

$\varphi\ (p^{\alpha})$ é o número de números naturais ≤ p^{α} que são primos com p^{α}. Como p é número primo, os números naturais que não são primos com p^{α} são aqueles que têm p como divisor, ou seja: p, 2p, 3p, …, $p^{\alpha-1}$p.

Estes naturais são em número de $p^{\alpha-1}$, pelo que os números naturais ≤ p^{α} que são primos com p^{α} são em número de p^{α} - $p^{\alpha-1}$.

■

Como 25 = 5^2, temos que $\varphi(5^2) = \ 5^2 - \ 5 = 20$, ou seja, existem 20 números entre 1 e 24 que são primos relativos a 25; a saber: 1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23 e 24.

3.5.4 Corolário. Se p é um número primo, então $\varphi\ (p) = \ p - \ 1$.

Demonstração:

Pela proposição anterior, fazendo α = 1, o resultado é imediato.

■

Como 31 é primo, pelo corolário anterior, existem 30 números naturais menores que 31 que são primos relativos a 31.

3.5.5 Definição. Uma função aritmética f é multiplicativa se f(mn) = f(m)f(n), quando m.d.c.(m , n) = 1.

3.5.6 Lema. Se m e n são primos entre si, então φ (mn) = φ(m)φ(n), ou seja, φ é uma função multiplicativa.

Demonstração:

Sejam R_m = {x_1, …, $x_{\varphi(m)}$} um sistema reduzido de resíduos módulo m, R_n = {y_1, …, $y_{\varphi(n)}$} um sistema reduzido de resíduos módulo n e

$$S = \{ay_i + bx_j : i = 1,\ldots, \varphi(n), j = 1, \ldots, \varphi(m)\}.$$

Queremos provar que S é um sistema reduzido de resíduos módulo mn. Como S tem $\varphi(m) \times \varphi(n)$ elementos, provaremos que $\varphi(mn) = \varphi(m)\varphi(n)$.

Para mostrar que S é um sistema reduzido de resíduos módulo mn, necessitamos de mostrar três coisas:

Primeiro: que cada $x \in S$ e mn são primos relativos;

Segundo: que todos os elementos de S são distintos;

Terceiro: qualquer que seja o número inteiro a, tal que, m.d.c. (a, mn) = 1, então $a \equiv s \pmod{mn}$ para algum $s \in S$.

Seja $x = my_i + nx_j$. Como m.d.c. (x_j , m) = 1 e m.d.c. (m , n) = 1, temos então que m.d.c. (x , m) = 1. Analogamente, m.d.c. (x , n) = 1. Como x é primo relativo de m e n, temos que m.d.c. (x , mn) = 1. Mostramos que cada elemento do conjunto S é primo relativo de mn.

Em seguida, suponhamos que $(my_i + nx_j) \equiv (my_k + nx_l) \pmod{mn}$. Então

$mn \mid ((my_i + nx_j) - (my_k + nx_l)) \Rightarrow my_i \equiv my_k \pmod{n}$. Como m.d.c. (m, n) = 1, temos que $y_i \equiv y_k \pmod{n}$. Mas então $y_i = y_k$, visto que R_n é um sistema reduzido de resíduos. De forma semelhante, concluímos que $x_j = x_l$. O que mostra que os elementos de S são distintos módulo mn.

Finalmente, suponhamos m.d.c. (a , mn) = 1. Como m.d.c. (m , n) = 1, então existem x e y, tais que mx + ny = 1. Então max + nay = a. Como m.d.c. (x, n) = 1 e m.d.c. (a , n) = 1, temos que m.d.c. (ax, n) = 1. Consequentemente, existe um s_i tal que $ax = s_i + tn$. Da mesma maneira, m.d.c. (ay , m) = 1, e também existe um r_j tal que $ay = r_j + um$. Então

$$m(s_i + tn) + n(r_j + um) = a \Rightarrow a = ms_i + nr_j + (t + u)mn \Rightarrow a \equiv mr_i + ns_j \pmod{mn},$$

o que demonstra o terceiro passo.

■

Podemos determinar $\varphi(20)$, utilizando o teorema anterior,

$$\varphi(20) = \varphi(5 \times 4) = \varphi(5) \times \varphi(4) = 4 \times 2 = 8.$$

3.5.7 Corolário. Seja m = $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ a factorização em números primos de m, então $\varphi(m) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1) = m \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$.

Demonstração:

Como φ é multiplicativa, temos que

$$\begin{aligned}
\varphi(m) &= \varphi\left(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}\right) = \varphi\left(p_1^{\alpha_1}\right).\varphi\left(p_2^{\alpha_2}\right) \ldots \varphi\left(p_k^{\alpha_k}\right) = \\
&= \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right)\left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right) \ldots \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right) = \\
&= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \ldots . p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right) = \\
&= p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right) = \\
&= m \prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right).
\end{aligned}$$

■

Vamos recorrer a este corolário, para determinar $\varphi(60)$. Temos que 2, 3 e 5 são os números primos que são divisores de 60, então

$$\varphi(60) = 60 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right) \times \left(1 - \frac{1}{5}\right) = 60 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 16 .$$

3.5.8 Lema. Seja n > 1 e m.d.c. (a, n) = 1. Se $a_1, a_2, \ldots, a_{\varphi(n)}$ são números inteiros positivos menores que n e primos relativos com n, então

$$aa_1, aa_2, \ldots, aa_{\varphi(n)}$$

são congruentes módulo n com $a_1, a_2, \ldots, a_{\varphi(n)}$ pela mesma ordem.

3.5.9 Teorema de Euler. Sejam a um número inteiro e m um número inteiro positivo tais que m.d.c. (a, m) = 1, então $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Demonstração:

Seja $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ um sistema reduzido de resíduos módulo m. Pelo lema anterior, $\{ar_1, ar_2, \ldots, ar_{\varphi(m)}\}$ é também um sistema reduzido de resíduos módulo m. Para cada elemento ar_i do segundo sistema existe um e um só elemento r_j do primeiro tal que $ar_i \equiv r_j \pmod{m}$.

Multiplicando membro a membro todas estas φ (m) congruências obtemos $ar_1ar_2 \ldots ar_{\varphi(m)} \equiv r_1r_2\ldots r_{\varphi(m)} \pmod m$ temos que

$$a^{\varphi(m)}r_1r_2 \ldots r_{\varphi(m)} \equiv r_1r_2\ldots r_{\varphi(m)} \pmod m.$$

Como todos os r_i são primos com m, também o seu produto é primo com m, pelo que pela teorema 3.3.7, ponto um, temos $a^{\varphi(m)} \equiv 1 \pmod m$.

■

Podemos aplicar este teorema para encontrar os dois últimos dígitos de 3^{1492}. O que é equivalente a determinar o menor resíduo não negativo de $3^{1492} \pmod{100}$. O m.d.c. (3, 100) = 1, logo, pelo teorema de Euler, $3^{\varphi(100)} \equiv 1 \pmod{100}$, ou seja, $3^{40} \equiv 1 \pmod{100}$, já que $\varphi(100) = 40$. Como $1492 \equiv 12 \pmod{40}$, então $3^{1492} \equiv 3^{12} \pmod{100}$. Como $3^4 = 81 \equiv -19 \pmod{100}$, então $3^8 \equiv (-19)^2 = 361 \equiv -39$ e assim concluímos que $3^{12} \equiv (-19) \times (-39) = 741 \equiv 41$. Os dois últimos dígitos de 3^{1492} são o 4 e o 1.

3.5.10 Corolário. Se m.d.c. (a, m) = 1 e n' é o menor resíduo de n, não negativo, módulo φ(m), então $a^n \equiv a^{n'} \pmod m$.

3.6 Raizes primitivas

3.6.1 Definição. – Sejam a e n números inteiros tais que m.d.c. (a, n) = 1. Então a ordem de a módulo n, com notação $ord_n(a)$ é o menor número inteiro k, tal que $a^k \equiv 1 \pmod n$.

A ordem de 2 módulo 31 é 5, visto que 5 é o menor número inteiro que satisfaz a condição $2^k \equiv 1 \pmod{31}$. Pois $2^1 \equiv 2 \pmod{31}$, $2^2 \equiv 4 \pmod{31}$, $2^3 \equiv 8 \pmod{31}$, $2^4 \equiv 16 \pmod{31}$ e $2^5 \equiv 1 \pmod{31}$.

Temos que a $ord_n(a) \leq \varphi(n)$, para m.d.c (a, n) = 1; visto que pelo teorema de Euler $a^{\varphi(n)} \equiv 1 \pmod n$.

3.6.2 Proposição. – Seja $a^m \equiv 1 \pmod n$; então $\mathrm{ord}_n(a) \mid m$.

Demonstração:

Seja k = $ord_n(a)$. Pelo algoritmo da divisão, existe um quociente q e um resto r tal que , m = kq + r, $0 \leq r < q$.

Se $ord_n a \nmid m$, então $r \neq 0$.

Temos então que $a^m \equiv a^{kq+r} \equiv a^{kq}a^r \equiv a^r \pmod n$, pelo que $a^r \equiv 1 \pmod n$. Como r < k, então r = 0 (k é o menor número inteiro positivo que satisfaz esta congruência) e temos que $ord_n(a) \mid m$.

■

3.6.3 Corolário. - Suponhamos que m.d.c. (a, n) = 1 e $a^i \equiv a^j \pmod n$; então $i \equiv j \pmod{ord_n(a)}$.

Demonstração:

Como m.d.c. (a, n) = 1, a^j é invertível e o seu inverso é $\left(a^{-1}\right)^j$. Daqui sai que $a^i a^{-j} \equiv a^j a^{-j} \pmod n$, logo $a^{i-j} \equiv 1 \pmod n$. Isto implica que $ord_n(a) \mid (i - j)$, ou seja, $(i - j) \equiv 0 \pmod{ord_n(a)}$ ou $i \equiv j \pmod{ord_n(a)}$.

■

3.6.4 Corolário. – Se m.d.c. (a, n) = 1, então a $ord_n(a) \mid \varphi(n)$. Em particular, se p é um número primo e m.d.c. (a, p) = 1, então $ord_p(a) \mid p - 1$.

3.6.5 Lema. – Se m.d.c. (a, n) = 1, então a $ord_n(a^k) = \frac{ord_n(a)}{\text{m.d.c. } (k,\ ord_n(a))}$.

Demonstração:

Seja $x = \frac{ord_n(a)}{\text{m.d.c. } (k,\ ord_n(a))}$). Por um lado,

$$\left(a^k\right)^x \equiv a^{kx} \equiv \left(a^{ord_n(a)}\right)^{\frac{k}{\text{m.d.c. } (k,\ ord_n(a))}} \equiv 1 \pmod n,$$

o que implica que $ord_n(a) \mid x$. por outro lado, se $l = ord_n(a^k)$, então $\left(a^k\right)^l \equiv a^{kl} \equiv 1 \pmod n$, logo a $ord_n(a) \mid kl$. Podemos escrever $kl = ord_n(a)c$ para algum $c \in \mathbb{Z}$. Se dividirmos, ambos os lados, pelo máximo divisor comum de k e $ord_n(a)$, temos que $x \mid l$. Pelo que $ord_n(a^k) = \frac{ord_n(a)}{\text{m.d.c. } (k,\ ord_n(a))}$.

■

Suponhamos que $ord_n(a) = 15$, então $ord_n(a^{20}) = \frac{15}{\text{m.d.c. } (20,15)} = \frac{15}{5} = 3$.

3.6.6 Corolário. – Se a tem ordem k módulo n. Então a^h tem ordem k se e só se m.d.c. (h, k) = 1.

3.6.7 Definição. – Se m.d.c. (a, n) = 1 e $ord_n(a) = \varphi(n)$, então a diz-se uma raiz primitiva módulo n, ou seja, o conjunto $\{a, a^2, a^3, \ldots, a^{\varphi(n)}\}$ é um sistema de resíduos módulo n.

3 é uma raiz primitiva módulo 31, pois $ord_{31}(3) = 30$. No entanto, nem todos os números naturais têm raízes primitivas.

3.6.8 Teorema. – Para $k \geq 3$, os números inteiros 2^k não têm raízes primitivas.

Demonstração:

Comecemos por mostrar que se a é um número ímpar, então para $k \geq 3$, $a^{2^{k-2}} \equiv 1 \pmod{2^k}$.

Para k = 3, temos a congruência $a^2 \equiv 1 \pmod 8$, que é verdadeira, pois $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$. Para k > 3, vamos provar pelo método de indução. Por hipótese de indução, seja verdadeira para k, a congruência $a^{2^{k-2}} \equiv 1 \pmod{2^k}$. O que é equivalente à equação $a^{2^{k-2}} = 1 + b2^k$, com $b \in \mathbb{Z}$. Elevando ambos os membros ao quadrado, obtemos

$$a^{2^{k-1}} = \left(a^{2^{k-2}}\right)^2 = 1 + 2\left(b2^k\right) + \left(b2^k\right)^2$$

$$= 1 + 2^{k+1}\left(b + b^2 2^{k-1}\right)$$

$$\equiv 1 \pmod{2^{k+1}},$$ o que prova a tese de indução, ou seja a congruência é válida para $k + 1$.

Os números inteiros que são primos com 2^k são os números ímpares; mas $\varphi\left(2^k\right) = 2^{k-1}$. O que prova, se a é um número ímpar e $k \geq 3$, então $a^{\frac{\varphi(2^k)}{2}} \equiv 1 \pmod{2^k}$ e, consequentemente, não existem raízes primitivas de 2^k.

■

3.6.9 Teorema. Se m.d.c. (m, n) = 1, onde m > 2 e n > 2, então o número inteiro $m \times n$ não tem raízes primitivas.

Demonstração:

Consideremos a um número inteiro tal que m.d.c. (a , m×n) = 1; então m.d.c. (a, m) = 1 e m.d.c. (a , n) = 1. E seja h = m.m.c. (φ(m), φ (n)) e d = m.d.c. (φ(m), φ (n)).

Como φ(m) e φ (n) são ambos pares, podemos concluir que d ≥ 2.

$$\text{Logo } h = \frac{\varphi(m)\varphi(n)}{d} \leq \frac{\varphi(mn)}{2}.$$

Temos que $a^{\varphi(m)} \equiv 1 \pmod{m}$, pelo teorema de Euler. Daqui tirámos a seguinte conclusão: $a^h = (a^{\varphi(m)})^{\frac{\varphi(n)}{d}} \equiv 1^{\frac{\varphi(n)}{d}} \equiv 1 \pmod{m}$.

De forma análoga, concluímos que $a^h \equiv 1 \pmod{n}$. Com estas duas últimas congruências e como m.d.c. (m , n) = 1, por hipótese, temos que

$$a^h \equiv 1 \pmod{m \times n}.$$

A ordem de m×n, como m e n são primos entre si, é inferior ou igual a $\frac{\varphi(m \times n)}{2}$, logo não existem raízes primitivas para m×n.

■

Do teorema anterior podemos tirar as conclusões que se encontram no próximo corolário.

3.6.10 Corolário. Um número inteiro n não tem raízes primitivas se verifica uma das seguintes propriedades:

(1) n é divisível por dois números primos ímpares;

(2) $n = 2^m p^k$, onde p é um número primo ímpar e m ≥ 2.

3.6.11 Teorema. Se p é um número primo e d | (p -1), então existem φ(d) números inteiros incongruentes módulo p, que têm ordem d.

De um modo particular, se substituirmos d por p – 1, concluímos que existem φ(p - 1) raízes primitivas de p. Logo todo o número primo tem raízes primitivas.

3.6.12 Lema. Se p é um número primo, então existe uma raiz primitiva de p tal que $r^{p-1} \not\equiv 1 \pmod{p^2}$.

Demonstração:

Como p é um número primo, então p tem raízes primitivas. Escolhemos uma delas, a qual designaremos por r. Se $r^{p-1} \not\equiv 1 \pmod{p^2}$, a demonstração está feita.

Caso contrário, consideremos a raiz primitiva de p: r + p = s. Temos então o seguinte: $s^{p-1} \equiv ((r + p)^{p-1} \equiv r^{p-1} + (p - 1)pr^{p-2} \pmod{p^2}$.

Como $r^{p-1} \equiv 1 \pmod{p^2}$, daqui $s^{p-1} \equiv (1 - pr^{p-2}) \pmod{p^2}$.

Considerando que r é raiz primitiva de p, m.d.c. (r , p) = 1 e $p \nmid r^{p-2}$,

então $s^{p-1} \not\equiv 1 \pmod{p^2}$.

■

3.6.13 Corolário. Se p é um número primo ímpar, então p^2 tem uma raiz primitiva. Se r é uma raiz primitiva de p, então ou r ou r + p é uma raiz primitiva de p^2.

Demonstração:

Se r é uma raiz primitiva de p, então a ordem de r módulo p^2 é p – 1 ou p(p – 1) = $\varphi(p^2)$. Da demonstração do teorema anterior, temos que se r tem ordem p – 1 módulo p^2, então r + p será raiz primitiva de p^2.

■

3.6.14 Lema. - Seja p um número primo ímpar e r uma raiz primitiva de p tal que $r^{p-1} \not\equiv 1 \pmod{p^2}$. Então para cada $k \geq 2$, $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$.

Demonstração:

A demonstração é feita por indução em k. Para k = 2, temos que $r^{p^{(2-2)}(p-1)} \not\equiv 1 \pmod{p^2}$, ou seja, $r^{p-1} \not\equiv 1 \pmod{p^2}$, o que é verdade por hipótese. Consideremos a incongruência verdadeira para todo $k \geq 2$ e vamos mostrar que a incongruência é verdadeira para k + 1. Como

$$\text{m.d.c. } (r , p^{k-1}) = \text{m.d.c. } (r , p^k) = 1,$$

pelo teorema de Euler, temos que $r^{p^{k-2}(p-1)} = r^{\varphi(p^{k-1})} \equiv 1 \pmod{p^{k-1}}$.

Daqui, concluímos que existe um número inteiro a que satisfaz a seguinte igualdade $r^{p^{k-2}(p-1)} = 1 + ap^{k-1}$, onde $p \nmid a$ pela nossa hipótese de indução. Elevando a p ambos os membros desta última equação obtemos o seguinte:

$$r^{p^{k-1}(p-1)} = (1 + ap^{k-1})^{p} \equiv 1 + ap^{k} (\text{mod } p^{k+1}).$$

Como o número inteiro a não é divisível por p, temos que $r^{p^{k-1}(p-1)} \not\equiv 1 (\text{mod } p^{k+1})$.

■

3.6.15 Teorema. Se p é um número ímpar e $k \geq 1$, então existe uma raiz primitiva para p^k.

Demonstração:

Pelos dois lemas anteriores podemos escolher uma raiz primitiva r de p tal que $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$; de facto, algum r satisfaz $r^{p-1} \not\equiv 1 \pmod{p^2}$. Queremos provar que r é uma raiz primitiva para todas as potências de base p.

Se n é a ordem de r módulo p^k. Temos então que n divide $\varphi(p^k) = p^{k-1}(p-1)$. Como $r^n \equiv 1 \pmod{p^k}$, implica que $r^n \equiv 1 \pmod{p}$, pelo que $(p-1) | n$. Consequentemente, $n = p^m(p-1)$, onde $0 \leq m \leq k-1$. Se $n \neq p^{k-1}(p-1)$, então $p^{k-2}(p-1)$ será dividido por n, logo $r^{p^{k-2}(p-1)} \equiv 1 \pmod{p^k}$, o que contradiz a forma como r foi escolhido. Temos então que $n = p^{k-1}(p-1)$ e r é uma raiz primitiva de p^k.

■

3.6.16 Corolário. Existem raízes primitivas de $2p^k$, onde p é um número primo ímpar e $k \geq 1$.

Demonstração:

Se r é uma raiz primitiva de p^k. Consideremos que r é um número inteiro ímpar; se fosse um número inteiro par, então $r + p^k$ seria um número inteiro ímpar e uma raiz primitiva de p^k. Então m.d.c. $(r, 2p^k) = 1$. A ordem n de r módulo $2p^k$ divide $\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k)$.

Mas $r^n \equiv 1 \pmod{2p^k}$ implica que $r^n \equiv 1 \pmod{p^k}$, então $\varphi(p^k) | n$. Logo concluímos que $n = \varphi(2p^k)$, ou seja, r é uma raiz primitiva de $2p^k$.

■

3.6.17 Teorema das raízes primitivas. Seja m > 1. Existe uma raiz primitiva módulo m se e só se verifica um dos casos:

$m \in \{2, 4\}$;

$m = p^k$, com p um número primo ímpar e $k \in \mathbb{N}$;

$m = 2p^k$, com p um número primo ímpar e $k \in \mathbb{N}$.

Demonstração:

1 é uma raiz primitiva de 2 e 3 é uma raiz primitiva de 4,como se prova a seguir: temos que $\varphi(2) = 1$ e $\varphi(4) = 2$, daqui obtemos que

$1^1 \equiv 1 \pmod 2$ logo 1 é raiz primitiva de 2; $3^1 \equiv 3 \pmod 4$ e $3^2 \equiv 1 \pmod 4$ logo 3 é raiz primitiva de 4. Está demonstrado o primeiro caso.

Os outros dois casos estão demonstrados pelo teorema e corolários anteriores.

■

3.7 Pequeno Teorema de Fermat

3.7.1 Definição. O coeficiente binomial com parâmetros n e $k \leq n$ é o número inteiro definido por $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

3.7.2 Teorema. Um número inteiro n é número primo se e só se $\binom{n}{k} \equiv 0 \pmod n$ para todo $1 \leq k \leq n-1$.

Demonstração: Suponhamos que n é número primo, e seja $1 \leq k \leq n-1$. Por definição, $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ é um número inteiro. Um dos factores do numerador desta fracção é o n, mas o seu denominador não contem nenhum factor n, pois tanto k como (n – k) são inferiores a n, logo k! e (n – k)! não têm nenhum factor n. Como n é primo, nunca desaparecerá do numerador da fracção, qualquer que seja a simplificação que se faça, ou seja, todo $\binom{n}{k}$ é múltiplo de n, concluímos então que $\binom{n}{k} \equiv 0 \pmod n$.

Suponhamos agora que $\binom{n}{k} \equiv 0 \pmod n$ para todo $1 \leq k \leq n-1$ e com vista a uma contradição que n é um número composto. Seja p um factor primo de n, e p^c a maior potência de p que divide n. Por hipótese temos que $\binom{n}{k} \equiv 0 \pmod n$, o que mostraremos ser falso.

Por definição, $\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)(n-2)\ldots(n-p+1)}{p!}$. No numerador, n é o único termo que tem factores de p, porque o menor múltiplo de p a seguir a n é n – p.

Como o numerador tem exactamente c factores de p, e o denominador tem só o próprio p como factor de p, concluímos que $\binom{n}{k}$ tem c -1 factores de p, e $p^c \nmid \binom{n}{k}$. O que significa que $\binom{n}{k}$ não é múltiplo de p^c, logo não pode ser múltiplo de n. O que contradiz a hipótese que $\binom{n}{k} \equiv 0 \pmod{n}$, então a nossa suposição é falsa. Pelo que n é um número primo.

■

3.7.3 Pequeno Teorema de Fermat. Sejam p um número primo e a um número inteiro positivo.

Então $a^p \equiv a \pmod{p}$. Em particular, se $p \nmid a$, então $a^{p-1} \equiv 1 \pmod{p}$.

Demonstração:

Vamos provar este teorema por indução em a. Para a = 1, temos que $a^{p-1} = 1$, logo $a^{p-1} \equiv 1 \pmod{p}$. Para hipótese de indução consideremos o teorema verdadeiro para a = n. Vamos provar o teorema para a = n + 1. Temos que $(n+1)^p = n^p + \binom{p}{1} n^{p-1} + \binom{p}{2} n^{p-2} + \ldots + \binom{p}{p-1} n + 1$.

Para $1 \leq k \leq p-1$, o coeficiente binomial $\binom{p}{k}$ é divisível por p, pelo teorema anterior. $\binom{p}{k} = \frac{p!}{k!(p-k)!}$, como p é primo, o factor p do numerador não pode ser "cortado" por nenhum dos factores do denominador, pois estes factores são menores que p. Logo, $(n+1)^p \equiv (n^p + 1) \pmod{p}$. Como por hipótese de indução, $n^p \equiv n \pmod{p}$, podemos concluir que $(n+1)^p \equiv (n+1) \pmod{p}$.

■

Podemos encontrar o menor resto da divisão de 3^{91} por 23, com a ajuda do Pequeno Teorema de Fermat. 23 é um número primo e 3 não é divisível por 23, pelo que $3^{22} \equiv 1 \pmod{23}$, como $91 = 4 \times 22 + 3$,então

$3^{91} \equiv (3^{22})^4 \times 3^3 \equiv 4 \pmod{23}$.

3.7.4 Definição. n é um pseudoprimo de base $a \in \mathbb{Z}$, se para n > 1 composto tem-se $a^{n-1} \equiv 1 \pmod{n}$.

Temos, por exemplo, que 91 é um pseudoprimo para a base 3 (3-pseudoprimo). Sabemos que 91 é um número composto, pois 91 = 7 × 13; vamos mostrar que $3^{90} \equiv 1 \pmod{91}$. Como

$3^2 \equiv 9 \pmod{91}$, $3^4 \equiv 81 \pmod{91}$, $3^8 \equiv 9 \pmod{91}$, $3^{16} \equiv 81 \pmod{91}$, $3^{32} \equiv 9 \pmod{91}$ e $3^{64} \equiv 81 \pmod{91}$, então

$3^{90} \equiv 3^{64} \times 3^{16} \times 3^8 \times 3^2 \pmod{91} \equiv 81 \times 81 \times 9 \times 9 \pmod{91} \equiv$

$\equiv 531441 \pmod{91} \equiv 1 \pmod{91}$, logo 91 é um 3-pseudoprimo.

3.7.5 Definição. Um número inteiro composto n diz-se um número de Carmichael se $a^{n-1} \equiv 1 \pmod{n}$ para todo o número inteiro a tal que m.d.c. (a , n) = 1.

O menor número Carmichael é o 561; no entanto, o conjunto dos números Carmichael é infinito. O que foi provado por Alford, Granville e Pomerance.

3.7.6 Teorema. (**Alford, Granville, Pomerance)** Existem infinitos números de Carmichael. Em particular, se C(x) define o número de números de Carmichael menores ou iguais a x, então $C(x) > x^{\frac{2}{7}}$ para x suficientemente grande.

3.7.7 Observação: Apesar da cardinalidade dos números de Carmichael não ser finita, a sua distribuição é fraca, o que nos permite confiar nalguns testes de primalidade.

3.7.8 Teorema. (Critério de Korselt) Um número n inteiro positivo ímpar é um número de Carmichael se, e só se, cada factor primo p de n satisfaz as seguintes condições:

1. p^2 não divide n;
2. p – 1 divide n – 1.

Demonstração:

Primeiro, vamos mostrar que se num número n a sua factorização não é livre de quadrados, então não pode ser um número Carmichael.

Suponhamos que a sua factorização de n tem quadrados. Então existe um primo p tal que $p^2 \mid n$. Pelo teorema 3.6.17 o grupo multiplicativo $\mathbb{Z}_{p^2}$ é cíclico (ou seja, tem uma raiz primitiva) e daqui concluímos que existe um gerador g (mod p^2). Como $\varphi(p^2) = p(p-1)$, temos que $g^{p(p-1)} \equiv 1 \pmod{p^2}$ e é a menor potência de g que é congruente com 1 módulo p^2. Agora seja $m = p_1 p_2 \ldots p_k$, onde $p_1, \ldots, p_k$ são outros números primos diferentes de p que dividem n. Note-se que p^k não é um número Carmichael, logo estes primos existem. Escolhamos uma solução b para o par de congruências

$$b \equiv g \pmod{p^2}$$

$$b \equiv 1 \pmod{m},$$

que existe pelo teorema chinês dos restos. Como $b \equiv g \bmod p^2$, temos que b também tem ordem multiplicativa $p(p-1) \pmod{p^2}$. Suponhamos que n era um número Carmichael. Então n seria um pseudoprimo para a base b e daqui temos que $b^{n-1} \equiv 1 \pmod{n}$. O que implica que $p(p-1) \mid n$, visto que p(p -1) é a ordem de b. Contudo, se $p \mid n$, temos que $n - 1 \equiv -1 \pmod{p}$. Por outro lado, se $p(p-1) \mid (n-1)$, temos que $n - 1 \equiv 0 \pmod{p}$, ou seja uma contradição. Pelo que n não pode ser um pseudoprimo para a base b e por conseguinte não é um número Carmichael.

Suponhamos agora que n é livre de quadrados, ou seja, $n = p_1 p_2 \ldots p_k$ com $k \geq 2$ e os p_i primos distintos. Consideremos primeiro que $(p_1 - 1) \mid (n-1)$ para $i = 1, \ldots, k$ e seja m.d.c. (b, n) = 1. Então

$$b^{n-1} \equiv b^{(p_1 - 1)k} \equiv 1^k \equiv 1 \pmod{p_i},\ i = 1, \ldots, k.$$

Temos então que $b^{n-1} \equiv 1 \pmod{p_i \ldots p_k} \equiv 1 \pmod{n}$. Por conseguinte, n é um pseudoprimo para a base b e como b é arbitrário com m.d.c. (b, n) = 1, segue-se que n é um número Carmichael.

Inversamente, suponhamos que $n = p_1 \ldots p_k$ é um número de Carmichael. Seja p_i, um desses primos e seja g um gerador do grupo multiplicativo de $\mathbb{Z}_{p_i}$. Um grupo que seja livre de quadrados é cíclico. Temos então que g tem ordem multiplicativa $p_i - 1 \pmod{p_i}$. Agora seja b uma solução do seguinte par de congruências

$$b \equiv g \pmod{p_i}$$

$$b \equiv 1 \pmod{\frac{n}{p_i}}.$$

Então b também tem ordem multiplicativa p – 1 (mod p_i). Temos ainda que m.d.c. (b, p_1) = 1 e m.d.c. (b, $\frac{n}{p_i}$) = 1 segue-se então que m.d.c. (b, n) = 1. Como n é um número Carmichael é um pseudoprimo para a base b e por isso

$b^{n-1} \equiv 1 \pmod{n} \Rightarrow b^{n-1} \equiv 1 \pmod{p_i}$. Concluímos que $(p_1 - 1)|(n-1)$, o que demonstra o teorema.

■

3.8 Resíduos Quadráticos

3.8.1 Definição de resíduo quadrático. Seja p um número primo ímpar e x um número inteiro, $1 \leq x \leq p-1$. x é um resíduo quadrático módulo p se a congruência $y^2 \equiv x \pmod{p}$ tiver uma solução $y \in \mathbb{Z}_p$. Se não tiver, diz – se um resíduo não quadrático.

Consideremos p = 13. Temos que

$$1^2 \equiv 12^2 \equiv 1,$$

$$2^2 \equiv 11^2 \equiv 4,$$

$$3^2 \equiv 10^2 \equiv 9,$$

$$4^2 \equiv 9^2 \equiv 3,$$

$$5^2 \equiv 8^2 \equiv 12,$$

$$6^2 \equiv 7^2 \equiv 10.$$

Temos então que os resíduos quadráticos de 13 são: 1, 3, 4, 9, 10 e 12. E os resíduos não quadráticos são: 2, 5, 6, 7, 8 e 11.

3.8.2 Teorema. (Critério de Euler) - Seja p > 2 um número inteiro primo. Então a é um resíduo quadrático módulo p se e só se $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Demonstração:

Suponhamos que a é um resíduo quadrático de p, então $x^2 \equiv a \pmod p$ admite uma solução, que será designada por x_1. Como m.d.c. (a, p) = 1, evidentemente m.d.c. (x_1, p) = 1. Recorrendo ao Pequeno Teorema de Fermat, temos que: $a^{\frac{p-1}{2}} \equiv (x_1{}^2)^{\frac{p-1}{2}} \equiv x_1{}^{p-1} \equiv 1 \pmod p$, o que prova a primeira implicação.

Em sentido inverso, temos que se $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ e seja r uma raiz primitiva de p. Então $a \equiv r^k \pmod p$ para algum número inteiro k, com $1 \leq k \leq p-1$. Podemos concluir então que $r^{\frac{k(p-1)}{2}} \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod p$.

Pela proposição 3.6.2, a ordem de r (nomeadamente, p – 1) divide o expoente $\frac{k(p-1)}{2}$. O que implica que k é um número par, seja k = 2j. Temos então que $(r^j)^2 = r^{2j} = r^k \equiv a \pmod p$, sendo r^j uma solução da congruência $x^2 \equiv a \pmod p$. o que prova que a é um resíduo quadrático do número primo p.

Se p é um número primo ímpar e m.d.c. (a, p) = 1, então

$(a^{\frac{(p-1)}{2}} - 1)\left((a^{\frac{(p-1)}{2}} + 1\right) = a^{p-1} - 1 \equiv 0 \pmod p$, esta última congruência é justificada pelo Pequeno Teorema de Fermat. Daqui podemos concluir que se verifica apenas uma e uma só das congruências seguintes:

$$a^{\frac{(p-1)}{2}} \equiv 1 \pmod p \text{ ou } a^{\frac{(p-1)}{2}} \equiv -1 \pmod p.$$

Se as congruências anteriores se verificassem simultaneamente, então teríamos $1 \equiv -1 \pmod p$, o que seria equivalente, a $p \mid 2$, o que não está de acordo com a nossa hipótese. Daqui concluímos que se a é um não resíduo quadrático não satisfaz a congruência $a^{\frac{(p-1)}{2}} \equiv 1 \pmod p$, logo terá que satisfazer $a^{\frac{(p-1)}{2}} \equiv -1 \pmod p$.

■

3.8.3 Corolário. Seja p um número primo ímpar e m.d.c. (a, p) = 1. Então a é um resíduo quadrático ou um resíduo não quadrático de p consoante $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ou $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, respectivamente.

Considerando p = 17, temos que $3^{\frac{17-1}{2}} = 3^8 = 6561 \equiv -1 \pmod{17}$, ou seja, 3 não é um resíduo quadrático de 17.

3.8.4 Definição. (Símbolo de Legendre) – Seja p um número primo > 2. Para a ≥ 0, o símbolo de Legendre, $\left(\frac{a}{p}\right)$ é definido da seguinte forma:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ se } & a \equiv 0 \pmod{p} \\ 1 \text{ se } & a \text{ é um resíduo quadrático módulo p} \\ -1 \text{ se } & a \text{ não é um resíduo quadrático módulo p.} \end{cases}$$

No caso de p = 13 e considerando o critério de Euler, obtemos o seguinte:

$$1^{\left(\frac{13-1}{2}\right)} \equiv 1 \pmod{13}$$

$$2^{\left(\frac{13-1}{2}\right)} = 2^6 = 64 \equiv -1 \pmod{13}$$

$$3^{\left(\frac{13-1}{2}\right)} = 3^6 = 729 \equiv 1 \pmod{13}$$

$$4^{\left(\frac{13-1}{2}\right)} = 4^6 = 4096 \equiv 1 \pmod{13}$$

$$5^{\left(\frac{13-1}{2}\right)} = 5^6 = 15525 \equiv -1 \pmod{13}$$

$$6^{\left(\frac{13-1}{2}\right)} = 6^6 = 46656 \equiv -1 \pmod{13}$$

$$7^{\left(\frac{13-1}{2}\right)} = 7^6 = 117649 \equiv -1 \pmod{13}$$

$$8^{\left(\frac{13-1}{2}\right)} = 8^6 = 262144 \equiv -1 \pmod{13}$$

$$9^{\left(\frac{13-1}{2}\right)} = 9^6 = 531441 \equiv 1 \pmod{13}$$

$$10^{\left(\frac{13-1}{2}\right)} = 10^6 = 1000000 \equiv 1 \pmod{13}$$

$$11^{\left(\frac{13-1}{2}\right)} = 11^6 = 1771561 \equiv -1 \pmod{13}$$

$$12^{\left(\frac{13-1}{2}\right)} = 12^6 = 2985984 \equiv 1 \pmod{13}.$$

Daqui podemos concluir que:

$$\left(\frac{1}{13}\right) = \left(\frac{3}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{9}{13}\right) = \left(\frac{10}{13}\right) = \left(\frac{12}{13}\right) = 1$$

$$\left(\frac{2}{13}\right) = \left(\frac{5}{13}\right) = \left(\frac{6}{13}\right) = \left(\frac{7}{13}\right) = \left(\frac{8}{13}\right) = \left(\frac{11}{13}\right) = -1$$

3.8.5 Teorema. Seja p um número primo ímpar e a e b números inteiros, os quais são primos relativos a p. Então o símbolo de Legendre tem as seguintes propriedades:

1. Se $a \equiv b \pmod{p}$, então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. $\left(\frac{a^2}{p}\right) = 1$.
3. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.
4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
5. $\left(\frac{1}{p}\right) = 1$ e $\left(-\frac{1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Demonstração:

1. Se $a \equiv b \pmod{p}$, então $x^2 \equiv a \pmod{p}$ e $x^2 \equiv b \pmod{p}$ têm exactamente as mesmas soluções. Desta forma $x^2 \equiv a \pmod{p}$ e $x^2 \equiv b \pmod{p}$, ou são ambas **solúveis**, ou nenhuma tem solução. Logo $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. a é uma solução trivial de $x^2 \equiv a^2 \pmod{p}$, logo $\left(\frac{a^2}{p}\right) = 1$.
3. É um corolário do critério de Euler.
4. Vamos utilizar esta última propriedade para provar a propriedade 4:

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Se fosse $\left(\frac{ab}{p}\right) \neq \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, teríamos $1 \equiv -1 \pmod{p}$ ou $2 \equiv 0 \pmod{p}$; o que não acontece desde que $p > 2$.

5. Na última propriedade, temos que a primeira igualdade é um caso particular da segunda propriedade; a outra igualdade obtém-se de três, substituído a por – 1. Como os resultados de $\left(\frac{-1}{p}\right)$ e $(-1)^{\frac{p-1}{2}}$ são ou 1 ou – 1, temos que $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$ implica que $\left(-\frac{1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

■

3.8.6 Observação: Das propriedades 2 e 4 do teorema anterior, podemos concluir que $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{a}{p}\right)$.

3.8.7 Corolário. Se p é um número primo ímpar, então

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 \text{ se } p \equiv 1 \pmod{4} \\ -1 \text{ se } p \equiv 3 \pmod{4} \end{cases}.$$

3.8.8 Teorema. Se p e q são números primos ímpares distintos, então $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, excepto quando $p \equiv q \equiv 3 \pmod{4}$, neste caso, $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.

3.8.9 Lema. Se p é um número primo ímpar, então $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$; por conseguinte, 2 é um resíduo quadrático se e só se $p \equiv \pm 1 \pmod{8}$.

3.8.10 Teorema. Se p é um número primo ímpar, então $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$.

Daqui, concluímos que existem precisamente $\frac{p-1}{2}$ resíduos quadráticos e $\frac{p-1}{2}$ resíduos não quadráticos.

Demonstração:

Seja r uma raiz primitiva de p. Sabemos que as potências r, r^2,..., r^{p-1} são uma permutação, módulo p, dos números inteiros 1, 2, ...,p – 1. Pelo que, para a, compreendido entre 1 e p – 1, inclusive, existe um único número inteiro positivo k ($1 \leq k \leq p - 1$), tal que $a \equiv r^k \pmod p$. Pelo critério de Euler, temos (*) $\left(\frac{a}{p}\right) = \left(\frac{r^k}{p}\right) \equiv (r^k)^{\frac{p-1}{2}} = \left(r^{\frac{p-1}{2}}\right)^k \equiv (-1)^k \pmod p$, como r é uma raiz primitiva, vem $r^{\frac{p-1}{2}} \equiv -1 \pmod p$. Mas $\left(\frac{a}{p}\right)$ e $(-1)^k$ são iguais a 1 ou a – 1, por (*). Se somarmos os símbolos de Legendre em questão, obtemos o seguinte:

$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = \sum_{k=1}^{p-1} (-1)^k = 0$, o que prova o teorema.

■

3.8.11 Proposição. Se p é um número primo ímpar e *a* ∈ ℤ é tal que m.d.c. (a, p) = 1, então a é um resíduo quadrático módulo p ⇔ $\left(\frac{a}{p}\right) = 1$.

Vamos aplicar algumas propriedades anteriores para determinar $(\frac{971}{15881})$.

$(\frac{971}{15881}) = (\frac{15881}{971})$ como são ambos números primos e $15881 \not\equiv 3 \pmod 4$;

$(\frac{15881}{971}) = (\frac{345}{971})$ porque $15881 \equiv 345 \pmod{971}$;

$(\frac{345}{971}) = (\frac{3}{971}) \times (\frac{5}{971}) \times (\frac{23}{971})$ pela propriedade 4 do teorema 3.8.5;

Como $5 \not\equiv 3 \pmod 4$, $3 \equiv 3 \pmod 4$, $23 \equiv 3 \pmod 4$ e $971 \equiv 3 \pmod 4$, pelo teorema 3.8.8, temos o seguinte: $(\frac{3}{971}) = -(\frac{971}{3})$, $(\frac{23}{971}) = -(\frac{971}{23})$ e $(\frac{5}{971}) = (\frac{971}{5})$. Logo $(\frac{345}{971}) = (\frac{971}{3}) \times (\frac{971}{5}) \times (\frac{971}{23})$.

$(\frac{345}{971}) = (\frac{2}{3}) \times (\frac{1}{5}) \times (\frac{5}{23})$, pois $971 \equiv 2 \pmod 3$, $971 \equiv 1 \pmod 5$ e

$971 \equiv 5 \pmod{23}$; como $(\frac{1}{5}) = 1$ pela propriedade 5 do teorema 3.8.5 e $(\frac{2}{3}) = (-1)^{\frac{3^2-1}{8}} = -1$ pelo lema 3.8.9, então

$(\frac{2}{3}) \times (\frac{1}{5}) \times (\frac{5}{23}) = - (\frac{5}{23}) = - (\frac{23}{5}) = - (\frac{3}{5}) = - (\frac{5}{3}) = - (\frac{2}{3}) = - (- 1) = 1$. Por fim, podemos concluir que 971 é um resíduo quadrático de 15881.

3.8. 12 Definição. (Símbolo de Jacobi). Seja n um número inteiro positivo e ímpar, cuja factorização num produto de factores primos é $n = p_1^{e_1} \dots p_k^{e_k}$. Seja $a \geq 0$ um número inteiro. O símbolo de Jacobi, $\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}$.

Vamos determinar $\left(\frac{21}{221}\right)$ utilizando o símbolo de Jacobi e algumas propriedades do símbolo de Legendre. Temos que $221 = 13 \times 17$, logo $\left(\frac{21}{221}\right) = \left(\frac{21}{13}\right) \times \left(\frac{21}{17}\right) =$ $= \left(\frac{8}{13}\right) \times \left(\frac{4}{17}\right) = \left(\frac{2}{13}\right) \times (\frac{2^2}{13}) \times \left(\frac{2^2}{17}\right) = \left(\frac{2}{13}\right) = (-1)^{\frac{13^2-1}{8}} = (- 1)^{21} = -1$. Concluímos então que 21 não é um resíduo quadrático de 221.

3.8.13 Proposição. Seja p um número primo ímpar e *a* um número inteiro tal que $p \nmid a$. Se *a* é um resíduo quadrático módulo p então *a* é um resíduo quadrático módulo p^k, para todo o $k \in \mathbb{N}$.

3.8.14 Proposição. Sejam $n \in \mathbb{N}$, ímpar e superior a 1, e $a \in \mathbb{Z}$, primo com n. *a* é um resíduo quadrático módulo n se e só se *a* é um resíduo quadrático módulo p para qualquer número primo p que divida n.

3.9 Problema do Logaritmo Discreto

3.9.1 Definição de logaritmo discreto. - Seja p um número primo, $\mathbb{Z}_p$ um grupo cíclico de ordem p - 1 e g uma raiz primitiva módulo p. Então para algum $a \in \{1, 2, \dots, p-1\}$ existe um expoente $c \in \{0, 1, 2, \dots, p-2\}$ tal que $a \equiv g^c \pmod p$.

Chamamos a c o logaritmo discreto de a na base g e representamo-lo da seguinte forma $c = \log_g a$. O cálculo do logaritmo discreto, quando p é um número primo grande, é bastante difícil. Até ao momento não se conhece nenhum algoritmo eficiente capaz de o calcular. O que nos coloca um problema – o Problema do Logaritmo Discreto.

3.9.2 Definição. Seja r uma raiz primitiva de n. Se m.d.c. (a, n) = 1, então chamamos índice de a relativo a r, ao menor número inteiro k que satisfaz a condição $a \equiv r^k \pmod{n}$. E denotamos por $\text{ind}_r a = k$.

Como 3 é uma raiz primitiva de 7 e $3^1 \equiv 3 \pmod 7$, $3^2 \equiv 2 \pmod 7$, $3^3 \equiv 6 \pmod 7$, $3^4 \equiv 4 \pmod 7$, $3^5 \equiv 5 \pmod 7$ e $3^6 \equiv 1 \pmod 7$. Temos então que $\text{ind}_3\ 1 = 6$, $\text{ind}_3\ 2 = 2$, $\text{ind}_3\ 3 = 1$, $\text{ind}_3\ 4 = 4$, $\text{ind}_3\ 5 = 5$ e $\text{ind}_3\ 6 = 3$.

3.9.3 Teorema. Se n tem uma raiz primitiva r e ind a é o índice de a relativo a r, então:

1) $\text{ind}\ (ab) \equiv (\text{ind}\ a + \text{ind}\ b) \pmod{\varphi(n)}$,
2) $\text{ind}\ a^k \equiv k\ \text{ind}\ a \pmod{\varphi(n)}$, para $k > 0$,
3) $\text{ind}\ 1 \equiv 0 \pmod{\varphi(n)}$, $\text{ind}\ r \equiv 1 \pmod{\varphi(n)}$,
4) $a \equiv b \pmod n$ se e só se $\text{ind}\ a = \text{ind}\ b$.

Demonstração:

1) Por definição de índice, temos que $r^{\text{ind}\ a} \equiv a \pmod n$ e $r^{\text{ind}\ b} \equiv b \pmod n$.

Multiplicando estas congruências membro a membro, obtemos

$$r^{\text{ind}\ a + \text{ind}\ b} \equiv ab \pmod n.$$

Mas como $r^{\text{ind}\ (ab)} \equiv ab \pmod n$, temos então que $r^{\text{ind}\ a + \text{ind}\ b} \equiv r^{\text{ind}\ (ab)} \pmod n$. Logo $\text{ind}\ a + \text{ind}\ b \equiv \text{ind}\ (ab) \pmod{\varphi(n)}$.

2) Temos que $r^{\text{ind}\ a^k} \equiv a^k \pmod n$ e, pelas regras das potências, $r^{k\ \text{ind}\ a} = r^{(\text{ind}\ a)^k} \equiv a^k \pmod n$; logo concluímos que $r^{\text{ind}\ a^k} \equiv r^{k\ \text{ind}\ a} \pmod n$. Daqui sai que $\text{ind}\ a^k \equiv k\ \text{ind}\ a \pmod{\varphi(n)}$.

3) Temos que $r^{\text{ind}\ a^o} \equiv r^{0\ \text{ind}\ a} \pmod n$. Pela alínea anterior, temos $\text{ind}\ 1 \equiv 0 \pmod{\varphi(n)}$. Na segunda parte, temos que $r^{\text{ind}\ r} \equiv 1 \pmod n$, logo $\text{ind}\ r \equiv 1 \pmod{\varphi(n)}$.

4) Se ind a = ind b, então $r^{\text{ind}\ a} \equiv r^{\text{ind}\ b} \pmod n$, pelo que concluímos que $a \equiv b \pmod n$. Inversamente, se $a \equiv b \pmod n$, então $r^{\text{ind}\ a} \equiv r^{\text{ind}\ b} \pmod n$. O

que implica que ind a – ind b é um múltiplo de φ (n). Como ambos os números têm que ser menores que φ (n), podemos concluir que ind a = ind b.

■

Com a ajuda destas propriedades, podemos resolver equações do tipo:

$7^x \equiv 4 \pmod{17}$.

Como 3 é uma raiz primitiva de 17, temos que:

$$\text{ind}_3 (7^x) = \text{ind}_3 (4)$$

$$x \ \text{ind}_3 (7) \equiv \ \text{ind}_3 (4) \pmod{\varphi (17)}.$$

Como $\text{ind}_3 (7) = 11$ e $\text{ind}_3 (4) = 12$, obtemos a seguinte equação equivalente $11x \equiv 12 \pmod{16}$, logo $x \equiv 4 \pmod{16}$.

O problema do logaritmo discreto, quando se utilizam números primos com bastantes algarismos, passa a ser mesmo uma grande tarefa descobrir os índices, pelo que se diz que o problema do logaritmo discreto é intratável. Foi com base neste facto que foi criado o criptosistema de chave pública ElGamal, que abordaremos mais à frente.

De momento, vamos estudar alguns algoritmos que podem pôr em causa a segurança deste sistema criptográfico, pois permitem atacar o problema do logaritmo discreto.

O algoritmo de Shanks é um desses algoritmos.

3.9.4 Algoritmo de Shanks (para o problema do logaritmo discreto em $\mathbb{Z}_p$):

Entrada: um elemento α, gerador do grupo cíclico $\mathbb{Z}_p$ de ordem p -1, um elemento $\beta \in \mathbb{Z}_p$ e $m = \left\lceil \sqrt{p - 1} \right\rceil$.

Saída: $x = \log_\alpha \beta$, com $x \in [0 , p -1]$.

1. Calcular $\alpha^{mj} \pmod{p}$, onde $0 \leq j \leq m - 1$.

2. Construir o conjunto S, formado pelos pares ordenados (j, α^{mj} (mod p)).
3. Calcular $\beta\alpha^{-i}$ (mod p), onde $0 \leq i \leq m - 1$.
4. Construir o conjunto L, formado pelos pares ordenados (i, $\beta\alpha^{-i}$ (mod p)).
5. Encontrar $(j, y) \in S$ e $(i, y) \in L$, isto é, pares ordenados com segundas coordenadas iguais.
6. Definir $x = \log_{\alpha}\beta = (mj + i)(\text{mod } (p - 1))$.

Vamos dar um exemplo deste algoritmo, com p = 103, um número primo, 5 uma raiz primitiva de p e propomo-nos a encontrar x, tal que, $5^x \equiv 41 \pmod{103}$. Para tal, temos que $m = \lceil\sqrt{102}\rceil = 11$ e calculámos $5^{11} \pmod{103} = 48$.

Para obtermos o conjunto S, vamos calcular os pares ordenados

$(j, 48^j \pmod{103})$, com $0 \leq j \leq 10$.

S = {(0, 1), (1, 48), (2, 38), (3, 73), (4, 2), (5, 96), (6, 76), (7, 43), (8, 4), (9, 89), (10, 49)}.

Temos que $5 \times 62 \equiv 1 \pmod{103}$, ou seja, 62 é o inverso de 5. O inverso é necessário para calcularmos os seguintes pares ordenados $(i, 41 \times (62^i) \pmod{103})$, com $0 \leq i \leq 10$, que formam o conjunto L.

L = {(0, 41), (1, 70), (2, 14), (3, 44), (4, 50), (5, 10), (6, 2), (7, 21), (8, 66), (9, 75), (10, 15)}.

Quando comparamos as segundas coordenadas dos dois conjuntos, constatamos que os pares ordenados $(4, 2) \in S$ e $(6, 2) \in L$ têm as segundas coordenadas iguais; logo pelo 6º passo do algoritmo, o nosso $x = 11 \times 4 + 6 = 50$. Ou seja, $5^{50} \equiv 41 \pmod{103}$.

Outro algoritmo para resolver o problema do logaritmo discreto é o Pohlig--Hellman. Neste algoritmo vamos considerar $\mathbb{Z}_p$, como grupo cíclico gerado por α, de ordem p – 1. Este algoritmo, calcula $\log_{\alpha}\beta \pmod{q^c}$, com q primo, tal que $p - 1 \equiv 0 \pmod{q^c}$ e $p - 1 \not\equiv 0 \pmod{q^{c+1}}$.

Neste algoritmo, temos que proceder à factorização em números primos de p – 1, ou seja, $p - 1 = \prod_{i=1}^{n} q_i^{c_i}$, onde os q_i's são números primos distintos. Para cada q_i ($1 \leq i \leq n$), vamos calcular $a_0, a_1, \ldots, a_{c_i - 1}$ onde $\log_\alpha \beta \bmod q_i^{c_i} = \sum_{t=0}^{c_i - 1} a_i q_i^t$.

3.9.5 O algoritmo de Pohlig-Hellman para o problema do logaritmo discreto em $\mathbb{Z}_p$, obedece às seguintes etapas:

1. Calcular $\gamma_j = \alpha^{\frac{(p-1)j}{q_i}} \pmod p$, para $0 \leq j \leq q_i - 1$
2. Se k = 0 então $\beta_k = \beta$
3. Enquanto $k \leq c_i - 1$ faz
   (a) Calcular $\delta = \beta_k^{\frac{(p-1)}{q_i^{k+1}}} \pmod p$
   (b) Encontrar j tal que $\delta = \gamma_j$
   (c) $a_k = j$
   (d) $\beta_{k+1} = \beta_k \alpha^{-a_k q_i^k} \pmod p$
   (e) $k = k + 1$

Finalmente, aplicaremos o teorema Chinês dos Restos para resolver o sistema de congruências $\log_\alpha \beta \pmod{q_i^{c_i}}$ ($1 \leq i \leq n$), cuja solução é o $\log_\alpha \beta$.

Exemplo: para ilustrar o algoritmo de Pohlig-Hellman, calculemos o expoente i, na seguinte congruência: $7^i \equiv 12 \pmod{41}$.

41 é um número primo e 7 é uma raiz primitiva de 41, logo $\text{ord}_{41}(7) = 40$.

A factorização de 40 em números primos é a seguinte $40 = 2 \times 2 \times 2 \times 5 = 2^3 \times 5$.

Para $0 \leq j \leq 4$ e $q_i = 5$, calculemos $\gamma_j = \alpha^{\frac{(p-1)j}{q_i}} \pmod p$: $\gamma_0 = 1$, $\gamma_1 = 37$, $\gamma_2 = 16$, $\gamma_3 = 18$ e $\gamma_4 = 10$. Avancemos agora, para o passo 3 (a) e temos que $\delta = 12^8 \pmod{41} = 18$ e daqui concluímos que $a_i = 3$, ou seja, $a = 3 \pmod 5$.

Para 2^3, calculemos a_0, a_1 e a_2, para obtermos $a = \sum_{t=0}^{2} a_i q_i^t$, com $q_i = 2$ e $k \leq 2$.

Para $0 \leq j \leq 1$ e $q_i = 2$, temos que $\gamma_0 = 1$ e $\gamma_1 = 40$, visto que $7^{20} \equiv 40 \pmod{41}$.

Como $\delta = 12^{20} \pmod{41} = 40$, podemos concluir que $a_0 = 1$. Para calcular a_1, temos que $\beta_1 = 12 \times 7^{-1} \pmod{41} = 31$ e $\beta_1^{\frac{40}{4}} \equiv 1$, logo $a_1 = 0$. Prosseguindo com o algoritmo, calculemos $\beta_2 = 31 \times 7^{-0} = 31$, logo $\beta_2^{\frac{40}{8}} = 31^5 \equiv 40 \pmod{41}$ e daqui se determina que $a_2 = 1$. Pelo exposto, temos que $a = 1 + 0 \times 2 + 1 \times 2^2 = 5 \pmod{8}$.

Vamos resolver o seguinte sistema: $\begin{cases} a \equiv 3 \pmod 5 \\ a \equiv 5 \pmod 8 \end{cases}$, aplicando o teorema Chinês dos Restos. Sejam $m = 5 \times 8 = 40$, $c_1 = 8$ e $c_2 = 5$, com $8y \equiv 1 \pmod 5$ e $5y \equiv 1 \pmod 8$, ou seja $d_1 = 2$ e $d_2 = 5$; então $x_0 = 3 \times 8 \times 2 + 5 \times 5 \times 5 = 173$, logo as soluções do sistema são dadas por $x = 173 + 40t$, com $t \in \mathbb{Z}$. Considerando $t = -4$, obtemos a solução 13, ou seja, $7^{13} \equiv 12 \pmod{41}$.

3.9.6 Algoritmo P - Pollard

Seja G um grupo cíclico com ordem prima p. Para aplicarmos o algoritmo ρ de Pollard, dividimos o grupo G em três partições S_1, S_2 e S_3, cujas cardinalidades sejam aproximadamente iguais e com a condição de $1 \notin S_2$.

Em seguida, calculamos a sequência $x_0, x_1, x_2, \ldots$, constituída por elementos de G, com $x_0 = 1$ e

$$x_{i+1} = f(x_i) = \begin{cases} \beta x_i, & \text{se } x_i \in S_1 \\ x_i^2, & \text{se } x_i \in S_2 \\ \alpha x_i, & \text{se } x_i \in S_3, \end{cases} \qquad \textbf{(3.9.6.1)}$$

para $i \geq 0$. Teremos, ainda, que determinar sequências $a_0, a_1, a_2, \ldots$ e $b_0, b_1, b_2, \ldots$, que satisfaz $x_i = \alpha^{a_i}\beta^{b_i}$ para $i \geq 0$: $a_0 = 0$, $b_0 = 0$, e para $i \geq 0$,

$$a_{i+1} = \begin{cases} a_i, & \text{se } x_i \in S_1 \\ 2a_i \pmod n, & \text{se } x_i \in S_2 \\ a_i + 1 \pmod n, & \text{se } x_i \in S_3, \end{cases} \qquad \textbf{(3.9.6.2)}$$

e

$$b_{i+1} = \begin{cases} b_i + 1 \pmod n, & \text{se } x_i \in S_1 \\ 2b_i \pmod n, & \text{se } x_i \in S_2 \\ b_i, & \text{se } x_i \in S_3. \end{cases} \qquad \textbf{(3.9.6.3)}$$

Vamos aplicar a este algoritmo o ciclo “Floyd’s”. Ou seja, calculamos os primeiros elementos da sequência x_{i+1}; de modo, a encontrar dois grupos de elementos: x_i e x_{2i}, tais que $x_i = x_{2i}$. Temos então que $\alpha^{a_i}\beta^{b_i} = \alpha^{a_{2i}}\beta^{b_{2i}}$, logo $\beta^{b_i - b_{2i}} = \alpha^{a_{2i} - a_i}$. Se aplicarmos o logaritmo de base α, a ambos os membros desta última equação obtemos $(b_i - b_{2i}) \log \alpha\ \beta \equiv (a_{2i} - a_i) \pmod n$, no caso de $b_i \not\equiv b_{2i}$ ($b_i \equiv b_{2i}$ ocorre com uma probabilidade muito baixa), a última equação permite-nos determinar $\log \alpha\ \beta$.

Depois, de definirmos as sequências anteriores, apresentamos então o **algoritmo ρ de Pollard**

Entrada: Um gerador α de um grupo cíclico de conjunto G de ordem prima n e um elemento $\beta \in G$.

Saída: O logaritmo discreto $x = \log_\alpha \beta$

1. $x_0 \leftarrow 1$, $a_0 \leftarrow 0$, $b_0 \leftarrow 0$.
2. Para i = 1, 2,… fazemos

   2.1 Usando as quantidades x_{i-1}, a_{i-1}, b_{i-1}, e x_{2i-2}, a_{2i-2}, b_{2i-2} calculadas previamente, calculemos x_i, a_i, b_i e x_{2i}, a_{2i}, e b_{2i} usando as equações **(3.9.6.1), (3.9.6.2) e (3.9.6.3)**

   2.2 Se $x_i = x_{2i}$, então:

   $r \leftarrow (b_i - b_{2i}) \pmod n$

   se r = 0 então termina, o algoritmo falhou; caso contrário, calculemos

   $x = r^{-1}(a_{2i} - a_i) \pmod n$ e retornamos x.

Tomemos o grupo $\mathbb{Z}_{59}^*$, para dar um exemplo do funcionamento deste último algoritmo. Como m.d.c. (5 , 59) = 1, pelo teorema de Euler, concluímos que $5^{58} \equiv 1 \pmod{59}$. A $\text{ord}_5\ (59) \mid 58$, $58 = 2 \times 29$, temos ainda que $5^2 \equiv 25 \pmod{59}$ e $5^{29} \equiv 1 \pmod{59}$, então existe um subgrupo G de $\mathbb{Z}_{59}^*$, gerado por 5 e de ordem prima.

Vamos dividir os elementos de G em três partições, do seguinte modo, $x \in S_1$, se $x \equiv 1 \pmod 3$, $x \in S_2$, se $x \equiv 0 \pmod 3$ e $x \in S_3$, se $x \equiv 2 \pmod 3$, para qualquer $x \in G$.

Tomando as considerações anteriores, vamos calcular $\log_5 45$. Para tal, vamos calcular alguns elementos x_{i+1}, a_{i+1} e b_{i+1} e com eles construir a seguinte tabela:

i	x_i	a_i	b_i	x_{2i}	a_{2i}	b_{2i}
1	45	0	1	19	0	2
2	19	0	2	27	1	3
3	29	0	3	28	4	12
4	27	1	3	28	8	26
5	21	2	6	28	16	25
6	28	4	12	28	3	23

Tabela 3.1 - o ciclo “Floyd’s” no algoritmo ρ de Pollard

Para i = 6, a tabela mostra-nos que $x_i = x_{2i} = 28$. Logo,

$r = (b_6 – b_{12}) \pmod{29} = 18$, $r^{-1} = 18^{-1} \pmod{29} = 21$ e $(a_{12} – a_6) \pmod{29} = 28$. Temos então que $\log_5 45 = (21 \times 28) \pmod{29} = 8$.

3.9.7 Algoritmo - Index-calculus

Outro algoritmo para calcular logaritmos discretos é o índex-calculus. Neste algoritmo temos de escolher, previamente, um pequeno conjunto de números primos do grupo cíclico G, de modo que “uma boa parte” dos elementos de G, possa ser escrita como decomposição dos factores primos que escolhemos.

Este algoritmo é o mais poderoso de todos os que referimos.

Entrada: gerador α de um grupo cíclico G de ordem n, e um elemento $\beta \in G$.

Saída: o logaritmo discreto $y = \log_{\alpha}\beta$

1. Escolher um subconjunto de números primos L = {p_1, p_2,…,p_t} de G, de modo que, uma parte dos elementos de G possa ser escrita como um produto de elementos de L.
2. Coligir relações lineares envolvendo logaritmos dos elementos em L.
    2.1 Seleccionar um número inteiro aleatório k, $0 \leq k \leq n\text{-}1$, e calcular α^k.
    2.2 Tentar escrever α^k como um produto dos elementos em L: $\alpha^k \equiv \prod_{i=1}^{t} p_i^{c_i}$, $c_i \geq 0$. **(3.9.7.1)**
    Se esta operação for bem sucedida, aplicar o logaritmo de base α a ambos os membros da equação anterior, de modo a obtermos uma relação linear $k \equiv \sum_{i=1}^{t} c_i \log_{\alpha} p_i \pmod{n}$. **(3.9.7.2)**
    2.3 Repetir os passos 2.1 e 2.2 até t + c relações da forma **(3.9.7.2)** serem obtidas.
3. Encontrar os logaritmos dos elementos L. Resolver, usando módulo n, o sistema linear de t + c equações (em t incógnitas) da forma **(3.9.7.2)** obtidas no passo 2 para obter os valores de $\log_{\alpha} p_i$, $1 \leq i \leq t$.
4. Calcular y
    4.1 Seleccionar um número inteiro aleatório k, $0 \leq k \leq n\text{-}1$, e calcular $\beta\alpha^k$.
    4.2 Tentar escrever $\beta.\alpha^k$ como um produto dos elementos em L: $\beta\alpha^k \pmod{n} = \prod_{i=1}^{t} p_i^{d_i}$, $d_i \geq 0$. **(3.9.7.3)**
    Se esta tentativa for infrutífera, então repetir o passo 4.1. Senão, aplicar o logaritmo de base α a ambos os membros da equação **(3.9.7.3)**, e obtemos
    $\log_{\alpha}\beta = (\sum_{i=1}^{t} d_i \log_{\alpha} p_i - k) \pmod{n}$;
    deste modo, calcular $y = (\sum_{i=1}^{t} d_i \log_{\alpha} p_i - k) \pmod{n}$ e retornar (y).

Vamos dar um exemplo deste algoritmo em $\mathbb{Z}_p^*$. Para o corpo $\mathbb{Z}_p$, p é um número primo e escolhemos os 5 primeiros números primos deste conjunto. Seja p = 2027 e L = {2, 3, 5, 7, 11} e pretendemos determinar x, tal que $2^x \equiv 13 \pmod{2027}$.

Aplicando o passo 2.2 do algoritmo, obtemos o seguinte:

$2^{1593} \pmod{2027} \equiv 33 = 3 \times 11$

$2^{983} \pmod{2027} \equiv 385 = 5 \times 7 \times 11$

$2^{1318} \pmod{2027} \equiv 1408 = 2^7 \times 11$

$2^{293} \pmod{2027} \equiv 63 = 3^2 \times 7$

$2^{1918} \pmod{2027} \equiv 1600 = 2^6 \times 5^2$

Como 2 é uma raiz primitiva de 2027, aplicando o $\log_2$ em ambos os lados de cada uma das congruências, as propriedades dos logaritmos e o corolário 3.6.3, se substituirmos $L_2 = \log_2 2 = 1$, $L_3 = \log_2 3$, $L_5 = \log_2 5$, $L_7 = \log_2 7$ e $L_{11} = = \log_2 11$, obtemos o seguinte sistema de equações:

$L_3 + L_{11} \equiv 1593 \pmod{2026}$

$L_5 + L_5 + L_{11} \equiv 983 \pmod{2026}$

$7L_2 + L_{11} \equiv 1318 \pmod{2026}$

$2L_3 + L_7 \equiv 293 \pmod{2026}$

$6L_2 + 2L_5 \equiv 1918 \pmod{2026}$.

Como $2026 = 2 \times 1013$ e 1013 é um número primo, vamos resolver o sistema anterior em módulo 2 e módulo 1013.

Em módulo 2, o sistema anterior fica reduzido ao seguinte:

$L_3 + L_{11} \equiv 1 \pmod{2}$

$L_5 + L_7 + L_{11} \equiv 1 \pmod{2}$

$L_2 + L_{11} \equiv 0 \pmod 2$

$L_7 \equiv 1 \pmod 2$

Como $L_2 = 1$, as soluções deste sistema são $L_2 \equiv L_5 \equiv L_7 \equiv L_{11} \equiv 1 \pmod 2$ e $L_3 \equiv 0 \pmod 2$.

Para módulo 1013, teremos o seguinte sistema:

$L_3 + L_{11} \equiv 580 \pmod{1013}$

$L_5 + L_7 + L_{11} \equiv 983 \pmod{1013}$

$L_{11} \equiv 298 \pmod{1013}$

$2L_3 + L_7 \equiv 293 \pmod{1013}$

$2L_5 \equiv 899 \pmod{1013}$

Temos então que $L_{11} \equiv 298 \pmod{1013}$. Como 507 é o inverso de 2 (mod 1013), concluímos que $L_5 \equiv 956 \pmod{1013}$. Destes dois resultados, sai que $L_3 \equiv 282 \pmod{1013}$ e $L_7 \equiv 742 \pmod{1013}$.

Aplicando o teorema Chinês dos Restos ao sistema: $\begin{cases} L_{11} \equiv 1 \pmod 2 \\ L_{11} \equiv 298 \pmod{1013}' \end{cases}$

como $c_1 = 2$, $c_2 = 1013$, $d_1 = 507$ e $d_2 = 1$, temos que

$$x_0 = 298 \times 2 \times 507 + 1 \times 1013 \times 1 = 303185,$$

logo a solução geral é $303185 + 2026\ t$, com $t \in \mathbb{Z}$; para $t = -149$, $L_{11} \equiv 1311 \pmod{2026}$. De modo análogo, resulta que $L_2 \equiv 1$, $L_3 \equiv 282$, $L_5 \equiv 1969$ e $L_7 \equiv 1755$.

Finalmente, podemos calcular o valor de x, tal que $2^x \equiv 13 \pmod{2027}$. Seja $k = 1397$, pelo que $13 \times 2^{1397} \pmod{2027} \equiv 110 = 2 \times 5 \times 11$. Aplicamos o último passo do algoritmo e obtemos:

$x = (1 + 1969 + 1311 - 1397) \pmod{2026} = 1884$. Logo $2^{1884} \equiv 13 \pmod{2027}$.

Em criptografia, a segurança é uma perda basilar. Normalmente, os números primos que são escolhidos para gerarem $\mathbb{Z}_p$, têm muitos dígitos, de forma que o problema do logaritmo discreto seja intratável, pelos algoritmos atrás expostos.

3. 10 Curvas Elípticas

A importância das curvas elípticas na criptografia deve-se ao facto de serem utilizadas em: testes de primalidade, na factorização de números inteiros e sistemas criptográficos assimétricos**.** Nalgumas curvas elípticas sobre corpos finitos, podemos associar uma estrutura de grupo abeliano, com uma operação binária, sobre os seus pontos, que definiremos mais adiante.

3.10.1 Definição. Seja $\mathbb{F}$ um corpo. Uma curva elíptica E($\mathbb{F}$) é o conjunto de todos os pontos (x, y) $\in \mathbb{F} \times \mathbb{F}$ que satisfazem a equação $y^2 + axy + by = x^3 + cx^2 + dx + e$, onde as variáveis x, y e os coeficientes a, b, c, d, e $\in \mathbb{F}$.

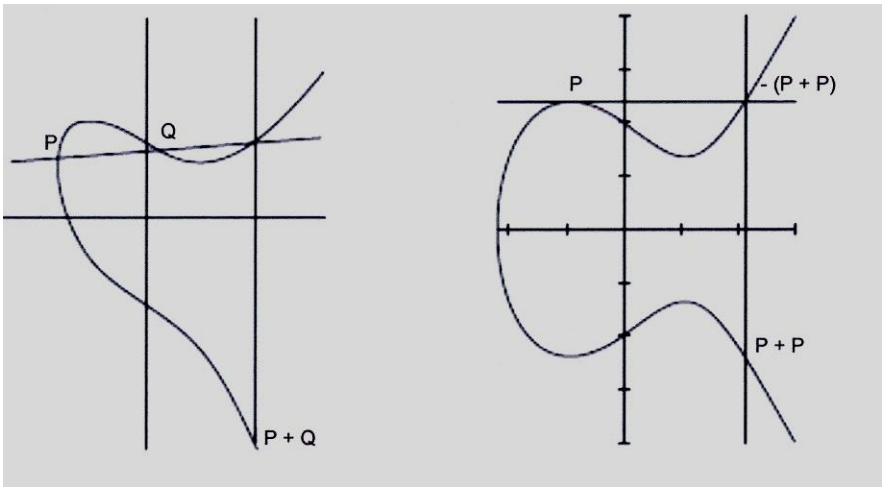
Em criptografia, devido ao facto como definimos a operação binária, só nos interessam as curvas em que seja possível traçar uma recta tangente em todos os seus pontos. O que acontece nas curvas não singulares. Nestas curvas, o polinómio $p(x) = x^3 + dx + e$ não tem raízes múltiplas, isto é, $\Delta \equiv 4d^3 + 27e^2 \not\equiv 0$.

3.10.2 Definição. Seja p > 3 um número primo. A curva elíptica $y^2 \equiv x^3 + dx + e$ em $\mathbb{Z}_p$ é o conjunto de soluções (x, y) $\in \mathbb{Z}_p \times \mathbb{Z}_p$ para a congruência $y^2 \equiv x^3 + dx + e \pmod p$, onde d e e $\in \mathbb{Z}_p$ são constantes tais que $4d^3 + 27e^2 \not\equiv 0 \pmod p$, mais o ponto O que chamamos de ponto no infinito.

Nestas curvas elípticas podemos associar uma operação binária denotada pelo símbolo +. Sejam P e Q dois pontos de E($\mathbb{F}$), definimos a operação binária da seguinte forma:

1. traçamos uma recta s definida por estes dois pontos;
2. pelo ponto de intersecção da recta s com a curva, traçamos uma recta vertical, r;
3. o outro ponto de intersecção da recta r com a curva será o ponto P + Q.

Para fazer 2P = P + P, procede-se de forma análoga à anterior, considerando agora a recta s, a recta tangente a P. O ponto 2P será o ponto considerado no passo 3. Como se pode observar nas seguintes figuras:



(a) (b)

Figura 3.1 - (a) $y^2 + xy = x^3 + 1$, (b) $y^2 = x^3 – 4x + 5$

Daqui a necessidade de consideramos para o nosso estudo as curvas elípticas não singulares.

Vamos definir a operação binária em E(𝔽), de modo a obter uma estrutura de grupo abeliano. Para tal, consideremos os seguintes pontos:

1. P + O = O + P = P para todo P ∈ E(𝔽).
2. Se P = (x, y) ∈ E(𝔽), então (x, y) + (x, - y) = O; ou seja, - P = (x, - y).
3. Seja P = (x_1, y_1) ∈ E(𝔽) e Q = (x_2, y_2) ∈ E(𝔽), então P + Q = (x_3, y_3), onde x_3 e y_3 são definidos da seguinte forma:

   $x_3 = \lambda^2 - x_1 - x_2$

   $y_3 = \lambda(x_1 – x_3) – y_1$

   e $\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, \text{ se } P \neq Q \\ \frac{3x_1^2 + d}{2y_1}, \text{ se } P = Q \end{cases}$

Daqui temos que: O é o elemento neutro da adição definida em E(𝔽); - P é o simétrico de P, para todo P ∈ E(𝔽); a adição de dois elementos de E(𝔽),

também é um elemento de E($\mathbb{F}$); (P + Q) + R = P + (Q + R) e (P + Q) = (Q + P), para P, Q e R ∈ E($\mathbb{F}$). Ou seja, (E($\mathbb{F}$), +) é um grupo abeliano.

Consideremos o seguinte exemplo: seja E o conjunto de pontos da curva elíptica $y^2 = x^3 + x + 6$ no corpo $\mathbb{Z}_{11}$. Vamos determinar os pontos de E. Para cada $x \in \mathbb{Z}_{11}$, calculemos $x^3 + x + 6$ (mod 11) e resolvemos a equação $y^2 \equiv x^3 + x + 6$ (mod11), em ordem a y. Primeiro, temos que

$$\Delta \equiv 4 \times 1^3 + 27 \times 6^2 \pmod{11} = 5 \neq 0.$$

Para cada valor de x obtido, verificámos se $z = x^3 + x + 6$ (mod 11) é um resíduo quadrático, aplicando o critério de Euler.

x	$x^3 + x + 6$ mod 11	É resíduo quadrático?	y
0	6	Não	
1	8	Não	
2	5	Sim	4, 7
3	3	Sim	5, 6
4	8	Não	
5	4	Sim	2, 9
6	8	Não	
7	4	Sim	2, 9
8	9	Sim	3, 8
9	7	Não	
10	4	Sim	2, 9

Os pontos de E são: (2,4), (2, 7), (3, 5), (3, 6), (5, 2), (5, 9), (7, 2), (7, 9), (8, 3), (8, 8), (10, 2), (10, 9) e O. Como qualquer grupo de ordem prima é cíclico, então existe um ponto de E, excepto o ponto infinito, que é gerador de E.

Tomando o ponto α = (2, 4), com as operações acima definidas, vamos determinar 2α e 3α.

Como 2 α = (2, 4) + (2, 4), temos que $\lambda = \frac{3 \times 2^2 + 1}{2 \times 4} \pmod{11} = \frac{13}{8} \pmod{11} =$

$= 13 \times 8^{-1} \pmod{11} = 13 \times 7 \pmod{11} = 3$, logo $x_3 = 3^2 - 2 - 2 \pmod{11} = 5$ e $y_3 = 3(2 - 5) - 4 \pmod{11} = -13 \pmod{11} = 9$, ou seja, 2 α = (5, 9).

Para determinar 3 α, consideremos 3 α = 2 α + α = (5, 9) + (2, 4), neste caso, como os pontos são diferentes, λ é calculado do seguinte modo:

$$\lambda = \frac{4 - 9}{2\text{-}5} \pmod{11} = \frac{-5}{-3} \pmod{11} = (-5) \times (-3)^{-1} \pmod{11} =$$

$$= (-5) \times (-4) \pmod{11} = 20 \pmod{11} = 9$$

pelo que $x_3 = (9^2 - 5 - 2) \pmod{11} = 8$ e $y_3 = [9(5 - 8) - 9] \pmod{11} =$ $= -36 \pmod{11} = 8$, temos então que 3 α = (8, 8).

Procedendo desta forma, chegámos à conclusão que α é um gerador de E, e os restantes pontos de E são gerados por α, da seguinte forma: α = (2, 4), 2α = (5, 9), 3α = (8, 8), 4α = (10, 9), 5α = (3, 5), 6α = (7, 2), 7α = (7, 9), 8α = (3, 6), 9α = (10, 2), 10α = (8, 3), 11α = (5, 2) e 12α = (2, 7).

O teorema a seguir dá-nos uma estimativa do número de pontos de uma curva elíptica sobre um corpo finito.

3.10.3 Teorema de Hasse. Seja p um número primo e E($\mathbb{Z}_p$) uma curva elíptica sobre $\mathbb{Z}_p$. Então, $p + 1 - 2\sqrt{p} \leq \#E(\mathbb{Z}_p) \leq p + 1 + 2\sqrt{p}$.

Aplicando este teorema ao estudo que fizemos em cima, temos que:

$$5{,}37 \cong 11 + 1 - 2\sqrt{11} \leq \#E(\mathbb{Z}_{11}) \leq 11 + 1 + 2\sqrt{11} \cong 18{,}63$$

Podíamos concluir que o número de pontos estaria entre 6 e 18.

3.11 Testes de primalidade

3.11.1 Definição. Se x é um número real positivo, então π (x) é o número de inteiros primos menores ou iguais a x.

Exemplo: π (20) = 8. (2, 3, 5, 7, 11, 13, 17 e 19 são os números primos menores que 20).

Para valores de x relativamente pequenos é fácil contar o número de números primos que são menores que x, mas à medida que x é substituído por valores maiores começa a ser difícil encontrar π (x).

Gauss conjecturou que $\pi(x) \sim \frac{x}{\ln(x)}$; conjectura essa que foi provada em 1898, de forma independente, por Hadamard e DE LA Vallée Poussin e que ficaria conhecida pelo teorema dos números primos.

3.11.2 Teorema dos números primos.

$$\pi(x) \sim \frac{x}{\ln(x)} \quad \text{ou} \quad \lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$

Como se pode ver no quadro em baixo à medida que n aumenta os valores de π (x) e $\frac{x}{\ln(x)}$ ficam cada vez mais próximos.

n	3	5	7	9	11
$\pi(10^n)$	168	9592	664579	50847534	4118054813
$\frac{10^n}{\ln 10^n}$	145	8686	620420	48254942	3948131654
$\frac{\pi(10^n)}{\frac{10^n}{\ln 10^n}}$	1,158	1,104	1,071	1,054	1,043

Esta relação é uma preciosa ferramenta para encontrar números primos; pois permite-nos estimar o número de números primos existentes num determinado intervalo. Como podemos ver pelo seguinte exemplo: considerando o intervalo [7 × 10^9, 9 × 10^9], quando calculamos $\frac{9\times10^9}{\ln(9\times10^9)} - \frac{7\times10^9}{\ln(7\times10^9)} \cong 83872411$; daqui

podemos concluir que, neste intervalo, aproximadamente 4,2% dos números inteiros são primos; ou seja, mais ou menos 1 em cada 23.

Esta procura de números primos pode ser facilitada se excluirmos os números pares, os que têm por algarismo das unidades o 5 e mais alguns se aplicarmos mais alguns critérios de divisibilidade. Para os restantes, teremos de recorrer aos testes de primalidade. O teste de primalidade é um algoritmo que determina se um dado número inteiro é um número primo ou não.

3.11.3 Lema. Se n não tem divisores a, tais que $1 < a \leq \sqrt{n}$, então n é primo.

Demonstração:

Suponhamos que n não tem divisores a, tais que $1 < a \leq \sqrt{n}$, e suponhamos que n é composto. Como n é composto, então existe um divisor b de n tal que $\sqrt{n} < b < n$ e podemos escrever n = bc para algum c, com $\sqrt{n} < c < n$. Isto implica o seguinte: $bc > \sqrt{n}\sqrt{n}$ = n. O que contradiz o facto de n = bc. Pelo que n não pode ser um número composto.

■

O lema anterior permite-nos aplicar o algoritmo da divisão trivial. Fazemos a divisão de n por cada um dos primeiros números primos p_1, …, p_t,… até encontrar uma que tenha resto zero. Percorremos somente os números primos até $\lfloor\sqrt{n}\rfloor$. Se não obtivermos para algum deles resto zero, então n é um número primo.

Um dos pontos fracos deste algoritmo é a sua pouca eficiência para números com muitos dígitos. Este algoritmo pode ser útil, se o número a factorar possui algum factor primo menor que 10^6. Em criptografia, este teste é pouco prático, pois só é viável para números inteiros pequenos ou para números inteiros que sejam divisíveis por um número primo pequeno.

Com o surgimento dos criptosistemas assimétricos, tornou-se de extrema importância saber se um número é primo ou composto. Para números com poucos algarismos o velhinho crivo de Eratóstenes ou a divisão trivial servem perfeitamente; no entanto, para números com centenas de dígitos, estes

algoritmos são obsoletos, pois não conseguem dar uma resposta em tempo útil! Estes testes são determinísticos, pois permitem saber com certeza absoluta se determinado número inteiro n é número primo ou não.

Além dos testes determinísticos, existem, também, os testes probabilísticos. Estes são mais rápidos que os determinísticos; mas, como o próprio nome indica, informam que um número é primo apenas com uma certa probabilidade.

De seguida, iremos apresentar mais alguns testes de primalidade.

3.11.4 Teste de Fermat.

O Pequeno Teorema de Fermat está na base deste teste de primalidade.

Para verificar se determinado número inteiro n é número primo ou não, utilizando o Pequeno Teorema de Fermat, podemos proceder da seguinte forma:

1. Escolher uma base a, tal que m.d.c. (a, n) = 1;
2. Verificar se $a^{n-1} - 1 \equiv 0 \pmod{n}$;
3. Após a análise de 2, tirar as seguintes conclusões:
    - 3.1 Se não verificar 2, então n não é número primo e dizemos que a base a é testemunha de que n é composto;
    - 3.2 Se verificar 2, então n passou no teste para a base a.

Se chegarmos até 3.2, não fica garantido que n seja primo. Por exemplo, para 341 temos o seguinte: $2^{341-1} - 1 \equiv 0 \pmod{341}$, mas $3^{341-1} \equiv 56 \pmod{341}$; ou seja, para a = 3 prova-se que 341 é um número composto, pois $341 = 11 \times 31$. Existem números compostos que verificam $a^{n-1} - 1 \equiv 0 \pmod{n}$; são chamados os pseudoprimos para a base a. Por exemplo, 341 é pseudoprimo para a base 2, mas 3 é testemunha que 341 é composto. O teste de Fermat é probabilístico, devido à existência dos pseudoprimos.

3.11.5 Proposição. Se n é um pseudoprimo de base 2, então $2^n - 1$ é um pseudoprimo de base 2.

Demonstração:

Seja $n' = 2^n - 1$. Queremos provar que $2^{n'} \equiv 2 \pmod{n'}$. Sabemos que $n \mid (n' - 1)$, porque $n' - 1 = 2^n - 2$ e n é um 2 – pseudoprimo. Seja $n' - 1 = nk$, com $k \in \mathbb{Z}$; então recorrendo à soma das séries geométricas, temos que

$$2^{n'-1} - 1 = 2^{nk} - 1 = (2^n - 1)\left(2^{n(k-1)} + \ldots + 2^n + 1\right) =$$

$$= n' \left(2^{n(k-1)} + \ldots + 2^n + 1\right).$$

Donde se conclui que $n' \mid (2^{n'-1} - 1)$, ou de forma equivalente $2^{n'-1} \equiv 1 \pmod{n'}$, ou seja $2^{n'} \equiv 2 \pmod{n'}$.

Para n' ser 2 – pseudoprimo, falta provar que n' é um número composto. Como n é um número composto, podemos escrever $n = ab$, com $a, b \in \mathbb{Z}$ e maiores que um. Através da fórmula da soma para as séries geométricas, obtemos

$2^n - 1 = 2^{ab} - 1 = \left(2^a - 1\right)\left(2^{a(b-1)} + \ldots + 1\right)$, daqui conclui-se que n' é um número composto, pelo que é 2 – pseudoprimo.

Logo há infinitos pseudoprimos de base 2.

■

Está provado que existem infinitos pseudoprimos. No entanto, existem apenas três para base 2 menor que mil, a saber: 341, 561 e 645. Para a mesma base, menores que um milhão existem 245. É devido à sua fraca distribuição, que o teste de Fermat tem alguma eficácia.

Considerando os números inteiros só até 10^9, temos que existem 50 847 534 primos e 5597 pseudoprimos na base 2. Para um número inteiro $n < 10^9$, que verifique $2^{n-1} - 1 \equiv 0 \pmod{n}$, a probabilidade de ser primo é igual a $1 - \frac{5597}{50847534} \cong 0{,}9998899258$, ou seja, bastante elevada. Se forem utilizadas diferentes bases a probabilidade de n ser primo aumenta, visto que, existem apenas 685 pseudoprimos para as bases 2, 3 e 5 menores que 10^9.

No caso de um número inteiro n verificar $a^{n-1} - 1 \equiv 0 \pmod{n}$, para diferentes bases a, então aumenta a probabilidade de n ser primo. Os já referidos

números de Carmichael apesar de serem infinitos têm uma distribuição muito fraca; por exemplo: só existem 8241 números Carmichael menores que 10^{12}.

Este teste não é capaz de distinguir os números primos dos números Carmichael. Pelo que, convém aplicar o critério de Korselt, antes de declararamos que o número é primo.

3.11.6 Teorema de Lucas (teste de primalidade de Lucas). Suponhamos que existe um número inteiro a tal que $a^{n-1} \equiv 1 \pmod{n}$, mas $a^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$, para todo primo q, tal que q |(n -1), então n é primo.

Demonstração:

Vamos demonstrar que a $ord_n(a) = n - 1$.

A congruência $a^{n-1} \equiv 1 \pmod{n}$ implica que a $ord_n(a) \mid (n-1)$. Seja $n - 1 = ord_n(a)k$ para algum k. Queremos mostrar que k = 1, suponhamos que k > 1 e um primo q divide k. Então q | (n – 1), e podemos escrever

$$a^{\frac{n-1}{q}} \equiv a^{\frac{ord_n(a)k}{q}} \equiv 1 \pmod{n}.$$

O que contradiz a hipótese do teorema, logo K = 1 e $ord_n(a) = n - 1$. Como a $ord_n(a) \mid \varphi(n)$, temos então que $\varphi(n) \geq n - 1$, mas $\varphi(n) \leq n - 1$; pelo que $\varphi(n) = n - 1$e n é primo.

■

Exemplo: Vamos verificar que 31 é primo recorrendo ao teste anterior. Consideremos n = 31; n – 1 = 30 = 2 × 3 × 5 a decomposição em factores primos. Para a = 3, temos:

$$3^{30} \equiv 1 \pmod{31}$$

$$3^{\frac{30}{5}} \equiv 16 \pmod{31}$$

$$3^{\frac{30}{3}} \equiv 25 \pmod{31}$$

$$3^{\frac{30}{2}} \equiv 30 \pmod{31}$$

Pelo teorema anterior, concluímos que 31 é um número primo.

Para utilizarmos este teste, temos de conhecer a factorização de n – 1.

3.11.7 Definição. Dizemos que um número n composto é um pseudoprimo de Euler relativamente à base b, se m.d.c. (n, b) = 1 e $b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n}$.

Exemplo: Seja n = 1105 = 5 × 13 × 17 e b = 2. Então temos $b^{\frac{n-1}{2}} \pmod{n} = 2^{\frac{1105-1}{2}} \pmod{1105} = 1$ e $\left(\frac{b}{n}\right) = \left(\frac{2}{1105}\right) = 1$. Então

$$2^{\frac{1105-1}{2}} \equiv \left(\frac{2}{1105}\right) \pmod{1105}.$$

Pelo que, 1105 é um pseudoprimo de Euler na base 2.

3.11.8 Teorema. Seja n um número ímpar composto, então n é um pseudoprimo de Euler no máximo para metade das bases b, com 1 < b < n e m.d.c (b , n) = 1.

Demonstração:

Suponhamos que n é um número ímpar composto. Primeiro vamos mostrar que se n não é pseudoprimo de Euler pelo menos para uma base b então n não é pseudoprimo pelo menos para metade das bases b, com 1 < b < n e m.d.c. (b , n) = 1. De seguida mostraremos que se n é número ímpar composto, então existe uma base b para a qual n não é um pseudoprimo de Euler.

Suponhamos que n é um número ímpar e composto e que n não é um pseudoprimo para a base b. Isto é, $b^{\frac{n-1}{2}} \neq \pm 1 \pmod{n}$.

Se n não é pseudoprimo para alguma base, então de certeza que n não é um pseudoprimo pelo menos para metade das bases possíveis. Suponhamos então que n é um pseudoprimo para a base b_1, ou seja, $b_i^{\frac{n-1}{2}} \equiv 1 \pmod{n}$.

Então temos o seguinte: $(bb_1)^{\frac{n-1}{2}} \equiv b^{\frac{n-1}{2}} b_1^{\frac{n-1}{2}} \neq \pm 1 \pmod{n}$. Assim, n não é pseudoprimo de Euler para a base bb_1. Por conseguinte, para toda a base b_i para a qual n é um pseudoprimo, n não é um pseudoprimo para a base bb_i.

Além disso, se b_i, b_j são distintos módulo n e bases para as quais n é um pseudoprimo de Euler, então bb_i não é congruente com bb_j (mod n). Temos então, o seguinte: se $\{b_1,\ldots,b_k\}$ são bases distintas para as quais n é um pseudoprimo de Euler, então $\{bb_1,\ldots,bb_k\}$ são bases distintas para as quais n não é um pseudoprimo de Euler. Daqui, existem pelo menos tantas bases para as quais n não é pseudoprimo, como para as quais é. Podemos então concluir que se existe pelo menos uma base b para a qual n é um pseudoprimo de Euler, então n é um pseudoprimo de Euler no máximo para metade das bases possíveis.

Vamos mostrar agora que existe uma base b para a qual n não é um pseudoprimo de Euler. Primeiro, suponhamos que existe um primo p, tal que $p^2 \mid n$. Seja g um gerador do grupo multiplicativo Z_{p^2}. A ordem de g é $\varphi(p^2)=p(p-1)$. Seja b solução do seguinte par de congruências:

$$b \equiv g \pmod{p^2}$$

$$b \equiv 1 \pmod{\frac{n}{p^2}}.$$

Então suponhamos que $b^{\frac{n-1}{2}} \equiv 1 \pmod{n}$. Logo $p(p-1) \mid (n-1)$, o que é impossível, visto que $p^2 \mid n$. De seguida, suponhamos que $b^{\frac{n-1}{2}} \equiv -1 \pmod{n}$, então $b^{n-1} \equiv 1 \pmod{n}$, desta forma $b^{n-1} \equiv 1 \pmod{p^2}$. Segue-se que $p(p-1) \mid (n-1)$. Mas então $p \mid (n-1)$, o que é uma contradição. Daqui, se n é divisível por um p^2, então b é uma base para a qual n não é um pseudoprimo de Euler.

Agora suponhamos que $n = p_1 \ldots p_k$, sendo p_i primos distintos. Seja g um resíduo não quadrático (mod p_1). Daqui $(\frac{g}{p_1}) = -1$. Escolhemos uma base b que satisfaça simultaneamente as seguintes congruências:

$$b \equiv g \pmod{p_1}$$

$$b \equiv 1 \pmod{p_i},\ i = 2,\ldots,k,$$

a qual existe pelo teorema do Chinês dos Restos. Pelo símbolo de Jacobi, temos que: $\left(\frac{b}{n}\right) = \left(\frac{b}{p_1}\right)\left(\frac{b}{p_2}\right)\ldots\left(\frac{b}{p_k}\right)$. Mas $\left(\frac{b}{p_1}\right)$ = - 1, visto que b ≡ g (mod p_1) e $\left(\frac{b}{p_i}\right) = \left(\frac{1}{p_i}\right)$ = 1. Logo $\left(\frac{b}{n}\right)$ = - 1.

Se n fosse um pseudoprimo para a base b, então $b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) (\mathrm{mod}\, n)$, pelo que $b^{\frac{n-1}{2}} \equiv -1\ (\mathrm{mod}\, n)$. Mas então $b^{\frac{n-1}{2}} \equiv -1\ (\mathrm{mod}\, p_2)$, o que é uma contradição, visto que b ≡ 1 (mod p_2). Consequentemente n não pode ser um pseudoprimo de Euler para a base b. Daqui, para todo n existe uma base para a qual, n não é um pseudoprimo de Euler, o que prova o teorema.

■

3.11.9 Teste de Solovay-Strassen.

Seja n um número inteiro ímpar.

Passo 1 – Escolhemos aleatoriamente k números inteiros, b_1, b_2,…,b_k, com $1 < b_i < n$

Passo 2 – Para i = 1,…, k

1. Determinamos m.d.c. (n, b_i).

   Se m.d.c. (b, n) > 1, então n é composto e pára.

2. Calculámos $b_i^{\frac{n-1}{2}}$ (mod n) e $\left(\frac{b_i}{n}\right)$.

   Se $b_i^{\frac{n-1}{2}} \not\equiv \left(\frac{b_i}{n}\right)$ (mod n), então n é composto e pára.

Passo 3 – A probabilidade de n ser primo é maior que 1 - $\frac{1}{2^k}$.

Apliquemos este teste a alguns números ímpares e retiraremos as respectivas conclusões. Seja n = 1121 e escolhamos para base 2. Temos que m.d.c. (1121, 2) = 1 e $2^{\frac{1121-1}{2}} = 2^{560} \equiv 137$ (mod 1121) e $\left(\frac{2}{1121}\right) = (-1)^{\frac{1121^2-1}{8}}$= = 1, como $\left(\frac{2}{1121}\right)$ = 1 ≢ 137 (mod 1121), então 1121 é um número composto.

Vamos testar 1123, para as bases 2, 3 e 5. Para a base 2, temos que m.d.c (2, 1123) = 1, $2^{\frac{1123-1}{2}} = 2^{561} \equiv -1 \pmod{1123}$ e $\left(\frac{2}{1123}\right) = (-1)^{\frac{1123^2-1}{8}} = -1$, podemos concluir que 1123 passou o teste para a base 2. O mesmo se verifica para as bases 3 e 5, logo podemos concluir que 1123 é número primo, com uma probabilidade de $1 - \frac{1}{2^3} = 0{,}875$. E de facto, 1123 é um número primo.

Consideremos agora n = 2821 e as seguintes bases: 3, 4, 9, 12, 16, 17, 25, 27 e 36. Quando aplicamos o teste de Solovay-Strassen, verificamos que 2821 passa o teste para todas as bases, o que nos leva a concluir que 2821 é um número primo com uma probabilidade de $1 - \frac{1}{2^9} \cong 0{,}998$. Valor muito próximo de 1, ou seja a probabilidade de 2821 ser primo é bastante elevada. Mas 2821 é um número de Carmichael, ou seja, é um número composto e tem a seguinte factorização: $2821 = 7 \times 13 \times 31$.

Os dois últimos exemplos, mostram-nos que a primalidade vinda deste teste é sempre relativa, apesar de um número passar o teste para muitas bases, nunca fica garantido que o número é primo!

Se p é um número primo, então a equação $x^2 \equiv 1 \pmod{p}$ tem duas soluções, $x = 1, -1 \pmod{p}$.

O número de soluções para $x^2 \equiv 1 \pmod{p}$ é maior que dois para números compostos.

3.11.10 Definição. Seja n um número inteiro e $n - 1 = 2^r s$. Então diz-se que n passa no teste dos pseudoprimos fortes se:

1. $a^s \equiv 1 \pmod{n}$
2. $a^{s2^i} \equiv -1 \pmod{n}$, para algum $0 \leq i < r$.

3.11.11 Definição. Um número n ímpar e composto, que passe no teste dos pseudoprimos fortes para a base a, chama-se um pseudoprimo forte para a base a.

3.11.12 Proposição. Se n é um número ímpar e pseudoprimo forte para a base 2, então $2^n - 1$ é um pseudoprimo forte para a base 2.

Demonstração: Na proposição 3.11.5 provamos que $2^n - 1$ é um 2 – pseudoprimo. Em particular, que n é composto.

Temos que $2^{n-1} \equiv 1 \pmod{n}$, pois n é um 2 – pseudoprimo. Podemos escrever $2^{n-1} - 1 = nk$, onde k é necessariamente um número ímpar. Seja $n' = 2^n - 1$. A factorização de $n' - 1 = 2^n - 2 = 2(2^{n-1} - 1) = 2nk$; por conseguinte, nk é um factor ímpar de $n' - 1$, e a sequência $\{x_0, x_1, \ldots, x_r\}$ tem somente dois termos, 2^{nk} e 2^{2nk}.

Obviamente que, $2^n - 1 \equiv 1 \pmod{2^n - 1}$, ou $2^n \equiv 1 \pmod{n'}$, o que implica que $2^{nk} \equiv 1 \pmod{n'}$, satisfaz a condição 1 na definição de pseudoprimos fortes para a base 2. Logo existem infinitos pseudoprimos fortes para a base 2.

■

Podemos concluir que existem infinitos pseudoprimos fortes para a base 2.

Existem 14884 2 - pseudoprimos menores que 10^{10}, mas só existem 3291 pseudoprimos fortes para base 2. No entanto, se considerarmos pseudoprimos fortes para diferentes bases, o panorama fica mais agradável. 1373653 é o menor pseudoprimo forte para as bases 2 e 3. Existem apenas 66 números inteiros menores que 10^6 que são pseudoprimos para as base 2 e 3. Só existem 13 que são menores ou iguais que 25×10^9 que são pseudoprimos fortes para as bases 2, 3 e 5, no entanto para as mesmas bases e menores que 25×10^9 existem 2522 pseudoprimos.

3.11.13 Algoritmo. (Teste simples de primalidade):

Dado $n \leq 25 \times 10^9$, este algoritmo determina se n é primo:

1. Se n falhar o teste de pseudoprimo forte para a base 2, então n é composto.
2. Se n falha o teste de pseudoprimo forte para a base 3, então n é composto.
3. Se n falha o teste de pseudoprimo forte para a base 5, então n é composto.

4. Se n é um dos 13 números que se encontra na tabela em baixo, então n é composto; de outro modo, n é primo.

	Base 7	Base 11	Base 13
25326001	Não	Não	Não
161304001	Não	Spsp	Não
960946321	Não	Não	Não
1157839381	Não	Não	Não
3215031751	Spsp	Psp	Psp
3697278427	Não	Não	Não
5764643587	Não	Não	Spsp
6770862367	Não	Não	Não
14386156093	Psp	Psp	Psp
15579919981	Psp	Spsp	Não
18459366157	Não	Não	Não
19887974881	Psp	Não	Não
21276028621	Não	Psp	Spsp

Tabela 3.2 – Pseudoprimos fortes para as bases 2, 3 e 5 e os resultados do teste para as bases 7,11 e 13.

Exemplo:

Consideremos n = 117371.

n – 1 = 2 × 58685, ou seja, s = 56685. Temos então que:

$$2^s \equiv -1 \pmod{n}$$

$$2^{2s} \equiv 1 \pmod{n}$$

$$3^s \equiv 1 \pmod{n}$$

Pelo que n é primo.

3.11.14 Definição. Um número na forma $F_k = 2^{2^k} + 1$ para algum $k \in \mathbb{N}_0$ diz-se um número de Fermat. Os números F_0, F_1, F_2, F_3 e F_4 são números primos. Em 1732, Euler mostrou que

$F_5 = 4294967297 = 641 \times 6700417$, ou seja, é um número composto.

3.11.15 Teste de Pepin. O número de Fermat $F_n = 2^{2^n} + 1$ é primo se e só se $3^{\frac{F_n - 1}{2}} \equiv -1 \pmod{F_n}$.

Demonstração:

Suponhamos que $3^{\frac{F_n - 1}{2}} \equiv -1 \pmod{F_n}$. Então $3^{F_n - 1} \equiv \left(3^{\frac{F_n - 1}{2}}\right)^2 \equiv (-1)^2 \equiv 1 \pmod{n}$. O único factor primo de $F_n - 1 = 2^{2^n}$ é o 2, então n é primo pelo teorema de Lucas.

Inversamente, seja F_n primo. Como 2^n é par, temos que $2^{2^n} \equiv 1 \pmod 3$, pelo que $F_n \equiv 2 \pmod 3$. Temos também que $F_n \equiv 1 \pmod 4$, então pelo símbolo de Legendre $\left(\frac{3}{F_n}\right)$ é – 1, isto é, 3 não é quadrado (mod F_n). Pelo critério de Euler, temos a congruência pretendida.

■

Vamos aplicar o teste de Pepin para verificar que 17 é um número primo. Temos então que: $3^{\frac{17-1}{2}} = 3^8$. Como $3^2 \equiv 9 \pmod{17}$, $3^4 \equiv 13 \pmod{17}$ e $3^8 \equiv -1 \pmod{17}$, logo 17 é um número primo.

3.11.16 Lema. (POCKLINGTON). Seja n um número inteiro. Suponhamos que $n - 1 = q^k r$, $k \geq 1$, onde q é primo e $q \nmid r$. Se existe a tal que $a^{n-1} \equiv 1 \pmod n$ e $\text{m.d.c.}\left(a^{\frac{n-1}{q}} - 1, n\right) = 1$, então para todo primo p | n temos $p \equiv 1 \pmod{q^r}$.

3.11.17 Teorema. Seja n um número ímpar e $n - 1 = 2^k q$ com q ímpar e $k \geq 1$. Se n é primo e $a \in \mathbb{Z}^*_n$, então $a^q \equiv 1 \pmod{n}$ ou existe um $i \in \{0, 1, 2, \ldots, k-1\}$ tal que

$$a^{2^i q} \equiv -1 \pmod{n} .$$

Definimos o conjunto $S(n) = \{a \in Z_n^* : a^d \equiv 1 \pmod{n} \text{ ou } a^{2^r d} \equiv -1 \pmod{n}\}$, com $0 \leq r < t$ e $n - 1 = 2^t d$. Quando $a \notin S(n)$, dizemos que n tem uma testemunha forte, a, da sua composição.

3.11.18 Teste de Miller-Rabin

Seja $n \in \mathbb{N}$, $n > 1$ e ímpar. $n - 1 = 2^s t$, com $s \in \mathbb{N}$ e t número ímpar.

Passo 1 – Escolhemos aleatoriamente k números inteiros, $b_1, b_2, \ldots, b_k$, com $1 < b_i < n$

Passo 2 – Para i = 1,…, k

1. Determinamos m.d.c. (n, b_i).
   Se m.d.c. $(b, n) > 1$, então n é composto e pára.
2. Para i = 1,..,k

   i) Calculamos $m_i = b_i^t \pmod{n}$

   j) Se $m_i = \pm 1$, então n é um pseudoprimo forte para a base b_i e avançamos para o próximo i. Se não

   k) Para j = 1,…,s – 1, calculamos $k_j = b_i^{2^j t} \pmod{n}$

   l) Se $k_j \equiv -1 \pmod{n}$, então n é um pseudoprimo forte para a base b_i e avançamos para o i seguinte. Se não avançamos para o j seguinte

   m) Se k_j não é congruente com -1 (mod n) para todo o j, então n é composto e para.

Passo 3 – A probabilidade de n ser primo é maior que $1 - \frac{1}{4^k}$.

Vamos ilustrar este teste com alguns exemplos.

Consideremos n = 1729 e b = 671. Temos que: 1729 – 1 = 1728 = $2^6 \times 27$, ou seja, s = 6 e t = 27. Apliquemos então o teste:

$$671^{27} \equiv 1084 \pmod{1729}$$

$$671^{27 \times 2} \equiv 1084^2 \equiv 1065 \pmod{1729}$$

$$671^{27 \times 2^2} \equiv 1065^2 \equiv 1 \pmod{1729}.$$

Podemos concluir que 1729 é um número composto.

Consideremos agora n = 104513, com b = 3. Temos que:

104513 – 1 = $2^6 \times 1633$, ou seja, s = 6 e t = 1633. Apliquemos o teste:

$$3^{1633} \equiv 88958 \pmod{104513}$$

$$3^{1633 \times 2} \equiv 88958^2 \equiv 10430 \pmod{104513}$$

$$3^{1633 \times 2^2} \equiv 10430^2 \equiv 91380 \pmod{104513}$$

$$3^{1633 \times 2^3} \equiv 91380^2 \equiv 29239 \pmod{104513}$$

$$3^{1633 \times 2^4} \equiv 29239^2 \equiv 2781 \pmod{104513}$$

$$3^{1633 \times 2^5} \equiv 2781^2 \equiv -1 \pmod{104513}.$$

Podemos concluir que 104513 é provavelmente um número primo. No entanto, precisaríamos de testar n para mais bases, para aumentarmos a probabilidade da sua primalidade.

3.11.19 Lema. Seja n ≥ 3 um número inteiro ímpar. S(n) = $\mathbb{Z}^*_n$ se, e somente se, n é primo.

3.11.20 Teorema. Se n ≥ 3 é um número ímpar composto, então o conjunto {1,…,n - 1} tem no máximo $\frac{n-1}{4}$ números que são primos com n e não são testemunhas da composição de n .

Demonstração:

Queremos estimar os números a ∈ {1, 2, …, n - 1} primos com n, tais que $a^d \equiv 1 \pmod{n}$ ou $a^{2^r d} \equiv -1 \pmod{n}$ para algum r ∈ {1, 2, …, s - 1}. Suponhamos que existe uma não testemunha, a. Suponhamos que satisfaz a segunda condição (na verdade, se $a^d \equiv 1 \pmod{n}$, então $a^{2^0 d} \equiv -1 \pmod{n}$).

Seja k o maior valor de r, para o qual existe um número inteiro a primo com n que satisfaz a segunda identidade. Consideremos m = 2^kd. Seja n = $\prod_p p^{e(p)}$ a factorização em números primos de n.

Sejam J, K, L e M subgrupos de $\mathbb{Z}_n^*$, definidos da seguinte forma:

$$J = \left\{a \in Z_n^* : \text{m.d.c. } (a, n) = 1 \text{ e } a^{n-1} \equiv 1 (\text{mod } (n))\right\}$$

$$K = \left\{a \in Z_n^* : \text{m.d.c. } (a, n) = 1 \text{ e } a^m \equiv \pm 1 \ (\text{mod } p^{e(p)}) \text{ para todo } p \mid n\right\}$$

$$L = \left\{a \in Z_n^* : \text{m.d.c. } (a, n) = 1 \text{ e } a^m \equiv \pm 1 \ (\text{mod } n)\right\}$$

$$M = \left\{a \in Z_n^* : \text{m.d.c. } (a, n) = 1 \text{ e } a^m \equiv 1 \ (\text{mod } n)\right\}$$

Temos M ⊆ L ⊆ K ⊆ J ⊆ $\mathbb{Z}_n^*$.

Todo o a ∈ S(n) também é elemento de L, pois se $a^d \equiv 1 \pmod{n}$, então $a^m = a^{2^k d} \equiv 1 \pmod{n}$. Provaremos que L é um subgrupo de índice pelo menos quatro de $\mathbb{Z}_n^*$.

O índice de M em K é uma potência de base 2, porque o quadrado de cada elemento de K pertence a M. Por conseguinte, o índice de L em K é também uma potência de base dois, seja 2^j. Se j ≥ 2, está demonstrado.

Se j = 1 ([K:L] = 2) então n tem dois divisores primos. Pelo teorema 3.7.8, concluímos que n não é um número Carmichael. O que implica que J é um subgrupo próprio de $\mathbb{Z}_n^*$ e o índice de J em $\mathbb{Z}_n^*$ é pelo menos dois. Temos então que o índice de L em $\mathbb{Z}_n^*$ é pelo menos quatro.

Por fim, seja j = 0. Então n = p^e, com e > 1. Mas então, |J| = p – 1, e $|\mathbb{Z}_n^* : J| = p^{e-1} \geq 4$, excepto quando p^e = 9. Se n = 9, então existem apenas dois

elementos pertencentes a S (n), o 1 e o – 1. Pelo exposto, podemos concluir que o número de elementos é $\leq \frac{n-1}{4}$.

■

Antes de apresentarmos o algoritmo AKS, vamos tecer algumas considerações sobre polinómios, com vista a um melhor entendimento deste último.

3.11.21 Definição. Seja R um anel comutativo com 1. Define-se polinómio na indeterminada x como sendo a expressão formal

$$r_0 + r_1x + r_2x^2 + \cdots + r_nx^n,$$

onde $r_0, r_1, \cdots, r_n \in R$, $n \in \mathbb{N}_0$.

Os elementos r_i são os coeficientes do polinómio.

O teste de primalidade AKS é baseado no seguinte resultado da Teoria dos Números: suponhamos que a e n são números inteiros, primos entre si, então n é primo se e só se os polinómios $(x + a)^n$ e $x^n + a$ são equivalentes módulo n.

3.11.22 Lema. Se m.d.c. (a, n) = 1, então $a^k \not\equiv 0 \pmod n$ para $k \geq 0$.

3.11.23 Teorema. Seja m.d.c. (a, n) = 1. Então n é primo se e só se $(x + a)^n \equiv (x^n + a) \pmod n$.

Demonstração:

Suponhamos que n é primo. Temos que $(x + a)^n = \sum_{k=0}^{n} x^{n-k} a^k$. Pelo teorema 3.7.2 todos os termos entre x^n e a são iguais a zero, pois $\binom{n}{k} \equiv 0 \pmod n$ para $1 \leq k \leq n - 1$. Pelo teorema 3.7.3 temos que $a^n \equiv a \pmod n$. Logo

$$(x + a)^n \equiv (x^n + a) \pmod n.$$

Tomemos por hipótese, $(x + a)^n \equiv (x^n + a) \pmod n$. Temos então que

$$(x + a)^n = \sum_{k=0}^{n} x^{n-k} a^k \equiv (x^n + a) \pmod n,$$

ou seja, $\binom{n}{k} a^k \equiv 0 \pmod{n}$ para $1 \leq k \leq n - 1$. Pelo lema anterior, como m.d.c. (a, n) = 1, sai que $a^k \not\equiv 0 \pmod{n}$ para $k \geq 0$, temos então que $\binom{n}{k} \equiv 0 \pmod{n}$ para $1 \leq k \leq n - 1$. Pelo teorema 3.7.2 temos que n é primo.

■

Com este teorema, analisando módulo n os termos que estão entre x^n e a temos um teste de primalidade infalível. O problema é que para valores de n muito grandes temos que calcular todos os termos e verificar se os que estão entre x^n e a são múltiplos de n ou não. O que torna este método pouco ou nada eficiente.

Em Agosto de 2002, o Professor Agrawal, mais dois alunos seus de doutoramento, Kayal e Saxena, apresentaram um algoritmo que ficaria conhecido por AKS. Baseando-se na ideia anterior, criaram um teste de primalidade mais eficiente. Em vez de analisarem os n – 1 termos, calcularam o resto da divisão de $(x - a)^n$ por $x^r - 1$, sendo r um primo bastante menor que o número n e analisam no máximo r – 1 termos.

3.11.24 Definição. Dois polinómios $f(x) = \sum_{i=1}^{n} a_i x^i$ e $g(x) = \sum_{i=1}^{n} b_i x^i$ são congruentes módulo n se os respectivos coeficientes são congruentes módulo n. Isto é, $f(x) \equiv g(x) \pmod{n}$ significa que $a_i \equiv b_i \pmod{n}$ para todo i.

Por exemplo, $(5x^3 + 3x^2 + 13x - 5) \equiv (9x^3 + 7x^2 + x + 3) \pmod{4}$.

3.11.25 Definição. Se f(x) e g(x) são polinómios, f(x) (mod g(x)) é o resto da divisão do polinómio f(x) por g(x).

Se $f(x) = 4x^4 + 3x^3 + 2x^2 + 5x + 7$ e $g(x) = x^2 + 1$, então f(x) (mod g(x)) = 2x + 9.

3.11.26 Definição. Dados os polinómios f(x), g(x), e h(x), dizemos que f(x) e g(x) são congruentes módulo h(x) e n, se os seus restos quando divididos por h(x) são congruentes (mod n). Isto é,

$f(x) \equiv g(x) \pmod{(h(x), n)}$ se $[f(x) \pmod{h(x)}] \equiv [g(x) \pmod{h(x)}] \bmod n$.

Neste caso, se considerarmos:

$f(x) = 5x^3 + 3x^2 + 12x - 4$, $g(x) = 10x^3 + 8x^2 + 17x + 26$ e $h(x) = x + 1$, temos que

f(x) (mod h(x)) = - 18 e g(x) (mod h(x)) = 7, -18 ≡ 7 (mod 5), então podemos concluir que f(x) ≡ g(x) (mod(x + 1, 5)).

3.11.27 Teorema. Se n e r são primos e a é um número inteiro, então

$$(x + a)^n \equiv (x^n + a)(\text{mod } (x^r - 1, n)).$$

Demonstração:

Resulta das definições de congruências de polinómios e do teorema anterior.

■

Se o teorema anterior fosse mais do que uma implicação, teríamos um teste de primalidade que nos garantiria se um determinado número seria primo ou não!

No entanto, o que pode acontecer é que dois polinómios diferentes tenham o mesmo resto quando divididos por $x^r - 1$, o que não garante que quando n é composto que $(x + a)^n \not\equiv (x^n + a) \text{ mod } (x^r - 1, n)$.

O que os autores deste teste nos mostraram, foi que se escolhermos um valor "certo" para o r, podemos diminuir, não só o número de termos, como também, substancialmente o número de a's a serem testados e garantir a fiabilidade na primalidade do número.

3.11.28 Teste AKS

Seja n > 1, um número inteiro.

1. Se $n = b^k$, com b, k ∈ $\mathbb{Z}$ e k > 1, então n é composto e paramos.
2. r:= 2;
3. Enquanto (r < n) fazemos {
4. Se m.d.c. (n, r) ≠ 1, então n é composto;
5. Se r é primo, então
6. Seja q o maior factor de r – 1
7. Se $\lceil q \geq 4\sqrt{r}\ \log_2(n) \rceil$ e $n^{\frac{r-1}{q}} \not\equiv 1$ (mod r), pare;
8. r: ← r + 1;
9. }
10. Para a = 1 até $2\sqrt{r}\log_2 n$

11. Se $(x + a)^n \not\equiv (x^n + a) \pmod{x^r - 1, n}$, então n é composto;
12. Retorna primo.

Este teste é determinístico e bastante eficiente. No entanto, o matemático Lenstra já lhe introduziu algumas alterações tornando-o mais rápido.

3.12 Algoritmos de factorização

Um dos casos notáveis da multiplicação, a diferença de quadrados, que aprendemos no 3º Ciclo do Ensino Básico, é utilizado neste método.

Se escrevemos um número n > 0, na forma $n = x^2 - y^2$, com x e y números inteiros positivos, então n = (x – y) (x + y), os factores de n são (x – y) e (x + y). Se n for um quadrado perfeito, então existe um $r \in \mathbb{Z}$, tal que $n = r^2$; neste caso, x = r e y = 0.

3.12.1 Algoritmo de Fermat

Dado n ímpar

1. $r = \lfloor \sqrt{n} \rfloor$
2. Se $n = r^2$, então fazemos x = r e y = 0
3. Senão enquanto $r < \frac{n+1}{2}$ ou s não for número inteiro fazemos

   $r = r + 1$

   $s = \sqrt{r^2 - n}$
4. Fazemos a = (r + s) e b = (r – s)
5. Retorna a e b.

3.12.2 Teorema. O algoritmo de Fermat funciona.

Demonstração:

Vamos mostrar que existe $x \geq \lfloor \sqrt{n} \rfloor$ tal que $\sqrt{x^2 - n}$ seja um número inteiro, o algoritmo efectua um número finito de passos.

Suponhamos que n = ab com a ≤ b. Este algoritmo procura números inteiros x e y tais que $n = x^2 - y^2 = (x - y)(x + y)$. Como $x - y \leq x + y$, então consideremos $a = x - y$ e $b = x + y$. O sistema de equações $\begin{cases} a = x - y \\ b = x + y \end{cases}$, tem solução $x = \frac{a + b}{2}$ e $y = \frac{b - a}{2}$. Como n é ímpar então a e b têm de ser ímpares. Donde, a + b e b – a são números pares, o que implica que $x = \frac{a + b}{2}$ e $y = \frac{b - a}{2}$ são números inteiros tais que $x^2 - y^2 = \left(\frac{a + b}{2}\right)^2 - \left(\frac{b - a}{2}\right)^2 = ab = n$. (*)

Se a = b, então o algoritmo pára no passo (2.). Suponhamos $1 < a < b < n$. Como $1 < b$ e $1 < a$ temos que $a - 1 > 0$, então $(a - 1) \times 1 < (a - 1) \times b \Rightarrow$

$$\Rightarrow a - 1 + (b + 1) < ab - b + (b + 1) \Rightarrow a + b < n + 1 \Rightarrow \frac{a + b}{2} < \frac{n + 1}{2}.$$

Por outro lado, pela equação (*) temos

$$\frac{(a + b)^2}{4} - \frac{(a - b)^2}{4} = n \Rightarrow \frac{(a + b)^2}{4} - n = \frac{(a - b)^2}{4} \geq 0.$$

Logo, $\frac{(a + b)^2}{4} - n \geq 0 \Rightarrow \frac{a + b}{2} \geq \sqrt{n} \geq \lfloor \sqrt{n} \rfloor$. Portanto, $\lfloor \sqrt{n} \rfloor \leq x < \frac{n + 1}{2}$.

Como a variável r é inicializada com o valor $\lfloor \sqrt{n} \rfloor$ e é aumentada de uma unidade em cada ciclo. Se n é composto, o algoritmo encontra um valor $r = \frac{a + b}{2}$ antes de chegar a $\frac{n + 1}{2}$.

■

3.12.3 Observação: Este algoritmo encontra rapidamente factores que estejam perto de $\sqrt{n}$.

Vamos factorizar n = 517, usando este método. O primeiro quadrado perfeito maior que 517 é $23^2 = 529$. De seguida, vamos calcular a sequência de r^2, com $r \geq 23$ e as diferenças $r^2 - n$.

$$23^2 - 517 = 529 - 517 = 12$$

$$24^2 - 517 = 576 - 517 = 59$$

$25^2 - 517 = 625 - 517 = 108$

$26^2 - 517 = 676 - 517 = 159$

$27^2 - 517 = 729 - 517 = 212$

$28^2 - 517 = 784 - 517 = 267$

$29^2 - 517 = 841 - 517 = 324 = 18^2$.

Temos então que $517 = 29^2 - 18^2 = (29 - 18) \times (29 + 18) = 11 \times 47$.

O **p – 1 de Pollard** algoritmo é eficiente quando o número a factorar tem um factor primo p, tal que o número p – 1 tem um factor $< 10^4$.

A ideia que se encontra a montante deste método é a seguinte: seja n o número que queremos factorar, e p um número primo que é divisor de n. Sabemos, pelo Pequeno Teorema de Fermat que $a^{p-1} \equiv 1 \pmod{p}$, para algum a, tal que m.d.c. (a, p) = 1. Se p – 1 divide um número M, então $a^M \equiv 1 \pmod{p}$, isto é, p | (a^M – 1). Como p | n e p | (a^M – 1), logo p divide m.d.c. (a^M – 1, n). Em vez de a^M – 1, vamos calcular (a^M – 1) (mod n) e m.d.c. ((a^M – 1) (mod n), n). Se o máximo divisor comum não for igual a n, então encontramos um factor não trivial de n. Este factor pode não ser p.

Mas sendo p – 1 de Pollard um algoritmo de factorização, o que queremos saber é quais são os factores de n, logo o p é desconhecido. Para determinarmos quais são os factores, vamos escolher um M tal que (p – 1) | M. O expoente M não pode ser muito grande, pois precisamos de calcular a^M num tempo razoável. Como desconhecemos a factorização em números primos de p – 1, M deve incluir todos os números primos até um limite superior B.

A forma mais fácil é fazermos M = k!, com k tomando valores naturais de uma forma crescente. Se todos os números primos divisores de p – 1 são menores ou iguais a que k $\leq$ B, então (p – 1) | k!, e teremos p | $(a^{k!} - 1 \pmod{n})$ e p | n, e podemos encontrar um factor não trivial através do m.d.c. $(a^{k!} - 1 \pmod{n}, n)$.

Exemplo: factorizemos n = 2479. Para tal, vamos determinar $2^{k!}$ (mod n) e o m.d.c. ($2^{k!}$ – 1 (mod n), n), para k $\in$ {1, 2, 3, 4, 5}.

$2^{1!} \equiv 2$ (mod n), m.d.c. (2 – 1, n) = 1,

$2^{2!} \equiv 4$ (mod n), m.d.c. (4 – 1, n) = 1,

$2^{3!} \equiv 64$ (mod n) m.d.c. (64 – 1, n) = 1,

$2^{4!} \equiv 1823$ (mod n) m.d.c. (1823 – 1, n) = 1,

$2^{5!} \equiv 618$ (mod n) m.d.c. (618 – 1, n) = 1,

$2^{6!} \equiv 223$ (mod n) m.d.c. (223 -1, n) = 37.

O factor 37 foi encontrado em 6 passos.

Na maior parte das vezes o máximo divisor comum é igual a 1, pelo que, em vez de procedermos como em cima, podemos determinar o máximo divisor comum de n, com o produto dos números $(a^{k!} – 1)(\text{mod } n)$, $(a^{(k + 1)!} – 1)(\text{mod } n)$,… para um pequeno número de factores.

Exemplo: Seja n = 15943; começamos por calcular $2^{1!}$ (mod n), $2^{2!}$ (mod n), e assim sucessivamente. Se $a_k \equiv 2^{k!}$ (mod n); então $a_{k+1} \equiv a_k^{k+1}$ (mod n). Podemos considerar o produto $Q_1 = (a_1 - 1)(a_2 – 1)…(a_{10} – 1)$ (mod n) e determinar o m.d.c. (Q_1, n); em seguida, para $Q_2 = (a_{11} – 1)(a_{12} – 1)…(a_{20} – 1)$ (mod n) , encontremos o m.d.c. (Q_2, n); até o mdc $(Q_t, n) \neq 1$, para algum $t \in \mathbb{N}$.

$Q_1 \equiv 6645$ (mod n), m.d.c. $(Q_1, n) = 1$,

$Q_2 \equiv 7988$ (mod n), m.d.c. $(Q_2, n) = 1$,

$Q_3 \equiv 1692$ (mod n), m.d.c. $(Q_3, n) = 1$,

$Q_4 \equiv 14453$ (mod n) m.d.c. $(Q_4, n) = 149$.

149 é um factor de n, o outro factor é 107.

No entanto, podemos depararmo-nos com alguma surpresa, como veremos no exemplo seguinte: consideremos n = 23489, $a_k = 2^{k!}$ (mod n) e Q_k como no exemplo anterior, ou seja, vamos determinar o máximo divisor comum a cada dez passos:

$Q_1 \equiv 21444 \pmod{n}$, m.d.c. $(Q_1, n) = 1$,

$Q_2 \equiv 12687 \pmod{n}$, m.d.c. $(Q_2, n) = 1$,

$Q_3 \equiv 1870 \pmod{n}$, m.d.c. $(Q_3, n) = 1$,

$Q_4 \equiv 1839 \pmod{n}$ m.d.c. $(Q_4, n) = 1$.

$Q_5 \equiv 0 \pmod{n}$, m.d.c. $(Q_5, n) = n$.

Isto aconteceu, porque todos os factores primos de n são tais que $(p - 1) \mid 50!$. Neste caso, temos que recomeçar o processo de $2^{40!} \pmod{n}$. Determinamos $2^{41!} \pmod{n}$ e m.d.c. $(2^{41!} \pmod{n}, n)$, $2^{42!} \pmod{n}$ e m.d.c. $(2^{42!} \pmod{n}, n)$, e assim sucessivamente até encontrarmos um máximo divisor comum diferente de um.

Como $2^{41!} \equiv 23074 \pmod{n}$ e m.d.c. (23074 -1, n) = 83, um dos factores de n é 83 e o outro 283.

3.12.4 Algoritmo p – 1 de Pollard. Dado um número n composto, este algoritmo de factorização calcula $a^{k!} \pmod{n}$ sucessivamente para $k \leq B$, B um limite pré-especificado. O m.d.c. $(a^{k!} - 1, n)$ é calculado a cada produto de 25 factores.

1. Seja a = 2, m = 1, Q = 1, $k \leftarrow 2$;
2. Seja $a = a^k \pmod{n}$, $Q = Q(a - 1) \pmod{n}$, k = k + 1, m = m + 1. Se m = 25, avançamos para o passo 3; se não, repetimos o passo 2.
3. Seja d = m.d.c. (Q, n); se $d \neq 1$ e $d \neq n$, retornaos n como um factor de n; se não avançamos para o passo 4.
4. Se d = n, então é necessário recuar e calcular o máximo divisor comum mais vezes. Se d = 1 e k < B, Q = 1, m = 1, e vamos para o passo 2; se não, se $m \geq B$, terminamos o algoritmo, n não tem um factor p em que p – 1 seja decomposto em factores primos pequenos.

3.12.5 Observação: Quando escolhemos uma chave do RSA, a escolha dos números primos p e q, deve ter em conta que p – 1 e q – 1 não tenham factores pequenos, pois o algoritmo p -1 de Pollard, põe em risco a segurança do RSA.

3.12.6 Crivo quadrático

Este método de factorização foi criado por C. Pomerance em 1981.

Dado um número inteiro n, o crivo quadrático procura números inteiros x, y tais que $x^2 \equiv y^2 \pmod{n}$ e $x \not\equiv \pm y \pmod{n}$. Logo, n é um divisor de $x^2 - y^2 = (x - y)(x + y)$ mas não divide x – y ou x + y. Pelo que,

g = m.d.c. (x – y, n) é um divisor próprio de n.

Como é que encontramos os números inteiros x e y, usando este método?

Seja $m = \lfloor \sqrt{n} \rfloor$ e $f(x) = (x + m)^2 - n$.

Vamos utilizar um exemplo para demonstrar este processo.

Seja n = 7429. Temos que $\sqrt{7429}$ = 86,19164693…, logo m = 86 e

f(x) = (x + m) – 7429.

$F(-3) = 83^2 - 7429 = -540 = -1 \times 2^2 \times 3^2 \times 5$

$F(1) = 87^2 - 7429 = 140 = 2^2 \times 5 \times 7$

$F(2) = 88^2 - 7429 = 315 = 3^2 \times 5 \times 7$

Temos então que

$83^2 \equiv -1 \times 2^2 \times 3^3 \times 5 \pmod{7429}$

$87^2 \equiv 2^2 \times 5 \times 7 \pmod{7429}$

$88^2 \equiv 3^2 \times 5 \times 7 \pmod{7429}$

Se multiplicarmos as duas últimas congruências, obtemos o seguinte:

$(87 \times 88)^2 \equiv (2 \times 3 \times 5 \times 7)^2 \pmod{7429}$.

Assim obtemos x = 87 × 88 (mod 7429) = 7656 (mod 7429) = 227 (mod 7429) e, por outro lado, $y = 2 \times 3 \times 5 \times 7 \pmod{7429} = 210 \pmod{7429}$. Como x = 227 e y = 210, então x + y = 437 e x – y =17, em que 17 e 437 são factores de 7429 e m.d.c. (17, 7429) = 17.

3.12.7 Algoritmo de Lenstra

Este método é baseado no método p – 1 de Pollard, já referido anteriormente.

Seja n um número inteiro composto, então tem uma factorização única em números primos. O nosso objectivo é encontrar um número primo p que seja um factor de n.

Para tal, vamos escolher uma curva elíptica, um ponto P que lhe pertença e um número k que é o produto de números primos pequenos elevados a potências pequenas (m.m.c. (1, 2, 3, …, B) ou k = B!, onde B é um certo número inteiro dado). Vamos calcular kP em $\mathbb{Z}_n$, onde $\mathbb{Z}_n$ é um anel, pois n é um número composto. As operações efectuadas em kP já foram descritas anteriormente.

Se não tivermos qualquer problema no cálculo de kP, é porque conseguimos calcular sempre λ, ou seja, λ teve sempre denominador c invertível em $\mathbb{Z}_n$, isto é m.d.c. (c, n) = 1. Neste caso, a nossa busca foi infrutífera. Ficamos então com duas saídas: ou aumentamos o valor de k, ou escolhemos outra curva elíptica e recomeçamos novamente o processo.

Se depararmos com problemas no cálculo de kP, é porque não conseguimos calcular algum dos λ, ou seja, um dos λ tem um denominador que não é invertível em $\mathbb{Z}_n$. Então 1 < m.d.c. (c, n) ≤ n, em que c é o denominador do λ que impediu a continuação do cálculo de kP, e duas situações podem ocorrer:

1. Se m.d.c. (c, n) < n, então c é um factor próprio de n;
2. Se m.d.c. (c, n) = n, vamos ter de continuar a trabalhar para encontrar um factor primo, para tal, vamos mudar de curva elíptica e recomeçar o processo.

Algoritmo de Lenstra.

Seja n ≥ 2 um número inteiro composto, para o qual vamos encontrar um factor primo.

1. Verificamos que m.d.c. (n, 6) = 1 e se n não tem a forma m^r para algum r ≥ 2.
2. Escolhemos números inteiros aleatórios a, x_1 e y_1 entre 1 e n.

3. Fazemos $b = y_1^2 - x_1^3 - ax_1 \pmod n$ (Seja C a curva $y^2 = x^3 + ax + b$ e $P = (x_1, y_1)$ um ponto de C).
4. Verificamos que m.d.c. $(4a^3 + 27b^2, n) = 1$. (Se for igual a n, vamos para o passo (2) e escolhemos um novo a. Se estiver entre 1 e n, então ele é um factor não trivial de n. Paramos.)
5. Calculamos kP mod n, para um valor elevado de k. Usando o método das duplicações sucessivas, ou considerando k = B!, sendo B natural e tomando, sucessivamente; valores crescentes. Se conseguirmos (é porque todos os λ's têm denominadores invertíveis em $\mathbb{Z}_n$), aumentamos o valor de k ou vamos para (2) e mudamos para outra curva elíptica. Caso contrário (é porque em alguma etapa do cálculo de kP o denominador c de λ é não invertível, isto é, m.d.c. (c, n) ≠ 1; vamos para (6).
6. Se m.d.c. (c, n) < n, encontramos um factor não trivial de n. Paramos. Se m.d.c. (c, n) = n vamos para (2) e escolhemos outra curva.

Vamos factorizar 6887, utilizando este algoritmo. Para tal, na família de curvas $y^2 = x^3 + ax + b$, consideremos a = 14 e P = (1512 , 3166) e calculemos o valor de b; $b = 3166^2 – 1512^3 – 14 \times 1512 \equiv 19 \pmod{6887}$.

O m.d.c. (6887,6) =1, pois 6887 não é divisível por 2 e 3. Com uma simples máquina de calcular, também verificamos que não existem m e r tal que $m^r = 6887$. O m.d.c. (20723, 6887) = 1, avançamos para o passo 5 e calculamos 2!P, 3!P, 4!P, 5!P e 6!P e obtemos os seguintes resultados:

$$2!P \equiv (3466, 2996)$$

$$3!P \equiv (3067, 396)$$

$$4!P \equiv (6507, 2654)$$

$$5!P \equiv (2783, 6278)$$

$$6!P \equiv (6141, 5581).$$

Até aqui conseguimos, infelizmente, encontrar λ, ou seja, até aqui λ teve sempre um denominador invertível em $\mathbb{Z}_n$. Podemos escolher um de dois

caminhos alternativos: ou continuamos a aumentar o valor de K, ou escolhemos outra curva elíptica; optemos pela primeira opção e vamos calcular 7!P. Consideremos Q = 6!P = (6141,5881) e calculemos 7Q. Para facilitar os cálculos, podemos escrever 7 na forma binária ($7 = 1 + 2 + 2^2$). Calculemos 2Q≡ (5380, 174) e 4Q ≡ 2 × 2Q ≡ (203, 2038), logo

$$7Q \equiv (Q + 2Q) + 4Q \equiv ((6141, 5581) + (5380, 174)) + (203, 2038) \equiv$$

$$\equiv (984, 589) + (203, 2038).$$

Esta última adição não se pode fazer, pois m.d.c. (203 – 984, 6887) ≠ 1; ou seja, o denominador de λ, não é invertível em $\mathbb{Z}_n$.

Pelo passo 6, m.d.c. (6106, 6887) = 71. Encontramos um factor de 6887, o 71. Se dividirmos 6887 por 71, obtemos 97. Como 97 é número primo, então a factorização de 6887 está concluída: 6887 = 71 × 97.

Exemplo de uma estratégia para factorizar um número inteiro em factores primos:

1. Procurar factores primos pequenos através da divisão, com primos menores que um número inteiro b_1, previamente estabelecido.

2. Aplicar o algoritmo ρ - Pollard, para encontrar factores primos p, com $b_1 \leq b_2$.

3. Utilizar o algoritmo de factorização com curvas elípticas para encontrar factores primos p, com $b_2 \leq p < b_3$.

4. Se todos falharem, aplicar o crivo quadrático.

Capítulo 4

Cifras

Quando se transmitem mensagens encriptadas é porque existe o receio que alguém, que não deve, se apodere do seu conteúdo; pondo desta forma, em risco: negócios, a vida privada, a segurança de pessoas, países e bens…

Neste capítulo, abordaremos alguns criptosistemas que nos permitem trocar mensagens com relativa segurança. Esta relatividade, está dependente do conjunto de chaves, que se utiliza. Quanto maior for a cardinalidade deste conjunto, maior será a segurança do criptosistema.

Ao longo deste capítulo vão aparecer três personagens: Berta, Duarte e Ricardo. Berta e Duarte trocarão diferentes mensagens entre si, usando os diversos criptosistemas; enquanto Ricardo será o intruso que procurará apoderar-se dessas mensagens que não lhe dizem respeito.

Em primeiro lugar, estudaremos algumas cifras simétricas, ou seja, as cifras que utilizam a mesma chave para encriptar e desencriptar uma mensagem, isto é, o processo para desencriptar uma mensagem é precisamente o oposto ao que a encriptou; passaremos pela troca de chaves e por fim, debruçar-nos-emos sobre as cifras assimétricas, as quais utilizam chaves diferentes para encriptar e desencriptar a mesma mensagem – uma pública e outra privada.

Nos diversos criptosistemas que se seguem utilizaremos a seguinte tabela:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Tabela 4.1 - Correspondência entre letras e números.

Esta correspondência permite-nos trabalhar no anel $\mathbb{Z}_{26}$.

4.1 Cifras simétricas

Apesar das várias cifras simétricas serem bastante diferentes entre si, há um modelo comum a todas elas. É com este modelo que são criados os diversos criptosistemas.

4.1.1Definição: Um criptosistema é um quíntuplo (P, C, K, E, D), onde são satisfeitas as seguintes condições:

1. P é um conjunto finito de símbolos;
2. C é um conjunto finito de símbolos;
3. K é um conjunto finito de chaves possíveis;
4. Para cada k ∈ K, existe uma regra de encriptação $e_k \in E$ e a correspondente regra de desencriptação $d_k \in D$. Cada $e_k : P \rightarrow C$ e $d_k : C \rightarrow P$ são funções tais que $d_k(e_k(x)) = x$, para todo o x ∈ P.

4.1.2 A cifra Shift

Esta cifra era aplicada nas mensagens que Júlio César encriptava.

O modelo desta cifra é o seguinte:

Seja P = C = K = $\mathbb{Z}_{26}$. Para $0 \leq k < 25$, define-se

$e_k(x) = (x + k) \pmod{26}$

$d_k(y) = (y - k) \pmod{26}$, com x, y ∈ $\mathbb{Z}_{26}$.

No entanto, existem só 25 chaves diferentes, o que torna esta cifra muito insegura!

Combinando a chave k = 8, Berta envia a Duarte a seguinte mensagem:

Mensagem: Che Guevara utilizava a cifra de Vernam

Para tal, converte as letras em números e aplica a cada um deles a função $e_8(x)$, como o demonstramos para a primeira letra

$$e_8(2) = (2 + 8) \pmod{26} = 10,$$

e 10 corresponde à letra k, prosseguindo desta forma, obtemos a seguinte mensagem encriptada:

KPMOCMDIZICBQTQHIDIIKQNZILMDMZVIU

Duarte para desencriptar a mensagem converte novamente as letras em números e aplica a função $d_8(x)$ a cada um dos números. Para a primeira letra, temos $d_8(10) = (10 - 8) \pmod{26} = 2$, que corresponde ao C, continuando este processo obtém a mensagem original.

É claro que se o Ricardo interceptar a mensagem, sabendo qual a cifra que foi utilizada não terá grande dificuldade em apoderar-se do seu verdadeiro significado!

4.1.3 A cifra Afim

Esta cifra tem o seguinte sistema criptográfico:

Sejam P = C = K = $\mathbb{Z}_{26}$ e $\mathrm{K} = \{(\mathrm{a}, \mathrm{b}) \in \mathbb{Z}_{26} : \mathrm{m.d.c.}\ (\mathrm{a}, 26) = 1\}$.

Para k = (a, b) ∈ K, define-se

e_k (x) = ax + b (mod 26)

d_k (y) = a^{-1}(y – b) (mod 26), com x, y ∈ $\mathbb{Z}_{26}$.

É necessário que m.d.c. (a, 26) = 1, para garantir que a função e_k(x) seja injectiva, deste modo, a função e(x) tem inversa, pois, só desta forma é que o criptosistema tem condições de ser aplicado! O que é garantido pelo teorema 3. 3.8.

A função e_k (x) = ax + b (mod 26) tem que ser injectiva pelas razões já expostas, o que não acontece para qualquer valor de a. Seja a = 4 e b = 3, utilizando a tabela 4.1, temos que e_k (1) = 4 × 1 + 3 = 7, 7 = 7 (mod 26), e e_k (14) = 4 × 14 + 3= 59, 7 = 59 (mod 26), pelo que as letras “A” e “O” vão dar as duas origem à mesma letra, “H”. O que causa problemas na decifração.

Se os nossos intervenientes escolherem a = 3 e b = 5, temos que m.d.c. (3, 26) = 1. O que lhes permite usar esta cifra para trocar mensagens. Como por exemplo:

Mensagem: Berlusconi perde dois dentes

Berta encripta a primeira letra da seguinte forma:

e_3(1) = (3 × 1 + 5) (mod26) = 8, e substituí **B** por **I**, repetindo este processo para todas as letras da mensagem, obtém, não os dentes do senhor, mas a seguinte mensagem encriptada:

IREMNHLVSDYREOROVDHORSKRH

Duarte calcula o 3^{-1} (mod 26), ou seja, 9. E aplica a função

$$d_3 = 9 \times (8 - 5)\ (\mathrm{mod}\ 26) = 1,$$

que substitui por **B**, percorrendo deste modo todas as letras da mensagem encriptada, obtém a mensagem original.

Esta cifra tem |K| = 12 × 26 = 312, pois $\varphi(26) = 26\ (1-\frac{1}{2})\ (1-\frac{1}{13}) = 12$. O que a torna pouco segura. Ricardo com um bocadinho de paciência e tempo descobria facilmente as mensagens trocadas entre Berta e Duarte.

4.1.4 A Cifra por permutação

Na cifra por permutação, as letras do texto simples são misturadas de acordo com uma permutação, que seja do conhecimento do emissor e do receptor.

Esta cifra tem o seguinte sistema criptográfico:

Seja m um número inteiro

$P = C = \mathbb{Z}^m{}_{26}$

K = conjunto de todas a permutações de 1,…, m.

$e_k\ (x_1, x_2, x_3, \ldots, x_m) = (x_\pi(1), x_\pi(2), x_\pi(3), \ldots, x_\pi(m))$

$d_k\ (y_1, y_2, y_3, \ldots, y_m) = (y_\pi{}^{-1}(1), y_\pi{}^{-1}(2), y_\pi{}^{-1}(3), \ldots, y_\pi{}^{-1}(m))$, d_k é a função inversa de e_k.

A cifra por permutação funciona do seguinte modo, suponhamos que Berta quer enviar a Duarte a seguinte mensagem: **HAITI VITIMA DA NATUREZA**

Para tal, vai utilizar a seguinte permutação $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 2 & 1 & 4 & 7 & 6 \end{pmatrix}$

Começa por dividir a mensagem em grupos de sete letras, do seguinte modo:

HAITIVI TIMADAN ATUREZA.

Em seguida, a cada um dos grupos aplica a permutação π, para reagrupar cada conjunto de letras, do seguinte modo: no primeiro grupo, para a primeira posição vem o I que estava na quinta posição, para a segunda posição vem o I que estava na terceira posição, para terceira posição vem o A que estava na segunda posição e assim sucessivamente, até obter estes novos grupos:

IIAHTIV DMITANA EUTARAZ.

Berta envia o seguinte texto em cifra: **IIAHTIVDMITANAEUTARAZ.**

Duarte, dividindo o texto em cifra em grupos de sete letras e aplicando a permutação $\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 5 & 1 & 7 & 6 \end{pmatrix}$, recupera a mensagem original.

Ricardo, após descobrir qual o criptosistema que está a ser utilizado, poderá apoderar-se da mensagem; para tal, tem que estar disposto a enfrentar até 7! chaves possíveis!

4.1.5 A cifra de Hill

Para esta cifra, tomemos o seguinte sistema criptográfico:

Tomemos m um número inteiro positivo fixo.

P = C = $\mathbb{Z}^m_{26}$

K = {matrizes invertíveis em $\mathbb{Z}_{26}$, m × m}

Para uma chave k ∈ K definem-se as funções:

e_k (x) = Kx

d_k (y) = K^{-1}y

Para se poder decifrar a mensagem é necessário que a matriz K seja invertível, o que poderá ser verificado através do cálculo do seu determinante, se o seu valor for primo com 26, então existe a matriz inversa, com as operações a serem efectuadas em módulo 26.

Exemplo da cifra de Hill

Seja K = $\begin{bmatrix} 1 & 3 & 5 \\ 1 & 2 & 4 \\ 2 & 4 & 7 \end{bmatrix}$, $|K| = 1$, como m.d.c.(1, 26) = 1 pelo que a matriz K tem inversa em $\mathbb{Z}_{26}$.

Texto simples: **BENFICA GANHA A SEGUNDA TAÇA DA LIGA**

Utilizando a tabela 4.1 e trocando as letras pelos números correspondentes, a mensagem corresponde a:

1 4 13 5 8 2 0 6 0 13 7 0 0 18 4 6 20 13 3 0 19 0 2 0 3 0 11 8 6 0

Podemos dividir este conjunto de números em subconjuntos de três elementos, da seguinte forma:

$$\begin{bmatrix}1\\4\\13\end{bmatrix}, \begin{bmatrix}5\\8\\2\end{bmatrix}, \begin{bmatrix}0\\6\\0\end{bmatrix}, \begin{bmatrix}13\\7\\0\end{bmatrix}, \begin{bmatrix}0\\18\\4\end{bmatrix}, \begin{bmatrix}6\\20\\13\end{bmatrix}, \begin{bmatrix}3\\0\\19\end{bmatrix}, \begin{bmatrix}0\\2\\0\end{bmatrix}, \begin{bmatrix}3\\0\\11\end{bmatrix} e \begin{bmatrix}8\\6\\0\end{bmatrix}$$

Neste momento, podemos cifrar a mensagem multiplicando a matriz do tipo 3 × 3 por cada uma das matrizes coluna, as operações aritméticas são feitas em $\mathbb{Z}_{26}$: $\begin{bmatrix}1&3&5\\1&2&4\\2&4&7\end{bmatrix}\begin{bmatrix}1\\4\\13\end{bmatrix} = \begin{bmatrix}0\\9\\5\end{bmatrix}$, deste modo **BEN** é substituído por **AJF**, continuando este processo até à última multiplicação, obtemos o seguinte texto em cifra: **AJFNDESMYIBCWAWBUBUBJGEIAUO.**

$K^{-1} = \begin{bmatrix}24&25&2\\1&23&1\\0&2&25\end{bmatrix}$ é a matriz inversa de K, com as operações aritméticas feitas em $\mathbb{Z}_{26}$.

O receptor para conseguir obter a mensagem original, inverte o processo, utilizando a matriz k^{-1}; tomemos como exemplo as três primeiras letras do texto em cifra **AJF**, que correspondem aos números 0, 9 e 5, fazendo a multiplicação de forma análoga

$\begin{bmatrix}24&25&2\\1&23&1\\0&2&25\end{bmatrix}\begin{bmatrix}0\\9\\5\end{bmatrix} = \begin{bmatrix}1\\4\\13\end{bmatrix}$, o que corresponde a **BEN,** após ter feito todas as multiplicações, ficaria conhecedor da excelente novidade!

4.1.6 A cifra de Vigenère

Esta cifra é polialfabética, ou seja, a mesma letra do texto simples pode ser substituída por várias letras diferentes, evitando deste modo que a mensagem sofra um ataque pela análise de frequências, para tal, utilizamos diferentes alfabetos de cifra.

Normalmente utiliza-se o quadro da figura 4.1, chamado quadro de Vigenère para cifrar mensagens.

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

Figura 4.1 – Cifra de Vigenère.

Para o uso desta cifra, Berta e Duarte recorrem a uma palavra-chave para estabelecerem uma comunicação segura, neste caso escolhem a palavra **árbitro**. É essa palavra-chave que vai permitir o uso de diferentes alfabetos de cifra.

Esta cifra tem o seguinte sistema criptográfico:

Tomemos m um número inteiro positivo fixo.

$P = C = \mathbb{Z}^{m}_{26}$

$K_m = \mathbb{Z}^m_{26}$

$\left| K_m \right| = 26^m$

Para uma chave $K = (K_1, K_2, K_3, \ldots, K_m)$

$e_k (x_1, x_2, x_3, \ldots, x_m) = (x_1 + K_1, x_2 + K_2, x_3 + K_3, \ldots, x_m + K_m)$

$d_k (y_1, y_2, y_3, \ldots, y_m) = (y_1 - K_1, y_2 - K_2, y_3 - K_3, \ldots, y_m - K_m)$, d_k é a função inversa de e_k.

Através de um exemplo, vamos ver como funciona esta cifra.

Berta, indignada, envia a Duarte, a seguinte mensagem: **A FRANÇA DÁ A MÃO AO MUNDIAL, HENRY I.**

Palavra-chave: **árbitro**.

Utilizando a tabela 4.1, a palavra-chave dá origem a K = (0, 17, 1, 8, 19, 17, 14), que tem comprimento 7, ou seja, m = 7. O que corresponde a

$$\left| K_7 \right| = 26^7 = 8031810176 \text{ chaves possíveis.}$$

Utilizando a tabela 4.1, podemos converter as letras em números da seguinte forma:

0 5 17 0 13 2 0 3 0 0 12 0 14 0 14 12 20 13 3 8 0 11 7 4 13 17 24 8.

De seguida, podemos começar por agrupá-los 7 a 7, obtemos então os seguintes conjuntos

0 5 17 0 13 2 0

3 0 0 12 0 14 0

14 12 20 13 3 8 0

11 7 4 13 17 24 8.

Agora a cada um destes conjuntos, adicionamos módulo 26 a palavra-chave e obtemos estes novos conjuntos:

0 22 18 8 6 19 14

3 17 1 20 19 5 14

14 3 21 21 22 25 14

11 24 5 21 10 15 22

Recorrendo, novamente, à tabela 4.1 obtemos o seguinte texto em cifra:

AWSIGTODRBUTFOODVVWZOLYFVKPW.

Duarte procede de forma semelhante para recuperar a mensagem, aplicando desta vez a respectiva função:

$$d_k (y_1, y_2, y_3,\ldots,y_7) = (y_1 - 0,\ y_2 - 17, y_3 - 1, y_4 - 8, y_5 - 19, y_6 - 17,\ y_7 - 8),$$

não esquecendo que a subtracção módulo 26, torna d_k a função inversa de e_k.

4.1.7 A cifra de One-time Pad

Em 1917, Gilbert Vernam criou a cifra One time Pad, também conhecida por cifra de Vernam. Nesta cifra, a chave é aleatória, tem o mesmo comprimento que o texto original e é usada uma única vez, daí o termo One-time – o que a torna inquebrável! Devido a esta característica tem sido usada em contextos militares e diplomáticos ao mais alto nível.

Para manter a sua segurança, normalmente, a chave é transportada por meios físicos seguros.

O seu uso é bastante fácil, tanto para encriptar como para desencriptar as mensagens.

A encriptação da mensagem é feita utilizando a operação binária XOR, semelhante à operação adição em $\mathbb{Z}_2$, que passamos a definir:

$\oplus: (\mathbb{Z}_2)^2 \rightarrow (\mathbb{Z}_2)$

(b, c) → b ⊕ c, esta operação é definida pelo seguinte quadro:

b	c	b ⊕ c
0	0	0
0	1	1
1	0	1
1	1	0

A cifra de Vernam, de um modo geral, funciona da seguinte forma: se n ≥ 1 é um número inteiro e P = C = K = $(\mathbb{Z}_2)^n$. Se quisermos enviar a mensagem x = (x_1, x_2,…,x_n), os intervenientes têm que ter na sua posse uma chave k, que foi criada aleatoriamente e com o mesmo comprimento que a mensagem, k = (k_1, k_2,…,k_n), então encriptamos a mensagem da seguinte forma:

$$e_k(x) = (x_1 + k_1, x_2 + k_2, \ldots, x_n + k_n) \pmod 2.$$

Para desencriptar a mensagem, procedemos de modo idêntico. Se

y = (y_1, y_2,…,y_n), então $d_k(y) = (y_1 + k_1, y_2 + k_2, \ldots, y_n + k_n) \pmod 2$.

Se Berta enviar a Duarte o nome do seu matemático preferido utilizando esta cifra, após os dois terem na sua posse a chave a utilizar, pode fazê-lo utilizando os números binários ASCII para as letras maiúsculas, que se encontram na tabela 2.11.

Mensagem: 10011101000001101001110010 00

Chave: 10011100011100010011011001 11

Encriptada: 00000001011101111010101011 11

Depois de enviar a mensagem ao Duarte, este só tem que utilizar a mesma chave e proceder da mesma forma:

Encriptada: 00000001011101111010101011 11

Chave: 10011100011100010011011001 11

Mensagem: 10011101000001101001110010 00

Agora só lhe resta consultar o ASCII para as letras maiúsculas, e fica a saber que **NASH** é o matemático preferido de Berta.

4.1.8 As cifras de fluxo

4.1.8.1 Definição – Uma cifra de fluxo é um séptuplo (P, C, K, L, F, E, D), para o qual são satisfeitas as seguintes condições:

1. P é um conjunto finito de símbolos;
2. C é um conjunto finito de símbolos;
3. K é um conjunto finito de chaves possíveis;
4. L é um conjunto finito chamado alfabeto chave de fluxo;
5. F = (f_1, f_2, …) é o gerador da chave de fluxo. Para i ≥ 1,

$$f_i : K \times P^{i-1} \rightarrow L$$

6. Para cada z ∈ L, existe uma regra de encriptação $e_z \in E$ e a correspondente regra de desencriptação $d_z \in D$. Cada $e_z : P \rightarrow C$ e $d_z : C \rightarrow P$ são funções tais que $d_k(e_k(x)) = x$ para todo o x ∈ P.

4.1.8.2 A cifra Autokey

Esta cifra de fluxo utiliza a própria mensagem na chave que utiliza para encriptar o texto, o seu funcionamento é o seguinte:

sejam P = C = K = L = $\mathbb{Z}_{26}$. Seja z_1 = K, e $z_i = x_{i-1}$ ($i \geq 2$). Para $0 \leq z \leq 25$, definimos:

$e_z(x) = x + z \pmod{26}$ e

$d_z(y) = y - z \pmod{26}$, com $x, y \in \mathbb{Z}_{26}$.

Se as nossas personagens, quiserem trocar mensagens através desta cifra, podem fazê-lo do seguinte modo: Berta e Duarte começam por escolher uma chave, seja 10. Só depois é que podem trocar mensagens. Se a mensagem a enviar for: **SALGUEIRO MAIA, O ÚLTIMO HERÓI PORTUGUÊS**; temos que transformá-la numa sequência de números, sendo o primeiro número a chave, utilizando a 4.1:

10 18 0 11 6 20 4 8 17 14 12 0 8 0 14 20 11 19 8 12 14 7 4 17 14 8 15 14 17 19 20 6 20 4 18

Berta encripta a mensagem da seguinte forma:

$e_{10} = (10 + 18) \pmod{26} = 2$

$e_{18} = (18 + 0) \pmod{26} = 18$

$e_0 = (0 + 11) \pmod{26} = 11$

e_{11} = (11 + 6) (mod 26) = 17,

….

e_4 = (4 +18) (mod 26) = 22.

A nova sequência gerada é a seguinte:

2 18 11 17 0 24 12 25 5 0 12 8 8 14 8 5 4 1 2 20 0 21 11 21 5 22 23 3 5 10 25 13 0 0 24 22

Voltando à tabela 4.1, a mensagem fica com o seguinte aspecto:

CSLRAYMZFAMIIOIFEBCUAVLVFWXDFKZNAAYW

Duarte converte as letras em números e desencripta-a do seguinte modo:

d_{10} = (2 – 10) (mod 26) = 18

d_{18} = (18 – 18) (mod 26) = 0

d_0 = (11 – 0) (mod 26) = 11

d_{11} = (17 – 11) (mod 26) = 6

….

d_4 = (22 – 4) (mod 26) = 18, recuperando a mensagem original!

4.2 A troca de chaves

Como já foi referido, com o aumento exponencial do uso da criptografia, um dos problemas mais prementes era a distribuição das chaves pelos diferentes intervenientes, pois os encargos económicos das empresas aumentavam, para que a troca de informação fosse segura! O método mais seguro para a distribuição de chaves era através da contratação de pessoal de extrema confiança!

Martin Hellman colocou a aritmética modular ao serviço da criptografia. A função Y^x (mod P), com Y, P $\in$ IN e Y < P, não é injectiva e com ela Hellman criou um esquema que permite uma troca de chaves segura, sem haver necessidade dos intervenientes se encontrarem.

O esquema de Hellman é o seguinte: duas pessoas, Berta e Duarte, podem trocar os valores Y e P de forma descontraída e natural, sem olharem a regras de segurança, pois não são estes os valores da chave, mas sim os valores que irão levar à chave. Por exemplo: Berta e Duarte podem combinar entre si que Y = 11 e P = 13, criando assim a função 11^x (mod13). Mais tarde, quando já

estão separados, cada um escolhe um número para si; Berta escolhe um número qualquer, por exemplo 3 e Duarte escolhe outro número ao acaso que pode ser 6 e procedem do seguinte modo:

1) Berta substitui x por 3 na função, 11^3 (mod 13) = 5;
2) Duarte faz a mesma coisa com o número por si escolhido, 11^6 (mod 13) = 12;
3) Berta e Duarte trocam entre si os números obtidos;
4) Berta substitui na função y pelo número enviado por Duarte e x por 3, 12^3 (mod 13) = 12;
5) Duarte age de forma análoga com o número que Berta lhe enviou, 5^6 (mod 13) = 12.

A chave encontrada é 12 e usam para trocar mensagens entre si!

Porque é que se faz quase tudo às claras e a chave é secreta?

Alguém que tenha escutado as conversas entre os nossos interlocutores, sabe a função Y^x (mod P) e os números trocados, 5 e 12; no entanto, não sabe os números que Berta e Duarte escolheram, 3 e 6, respectivamente. Como a função Y^x (mod P) não é injectiva, apesar de ser fácil neste exemplo, através de algumas tentativas, encontrar os números 3 e 6, tudo se complica quando se escolhe para Y e P números muito maiores, inverter todo o processo não é tarefa fácil!

4.3 As cifras assimétricas

Os problemas associados aos criptosistemas da chave pública

1. **Knapsach.** Dado um conjunto de números inteiros, encontrar um subconjunto cuja soma seja um número N dado.
2. **Logaritmo discreto.** Se p é um número primo, e g e M números inteiros, encontrar um número inteiro x tal que $g^x \equiv M$ (mod p); e suas variantes para corpos finitos e grupos abelianos.

3. **Factorização.** Se N é o produto de dois primos, então procuremos resolver algum dos seguintes problemas:
    - **(A)** Factorizar N (Problema da Factorização).
    - **(B)** Dados M e C, encontrar d tal que $M^d \equiv C \pmod N$ (problema RSA);
    - **(C)** Dados números inteiros e e C, encontrar M tal que $M^e \equiv C \pmod N$ (Problema inverso de RSA)
    - **(D)** Dado um número inteiro x, decidir se existe um número inteiro y tal que $x \equiv y^2 \pmod N$ (Problema dos resíduos quadráticos).

4.3.1 O criptosistema RSA

Whitfied Diffie concebeu a ideia da criptografia da chave pública, no entanto não foi capaz de a colocar em prática, esta última parte estava guardada para Ronald Rivest, Adi Shamir, cientistas informáticos, e Leonard Adleman, matemático, aos quais este criptosistema deve o seu nome.

Este criptosistema baseia-se no seguinte:

seja n = pq, onde p e q são dois números primos. Seja P = C = $\mathbb{Z}_n$, e defina-se

K= $\{(n, p, q, a, b) : n = p \times q$, p e q são números primos, $ab \equiv 1 \pmod{\varphi(n)}\}$.

Para $K = (n, p, q, a, b)$, define-se:

$e_k(x) = x^b \pmod n$ e $d_k(y) = y^a \pmod n$, com $x, y \in \mathbb{Z}_n$. Os valores n e b são públicos, e os valores p, q e a são secretos.

Esta cifra baseia-se na escolha de dois números primos e na aritmética modular. O processo inicia-se com a criação, por parte do receptor, de uma chave pública e uma chave privada, através do processo seguinte:

1) Escolher os dois números primos, p e q;
2) Calcular n = pq;
3) Calcular φ (n) = (p – 1)(q-1);
4) Escolher um número inteiro **b**, tal que, 1< **b** < φ (n) e m.d.c. (**b**, φ (n)) = 1;

5) Determinar um número inteiro **a**, tal que $1 < \mathbf{a} < \varphi(n)$ e $\mathbf{a} \times \mathbf{b} = 1 (\text{mod } \varphi(n))$.

Podemos ilustrar este processo. Berta cria uma chave pública e outra privada da seguinte forma:

1) De um modo geral, por razões de segurança, os primos escolhidos são enormes; no entanto por uma questão prática Berta escolhe p = 13 e q = 17;

2) n = 221;

3) $\varphi(221) = 192$;

4) $\mathbf{b} = 5$; $1 < \mathbf{b} < \varphi(221)$;

5) $\mathbf{a} = 77$**;** $5 \times 77 = 1 \text{ (mod } 192)$.

Neste caso, a chave pública é (221, 5) e a chave privada é (221, 77). Berta pode imprimir a chave pública num cartão-de-visita. Como o próprio nome indica esta chave tem de ser pública, para se poderem trocar mensagens.

Agora, qualquer indivíduo pode cifrar e enviar uma mensagem para Berta, utilizando uma chave do conhecimento geral, mas no máximo sigilo. Para tal, procede do seguinte modo:

1) Após converter as letras em números, utilizando por exemplo a tabela 4.1 da página 106, cifra o texto simples utilizando a fórmula $c = m^{\mathbf{b}} \text{ (mod } n)$, onde m é um número que substitui uma letra do texto simples e c um número que substitui m no texto em cifra;

2) Quando Berta recebe a mensagem cifrada, utiliza a fórmula $m = c^{\mathbf{a}} \text{ (mod } n)$, onde c e m são os definidos no passo anterior, para tornar a mensagem legível.

Utilizando as chaves criadas no exemplo anterior, vamos ilustrar estes processos com o seguinte exemplo: Duarte utiliza este criptosistema para enviar a seguinte mensagem: **MOURINHO ASSINA PELO REAL MADRID.**

Convertendo as letras em números, através da tabela 4.1, temos a seguinte correspondência:

12 14 20 17 8 13 7 14 0 18 18 8 13 0 15 4 11 14 17 4 0 11 12 0 3 17 8 3

Duarte aplica a função $c = m^5 \pmod{221}$,a cada um dos números anteriores, para obter a mensagem cifrada.

$c_1 \equiv 12^5 \pmod{221} \Longrightarrow c_1 = 207$

$c_2 \equiv 14^5 \pmod{221} \Longrightarrow c_2 = 131$

$c_3 \equiv 20^5 \pmod{221} \Longrightarrow c_3 = 141$

$c_4 \equiv 17^5 \pmod{221} \Longrightarrow c_4 = 153$

$c_5 \equiv 8^5 \pmod{221} \Longrightarrow c_5 = 60$

$c_6 \equiv 13^5 \pmod{221} \Longrightarrow c_6 = 13$

$c_7 \equiv 7^5 \pmod{221} \Longrightarrow c_7 = 11$

$c_8 \equiv 14^5 \pmod{221} \Longrightarrow c_8 = 131$

$c_9 \equiv 0^5 \pmod{221} \Longrightarrow c_9 = 0$

$c_{10} \equiv 18^5 \pmod{221} \Longrightarrow c_{10} = 18$

$c_{11} \equiv 18^5 \pmod{221} \Longrightarrow c_{11} = 18$

$c_{12} \equiv 8^5 \pmod{221} \Longrightarrow c_{12} = 60$

$c_{13} \equiv 13^5 \pmod{221} \Longrightarrow c_{13} = 13$

$c_{14} \equiv 0^5 \pmod{221} \Longrightarrow c_{14} = 0$

$c_{15} \equiv 15^5 \pmod{221} \Longrightarrow c_{15} = 19$

$c_{16} \equiv 4^5 \pmod{221} \Longrightarrow c_{16} = 140$

$c_{17} \equiv 11^5 \pmod{221} \Longrightarrow c_{17} = 163$

$c_{18} \equiv 14^5 \pmod{221} \Longrightarrow c_{18} = 131$

$c_{19} \equiv 17^{5} \pmod{221} \Longrightarrow c_{19} = 153$

$c_{20} \equiv 4^{5} \pmod{221} \Longrightarrow c_{20} = 140$

$c_{21} \equiv 0^{5} \pmod{221} \Longrightarrow c_{21} = 0$

$c_{22} \equiv 11^{5} \pmod{221} \Longrightarrow c_{22} = 163$

$c_{23} \equiv 12^{5} \pmod{221} \Longrightarrow c_{23} = 207$

$c_{24} \equiv 0^{5} \pmod{221} \Longrightarrow c_{24} = 0$

$c_{25} \equiv 3^{5} \pmod{221} \Longrightarrow c_{25} = 22$

$c_{26} \equiv 17^{5} \pmod{221} \Longrightarrow c_{26} = 153$

$c_{27} \equiv 8^{5} \pmod{221} \Longrightarrow c_{27} = 60$

A mensagem a enviar é a seguinte:

207 131 141 153 60 13 11 131 0 18 18 60 13 0 19 140 163 131 153 140 0 163 207 0 22 153 60

Após receber esta mensagem, fazendo uso da chave privada, Berta reverte o processo de modo a saber a mensagem, da seguinte forma:

$m_1 = 207^{77} \pmod{221} \Longrightarrow m_1 = 12$, que corresponde a letra M.

Berta pode calcular m_1, de várias formas, uma delas, utilizando uma simples máquina de calcular, pode ser a seguinte:

$207^{2} \pmod{221} = 196$

$207^{4} \pmod{221} = 183$

$207^{8} \pmod{221} = 118$

$207^{16} \pmod{221} = 1$

$207^{32} \pmod{221} = 1$

$207^{64} \pmod{221} = 1$

$207^{77} \pmod{221} = 207^{64} \pmod{221} \times 207^{8} \pmod{221} \times 207^{4} \pmod{221} \times 207 \pmod{221} = (1 \times 118 \times 183 \times 207) \pmod{221} = 12$.

Esta forma de reverter o processo torna-se um trabalho árduo, se os números primos forem números com muitos dígitos.

A força desta cifra reside no facto de não existirem, actualmente, algoritmos capazes de decompor em factores primos, de uma forma rápida, um número enorme. Como escreve o Professor Jorge Buescu, referindo-se à segurança deste método, no seu livro *O Mistério do Bilhete de Identidade e Outras Histórias*: "O perigo não vem dos computadores. Na verdade, a evolução dos computadores vem tornar o método RSA mais seguro. A razão é que o tempo para a multiplicação de dois números cresce mais devagar (polinomialmente) do que o necessário para a sua factorização (que, tanto quanto se sabe, cresce exponencialmente)… O perigo não vem dos computadores – vem da Matemática."

4.3.1.1 Proposição – Seja $n = p \times q$ um produto de dois números primos distintos. Então determinar $\varphi(n)$ é equivalente a factorizar n.

Demonstração: Se conhecemos a factorização de n, então

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

Por outro lado, se n e $\varphi(n)$ são conhecidos, então é fácil calcular os factores p e q. Como $n = pq$, podemos escrever $q = \frac{n}{p}$ e substitui-lo na fórmula $\varphi(n)$. Ou seja,

$\varphi(n) = (p - 1)(q - 1) = (p - 1)\left(\frac{n}{p} - 1\right)$. Simplificando esta equação, obtemos a seguinte equação do segundo grau $p^2 - (n + 1 - \varphi(n))p + n = 0$. Tratando-se de uma equação do 2º grau, é fácil de calcular o valor de p, e q sai de imediato. O que mostra que determinar $\varphi(n)$ é equivalente a factorizar n.

■

Se soubermos os seguintes valores $n = 221$ e $\varphi(n) = 192$, considerando a demonstração do teorema anterior, podemos fazer:

p^2 - (221 + 1 – 192)p + 221 = 0, que é equivalente à seguinte equação:

p^2 - 30 p + 221 = 0. Aplicando a fórmula resolvente, encontramos as seguintes soluções p = 17 ou p = 13. Ou seja, os dois factores de n.

De seguida, mostraremos que existe um método que descreve o cálculo do exponente a desconhecendo φ(n), o que nos levará à factorização de n. Sabemos que ab $\equiv$ 1 (mod φ(n)). O algoritmo que vamos descrever é probabilístico, além de estar dependente das escolhas aleatórias que fazemos, nem sempre nos dá uma resposta correcta.

O algoritmo é baseado no facto da equação $x^2 \equiv 1$ (mod n) ter quatro soluções quando n é o produto de dois números primos distintos. Qualquer solução α de $x^2 \equiv 1$ (mod n) é tal que $n \mid (\alpha - 1) \times (\alpha + 1)$. Como $\alpha \not\equiv \pm 1$ (mod n), podemos calcular um factor de n, determinando m.d.c. $(\alpha - 1, n)$ ou m.d.c. (α + 1, n).

Suponhamos que conhecemos a tal que ab ≡ 1 (mod φ(n)). Como ab – 1 é um múltiplo de φ(n), logo é um número par, pelo que, podemos escrever ab – 1 = 2^rs, onde s é número ímpar. Escolhamos aleatoriamente, um número w tal que 0 < w < n e calculemos a sequência seguinte: $z_0 = w^s$ (mod n), $z_1 = z_0^2$ (mod n),…, $z_i = z_{i-1}^2$ (mod n),…, $z_r = z_{r-1}^2$ (mod n). Note-se que $z_i = w^{2^i s}$ (mod n). Como φ(n)| (ab -1) = 2^rs, pelo teorema de Euler, temos que o último termo da sequência, z_r, é 1. Se o primeiro termo da sequência não é 1, então precisamos de encontrar um número $z_k \not\equiv 1$ (mod n) tal que $z_k^2 \equiv 1$ (mod n). E esperemos que $z_k \not\equiv$ - 1 (mod n). Se existir z_k com estas propriedades; então encontramos uma raiz quadrada da unidade módulo n, e podemos factorar n.

Exemplo: Consideremos n = 13289 e b = 7849 uma chave pública. Suponhamos que o expoente de desencriptação é a = 2713. Utilizando o método anterior, podemos factorizar n. Temos que ab -1 = 2^rs, com r = 8 e s = 83181. Escolhemos aleatoriamente w = 493. Então $x_0 = w^s$ (mod n) = 5032. Se $x_i = x_{i-1}^2$ (mod n), então x_1 = 5479, x_2 = 12879, x_3 = 8632 e x_4 = 1, ou seja,

$8632^2 \equiv 1 \pmod{n}$; calculando o m.d.c. (8632 – 1, n) obtemos um factor próprio de n. Neste caso 137, pelo que o outro factor é 97.

Este algoritmo falha sempre $z_0 = 1$ ou se existe um índice k tal que $z_k = -1$.

Em 1977, Martin Gardner, imprimiu um texto em cifra e forneceu a seguinte chave pública: N = 114 381 625 757 888 867 669 235 779 976 146 612 010 218 296 721 242 362 562 561 842 935 706 935 245 733 897 830 597 123 563 958 705 058 989 075 147 599 290 026 879 543 541, e desafiou os interessados a decifrar a sua mensagem. O desafio durou dezassete anos, e foram necessários seiscentos computadores ligados em rede para quebrar a cifra.

Hoje em dia, são utilizados números muito maiores do que aqueles que Gardner usou, de forma a garantir a circulação da informação em segurança. Podemos dizer, que neste momento, é o gato que joga ao ataque!

4.3.1.2 Teorema: Seja (n, b) a chave pública de RSA e a a correspondente chave privada. Então $\left(m^b\right)^a \pmod{n} = m$, para algum número inteiro m, com $0 \leq m < n$.

Demonstração:

Como $ab \equiv 1 \pmod{(p-1)(q-1)}$, existe um número inteiro l com

$ab = 1 + l(p - 1)(q - 1)$.

Por conseguinte, $\left(m^b\right)^a = m^{ba} = m^{1 + l(p-1)(q-1)} = m\left(m^{(p-1)(q-1)}\right)^l$. Temos então que

$\left(m^b\right)^a \equiv m\left(m^{(p-1)}\right)^{(q-1)l} \equiv m \pmod{p}$.

Se p não é um divisor de m, então pelo Pequeno Teorema de Fermat, verifica-se a congruência acima indicada. Por outro lado, se for um divisor de m, então de ambos os lados temos as congruências iguais a 0 módulo p. De modo análogo, temos que $\left(m^b\right)^a \equiv m \pmod{q}$.

Como p e q são números primos distintos, temos que $\left(m^b\right)^a \equiv m \pmod{n}$.

(a afirmação deve-se ao facto de $0 \leq m < n$.)

■

4.3.1.3 A escolha dos números primos p e q.

Além de p e q serem números primos enormes, temos que ter algum cuidado na sua escolha.

p - 1 e q – 1 não devem ter factores pequenos.

4.3.1.4 A escolha de b

O número b da chave pública deve ser tão pequeno quanto possível. No entanto, b tem de ser diferente de dois, pois o mdc (b, (p – 1)(q – 1)) = 1; como p -1 e q – 1 são pares o m.d.c. (b, (p – 1)(q – 1)) ≥ 2, se b for par.

Estes são apenas dois exemplos, dos cuidados que devem ser tomados, aquando da criação de um criptosistema RSA. Pois os testes de primalidade e os algoritmos de factorização referidos no capítulo anterior são utilizados por criptógrafos e criptanalistas respectivamente, tanto para descobrir números primos com muitos algarismos, como para quebrar a chave através da factorização do produto de dois números com algumas centenas de dígitos.

4.3.2 O criptosistema ELGamal

O criptosistema ElGamal é baseado no problema do logaritmo discreto. $\mathbb{Z}_p$ é um corpo finito, onde p é um número primo.

O criptosistema ElGamal em $\mathbb{Z}_p$ tem a seguinte forma:

Seja p um número primo tal que o problema do logaritmo discreto em $\mathbb{Z}_p$ é intratável, e $\alpha \in \mathbb{Z}_p^*$ uma raiz primitiva. Sejam P = $\mathbb{Z}_p^*$ × $\mathbb{Z}_p^*$, e defina-se

$$K = \{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod p\}.$$

Os valores p, α e β são públicos, e a é secreto.

Para $K = (p, \alpha, a, \beta)$, e para um número $k \in \mathbb{Z}_{p-1}$, secreto, e escolhido de forma aleatória define-se a função

e_k (x, k) = (y_1, y_2), com (x, k) ∈ $\mathbb{Z}_p^*$ × $\mathbb{Z}_{p-1}$ e (y_1, y_2) ∈ $\mathbb{Z}_p^*$ × $\mathbb{Z}_p^*$, onde $y_1 = \alpha^k \pmod p$ e $y_2 = x\beta^k \pmod p$.

Para $y_1, y_2 \in \mathbb{Z}_p^*$, define-se $d_k(y_1, y_2) = y_2(y_1^{\alpha})^{-1} \pmod p$.

Exemplo: Se Duarte quiser enviar uma mensagem secreta para Berta, utilizando este criptosistema, tem que conhecer a chave pública de Berta. Para

tal , Berta procede da seguinte forma: começa por escolher um número primo, p = 2357 e uma raiz primitiva módulo 2357, α = 2. Para a chave privada Berta escolhe, a = 1751 ($1 \leq a \leq p - 2$) e calcula 2^{1751} (mod 2357) = 1185.

A chave pública de Berta é (2357, 2, 1185).

Para encriptar a mensagem: **ORLANDO TAMAYO MORREU DE PÉ NÃO VIVEU DE JOELHOS**; Duarte selecciona aleatoriamente um número inteiro k = = 1520 ($1 \leq k \leq 2355$) e calcula

$y_1 = 2^{1520}$ (mod 2357) = 1430 e $y_2 = 14 \times 1185^{1520}$ (mod 2357) = 892.

Fazendo cálculos análogos, com esta chave pública, elaboramos uma tabela que converte o alfabeto latino em números que serão utilizados no envio da mensagem. A tabela é a seguinte:

A	0	0
B	1	2084
C	2	1811
D	3	1538
E	4	1265
F	5	992
G	6	719
H	7	446
I	8	173
J	9	2257
K	10	1984
L	11	1711
M	12	1438
N	13	1165
O	14	892
P	15	619
Q	16	346
R	17	73
S	18	2157
T	19	1884
U	20	1611
V	21	1338
W	22	1065
X	23	792
Y	24	519
Z	25	246

Tabela 4.2 - Conversão do alfabeto latino, utilizando o criptosistema ElGamal, aplicando a chave pública (2357, 2, 1185).

Temos então que $y_1 = 1430$ e utilizando y_2, temos que a mensagem encriptada é a seguinte: 892 73 1711 0 1165 1538 892 1884 0 1438 0 519 892 1438 892 73 73 1265 1611 1538 1265 619 1265 1165 0 892 1338 173 1338 1265 1611 1538 1265 2257 892 1265 1711 446 892 2157

Para desencriptar a mensagem Berta calcula

$$y^{p-1-a} = 1430^{605} \pmod{2357} = 872.$$

A mensagem original m, é obtida calculando: $m = 892 \times 872 \pmod{2357} = 14$.

Aplicando este último cálculo a todos os números da mensagem Berta consegue obter a mensagem original.

4.3.3 O criptosistema de MASSEY- OMURA

Neste criptosistema utilizámos um corpo finito $\mathbb{Z}_p$, quanto maior for o número primo p, maior será a sua segurança.

Este criptosistema, apesar de ser bastante simples de implementar, tem uma fragilidade – é o facto do vai e vem e torna a ir!

Quem pretende enviar a mensagem escolhe um $\mathbf{e_1} \in \mathbb{Z}_{p-1}$, tal que m.d.c. ($\mathbf{e_1}$, p-1) = 1, pois como $\mathbb{Z}_{p-1}$ é um anel, nem todos os seus elementos têm inverso. Através da igualdade de Bezout, vamos calcular $\mathbf{d_1} \in \mathbb{Z}_{p-1}$, tal que $\mathbf{e_1} \times \mathbf{d_1} \equiv 1 \pmod{p-1}$.

Por sua vez, o receptor, que tem previamente conhecimento do corpo $\mathbb{Z}_p$, através do qual se efectuarão as trocas de mensagens, procede como o emissor e também escolhe um $\mathbf{e_2} \in \mathbb{Z}_{p-1}$, tal que m.d.c. ($\mathbf{e_2}$, p-1) = 1 e calcula o $\mathbf{d_2} \in \mathbb{Z}_{p-1}$, tal que $\mathbf{e_2} \times \mathbf{d_2} \equiv 1 \pmod{p-1}$.

Vamos explicar o funcionamento deste criptosistema através dum exemplo. Suponhamos que Berta e Duarte escolhem o corpo $\mathbb{Z}_{709}$ para trocar mensagens.

Berta vai enviar a seguinte mensagem: **PORTUGAL VAI À TERRA DOS BAFANA BAFANA**. Como $25 \times 26 + 25 = 675 < 709$, podemos agrupar as letras da frase duas a duas e pela ordem que aparecem na mesma: PO, RT, UG, AL, VA, IA, TE, RR, AD, OS, BA, FA, NA, BA, FA e NA, e converter cada grupo num número, da seguinte forma: no caso de PO, fazemos a sua conversão, utilizando a tabela 4.1, em (15,14), podemos multiplicar o primeiro

número por 26 e adicionar ao resultado 14, ou seja, (15 × 26 + 14) que dá o resultado 404, fazendo o mesmo aos restantes grupos, obteremos a seguinte mensagem: 404 461 526 11 546 208 498 459 3 382 26 130 338 26 130 e 138.

Neste caso Berta escolhe para $\mathbf{e_1}$ = 97 e $\mathbf{d_1}$ = 73; o Duarte utiliza o $\mathbf{e_2}$ = 53 e $\mathbf{d_2}$ = 521. Berta recorre à exponenciação modular em 709 e transforma, utilizando o expoente 97, cada um dos números da mensagem da seguinte forma:

$404^2 \pmod{709} \equiv 146$

$404^4 \pmod{709} \equiv 146^2 \pmod{709} \equiv 46$

$404^8 \pmod{709} \equiv 46^2 \pmod{709} \equiv 698$

$404^{16} \pmod{709} \equiv 698^2 \pmod{709} \equiv 121$

$404^{32} \pmod{709} \equiv 121^2 \pmod{709} \equiv 461$

$404^{64} \pmod{709} \equiv 461^2 \pmod{709} \equiv 530.$

Como 97 = 64 + 32 +1, recorrendo, novamente, as regras da proposição 3.3.6, temos que $404^{97} \pmod{709} \equiv (404^{64} \times 404^{32} \times 404) \pmod{709} \equiv (530 \times 461 \times 404) \pmod{709} \equiv 213$.

Procedendo desta forma para cada um dos números da mensagem, esta é convertida em: 213 412 554 435 285 174 596 350 299 210 507 567 23 507 567 e 23. Neste momento, Berta envia-a ao Duarte, podendo utilizar um canal aberto!

Duarte recebe a mensagem, mas não a percebe, por enquanto! Para cada um dos números que recebeu, vai servir-se do seu $\mathbf{e_2}$ e utilizando o mesmo processo que a Berta aplicou anteriormente, converte a mensagem numa nova série de números que para ele ainda não fazem sentido. Neste momento a série de números é a seguinte: 362 62 707 179 426 514 11 115 180 22 236 225 384 236 225 e 384.

Duarte reenvia estes números para a Berta, para a qual deixaram de ter sentido; se por acaso, Duarte enviou um número errado, Berta não se apercebe! Neste momento, Berta pega no seu $\mathbf{d_1}$ e mais uma vez aplica todo o processo inicial, obtendo esta série de números: 241 431 490 300 560 637 448 281 614 270 494 127 10 494 127 e 10. E envia-a, pela última vez, para o Duarte.

Finalmente, Duarte saberá o conteúdo da mensagem, para tal, através do seu $\mathbf{d_2}$, vai encontrar os números iniciais da mensagem, como mostramos para o primeiro número:

$241^2 \pmod{709} \equiv 652$

$241^4 \pmod{709} \equiv 652^2 \pmod{709} \equiv 413$

$241^8 \pmod{709} \equiv 413^2 \pmod{709} \equiv 409$

$241^{16} \pmod{709} \equiv 409^2 \pmod{709} \equiv 666$

$241^{32} \pmod{709} \equiv 666^2 \pmod{709} \equiv 431$

$241^{64} \pmod{709} \equiv 431^2 \pmod{709} \equiv 3$

$241^{128} \pmod{709} \equiv 3^2 \pmod{709} \equiv 9$

$241^{256} \pmod{709} \equiv 9^2 \pmod{709} \equiv 81$

$241^{512} \pmod{709} \equiv 81^2 \pmod{709} \equiv 180.$

Como 521 = 512 + 8 + 1 e utilizando as propriedades da proposição 3.3.6, temos que

$$241^{521} \pmod{709} \equiv (241^{512} \times 241^8 \times 241) \pmod{709} \equiv$$
$$\equiv (180 \times 409 \times 241) \pmod{709} \equiv 404.$$

Deste modo, Duarte recuperará todos os números da mensagem inicial: agora basta dividir cada um dos números por 26; o quociente será a primeira letra de cada grupo e o resto a segunda. Neste primeiro caso, quando Duarte dividir 404 por 26, obterá como quociente 15 que corresponde à letra P e 14 como resto, que corresponde à letra O; procedendo desta forma com todos os números obtidos da mensagem inicial, Duarte obterá a mensagem original, ficando a saber o que Berta lhe queria dizer.

De uma forma geral, este método funciona da seguinte forma: os dois interlocutores escolhem um número primo, p, grande (quanto maior for o número primo, maior será a segurança do criptosistema), cada um deles escolhe um $\mathbf{e_i} \in \mathbb{Z}_{p-1}$ e com m.d.c. ($\mathbf{e_i}$, p – 1) = 1 e calculam um $\mathbf{d_i} \in \mathbb{Z}_{p-1}$, tal que $\mathbf{e_i} \times \mathbf{d_i} \equiv 1 \pmod{p-1}$.

Após converter as letras em números, o emissor começa, para enviar a mensagem m, por calcular $m^{e_1} \pmod{p}$ e remete-a para o receptor; este calcula $(m^{e_1})^{e_2} \pmod{p}$ e devolve-a ao emissor; neste início da segunda volta, o emissor calcula:

$[(m^{e_1})^{e_2}]^{d_1}$ (mod p) $\equiv (m^{e_1 d_1})^{e_2}$ (mod p) $\equiv (m^1)^{e_2}$ (mod p) $\equiv (m^{e_2})$ (mod p), e pela última vez, envia-a ao receptor que, finalmente, calcula:

$(m^{e_2})^{d_2}$ (mod p) $\equiv (m^1)$ (mod p) $\equiv m$ (mod p); recuperando a mensagem inicial.

No entanto, este criptosistema tem uma brecha. Se a mensagem for interceptada por Ricardo, quando do primeiro envio, e se este souber qual o grupo finito que está a ser utilizado na troca de mensagens, então pode, através de um $\mathbf{e_3} \in \mathbb{Z}_{p-1}$ com m.d.c. ($\mathbf{e_3}$, p-1) = 1 e um $\mathbf{d_3} \in \mathbb{Z}_{p-1}$, tal que, $\mathbf{e_3} \times \mathbf{d_3} \equiv 1$ (mod p – 1), fazer os seus cálculos e reenviar a mensagem a Berta. Esta, na completa ignorância, faz os cálculos com os números que o Ricardo lhe enviou e reenvia-lhe a mensagem, possibilitando, desta forma, que Ricardo se apodere do conteúdo da mensagem. Podemos evitar esta brecha, através de um sistema de autenticação, que nos permita saber se a mensagem é reenviada de fonte segura.

4.3.4 O criptosistema Menezes-Vanstone

Seja E uma curva elíptica definida em $\mathbb{Z}_p$ (com p > 3 e primo), tal que, E contem um subgrupo cíclico H, para o qual o problema do logaritmo discreto é intratável.

Seja P = $\mathbb{Z}_p^* \times \mathbb{Z}_p^*$, C = $E \times \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ e definimos

K = {(E, α, a, β) : β = aα}, onde α ∈ E. Os valores α e β são públicos e a é secreto.

Para K = (E, α, a, β), k $\in Z_{|H|}$ um número escolhido de forma aleatória e x = (x_1, x_2) $\in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$, definimos:

e_k = (x, k) = (y_0, y_1, y_2), onde

y_0 = kα

(c_1, c_2) = k β.

y_1 = c_1 x_1 (mod p) e

y_2 = c_2 x_2 (mod p).

Para o texto cifrado y = (y_0, y_1, y_2), definimos

d_k (y) = ($y_1 c_1^{-1}$ (mod p), $y_2 c_2^{-1}$ (mod p)), em que

ay_0 = (c_1, c_2).

Vamos ilustrar este criptosistema com o seguinte exemplo: Berta vai escolher a curva elíptica $y^2 = x^3 + x + 6$ e o número primo 29, logo$4 \times 1^3 + 27 \times 6 = 166 \equiv$ $\equiv 21 \pmod{29}$, ou seja, 166 não é múltiplo de 29. Temos então que E é constituído pelos seguintes pontos: (0 , 8), (0 , 21), (2 , 4), (2 , 25), (3 , 6), (3 , 23), (4 , 4), (4 , 25), (5 , 7), (5 , 22), (6 ,5), (6 , 24), (8 , 2), (8 , 27), (10 , 1), (10, 28), (12, 8), (12, 21), (14 , 3), (14 , 26), (16 , 0), (17 , 8), (17 , 21), (20 , 14), (20 , 15), (22 , 2), (22, 27), (23 , 4), (23 , 25), (25 , 5), (25 , 24), (26 , 11), (26 , 18), (27 ,5), (27 , 24), (28, 2) e (28, 27).

Berta escolhe $\alpha = (5, 22)$ e $a = 8$. Pelo que $\beta = 8 \times (5 , 22) = (22 , 2)$; temos então que os valores públicos são (5 , 22) e (22 , 2) ; o valor secreto é 8.

Se Duarte quiser enviar a Berta o seguinte poema:

Esta é a madrugada que eu esperava

O dia inicial inteiro e limpo

Onde emergimos da noite e do silêncio

E livres habitamos a substância do tempo. S

Para tal, utilizando a tabela 4.1, Duarte converte cada uma das letras do poema de Sophia de Mello Breyner Andresen no número correspondente, ou seja:

4 18 19 0 4 0 12 0 3 17 20 6 0 3 0 16 20 4 4 20 4 18 15 4 17 0 21 0 14 3 8 0 8 13 8 2 8 0 11 8 13 19 4 8 17 14 4 11 8 12 15 14 14 13 3 4 4 12 4 17 6 8 12 14 18 3 0 13 14 8 19 4 4 3 14 18 8 11 4 13 2 8 14 4 11 8 21 17 4 18 7 0 1 8 19 0 12 14 18 0 18 20 1 18 19 0 13 2 8 0 3 14 19 4 12 15 14 18

Escolhendo um número inteiro k, entre 0 e #E, neste caso pode ser k = 9 e utilizando a chave pública que Berta disponibilizou para o mundo, Duarte encripta o poema da seguinte forma: pela ordem que os números aparecem em cima, vai formando pares ordenados, começando pelo (4 , 18) e assim sucessivamente até ao último (14 , 18), como o número de letras do poema é ímpar, a segunda coordenada do último par ordenado é um S de Sophia.

Duarte define então a seguinte função $e_9 (x, 9) = (y_0, y_1, y_2)$, onde $x = (x_1 , x_2)$, $y_0 = 9(5, 22) = (8 , 2)$; $(c_1, c_2) = 9(22 , 2) = (3 , 6)$. Neste momento, Duarte cifra o primeiro par ordenado, (4 , 18), da seguinte forma:

$$y_1 = c_1 \times x_1 \pmod{29}$$

$$= 3 \times 4 \pmod{29}$$
$$= 12$$

$$y_2 = c_2 \times x_2 \pmod{29}$$
$$= 6 \times 18 \pmod{29}$$
$$= 21.$$

Duarte envia a Berta a seguinte cifra ((8,2), 12, 21) que corresponde às duas primeiras letras que foram cifradas: E e S. Em seguida, utilizando o mesmo (c_1 , c_2), envia o resto do poema encriptado que corresponde ao seguinte:

28 0 12 0 7 0 9 15 2 7 0 18 0 9 2 24 12 4 12 21 16 24 22 0 5 0 13 18 24 0 24 20 24 12 24 0 4 19 10 27 12 19 22 26 12 8 24 14 16 26 13 20 9 24 12 14 12 15 18 19 7 26 25 18 0 20 13 19 28 24 12 18 13 21 24 8 12 20 6 19 13 24 4 19 5 15 12 21 21 0 3 19 28 0 7 26 25 0 25 4 3 21 28 0 10 12 24 0 6 26 28 24 7 3 13 21.

Após receber este conjunto de números correspondentes à mensagem encriptada mais o par ordenado (8, 2) utiliza a função

$$d(y) = (y_1 c_1^{-1} \pmod{p}, y_2 c_2^{-1} \pmod{p}), \text{ onde } ay_0 = (c_1, c_2)$$

para desencriptar a mensagem. Para tal calcula, os inversos de c_1 e c_2 módulo 29, que neste caso são 10 e 5, respectivamente; e aplica os seguintes cálculos:

$$z_1 = y_1 \times c_1^{-1} \pmod{29}$$
$$= 12 \times 3^{-1} \pmod{29}$$
$$= 12 \times 10 \pmod{29}$$
$$= 4$$

$$z_2 = y_2 \times c_2^{-1} \pmod{29}$$
$$= 21 \times 6^{-1} \pmod{29}$$
$$= 21 \times 5 \pmod{29}$$
$$= 18$$

E aplicando, sucessivamente, os cálculos anteriores ao resto da mensagem ficaria a conhecer o poema 25 de Abril de Sophia de Mello Breyner Andresen.

É claro, que mais uma vez utilizamos um número primo pequeno, o que não torna o problema do logaritmo discreto intratável, como é feito habitualmente.

O modo como este criptosistema foi concebido, o facto de Berta determinar β, no subgrupo cíclico H, a partir de um a, que é secreto, e de um $\alpha \in H$, permite uma comunicação secreta e segura: Berta começa por calcular $\beta = a\alpha$, quando Duarte utiliza o seu k secreto e calcula y_0 e (c_1 , c_2), temos que:

$$\beta = a\alpha \Leftrightarrow k\beta = ka\alpha \Leftrightarrow (c_1 , c_2) = ak\alpha \Leftrightarrow (c_1 , c_2) = ay_0,$$

como o y_0 é enviado para Berta, esta sem conhecer o k utilizado pelo Duarte, com o seu a secreto determina (c_1 , c_2), o que lhe permite desencriptar a mensagem.

Ricardo, se quiser bisbilhotar a mensagem, terá que se esforçar bastante e pedir ajuda à tecnologia para obter algum êxito – é melhor ingressar nos serviços secretos de algum país!

Capítulo 5

Assinaturas digitais

Já lá vai o tempo, em que bastava a palavra de cavalheiros para se selarem acordos, fazerem-se negócios, etc. Hoje em dia, por falta de cavalheiros, devido às novas tecnologias, ou aos dois factores em conjunto: os acordos e os negócios podem ser feitos através de simples assinaturas digitais.

Neste momento o velhinho BI, que fisicamente também servia para reconhecer a assinatura, está a ser substituído pelo moderno cartão do cidadão, no qual a nossa assinatura digital já vem incorporada! Neste momento, duas pessoas podem fechar um negócio, estando a milhares de quilómetros de distância!

Não podemos dizer que este modernismo todo se deve só à tecnologia; pois muita matemática está por trás dessa tecnologia. Os esquemas que se utilizam neste tipo de assinaturas têm muita da matemática utilizada na criptografia da chave pública.

As assinaturas digitais garantem, principalmente, a autenticidade do emissor e a não repudiação do que é enviado.

5.1 Definição: Um esquema de assinatura digital é um 5 - uplo (P, A, K, S, V), onde se verificam as seguintes condições:

1. P é um conjunto finito de possíveis mensagens;
2. A é um conjunto finito de possíveis assinaturas;
3. K, o espaço das chaves, é um conjunto finito de chaves possíveis;
4. Para cada k ∈ K, existe um algoritmo para assinar $sig_k \in S$ e um correspondente algoritmo de verificação $ver_k \in V$. Cada $sig_k : P \rightarrow A$ e $ver_k : P \times A \rightarrow \{verdadeiro, falso\}$ são funções que satisfazem a equação $\text{ver}(x, y) = \begin{cases} \text{verdadeiro}, & \text{se } y = \text{sig}(x) \\ \text{falso}, & \text{se } y \neq \text{sig}(x) \end{cases}$, para toda mensagem x ∈ P e para toda a assinatura y ∈ A.

5.2 O esquema da assinatura RSA

Seja n = pq, onde p e q são números primos. Seja P = A = $\mathbb{Z}_n$, e defina-se $K = \{(n, p, q, a, b) : n = p \times q, \text{ p e q são números primos, } ab \equiv 1 \pmod{\varphi(n)}\}$.

Os valores n e b são públicos, e os valores p, q e a são secretos.

Para $K = (n, p, q, a, b)$, define-se $sig_k(x) = x^a \pmod n$ e

$ver_k(x, y) = \text{verdadeiro} \Leftrightarrow x \equiv y^b \pmod n$, com $(x, y) \in \mathbb{Z}_n$.

Consideremos agora p = 23 e q = 31, temos então n = 23 × 31 = 713. Calculemos $\varphi(713)$ = 22 × 30 = 660 e escolhemos a = 7; como m.d.c. (7 , 660) = 1, então existe um $b \in \mathbb{Z}_{660}$ tal que $ab \equiv 1 \pmod{660}$; neste caso b = 283.

Os valores 713 e 283 são públicos e os valores 23, 31 e 7 são secretos.

Berta escolhe x = 85 e aplica o algoritmo para assinar:

$$sig_k(85) = 85^7 \pmod{713} = 432.$$

A sua assinatura digital é (85 , 432). Pode enviá-la ao Duarte, assinando uma mensagem, de forma a confirmar a sua autenticidade.

Como é que Berta pode enviar a sua assinatura digital de forma segura?

Pode enviá-la utilizando o criptosistema RSA; para tal, suponhamos que Duarte tem uma chave pública, (893 , 527) e uma chave privada, (893, 11), logo Berta encripta, utilizando a exponenciação modular, a sua assinatura utilizando a chave pública de Duarte, desta forma o par ordenado (85, 432) dá lugar ao par ordenado (358 , 770). Duarte aplica a sua chave privada ao par ordenado recebido e obtém (85, 432). Neste momento, aplica o algoritmo de verificação para verificar a autenticidade da mensagem: $x \equiv y^b \pmod n$, onde x = 85, y = 432 e b = 283. Como $432^{283} \pmod{713} = 85 \Leftrightarrow$ verdadeiro = $ver_k(x, y)$. Pelo que, a mensagem pode ser atribuída à Berta.

5.3 O esquema da assinatura ElGamal

Sejam p um número primo tal que o problema do logaritmo discreto em $\mathbb{Z}_p$ é intratável, e $\alpha \in \mathbb{Z}_p^*$ uma raiz primitiva. Sejam $P = \mathbb{Z}_p^*$, $A = \mathbb{Z}_p^* \times \mathbb{Z}_{p-1}$, e defina-se $K = \{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod p\}$.

Os valores p, α e β são públicos, e a é secreto.

Para $K = (p, \alpha, a, \beta)$, e para um número $k \in \mathbb{Z}_{p-1}$, secreto, e escolhido de forma aleatória define-se a função sig_k (x, k) = (γ, δ), onde $\gamma = \alpha^k \pmod p$ e $\delta = (x - a\gamma)k^{-1} \pmod{p-1}$.

Para x, $\gamma \in \mathbb{Z}_p^*$ e $\delta \in \mathbb{Z}_{p-1}$, define-se

$$ver_k(x, \gamma, \delta) = \text{verdadeiro} \Leftrightarrow \beta^\gamma \gamma^\delta \equiv \alpha^x \pmod p.$$

Vamos ilustrar este esquema, com p = 479, cuja raiz primitiva é 13, P = $\mathbb{Z}_{479}^*$ e A = $\mathbb{Z}_{479}^* \times \mathbb{Z}_{478}$.

Consideremos o valor secreto a = 50 e calculemos $\beta = 13^{50} \pmod{479} = 163$. Temos então K = (479, 13, 50, 163). Os valores 479, 13 e 163 são públicos e 50 é o valor secreto.

Berta assina uma mensagem, utilizando este esquema de assinatura, do seguinte modo:

Escolhe x = 85 e k = 11, como m.d.c. (11 , 478) = 1, então existe o inverso de 11 módulo 478; tem que $11^{-1} \pmod{478} = 87$. Neste momento, calcula:

$$\gamma = 13^{11} \pmod{479} = 237$$

$$\delta = (85 - 50 \times 237) \times 87 \bmod (478) = 321.$$

A sua assinatura digital é (237, 321). Duarte, após receber este par ordenado para a mensagem 85, aplica o seguinte algoritmo de verificação:

$$ver_k(x, \gamma, \delta) = \text{verdadeiro} \Leftrightarrow \beta^\gamma \gamma^\delta \equiv \alpha^x \pmod p.$$

Logo, $(163^{237} \times 237^{321}) \pmod{479} = 259$ e $13^{85} \pmod{479} = 259$; Duarte conclui que $ver_k(x, \gamma, \delta) = \text{verdadeiro}$.

5.4 O esquema da assinatura Digital Standard

A Assinatura Digital Standard é uma modificação do Esquema da Assinatura de ElGamal. Foi publicada a 19 de Maio de 1994 e adoptada como standard em Dezembro do mesmo ano.

Seja p um número primo com 512-bit, ou seja números primos com cerca de 160 dígitos decimais, tal que o problema do logaritmo discreto em $\mathbb{Z}_p$ é intratável, e seja q um número primo com 160-bit que divide p – 1. Seja $\alpha \in \mathbb{Z}_p$ uma q-ésima raiz de 1 módulo p. Seja P = $\mathbb{Z}_p^*$, A = $\mathbb{Z}_q \times \mathbb{Z}_q$, e definimos

$$K = \{(p, q, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod p\}.$$

Os valores p, q, α e β são públicos, e a é secreto.

Para K = (p, q, α, a, β), e para um número (secreto) k, escolhido de forma aleatória entre todos os números inteiros positivos menores que q, definimos sig_k (x, k) = (γ, δ), onde $\gamma = \left(\alpha^k \pmod p\right) \pmod q$ e $\delta = (x + a\gamma)k^{-1} \pmod q$.

Para x ∈ $\mathbb{Z}_p^*$ e $\gamma, \delta \in \mathbb{Z}_q$, a verificação é feita pelos seguintes cálculos:

$e_1 = x\,\delta^{-1} \pmod q$

$e_2 = \gamma\delta^{-1} \pmod q$

ver_k (x, γ, δ) = verdadeiro ⇔ $(\alpha^{e_1}\beta^{e_2} \pmod p) \pmod q = \gamma$.

Desta vez, Berta usará o esquema da Assinatura Digital Standard para assinar a sua mensagem, para que Duarte não tenha dúvidas que a mensagem é autêntica. Para tal, consideremos q = 53, p = 2 × 53 + 1 = 107, 2 é a raiz primitiva de 107 e x = 30.

Berta calcula α = 2^2 (mod 107) = 4, escolhe a = 85 e k = 40, o que lhe permite calcular β = 4^{85} (mod 107) = 92. Como m.d.c. (40 , 53) = 1, Berta determina 40^{-1} (mod 53) = 4.

Neste momento, Berta faz os seguintes cálculos:

$\gamma = (4^{40} \pmod{107}) \pmod{53}$ = 76 (mod 53) = 23

$\delta = (30 + 85 \times 23) \times 4 \pmod{53} = 43.$

A sua assinatura é (23, 43) para x = 30.

Depois de receber, por um canal seguro, o par ordenado anterior e o valor 30; Antes de aplicar o algoritmo de verificação, Duarte faz os seguintes cálculos:

43^{-1} (mod 53) = 37;

e_1 = (30 × 37) (mod 53) = 50;

e_2 = (23 × 37) (mod 53) = 3.

Agora verifica a veracidade da assinatura.

$\left(4^{50}92^{3} \pmod{107}\right)$ (mod 53) = 23, pelo que ver_k (x, γ, δ) = verdadeiro.

Capítulo 6

Conclusão

Mas aqui tenho de lidar com um equívoco.
Diz-se com frequência que os matemáticos puros
se gabam da inutilidade do seu trabalho e do facto
de este não ter quaisquer aplicações práticas.
A imputação baseia-se geralmente numa frase
irreflectida atribuída a Gauss, no sentido que,
se a matemática é a rainha das ciências, então
a teoria dos números será, pela sua suprema
inutilidade, a rainha das matemáticas…
G. H. hardy, in Apologia de Um Matemático.

Se é verdade ou não que se gabavam da inutilidade do seu trabalho, não sabemos! O que o tempo demonstrou é que não se podem gabar, pelo menos da inutilidade! Pois, hoje, a Teoria dos Números é utilizada todos os dias por grande parte da humanidade e um enorme número de vezes.

Muitas vezes, o conhecimento está a frente da tecnologia; foi este o caso. A Teoria dos Números, durante séculos, esteve à espera de alguma aplicabilidade, até que num belo dia da segunda metade do século vinte, passou de rainha das matemáticas a criada, para todo o serviço, da criptologia. Tanto a criptografia como a criptanálise servem-se da Teoria dos Números para encontrar números primos com centenas de algarismos, factorizar produtos com centenas ou milhares de algarismos, métodos criptográficos cada vez mais seguros, métodos para quebrar a segurança dos mesmos; enfim, ajudou, e continua a ajudar, a revolucionar o nosso modo de vida nos últimos anos!

Sendo esta uma dissertação do mestrado de Matemática Para Professores, teceremos algumas considerações sobre o actual Ensino da Matemática, no nosso país.

Em primeiro lugar, contamos uma pequena história. Quando da parte escolar deste mestrado, na cadeira História e Teoria dos Números, o Professor Jorge Nuno ensinou-nos a calcular o dia da semana a partir de uma data qualquer. Nas aulas de Estudo Acompanhado e do PAM (aulas que são atribuídas à disciplina de Matemática devido ao Plano de Acção para a Matemática) resolvemos explicar aos alunos do 7º ano de escolaridade, com as devidas adaptações da linguagem matemática, esse método e, apenas, com a ajuda de uma máquina de calcular científica os alunos conseguiram calcular os dias da semana em que tinham nascido, os quais foram confirmados com ajuda dos calendários do telemóvel. E até a professora de Francês, que fazia par pedagógico na disciplina de Estudo Acompanhado e cujo casamento já deve ter passado as bodas de prata, se entusiasmou com o método e resolveu calcular o dia da semana em que se tinha casado – embora soubesse, queria ter a certeza que o método era infalível!

Este é um exemplo, em que os alunos de uma faixa etária baixa conseguem perceber e entusiasmarem-se com a Matemática!

Neste momento, em Portugal, o vector que representa o rumo do Ensino da Matemática tem a direcção certa, apenas tem que mudar o sentido! O que não é mau de todo, pois direcção já temos, só nos falta o sentido!

A massificação do Ensino está feita; agora temos que por os alunos a pensar! Não é esta tese que o vai fazer, nem é esse o seu principal objectivo. No entanto, a criptografia e criptanálise podem ajudar os alunos na sua concentração e persistência perante a resolução de problemas, e a combater a frustração de ao ler um problema não ter logo o método de o resolver na cabeça, acabando por desistir, porque simplesmente é Matemática!

Algumas das cifras que foram descritas nesta tese, podem ser explicadas aos alunos do Ensino Básico e Secundário, com as devidas adaptações de

linguagem e consoante as suas faixas etárias; e a pouco e pouco, podemos responder à célebre pergunta: Para que serve a Matemática?

Em relação ao tema da tese, a nível pessoal, proporcionou uma vasta aprendizagem, tanto ao nível da Matemática, como da História da Matemática e da Humanidade, às vezes, os pormenores modificam muito os acontecimentos – como a desencriptação do telegrama de Arthur Zimmermann, por parte dos britânicos, que obrigou os Estados Unidos a entrarem na Primeira Guerra Mundial e a ajudarem a derrotar a Alemanha. A nível profissional, permitiu relembrar matérias que já estavam na "gaveta" e aprender outras que certamente ajudarão na prática do ensino – por vezes uma boa história, ajuda a captar a atenção dos alunos!

A criptografia tem muitos caminhos que podem ser percorridos. Como é óbvio não se podia calcorrear todos; pois além de serem muitos, alguns são bastante longos e não fariam sentido neste trabalho. Muitos criptosistemas ficaram de fora, outras abordagens poderiam ter sido feitas, como por exemplo os problemas N e NP. Talvez, numa outra oportunidade, sigamos outros caminhos e aprofundemos outras matérias relacionadas com este tema.

Por fim, foi um prazer explorar este assunto. Abriram-se as portas de um mundo que nos era completamente desconhecido e no qual gostámos de estar estes dois anos!

Bibliografia

[1] Brison, J. Owen. (2003). *Teoria de Galois*. Departamento de Matemática. Faculdade de Ciências da Universidade de Lisboa.

[2] Buchmann, Johannes A. (2004). *Introduction to Cryptography*. Springer.

[3] Buescu, Jorge. (2005). *O Mistério do Bilhete de Identidade e Outras Histórias*. Gradiva.

[4] Burton, David M. (1980). *Elementary Number Theory*. Allyn and Bacon Inc.

[5] Caldeira, C. & Almeida, P. (2007) *Códigos e Criptografia*, consultado em Abril de 2008 em http://www.mat.uc.pt/~pedro/lectivos/CodigosCriptografia/

[6] Christensen, C. (2007). *Polish Mathematicians Finding Patterns in Enigma Messages*. *Mathematics Magazine*, 80, 4, pp. 247-273.

[7] Crandall, Richard & Pomerance, Carl. (2000). *Prime Numbers. A Computational Perspective*. Springer.

[8] Fine, Benjamin & Rosenberger, Gerhard. (2007). *Number Theory. An Introduction via the Distribution of Primes.* Birkäuser.

[9] Fernandes, Rui Loja & Ricou, Manuel. (2004). – *Introdução à Álgebra*. IST Press.

[10] Hardy, G. H. (1940). *Apologia de Um Matemático*. Traduzido por Daniela Kato. Revisão cientifica por Jorge Nuno Silva. Gradiva.

[11] Irving, S. Ronald. (2000). *Integers, polynomials and rings*. Springer.

[12] Jones, Gareth & Jones, J. Mary. *Elementary Number theory*. Springer.

[13] Kahn, David. (1973). *The Codebreakers*. The New American Library, Inc.

[14] Koblitz, Neal. (1994). *A Course in Number Theory and Cryptography*. Springer.

[15] Koblitz, Neal. (1998). *Algebraic Aspects of Cryptography.* Springer.

[16] Kumanduri, Ramanujachary & Romero, Cristina. (1998). *Number Theory with Computer applications*. Prentice Hall, Inc.

[17] Monteiro, J. António & Matos, Isabel (2001). *Álgebra, Um Primeiro Curso*. Escolar Editora.

[18] Quaresma, Pedro & Pinho, Augusto. (2009). *Criptoanálise.* Gazeta de Matemática nº 157.

[19] Queiró, João Filipe. (2002). *Teoria dos Números*. Departamento de Matemática – Universidade de Coimbra.

[20] Salomaa, Art. (1996). *Public-Key Cryptography*. Springer.

[21] Silveira, F. & Winterle, P. (s/d) *Matrizes e Criptografia*, consultado em Maio de 2008 em

http://www.pucrs.br/famat/demat/facin/algainf/criptografia.pdf

[22] Silverman, H.J. (2009). *The Arithmetic of Elliptic Curves*. Springer.

[23] Singh, S. (2001 [1999]). *O Livro dos Códigos*. Traduzido por A. F. Bastos. Lisboa: Temas & Debates.

[24] Singh, S. (1997). A Solução do Último Teorema de Fermat. Traduzido por A. M. Baptista. Relógio D'Água.