
Criptografia RSA

Daniele Helena Bonfim

SERVIÇO DE PÓS-GRADUAÇÃO DO ICMC-USP

Data de Depósito:

Assinatura: _____

Daniele Helena Bonfim

Criptografia RSA

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Ciências – Programa de Mestrado Profissional em Matemática. *VERSÃO REVISADA*

Área de Concentração: Matemática

Orientador: Prof. Dr. Marcelo Rempel Ebert

USP – São Carlos
Março de 2017

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados fornecidos pelo(a) autor(a)

B634c Bonfim, Daniele Helena
Criptografia RSA / Daniele Helena Bonfim; orientador
Marcelo Rempel Ebert. -- São Carlos -- SP, 2017.
91 p.

Dissertação (Mestrado - Programa de Pós-graduação em
Mestrado Profissional em Matemática em Rede Nacional)
-- Instituto de Ciências Matemáticas e de Computação,
Universidade de São Paulo, 2017.

1. Criptografia. 2. RSA. 3. Congruência modular.
4. Teoria dos Números. I. Ebert, Marcelo Rempel, orient.
II. Título.

Daniele Helena Bonfim

Cryptography RSA

Master dissertation submitted to the Instituto de Ciências Matemáticas e de Computação – ICMC-USP, in partial fulfillment of the requirements for the degree of Mathematics Professional Master's Program.
FINAL VERSION

Concentration Area: Mathematics

Advisor: Prof. Dr. Marcelo Rempel Ebert

USP – São Carlos
March 2017

Dedico este trabalho á minha mãe, Maria José; ao meu marido, Pedro; à minha irmãzinha Ana Luiza; à minha vó Maria da Penha; ao meu pai Lázaro; ao professor Luciano Pedroso que me apresentou ao PROFMAT, assim como aos meus professores da graduação Maria de Fátima Bernades, Wagner Bernardes, Waldemar Gianini e Fernando Oliveira; aos meu queridos alunos do PIC: Deivid Cezar da Silva, Gustavo Teixeira Simões, Jonas Cassiano Costa, André Rodrigues Gomes Silva, Leonardo Siqueira Aprile Pires, Cibele Louise de Almeida Cardoso, Rafael Vasconcelos Martins, Vanessa de Oliveira, Pedro Henrique Silva Alves, Jean Lima Alves, Layane Avila, Matheus de Oliveira Gonçalves, Hugo Rodrigues Salomão, Leticia Maria Costa, Merhy End Dias Faria; aos meu professores Marcelo Rempel Ebert, Kátia Andréia Gonçalves de Azevedo e Vanessa Rolnik Artioli do PROFMAT.

AGRADECIMENTOS

Agradeço primeiramente à Deus e à minha mãe, que me deu muito apoio em todos os momentos. Ao meu marido, Pedro, que teve extrema paciência e sempre me apoiou. Ao IMPA que teve a iniciativa de proporcionar o PROFMAT, à USP, ao meu orientador Marcelo Rempel Ebert e à CAPES que proporcionou a aplicação nas aulas do Programa de Iniciação Científica da Obmep, assim como a todos os professores que me ajudaram a aprofundar meus conhecimentos e a realizar este sonho.

*“Precisamos nos comunicar
Da rotina escapar
Ao amor nos entregar.
Algumas coisas gritamos ao mundo,
Outras guardadas estão bem lá no fundo
Da alma, ou do coração.
Mas pra sempre assim não ficarão.
Muitas vezes não queremos falar,
Porque nem todos precisam escutar,
Por isso minha mensagem vou criptografar
Para que só alguns possam receptor”
(Daniele Helena Bonfim)*

RESUMO

BORGES, DANIELE H. B.. **Criptografia RSA**. 2017. 91 f. Dissertação (Mestrado em Ciências – Programa de Mestrado Profissional em Matemática) – Instituto de Ciências Matemáticas e de Computação (ICMC/USP), São Carlos – SP.

Neste trabalho é apresentado um pouco da história da criptografia, assim como sua importância nos dias atuais, a base da teoria dos números e de congruência modular necessárias para compreender a criptografia RSA, que é o foco deste trabalho. A criptografia RSA é a mais usada atualmente por causa da dificuldade em ser decodificada. Foi elaborada e apresentada uma aula aos alunos do ensino fundamental e médio participantes do Programa de Iniciação Científica Júnior da OBMEP, sendo mostrado o porquê ela funciona, os métodos de codificação e decodificação.

Palavras-chave: Criptografia, RSA, Congruência modular, Teoria dos Números.

ABSTRACT

BORGES, DANIELE H. B.. **Criptografia RSA**. 2017. 91 f. Dissertação (Mestrado em Ciências – Programa de Mestrado Profissional em Matemática) – Instituto de Ciências Matemáticas e de Computação (ICMC/USP), São Carlos – SP.

In this work some of the history of cryptography is presented, as well as its nowadays applications. The RSA encryption is the most widely used because of the difficulty to being decoded. In order to understand the RSA encryption, which is the focus of this work, we recall some basis of number theory and modular congruence. Also, it was prepared and presented a lecture to the students of middle and high school participants in the Program of Junior Scientific Initiation of OBMEP, being shown why it works, methods of encoding and decoding.

Keywords: Cryptography, RSA, Modular congruence, Number Theory.

LISTA DE ILUSTRAÇÕES

Figura 1 – Crivo de Eratóstenes	44
Figura 2 – Criptografia em sites	49
Figura 3 – Criptografia em sites	50
Figura 4 – Como funciona a criptografia	52
Figura 5 – Citale Espartano	54
Figura 6 – Frequência das letras no alfabeto (Brasil)	54
Figura 7 – Cifra 1	57
Figura 8 – Cifra 2	57
Figura 9 – Cifra 3	58
Figura 10 – 3×2 - Três linhas por duas colunas	58
Figura 11 – Tabela de consulta para letras e números em Braille	59
Figura 12 – Programação dos Primeiros Encontros do G4	74
Figura 13 – Programação dos Primeiros Encontros do G3	74
Figura 14 – Encontrando N	76
Figura 15 – Encontrando φ_N	76
Figura 16 – Fatoração de φ_N	76
Figura 17 – Encontrando d	77
Figura 18 – Codificando a mensagem	77
Figura 19 – Codificando a mensagem	78
Figura 20 – Decodificando a mensagem	78
Figura 21 – Decodificando a mensagem	79

LISTA DE TABELAS

Tabela 1 – Diagrama - Algoritmo de Euclides	28
Tabela 2 – Maiores pares de primos gêmeos conhecidos	45
Tabela 3 – Tabela para Cifra de Blaise de Vigenère	56
Tabela 4 – Criptografando com a Cifra de Blaise	56
Tabela 5 – Código Morse	62
Tabela 6 – Criptografia convencional e de chave pública	63
Tabela 7 – Tabela Para Conversão	64

SUMÁRIO

1	INTRODUÇÃO	21
2	ARITMÉTICA BÁSICA	25
2.1	Divisão nos Inteiros	25
2.2	O algoritmo de Euclides	26
2.3	Equações diofantinas lineares	32
2.4	Os números primos	34
2.5	Congruência e Propriedades	37
2.6	Congruências Lineares	39
2.7	Teorema Chinês do Resto	41
2.8	Métodos Para Achar Números Primos	43
2.9	Como Encontrar Números Primos Grandes	43
2.10	Teste de Primalidade	46
3	CRIPTOGRAFIA	49
3.1	Tipos	52
3.1.1	<i>Heródoto</i>	53
3.1.2	<i>Bastão de Licurgo</i>	53
3.1.3	<i>Método de César</i>	53
3.1.4	<i>Anagrama</i>	55
3.1.5	<i>Blaise de Vigenère</i>	55
3.1.6	<i>A cifra de Beale</i>	55
3.1.7	<i>Braille</i>	56
3.1.8	<i>Disco de Alberti</i>	58
3.1.9	<i>Máquina Enigma</i>	60
3.1.10	<i>Máquina Colossus</i>	61
3.1.11	<i>Código Morse</i>	61
3.1.12	<i>Sistema Binário</i>	61
3.2	RSA	62
3.2.1	<i>Como Funciona?</i>	63
3.2.2	<i>Por que funciona?</i>	70
3.2.3	<i>Segurança</i>	71

4	APLICAÇÕES DA CRIPTOGRAFIA RSA NO PROGRAMA DE INICIAÇÃO CIENTÍFICA OBMEP	73
4.1	Planejamento	73
4.2	A aplicação	75
4.3	MAXIMA	75
4.4	Resultados	79
	REFERÊNCIAS	81
	APÊNDICE A PROPRIEDADE ARQUIMEDIANA	85
	APÊNDICE B OS PROBLEMAS DO PRÊMIO MILLENNIUM	87
B.1	A hipótese de Riemann	88
B.2	P versus NP	89
B.3	Curiosidades	90

INTRODUÇÃO

Neste trabalho será apresentado a Criptografia, que estuda o ato de cifrar mensagens, derivada do grego *cryptos* que significa “secreto, oculto”, usada para codificar mensagens de forma que somente o destinatário e o remetente compreendam. Segundo [Coutinho \(2008, p. 1\)](#) é o estudo dos: “métodos para codificar uma mensagem de modo que só seu destinatário consiga interpretá-la”.

Durante a história é possível perceber o quanto a Criptografia evoluiu para que as mensagens fossem mais seguras de serem transmitidas, já que, com seu surgimento também veio a Criptoanálise que estuda os métodos de quebrar ou decifrar mensagens cifradas.

Para compreender melhor o processo veja o exemplo: Ana quer enviar uma mensagem à Felipe, contudo ela quer que somente ele leia e compreenda a mensagem, para isso ela irá escrever a mensagem e cifrá-la ou codificá-la antes de enviar, de modo que, quando Felipe receber ele terá que decifrar a mesma. O ato de Ana é para que caso uma terceira pessoa intercepte a mensagem, esta não possa ler ou compreender.

Segundo [Diffie e Hellman \(2007, p. 30\)](#): “A criptografia é o estudo de sistemas “matemáticos” envolvendo dois tipos de problemas de segurança: privacidade e autenticação”.

Atualmente está presente na linguagem de computadores, quando é enviado um e-mail, nas senhas de bancos e redes sociais, dentre outros, mas ela não é um conteúdo presente no Ensino Médio atual. No Conteúdo Básico Comum (CBC) de Minas Gerais ([CARNEIRO; SPIRA; SABATUCCI, 2016](#)) ela não aparece, nem nos Parâmetros Curriculares Nacionais (PCNs) de Matemática ([BRASIL, 1997](#)).

Contudo, segundo os PCNs, é preciso que haja contextualização nos conteúdos ensinados, pois todo conhecimento envolve uma relação entre sujeito e objeto, ou seja,

entre o aluno e a matéria, assim se o conhecimento é trabalhado de modo contextualizado a escola irá retirar o aluno da sua condição de expectador passivo e fazer com que ele se interesse mais pelo conteúdo (BRASIL, 1997).

No CBC de Minas Gerais é possível observar a abertura para o estudo de situações problemas envolvendo conteúdos abordados em sala de aula, para que haja uma fixação maior e também, como método de conseguir um interesse maior por parte do aluno (CARNEIRO; SPIRA; SABATUCCI, 2016).

Muitos estudiosos defendem a contextualização do conteúdo como forma não só de reter a atenção do aluno por mais tempo, mas também fazer com que ele compreenda a utilização daquele conhecimento. De acordo com Fonseca (1995, p. 53):

As linhas de frente da Educação Matemática tem hoje um cuidado crescente com o aspecto sociocultural da abordagem Matemática. Defendem a necessidade de contextualizar o conhecimento matemático a ser transmitido, buscar suas origens, acompanhar sua evolução, explicitar sua finalidade ou seu papel na interpretação e na transformação da realidade do aluno. É claro que não se quer negar a importância da compreensão, nem tampouco desprezar a aquisição de técnicas, mas busca-se ampliar a repercussão que o aprendizado daquele conhecimento possa ter na vida social, nas opções, na produção e nos projetos de quem aprende. (FONSECA, 1995, p. 53)

D'Ambrosio (1997) também defende a contextualização, principalmente em matemática, para que o aluno possa levar os conteúdos para o cotidiano com o objetivo de fazer com que ele a entenda e compreenda, não somente decore conteúdos os quais não têm finalidade.

Segundo Tamarozzi (2004, p. 69): “a criptografia é tão antiga quanto a própria escrita; já estava presente no sistema de escrita hieroglífica dos egípcios”, por isso é uma importante ferramenta, seja no Ensino Fundamental ou Médio, para a construção de um material útil como atividades e jogos de codificação, de forma com que o aluno possa fixar conteúdos matemáticos, como, por exemplo, funções e matrizes.

De acordo com Cantoral (2003), o tema Criptografia é uma ferramenta atual, que permite contextualizar algumas matérias, fazendo com que o aluno se interesse mais e desperte a atenção pelos conteúdos desenvolvidos na sala de aula.

Trivinos (1987) defende o estudo da exploração por parte do aluno, de modo que ele possa aumentar a experiência em torno de um problema, aprofundando os estudos em sua realidade específica.

De acordo com BRASIL (1997, p. 19):

Recursos didáticos como jogos, livros, vídeos, calculadoras, computadores e outros materiais têm um papel importante no processo de ensino e aprendizagem. Contudo, eles precisam estar integrados a situações que levem ao exercício da análise e da reflexão, em última instância, a base da atividade matemática.

A criptografia pode ser então uma motivadora em algumas situações problemáticas para o processo de ensino-aprendizagem, podendo ser uma matéria auxiliar inclusive no ensino do uso da calculadora.

Neste trabalho será visto em específico a Criptografia RSA e a base aritmética necessária para sua compreensão, também sendo mostrado um pouco da história por trás da linguagem dos códigos.

Além disso será abordado um pouco sobre o programa MAXIMA, que foi usado como auxiliar já que, para exemplos mais complexos de criptografia RSA cálculos à mão tornam-se impossíveis, precisando assim de auxílio de programas.

O objetivo deste trabalho é abordar principalmente a criptografia RSA, de forma a introduzir ao aluno um pouco da história, alguns métodos mais simples, a Teoria dos Números e por fim o método RSA, abordando: sua importância, o porquê ele é seguro, como ele funciona e alguns exercícios e atividades para exploração do conteúdo.

Com este método de criptografia é possível aprofundar conteúdos com os alunos que são introduzidos desde os primeiros anos do Ensino Fundamental, levando-o a observar a importância desses, aumentando o interesse em matemática.

ARITMÉTICA BÁSICA

2.1 Divisão nos Inteiros

Dados dois números $d, m \in \mathbb{Z}$, dizemos que d divide m , ou que m é um múltiplo de d , ou ainda que d é um divisor de m se existir um número $q \in \mathbb{Z}$ tal que $m = qd$. Neste caso, usa-se a notação $d \mid m$.

Se isso não acontecer, ou seja, se d não dividir m escreve-se $d \nmid m$.

Lema 1. Sejam $a, b, c, d \in \mathbb{Z}$. Tem-se:

- (1) (“d divide”) Se $d \mid a$ e $d \mid b$ então $d \mid (ax + by)$ para qualquer combinação linear de a e b com coeficientes $x, y \in \mathbb{Z}$.
- (2) (Limitação) Se $d \mid a$ então $a = 0$ ou $|d| \leq |a|$.
- (3) (Transitividade) Se $a \mid b$ e $b \mid c$ então $a \mid c$.

Demonstração. Se $d \mid a$ e $d \mid b$, então pode-se escrever $a = dq_1$ e $b = dq_2$ com $q_1, q_2 \in \mathbb{Z}$, logo $ax + by = d(q_1x + q_2y)$. Como $q_1x + q_2y \in \mathbb{Z}$, tem-se $d \mid ax + by$, donde conclui-se (1).

Para mostrar (2), suponha que $d \mid a$ e $a \neq 0$. Neste caso, $a = dq$ com $q \neq 0$, assim $|q| \geq 1$ e $|a| = |d||q| \geq |d|$.

Finalmente provaremos (3). Se $a \mid b$ e $b \mid c$, então existem $q_1, q_2 \in \mathbb{Z}$ tais que $b = aq_1$ e $c = bq_2$, logo $c = aq_1q_2$ e portanto $a \mid c$. \square

Teorema 1. (Divisão Euclidiana) Dados $a, b \in \mathbb{Z}$ com $b \neq 0$, então existem únicos $q, r \in \mathbb{Z}$ tais que

$$a = bq + r \text{ e } 0 \leq r < |b|.$$

Neste caso q é chamado de quociente e r de resto.

Demonstração. Considere o conjunto:

$$S = \{x = a - by; y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\}).$$

Como o conjunto dos Naturais não permite cota superior (Propriedade Arquimediana), existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$, logo $a - nb > 0$, mostrando que S não é vazio.

O conjunto S é limitado inferiormente por 0 , logo, pelo princípio da Boa Ordenação, tem-se que S possui um menor elemento r .

Suponhamos então que $r = a - bq$. Sabendo que $r \geq 0$ é preciso mostrar que $r < |b|$.

Presuma por absurdo que $r \geq |b|$, isso implica que existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |b| + s$, com $0 \leq s < r$. Mas isso contradiz o fato de r ser um menor elemento de S , pois $s = a - (q \pm 1)b \in S$, com $s < r$.

Para provarmos a unicidade, suponha que $a = bq + r = bq' + r'$, onde $q, q', r, r' \in \mathbb{Z}$, $0 \leq r < |b|$ e $0 \leq r' < |b|$. Assim tem-se que $-|b| < -r \leq r' - r \leq r' < |b|$. Logo, $|r' - r| < |b|$. Por outro lado, $b(q - q') = r' - r$, o que implica que $|b||q - q'| = |r' - r| < |b|$, o que só é possível se $q = q'$ e conseqüentemente, $r = r'$. \square

2.2 O algoritmo de Euclides

Dados a e b ambos diferentes de zero e pertencentes ao conjunto dos números inteiros, cada um pode ser associado à um conjunto finito de divisores D_a e D_b de a e b , respectivamente. Temos que a intersecção destes conjuntos nunca é vazia, pois pelo menos o número 1 é comum aos dois conjuntos. Como a intersecção é não vazia e finita (já que os dois conjuntos o são) pode-se determinar um maior elemento nesta intersecção, chamado de Máximo Divisor Comum (mdc). Por razões técnicas, usaremos a seguinte definição equivalente:

Definição 1. Dado um número inteiro $d \geq 0$ e d é um máximo divisor comum de a e b , se possuir as seguintes propriedades:

1. d é um divisor comum de a e b , e
2. d é divisível por todo divisor comum de a e b .

A notação usada para Máximo Divisor Comum entre a e b é (a, b) .

Observação 1. Sejam a e b números inteiros não nulos, e suponha que exista $d = (a, b)$. Seja c um divisor comum de a e b , então $|c|$ divide d e, portanto $c \leq |c| \leq d$. Isso nos mostra que o máximo divisor comum de dois números, não ambos nulos, quando existe, é efetivamente o maior entre todos os divisores comuns desses números. Desta maneira, conclui-se a existência do mdc conforme definição acima.

Proposição 1. O máximo divisor comum de a e b é único.

Demonstração. A segunda condição implica que, se d e d' são dois mdc de um mesmo par de números, então, $d \mid d'$ e $d' \mid d$, o que juntamente com as condições $d \geq 0$ e $d' \geq 0$, implica que $d = d'$. Ou seja, o mdc de dois números, quando existe é único. \square

Exemplo 1. Temos que $(28, 36) = 4$, pois $D_{28} = \{\pm 1, \pm 2, \pm 4, \pm 7, \pm 14, \pm 28\}$ e $D_{36} = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 9, \pm 12, \pm 18, \pm 36\}$.

Como o mdc de a e b não depende da ordem em que a e b são tomados, temos que

$$(a, b) = (b, a).$$

Se a é um número inteiro, tem-se claramente que $(0, a) = |a|$, $(1, a) = 1$ e que $(a, a) = |a|$. Para todo $b \in \mathbb{Z}$, temos que

$$a \mid b \Leftrightarrow (a, b) = |a|.$$

De fato, se $a \mid b$, temos que $|a|$ é um divisor comum de a e b , e se c é um divisor de a e b , então c divide $|a|$, o que mostra que $|a| = (a, b)$. Reciprocamente, se $(a, b) = |a|$, segue-se que $|a|$ divide b , logo $a \mid b$.

Dados $a, b \in \mathbb{Z}$, se existir o mdc entre a e b , então

$$(a, b) = (-a, b) = (a, -b) = (-a, -b).$$

Assim para efeito do cálculo do mdc de dois números, podemos supô-los não negativos.

O *algoritmo de Euclides* ou *algoritmo das divisões sucessivas* é uma forma eficiente de encontrar o mdc entre dois números. Tal algoritmo se baseia na divisão euclidiana.

Lema 2. (Euclides) Se $a = bq + r$, então $(a, b) = (b, r)$.

Demonstração. Para provar este teorema é preciso verificar se $D_a \cap D_b = D_b \cap D_r$. Se $d \in D_a \cap D_b$ tem-se que $d \mid a$ e $d \mid b$, logo $d \mid (a - bq) \Leftrightarrow d \mid r$ e portanto $d \in D_b \cap D_r$.

Por outro lado, se $d \in D_b \cap D_r$ implica que $d \mid b$ e $d \mid r$, logo $d \mid (bq + r) \Leftrightarrow d \mid a$. Logo $d \in D_a \cap D_b$. Portanto $D_a \cap D_b = D_b \cap D_r$ e $(a, b) = (b, r)$. \square

No que segue, vamos aplicar o Lema 2 para calcular o (a, b) . Vamos supor que $1 < b < a$. Se $b \mid a$ então $(a, b) = b$. Se $b \nmid a$, pela divisão euclidiana, pode-se escrever: $a = bq_1 + r_1$ com $0 < r_1 < b$, e pelo Lema 2 tem-se duas possibilidades:

$$(1) \quad r_1 \mid b \Leftrightarrow (a, b) = (r_1, b) = r_1$$

- (2) $r_1 \nmid b$, então pode-se efetuar a divisão euclidiana de b por r_1 , obtendo $b = r_1q_2 + r_2$ com $0 < r_2 < r_1$. Novamente há duas possibilidades r_2 dividir ou não r_1 , podendo ser aplicado o algoritmo sucessivamente, gerando uma sequência decrescente finita de r_j , $j = 1, 2, \dots$. (o que sempre ocorre, pois o conjunto dos Naturais tem um menor elemento).

Este algoritmo pode ser escrito da seguinte forma de diagrama:

1. $a = bq_1 + r_1$, com $0 < r_1 < b$;
2. $b = r_1q_2 + r_2$, com $0 < r_2 < r_1$;
3. $r_1 = r_2q_3 + r_3$, com $0 < r_3 < r_2$;
- ⋮
4. $r_{n-2} = r_{n-1}q_n + r_n$, com $0 < r_n < r_{n-1}$;
5. $r_{n-1} = r_nq_{n+1}$.

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

Tabela 1 – Diagrama - Algoritmo de Euclides

Desta forma, conclui-se que $r_n = (a, b)$.

No que segue, apresentamos outra idéia relacionada ao cálculo do mdc. Sejam $a, b \in \mathbb{Z}$ define-se o conjunto:

$$I(a, b) = \{xa + yb; x, y \in \mathbb{Z}\}.$$

Observa-se que se a e b não são simultaneamente nulos, então $I(a, b) \cap \mathbb{N} \neq \emptyset$. De fato, tem-se que $a^2 + b^2 = a \times a + b \times b \in I(a, b) \cap \mathbb{N}$.

Teorema 2. Sejam $a, b \in \mathbb{Z}$, não ambos nulos. Se $d = \min I(a, b) \cap \mathbb{N}$, então:

- (1) d é o mdc de a e b ; e
- (2) $I(a, b) = d\mathbb{Z}$.

Para provar que $d = (a, b)$ basta verificar que:

- i) $d|a$ e $d|b$,

ii) Se $c|a$ e $c|b$, então $c|d$.

Demonstração. (Teorema 2)

(1) Suponha que c divida a e b , logo c divide todos os números naturais da forma $xa + yb$. Portanto, c divide todos os elementos de $I(a, b)$, e, conseqüentemente, $c|d$. Para mostrar que d divide todos os elementos de $I(a, b)$: seja $z \in I(a, b)$ e suponha, por absurdo, que $d \nmid z$. Logo pela divisão Euclidiana,

$$z = dq + r, \text{ com } 0 < r < d. \quad (2.1)$$

Como $z = xa + yb$ e $d = ma + nb$ para alguns $x, y, n, m \in \mathbb{Z}$, segue-se de (2.1) que

$$r = (x - qm)a + (y - qn)b \in I(a, b) \cap \mathbb{N},$$

o que é um absurdo, pois $d = \min I(a, b) \cap \mathbb{N}$ e $r < d$. Em particular, $d|a$ e $d|b$. Assim, fica provado que d é o mdc de a e b .

(2) Dado que todo elemento $I(a, b)$ é divisível por d , tem-se que $I(a, b) \subset d\mathbb{Z}$. Por outro lado, para todo $ld \in d\mathbb{Z}$, tem-se que:

$$ld = l(ma + nb) = (lm)a + (ln)b \in I(a, b)$$

e, portanto, $d\mathbb{Z} \subset I(a, b)$. Em conclusão, tem-se que $I(a, b) = d\mathbb{Z}$.

□

Corolário 1. Quaisquer que sejam $a, b \in \mathbb{Z}$, não ambos nulos, e $n \in \mathbb{N}$, tem-se que

$$(na, nb) = n(a, b).$$

Demonstração. Note inicialmente que

$$I(na, nb) = nI(a, b) (= \{nz, z \in I(a, b)\}).$$

Logo, segue do Teorema 2

$$(na, nb) = \min\{I(na, nb) \cap \mathbb{N}\} = \min\{nI(a, b) \cap \mathbb{N}\} = n \min\{I(a, b) \cap \mathbb{N}\} = n(a, b).$$

□

Definição 2. Dois números inteiros a e b são primos entre si se $(a, b) = 1$.

Proposição 2. Dois números inteiros a e b são primos entre si se, e somente se, existem números inteiros m e n tais que $ma + nb = 1$.

Demonstração. Suponha que a e b são primos entre si, i.e., $(a, b) = 1$. Logo, pelo Teorema 2, temos que existem números inteiros m e n tais que $ma + nb = 1$, donde segue a primeira parte da proposição.

Reciprocamente, suponha que existam números inteiros m e n tais que $ma + nb = 1$. Se $d = (a, b)$, temos que $d \mid ((ma + nb))$, o que mostra que $d \mid 1$, e, portanto, $d = 1$. \square

Teorema 3. (Lema de Gauss) Sejam a , b e c números inteiros. Se $a \mid bc$ e $(a, b) = 1$, então $a \mid c$.

Demonstração. Se $a \mid bc$, então existe $e \in \mathbb{Z}$ tal que $bc = ae$.

Se $(a, b) = 1$, então, pela Proposição 2, temos que existem $m, n \in \mathbb{Z}$ tais que

$$ma + nb = 1.$$

Multiplicando por c ambos os lados da igualdade acima, temos que

$$c = mac + nbc.$$

Substituindo bc por ae nesta última igualdade, temos que

$$c = mac + nae = a(mc + ne),$$

e portanto $a \mid c$. \square

Dados dois números inteiros a e b , dizemos que c é um *múltiplo comum* de a e b , se c é múltiplo simultaneamente de a e b . Defini-se o mínimo múltiplo comum (mmc) entre a e b como o menor múltiplo comum entre estes dois números. Por razões técnicas, usaremos a seguinte definição equivalente:

Definição 3. Um inteiro $m \geq 0$ é dito um mínimo múltiplo comum dos números inteiros a e b , se possuir as seguintes propriedades:

1. m é um múltiplo comum de a e b , e
2. se c é um múltiplo comum de a e b , então $m \mid c$.

A notação usada para Mínimo Múltiplo Comum entre a e b é $[a, b]$.

Observação 2. Se m é o mmc de a e b e c é um múltiplo comum de a e b , então $m \mid c$. Portanto se c é positivo, temos que $m \leq c$, mostrando-se que m é o menor dos múltiplos comuns positivos de a e b .

Exemplo 2. Temos que $[2, 5] = 10$, $[3, 5] = 15$ e $[6, 8] = 24$.

Proposição 3. O mínimo múltiplo comum dos números inteiros a e b é único.

Demonstração. Se m e m' são dois mínimos múltiplos comuns de a e b , então, do segundo item da definição acima, temos que $m \mid m'$ e $m' \mid m$. Como m e m' são números inteiros não negativos, temos que $m = m'$, o que mostra que o mínimo múltiplo comum é único. \square

É possível calcular o mmc entre dois números em termos do mdc pela proposição abaixo:

Proposição 4. Sejam a e b dois números naturais, então

$$(a, b) \times [a, b] = ab.$$

Para provar que $m = [a, b]$ basta verificar que:

- i) $a \mid m$ e $b \mid m$;
- ii) se $a \mid c$ e $b \mid c$, então $m \mid c$.

Demonstração. Se $a = 0$ ou $b = 0$, a igualdade é satisfeita. Sejam $a, b \in \mathbb{N}$ e $m = \frac{ab}{(a,b)}$. Como $m = a \frac{b}{(a,b)} = b \frac{a}{(a,b)}$.

Desta forma $a \mid m$ e $b \mid m$, portanto m é um múltiplo comum de a e b .

Seja c um múltiplo comum de a e b , logo $c = na = n'b$. Segue assim que: $n \frac{a}{(a,b)} = n' \frac{b}{(a,b)}$.

Como $\frac{a}{(a,b)}$ e $\frac{b}{(a,b)}$ são primos entre si (já que a e b são divididos pelo máximo divisor entre eles), $\frac{a}{(a,b)}$ divide n' , e, portanto, $m = \frac{a}{(a,b)}b$ divide $n'b$ que é igual a c . \square

As noções de mdc e mmc podem ser generalizadas.

Proposição 5. Dados números inteiros n_1, n_2, \dots, n_m todos não nulos, existe o seu mdc e

$$(n_1, n_2, \dots, n_m) = (n_1, \dots, n_{m-2}, (n_{m-1}, n_m)).$$

Demonstração. Provaremos por indução sobre $m \geq 2$. É fácil ver que para $m = 2$, o resultado é válido. Partiremos do princípio que o resultado vale para m .

Para provar que o resultado é válido para $m + 1$, basta mostrar que se d é o mdc de $n_1, \dots, (n_m, n_{m+1})$, então d é o mdc de n_1, \dots, n_m, n_{m+1} .

Seja d o mdc de $n_1, \dots, (n_m, n_{m+1})$. Logo $d \mid n_1, d \mid n_2, \dots, d \mid n_{m-1}$, e $d \mid (n_m, n_{m+1})$. Portanto, $d \mid n_1, d \mid n_2, \dots, d \mid n_{m-1}, d \mid n_m, d \mid n_{m+1}$.

Por outro lado, seja c divisor comum de $n_1, n_2, \dots, n_m, n_{m+1}$, logo c é um divisor comum de n_1, n_2, \dots, n_{m-1} e (n_m, n_{m+1}) , e, portanto, $c \mid d$. \square

Proposição 6. Sejam n_1, n_2, \dots, n_k números inteiros não nulos. Então existe o número $[n_1, n_2, \dots, n_k]$ e

$$[n_1, n_2, \dots, n_k] = [n_1, n_2, \dots, n_{k-2}, [n_{k-1}, n_k]].$$

Demonstração. Sejam $m = [n_1, n_2, \dots, n_{k-2}, [n_{k-1}, n_k]]$. Logo, n_1, n_2, \dots, n_{k-2} e $[n_{k-1}, n_k]$ dividem m . Como $n_{k-1} \mid [n_{k-1}, n_k]$ e $n_k \mid [n_{k-1}, n_k]$, segue que m é um múltiplo comum de n_1, n_2, \dots, n_k .

Por outro lado, suponha que c seja múltiplo comum de n_1, n_2, \dots, n_k . Logo, $n_1 \mid c$, $n_2 \mid c$, \dots , $n_{k-2} \mid c$ e $[n_{k-1}, n_k] \mid c$, daí segue que c é múltiplo de $m = [n_1, n_2, \dots, n_{k-2}, [n_{k-1}, n_k]]$. \square

Proposição 7. Sejam a_1, a_2, \dots, a_r números inteiros não nulos então vale:

$$(a_1, [a_2, a_3, \dots, a_r]) = [(a_1, a_2), (a_1, a_3), \dots, (a_1, a_r)].$$

Demonstração. Seja d o mdc entre a_1 e $[a_2, a_3, \dots, a_r]$ isso implica que $d \mid a_1$ e $d \mid [a_2, a_3, \dots, a_r]$. De acordo com o Lema 1: $d \leq a_1$ e $d \leq [a_2, a_3, \dots, a_r]$.

Seja $d' = [(a_1, a_2), (a_1, a_3), \dots, (a_1, a_r)]$ isso implica que $(a_1, a_2) \mid d'$, $(a_1, a_3) \mid d'$, \dots , $(a_1, a_r) \mid d'$, além disso $(a_1, a_2) \mid a_1$, $(a_1, a_3) \mid a_1$, \dots , $(a_1, a_r) \mid a_1$, como cada elemento a_2, a_3, \dots, a_r pode não ter divisor em comum com a_1 : $d' \leq a_1$ e $d' \mid a_1$ implicando que $d' = d$. \square

2.3 Equações diofantinas lineares

As equações diofantinas lineares em duas variáveis são equações na forma:

$$aX + bY = c, \tag{2.2}$$

em que $a, b, c \in \mathbb{Z}$, são dados, e busca-se por soluções inteiras X, Y .

Nem sempre este tipo de equação tem solução no conjunto dos inteiros, sendo que condições necessárias e suficientes dão dadas na seguinte proposição:

Proposição 8. Sejam $a, b, c \in \mathbb{Z}$ e $d = (a, b)$. A equação $aX + bY = c$ admite solução nos números inteiros se, e somente se, $d \mid c$.

Demonstração. Pelo Teorema 2, tem-se que:

$$I(a, b) = \{ma + nb; m, n \in \mathbb{Z}\} = d\mathbb{Z},$$

em que $d = (a, b)$. Assim é claro que a equação $aX + bY = c$ admite solução se, e somente se, $c \in I(a, b)$, o que é equivalente a $c \in d\mathbb{Z}$, que por sua vez, é equivalente a $d \mid c$. \square

Suponha que $(a, b) = 1$. Pelo resultado anterior, temos que (2.2) admite solução. No que segue, vamos caracterizar o conjunto de todas as soluções.

Proposição 9. Seja x_0, y_0 uma solução da equação $aX + bY = c$, onde $(a, b) = 1$. Então, as soluções x, y em \mathbb{Z} da equação são

$$x = x_0 + tb, \quad y = y_0 - ta; \quad t \in \mathbb{Z}.$$

Demonstração. Sejam x, y uma solução de $aX + bY = c$, logo,

$$ax_0 + by_0 = ax + by = c. \quad (2.3)$$

Consequentemente, $a(x - x_0) = b(y_0 - y)$. Como $(a, b) = 1$, segue-se que $b|(x - x_0)$. Logo, $x - x_0 = tb, t \in \mathbb{Z}$.

Substituindo a expressão de $x - x_0$ em (2.3), segue-se que

$$y_0 - y = ta,$$

o que prova que as soluções são do tipo exibido.

Por outro lado, x, y , como no enunciado, é solução, pois

$$ax + by = a(x_0 + tb) + b(y_0 - ta) = ax_0 + by_0 = c.$$

□

Desta proposição segue que a equação diofantina $aX + bY = c$, com $(a, b) = 1$, admite infinitas soluções em \mathbb{Z} .

Um método para encontrar uma solução particular de uma equação diofantina é obtido usando o algoritmo de euclidiano estendido, a saber, supondo que $(a, b) = 1$, pela Proposição 2 existem $m, n \in \mathbb{Z}$ tais que

$$ma + nb = 1.$$

Multiplicando ambos os membros da igualdade acima por c , obtêm-se

$$cma + cnb = c.$$

Logo, $x_0 = cm$ e $y_0 = cn$ é uma solução particular da equação e usando a Proposição 9 é possível encontrar as demais soluções.

2.4 Os números primos

Nesta seção apresentaremos alguns resultados sobre números primos, cujo conceito é fundamental para a aritmética e uma base para a teoria de criptografia.

Definição 4. Um número natural maior que 1 que só possui como divisores positivos 1 e ele próprio é chamado de número primo.

Proposição 10. Dados dois números primos p e q e um número inteiro a qualquer. Temos que:

I) Se $p \mid q$, então $p = q$.

II) Se $p \nmid a$, então $(p, a) = 1$.

Demonstração. (I) Como $p \mid q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Sendo p primo, tem-se que $p > 1$, o que acarreta $p = q$.

(II) Seja $(p, a) = d$, temos que $d \mid p$ e $d \mid a$. Portanto, $d = p$ ou $d = 1$. Mas $d \neq p$, pois $p \nmid a$ e, conseqüentemente, $d = 1$. \square

Se um número n não é primo diz-se que ele é composto. Portanto, se um número natural $n > 1$ é composto, existirá um divisor natural n_1 de n tal que $1 < n_1 < n$. Logo, existirá um número natural n_2 tal que:

$$n = n_1 n_2, \text{ com } 1 < n_1 < n \text{ e } 1 < n_2 < n$$

Por exemplo, 2, 3, 5, 7, 11 e 13 são números primos, enquanto que 4, 6, 8, 9, 10 e 12 são compostos.

Proposição 11. (Lema de Euclides) Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Demonstração. Basta provar que, se $p \mid ab$ e $p \nmid a$, então $p \mid b$. Mas, se $p \nmid a$, temos que $(p, a) = 1$, e o resultado segue-se do Lema de Gauss (Teorema 3). \square

Lembrando algumas propriedades da divisibilidade de acordo com o Lema 1.

Todo número natural pode ser escrito na forma fatorada por números primos:

Teorema 4. (Teorema Fundamental da Aritmética). Sejam $n \geq 2$ um número natural, pode-se escrever n de uma única forma como um produto

$$n = p_1 \cdots p_m$$

onde $m \geq 1$ é um natural e $p_1 \leq \cdots \leq p_m$ são primos.

Demonstração. Se n é um número primo não há o que demonstrar, pois basta que se faça $m = 1 \Rightarrow p_1 = n$. Se n é composto, seja $p_1 > 1$ o menor dos divisores positivos de n . Pode-se provar que p_1 é primo. De fato, caso contrário existiria um p , com $1 < p < p_1$ tal que $p \mid p_1$, donde $p \mid n$, o que iria contradizer a escolha de p_1 como menor divisor. Assim n pode ser escrito como $n = p_1 n_1$.

Se n_1 for primo a prova está finalizada, mas se n_1 for composto, seja $p_2 > 1$ o menor dos divisores positivos de n_1 . Pode-se provar que p_2 é primo, logo $n = p_1 p_2 n_2$. Repete-se o processo até que encontra-se um n_r primo.

Como $n_1, n_2, n_3, \dots, n_r$ é uma sequência decrescente, onde todos os termos pertencem aos naturais, será finita.

Os primos da sequência $p_1, p_2, p_3, p_4, \dots, p_m$ não são necessariamente distintos, assim a forma de n será:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} p_4^{\alpha_4} \cdots p_m^{\alpha_m}.$$

Precisa-se provar a unicidade da fatoração. Para $n = 2$ a afirmação é verdadeira. Se n for primo também não há nada o que provar. Para isso suponha que n seja composto e tenha duas fatorações:

$$n = p_1 p_2 p_3 p_4 \cdots p_m = q_1 q_2 q_3 q_4 \cdots q_n.$$

É preciso provar que $m = n$ e que cada p_i é igual a algum dos q_j . Como p_1 divide $q_1 q_2 q_3 q_4 \cdots q_n$, e como ambos são primos, logo p_1 divide um dos fatores q_j , donde a menos da ordem podemos supor $p_1 = q_1$. Da mesma forma p_2 divide um dos fatores q_j , como ambos são primos, implica que $p_2 = q_2$, repetindo o processo por indução tem-se que $m = n$, logo as fatorações $p_1 p_2 p_3 p_4 \cdots p_m$ e $q_1 q_2 q_3 q_4 \cdots q_n$ são idênticas. \square

Teorema 5. A sequência dos números primos é infinita.

Demonstração. Suponhamos que a sequência de números primos seja finita.

Deste modo temos que a listagem de todos os primos é $p_1, p_2, p_3, p_4, \dots, p_m$. Agora considere o número $K = p_1 p_2 p_3 p_4 \cdots p_m + 1$, ele não pode ser divisível por nenhum dos números primos listados, como K é maior que qualquer um dos primos listados e não é divisível por nenhum deles, pelo Teorema 4, K é um número primo ou é composto (escrito em fatores primos), desta forma há um primo que não pertence à nossa lista, implicando que a sequência de números primos não pode ser finita. \square

Além de Euclides, outros matemáticos provaram este teorema como, por exemplo, Kummer, Hermite, Goldbach, Euler, Thue, Perott, Auric, Métrod, dentre outros ([RIBENBOIM, 2012](#)).

Lema 3. Seja p um número primo. Os números $\binom{p}{i} = \frac{p!}{(p-i)!i!}$, onde $0 < i < p$, são todos divisíveis por p .

Demonstração. É trivial para $i = 1$. Para $1 < i < p$, como

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i!}$$

é um inteiro, segue que $i!|p(p-1)\cdots(p-i+1)$. Por outro lado, como $(i!, p) = 1$, então $i!|(p-1)\cdots(p-i+1)$, donde por definição $p | \binom{p}{i}$. \square

Teorema 6. (*Pequeno Teorema de Fermat*) Seja p um número primo, tem-se que p divide o número $a^p - a$, para todo número inteiro a .

Demonstração. Se $p = 2$ então $2|(a^2 - a)$ já que $a^2 - a = a(a-1)$ e a ou $a-1$ é par.

Para p ímpar provaremos o resultado por indução, assumindo que $a \geq 0$. O resultado é óbvio para $a = 0$, pois $p|0$. Suponha que seja válido para a , provaremos para $a+1$. Pela fórmula do Binômio de Newton:

$$(a+1)^p - (a+1) = a^p - a + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a.$$

Pelo Lema 3 e pela hipótese de indução, o segundo membro da equação é divisível por p .

Para concluir a prova no caso $a < 0$, basta observar que $(-a)^p - (-a) = -a^p + a = -[a^p - a]$. \square

Deste teorema é possível concluir o Corolário abaixo:

Corolário 2. Se p é um número primo e se a é um número inteiro não divisível por p , então p divide $a^{p-1} - 1$

Demonstração. De acordo com o Teorema 6, temos que $p|a^p - a \Leftrightarrow p|a(a^{p-1} - 1)$. Como $(a, p) = 1$ então p divide $a^{p-1} - 1$. \square

Pelo algoritmo da divisão quando divide-se um número por 6, os restos possíveis são 0, 1, 2, 3, 4 e 5, ou seja, qualquer número pode ser escrito em uma das formas $6k$, $6k+1$, $6k+2$, $6k+3$, $6k+4$ ou $6k+5$.

Se p é um número primo maior que 3 ele não pode ser par, logo ele é da forma $6k+1$, $6k+3$, ou $6k+5$, mas como todo número da forma $6k+3$ é divisível por 3, p só pode ser da forma $6k+1$ ou $6k+5$.

Proposição 12. Existem infinitos primos da forma $6k+5$.

Demonstração. Para provar que existem infinitos números primos da forma $6k + 5$ suponha, por absurdo, que existe um número finito de primos nesta forma.

Sejam estes números: $5, p_1, p_2, p_3, \dots, p_n$, todos distintos, e considere o número $P = 6p_1p_2p_3 \cdots p_n + 5$, P não é divisível por nenhum dos primos $5, p_1, p_2, p_3, \dots, p_n$.

Podemos afirmar que P possui um fator primo da forma $6k + 5$ distinto dos anteriores. De fato, caso contrário, se todos fossem da forma $6k + 1$, como o produto de dois números desta forma é sempre igual a outro da forma $6k' + 1$, donde uma contradição. \square

No que segue, enunciamos um resultado mais geral conhecido como Teorema de Dirichlet ou *Teorema dos Primos em Progressão Aritmética*:

Teorema 7. (Teorema dos Primos em Progressão Aritmética). Se a e b são inteiros relativamente primos entre si, então a progressão aritmética $an + b, n = 1, 2, 3, \dots$ contém um número infinito de primos.

A demonstração usual deste teorema usa variáveis complexas. Muitos casos particulares admitem demonstrações elementares mais ou menos simples. É possível encontrar a demonstração em <http://www.mat.puc-rio.br/nicolau/papers/mersenne/node10.html>.

2.5 Congruência e Propriedades

Seja m um número natural. Diremos que dois números inteiros a e b são *congruentes* módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m , escreve-se

$$a \equiv b \pmod{m}.$$

Por exemplo, $6 \equiv 11 \pmod{5}$, já que quando dividimos 6 por 5 o resto é 1 e quando dividimos 11 por 5 o resto também é 1. Outro exemplo é $241 \equiv 1 \pmod{2}$.

Observa-se que todo número inteiro é congruente módulo m ao seu resto $0 \leq r < m$ da divisão euclidiana por m , como no exemplo acima.

Quando a relação $a \equiv b \pmod{m}$ for falsa, diremos que a e b *não são congruentes*, ou que são *incongruentes*, módulo m . Escrevemos, nesse caso, $a \not\equiv b \pmod{m}$.

Como o resto da divisão de um número inteiro por 1 é sempre nulo, implica que $a \equiv b \pmod{1}$ para quaisquer a e $b \in \mathbb{Z}$. Portanto, consideraremos sempre $m > 1$.

Proposição 13. Suponha que $a, b, m \in \mathbb{Z}$, com $m > 1$. Tem-se que $a \equiv b \pmod{m}$ se, e somente se, $m \mid b - a$.

Demonstração. Sejam $a = mq + r$, com $0 \leq r < m$ e $b = mq' + r'$, com $0 \leq r' < m$, as divisões euclidianas de a e b por m , respectivamente. Logo,

$$b - a = m(q' - q) + (r' - r).$$

Portanto, $a \equiv b \pmod{m}$ se, e somente se, $r = r'$, o que, em vista da igualdade acima, é equivalente a dizer que $m \mid b - a$, já que $|r - r'| < m$. \square

Temos as propriedades de congruência:

Proposição 14. Seja $n \in \mathbb{N}$ e $n > 1$, Para todos $a, b, c \in \mathbb{Z}$, tem-se que:

- (1) (*Reflexividade*) $a \equiv a \pmod{n}$;
- (2) (*Simetria*) se $a \equiv b \pmod{n}$ então $b \equiv a \pmod{n}$;
- (3) (*Transitividade*) se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então $a \equiv c \pmod{n}$;
- (4) (*Compatibilidade com a soma e a diferença*) se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então $a + c \equiv b + d \pmod{n}$ e $a - c \equiv b - d \pmod{n}$,
Desta pode ser concluída uma propriedade em particular: se $a \equiv b \pmod{n}$, então $ka \equiv kb \pmod{n}$ para todo $k \in \mathbb{Z}$;
- (5) (*Compatibilidade com o produto*) se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então $ac \equiv bd \pmod{n}$.
Em particular, se $a \equiv b \pmod{n}$, então $a^m \equiv b^m \pmod{n}$ para todo $m \in \mathbb{N}$;
- (6) (*Cancelamento*) se $(c, n) = 1$, então $ac \equiv bc \pmod{n} \Leftrightarrow a \equiv b \pmod{n}$.
- (7) Se $c \neq 0$, então $ac \equiv bc \pmod{n} \Leftrightarrow a \equiv b \pmod{\frac{n}{(c, n)}}$.

Demonstração. (4): Suponha que $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$. Deste modo $n \mid (b - a)$ e $n \mid (d - c)$ isso implica que $n \mid (b - a) \pm (d - c)$ e $n \mid (b \pm d) - (a \pm c)$.

(5): como $n \mid (b - a)$ e $n \mid (d - c)$ segue que $n \mid d(b - a)$ e $n \mid a(d - c)$. Desta forma pode-se concluir que $n \mid d(b - a) + a(d - c)$, ou seja, $n \mid bd - ac$.

Deixamos os itens (1) – (3) e (6) – (7) como um exercício ao leitor. \square

Algumas propriedades adicionais que serão utilizadas:

Proposição 15. Sejam $a, b \in \mathbb{Z}$ e m, n, m_1, \dots, m_r inteiros maiores que 1. Tem-se que:

- (1) se $a \equiv b \pmod{m}$ e $n \mid m$ então $a \equiv b \pmod{n}$;
- (2) $a \equiv b \pmod{m_i}, \forall i = 1, \dots, r \Leftrightarrow a \equiv b \pmod{[m_1, \dots, m_r]}$;
- (3) se $a \equiv b \pmod{m}$, então $(a, m) = (b, m)$.

Demonstração. (1) Se $a \equiv b \pmod{m}$, então $m|b-a$. Como $n|m$, segue-se que $n|b-a$. Logo, $a \equiv b \pmod{n}$.

(2) Se $a \equiv b \pmod{m_i}$, $i = 1, \dots, r$, então $m_i|b-a$, para todo i . Sendo $b-a$ um múltiplo de cada m_i , segue-se que $[m_1, \dots, m_r]|b-a$, o que prova que $a \equiv b \pmod{[m_1, \dots, m_r]}$. A recíproca decorre do primeiro item.

(3) Se $a \equiv b \pmod{m}$, então $m|b-a$ e, portanto, $b = a + tm$ com $t \in \mathbb{Z}$. Logo, pelo Lema 2, tem-se que

$$(a, m) = (a + tm, m) = (b, m).$$

□

O Pequeno Teorema de Fermat pode ser escrito na seguinte forma:

Corolário 3. Se p é um número primo e $a \in \mathbb{Z}$, então

$$a^p \equiv a \pmod{p}.$$

Se $p \nmid a$, isso implica que

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

A prova segue do Teorema 6 e do Corolário 2.

2.6 Congruências Lineares

A resolução de problemas de congruências do tipo:

$$aX \equiv b \pmod{m}, \text{ onde } a, b, m \in \mathbb{Z}, m > 1,$$

é o problema de determinar se existem números $x \in \mathbb{Z}$ tais que $ax \equiv b \pmod{m}$.

É preciso inicialmente um critério para decidir se tais congruência admitem solução

Proposição 16. Dados $a, b, m \in \mathbb{Z}$, com $m > 1$, a congruência

$$aX \equiv b \pmod{m}$$

possui solução se, e somente se, $(a, m)|b$.

Demonstração. Suponha que a congruência $aX \equiv b \pmod{m}$ tenha uma solução x ; logo, temos que $m|(ax - b)$, o que equivale à existência de y pertencente aos inteiros tal que $ax - b = my$. Portanto, a equação $aX - mY = b$ admite solução. A Proposição 8 implica que $(a, m)|b$.

Reciprocamente, suponha que $(a, m)|b$. Logo, em virtude das Proposições 8 e 9 a equação $aX - mY = b$ admite uma solução x, y . Portanto, $ax = b + my$ e, conseqüentemente, x é solução da congruência pois, $ax \equiv b \pmod{m}$. □

Nota-se que se x_0 é solução da congruência $aX \equiv b \pmod{m}$, então todo x tal que $x \equiv x_0 \pmod{m}$ é também solução da congruência, pois

$$ax \equiv ax_0 \equiv b \pmod{m}.$$

Portanto, toda solução particular determina, automaticamente, uma infinidade de soluções da congruência. Essas soluções serão identificadas (módulo m), já que são congruentes entre si, e, conseqüentemente, se determinam mutuamente.

O seguinte resultado nos fornece uma coleção completa de soluções duas a duas incongruentes módulo m , as quais serão chamadas de *sistema completo de soluções incongruentes* da congruência.

Teorema 8. Sejam $a, b, m \in \mathbb{Z}$, com $m > 1$ e $(a, m) | b$. Se x_0 é uma solução da congruência $aX \equiv b \pmod{m}$, então

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \dots, x_0 + (d-1)\frac{m}{d},$$

onde $d = (a, m)$ formam um sistema completo de soluções incongruentes da congruência.

Demonstração. Pela Proposição 16, sabe-se que a congruência admite solução.

É preciso mostrar que os números $x_0 + i\frac{m}{d}$, com $i \in \mathbb{N}$, são soluções. De fato,

$$a(x_0 + i\frac{m}{d}) = ax_0 + i\frac{a}{d}m \equiv ax_0 \equiv b \pmod{m}.$$

Além disso, esses números são dois a dois incongruentes módulo m . De fato, se, para $i, j < d$,

$$x_0 + i\frac{m}{d} \equiv x_0 + j\frac{m}{d} \pmod{m},$$

então

$$i\frac{m}{d} \equiv j\frac{m}{d} \pmod{m}.$$

Pelo item 7 da Proposição 14 e como

$$\frac{m}{(a/d, m)} = d,$$

segue-se que $i \equiv j \pmod{d}$, implicando que $i = j$.

Finalmente, é preciso mostrar que toda solução x da congruência $aX \equiv b \pmod{m}$ é congruente, módulo m , a $x_0 + i\frac{m}{d}$ para algum $i < d$. De fato, seja x uma solução qualquer da congruência. Logo,

$$ax \equiv ax_0 \pmod{m},$$

e

$$\frac{a}{d}x \equiv \frac{a}{d}x_0 \pmod{\frac{m}{d}}.$$

Como $(\frac{a}{d}, \frac{m}{d}) = 1$, segue do item (6) da Propriedade 14 que

$$x \equiv x_0 \pmod{\frac{m}{d}}.$$

Logo, $x - x_0 = km/d$. Pela divisão euclidiana, existe $i < d$ tal que $k = qd + i$ e, portanto,

$$x = x_0 + qm + i \frac{m}{d} \equiv x_0 + i \frac{m}{d} \pmod{m}.$$

□

2.7 Teorema Chinês do Resto

Considere o sistema de congruências da forma:

$$X \equiv c_i \pmod{m_i}, i = 1, \dots, r. \quad (2.4)$$

O resultado seguinte nos fornece um método para resolvê-lo:

Teorema 9. Se $(m_i, m_j) = 1$, para todo par m_i, m_j com $i \neq j$, então o sistema (2.4) possui uma única solução módulo $M = m_1 m_2 \cdots m_r$. As soluções são

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

onde $t \in \mathbb{Z}$, $M_i = M/m_i$ e y_i é a solução de $M_i Y \equiv 1 \pmod{m_i}$, $i = 1, \dots, r$.

Demonstração. Primeiramente será provado que x é uma solução simultânea do sistema (2.4). De fato, como $m_i | M_j$, se $i \neq j$, e $M_i y_i \equiv 1 \pmod{m_i}$, segue-se que

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

Por outro lado, se x' é outra solução do sistema (2.4), então

$$x \equiv x' \pmod{m_i}, \forall i, i = 1, \dots, r.$$

Como $(m_i, m_j) = 1$, para $i \neq j$, segue-se que

$$[m_1, \dots, m_r] = m_1 \cdots m_r = M$$

e, conseqüentemente, pela Proposição 15 item (2), tem-se que $x \equiv x' \pmod{M}$. □

Proposição 17. O sistema de congruências

$$X \equiv c_1 \pmod{m_1}, X \equiv c_2 \pmod{m_2} \quad (2.5)$$

admite solução se, e somente se $c_2 \equiv c_1 \pmod{(m_1, m_2)}$. Além disso, dada uma solução a do sistema, um número a' é também uma solução se, e somente se, $a' \equiv a \pmod{[m_1, m_2]}$.

Demonstração. O sistema (2.5) admite uma solução se, e somente se, existem $a, y, z \in \mathbb{Z}$ tais que $a - c_1 = ym_1$ e $a - c_2 = zm_2$. Assim, a existência de soluções do sistema é equivalente à soluções da equação diofantina $ym_1 - zm_2 = c_2 - c_1$. Por sua vez, essa equação diofantina possui solução se, e somente se, (m_1, m_2) divide $c_2 - c_1$, o que equivale a $c_2 \equiv c_1 \pmod{(m_1, m_2)}$.

Suponhamos que a seja uma solução do sistema (2.5). Se a' é uma outra solução do sistema, então $a' \equiv c_1 \pmod{m_1}$ e $a' \equiv c_2 \pmod{m_2}$, o que, em vista da Proposição 15 ítem (2), implica que $a' \equiv a \pmod{[m_1, m_2]}$.

Por outro lado, se um número a' é tal que $a' \equiv a \pmod{[m_1, m_2]}$, então $a' \equiv a \pmod{c_1 \pmod{m_1}}$ e $a' \equiv a \pmod{c_2 \pmod{m_2}}$. Portanto, a' é solução do sistema (2.5). \square

Teorema 10. (Teorema Chinês dos Restos Generalizado) O sistema de congruências

$$X \equiv c_i \pmod{m_i}, i = 1, \dots, r$$

admite solução se, e somente se,

$$c_i \equiv c_j \pmod{(m_i, m_j)}, \forall i, j = 1, \dots, r.$$

Nesse caso, a solução é única módulo $[m_1, \dots, m_r]$.

Demonstração. Esta prova será feita por indução sobre r . O caso $r = 2$ é dado pela Proposição 17.

Suponhamos que a propriedade seja válida para $r - 1$. Pela hipótese de indução, temos que o sistema $X \equiv c_i \pmod{m_i}, i = 1, \dots, r - 1$, admite uma única solução c módulo $[m_1, \dots, m_{r-1}]$. Temos que mostrar agora que o sistema

$$X \equiv c \pmod{[m_1, \dots, m_{r-1}]}$$

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

possui uma solução única módulo $[m_1, \dots, m_r]$. Para estabelecer isso, em vista do caso $r = 2$, só falta mostrar que

$$c_r \equiv c \pmod{(m_r, [m_1, \dots, m_{r-1}])}.$$

Como temos que $c \equiv c_i \pmod{m_i}$ para $i = 1, \dots, r - 1$, segue-se, por mais forte razão, que $c \equiv c_i \pmod{(m_r, m_i)}$. Por outro lado, por hipótese, sabemos que $c_r \equiv c_i \pmod{(m_r, m_i)}$, para todo i , logo $c_r \equiv c \pmod{(m_r, m_i)}$, para todo $i = 1, \dots, r - 1$, e pelo item 2 da Proposição 15 segue que

$$c_r \equiv c \pmod{[(m_r, m_1), (m_r, m_2), \dots, (m_r, m_{r-1})]}.$$

O resultado agora segue da Proposição 7, que garante que

$$(m_r, [m_1, \dots, m_{r-1}]) = [(m_r, m_1), (m_r, m_2), \dots, (m_r, m_{r-1})].$$

Temos também que a solução do sistema é única módulo

$$[m_r, [m_1, \dots, m_{r-1}]] = [m_1, \dots, m_{r-1}, m_r].$$

□

2.8 Métodos Para Achar Números Primos

Um método conhecido na escola, no final do Ensino Fundamental I e início do Ensino Fundamental II é o Crivo de Eratóstenes, criado por Eratóstenes no século II A.C., deve ser composto por todos os números menores que n (dado de maneira arbitrária) (CARNEIRO; SPIRA; SABATUCCI, 2016). Ele foi o primeiro matemático que tentou sistematizar o conjunto dos números primos (COUTINHO, 2008). Este método consiste no seguinte: escreve-se todos os números, por exemplo, para $n = 250$, deve ser escrito os números de 2 à 250, risca-se primeiro os múltiplos de 2 superiores à ele, depois todos os múltiplos de 3 superiores à ele, e assim por diante: cortando todos os múltiplos do próximo primo, menos ele mesmo até o primo p tal que p^2 não ultrapasse n , neste caso em particular: $p^2 < 250$, ou seja, até o número 15. Observe a figura 1, de acordo com (HEFEZ, 2005, p. 35).

Desta forma, foi retirado todos os múltiplos dos primos 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241.

Este critério é baseado no seguinte teorema:

Teorema 11. Se n não é primo, então n possui, necessariamente, um fator primo menor do que ou igual a \sqrt{n} .

Demonstração. Sendo n composto então $n = n_1 \times n_2$ onde $1 < n_1 < n$, $1 < n_2 < n$. Sem perda de generalidade suponha $n_1 \leq n_2$. Logo n_1 tem que ser $\leq \sqrt{n}$ pois, caso contrário, teríamos $n = n_1 \times n_2 > \sqrt{n} \times \sqrt{n} = n$ o que é absurdo. Logo, como pelo Teorema 4, n_1 possui algum fator primo p , este deve ser $\leq \sqrt{n}$. Como p , sendo um fator primo de n_1 é também um fator de n , logo a demonstração está completa. □

Como consequência, se n não possui um fator primo $\leq \sqrt{n}$, então n é primo.

2.9 Como Encontrar Números Primos Grandes

Os números primos são procurados até hoje, quanto maior o número achado mais difícil de quebrar o código na criptografia RSA, assim tem-se alguns recordes de primos,

	②	③	4	⑤	6	⑦	8	9	10	⑪	12
⑬	14	15	16	⑰	18	⑱	20	21	22	⑳	24
25	26	27	28	⑳	30	㉑	32	33	34	35	36
⑳	38	39	40	㉒	42	㉓	44	45	46	㉔	48
49	50	51	52	㉕	54	55	56	57	58	㉖	60
⑥①	62	63	64	65	66	⑥⑦	68	69	70	⑦①	72
⑦③	74	75	76	77	78	⑦⑨	80	81	82	⑧③	84
85	86	87	88	⑧⑨	90	91	92	93	94	95	96
⑨⑦	98	99	100	⑩①	102	⑩③	104	105	106	⑩⑦	108
⑩⑨	110	111	112	⑪③	114	115	116	117	118	119	120
121	122	123	124	125	126	⑫⑦	128	129	130	⑬①	132
133	134	135	136	⑬⑦	138	⑬⑨	140	141	142	143	144
145	146	147	148	⑭⑨	150	⑮①	152	153	154	155	156
⑮⑦	158	159	160	161	162	⑯③	164	165	166	⑰⑦	168
169	170	171	172	⑰③	174	175	176	177	178	⑰⑨	180
⑱①	182	183	184	185	186	187	188	189	190	⑲①	192
⑲③	194	195	196	⑲⑦	198	⑲⑨	200	201	202	203	204
205	206	207	208	209	210	⑳①	212	213	214	215	216
217	218	219	220	221	222	㉑③	224	225	226	㉒⑦	228
㉓⑨	230	231	232	㉔③	234	235	236	237	238	㉕⑨	240
㉖①	242	243	244	245	246	247	248	249	250		

Figura 1 – Crivo de Eratóstenes

observe a tabela 2, que contém récords de primos gêmeos (p e q são primos e $|p - q| = 2$) (MARTINEZ *et al.*, 2013, p. 367).

Contudo estas tabelas podem se tornar obsoletas em um curto período de tempo, por isso o site <https://primes.utm.edu/largest.html> mantêm uma tabela atualizada dos dez maiores primos, consultada no dia 15 de outubro de 2015 o maior número primo era $2^{57885161} - 1$, com 17.425.170 dígitos, descoberto no ano de 2013. Mas em 19 de janeiro de 2016 foi publicado um novo recorde: $2^{74207281} - 1$ com 22.338.618 dígitos ambos descobertos por *GIMPS* (Great Internet Mersenne Prime Search by Woltman e Kurowski) (CALDWELL, 2016).

Estes primos foram descobertos em um projeto para encontrar primos de Mersenne, que são da forma: $2^n - 1$ (WOLTMAN; KUROWSKI, 2016).

Em criptografia RSA, é fundamental, para a criação da chave pública, que saiba-se encontrar números primos grandes. Para garantir a segurança da codificação, o ideal é

Primo	Número de dígitos	Data
$3756801695685 \times 2^{666669} \pm 1$	200700	2011
$65516468355 \times 2^{333333} \pm 1$	100355	2009
$2003663613 \times 2^{195000} \pm 1$	58711	2007
$194772106074315 \times 2^{171960} \pm 1$	51780	2007
$100314512544015 \times 2^{171960} \pm 1$	51780	2006
$16869987339975 \times 2^{171960} \pm 1$	51779	2005
$33218920 \times 2^{169690} \pm 1$	51090	2002
$22835841624 \times 7^{54321} \pm 1$	45917	2010
$1679081223 \times 2^{151618} \pm 1$	45651	2012
$84966861 \times 2^{140219} \pm 1$	42219	2012
$12378188145 \times 2^{140002} \pm 1$	42155	2010
$23272426305 \times 2^{140001} \pm 1$	42155	2010
$8151728061 \times 2^{125987} \pm 1$	37936	2010

Tabela 2 – Maiores pares de primos gêmeos conhecidos

que cada número primo possua mais de cem algarismos.

De acordo com [Martinez *et al.* \(2013\)](#) existem progressões aritméticas arbitrariamente grandes formadas exclusivamente por números primos, isso foi provado por Ben Green e Terence Tao, onde a maior conhecida é:

$$43142746595714191 + 5283234035979900 \times n$$

para todo $n = 0, 1, \dots, 25$, que foi descoberta em 12 de abril de 2010 por Benoît Perichon em um projeto do *PrimeGrid* disponível no site <http://www.primegrid.com/> ([RACKSPACE, 2016](#)).

De acordo com [OEIS \(2016\)](#) e [Ballinger e Rodenkirch \(2016\)](#) existem outros projetos para procurar primos grandes, provando algumas conjecturas, como a de Sierpinski, a de Riesel, ou os números de Brier (que são simultaneamente de Sierpinski e de Riesel).

Dada esta necessidade de encontrar primos grandes, de acordo com [Martinez *et al.* \(2013, p. 332\)](#):

A relevância desse problema tem crescido imensamente em anos recentes devido à utilização intensa de números primos em algoritmos de criptografia, como os algoritmos RSA e El Gamal para criptografia pública. Dessa forma o problema do teste de primalidade se tornou um importante problema para a ciência da computação teórica. Sobre esse ponto de vista duas coisas são requeridas: um certificado de prova que o algoritmo realmente produz a resposta correta; e uma medida da eficiência do algoritmo, isto é, quão bem o algoritmo faz uso dos recursos computacionais (como o tempo ou número de passos executados, espaço ou memória utilizada) em função do tamanho da entrada do problema para a obtenção da solução.

Para encontrar primos que possuam esse tamanho, a aplicação de algoritmos de-

terminísticos¹ como o Crivo de Eratóstenes é inviável, pois o tempo gasto é muito grande. A solução para esse problema é utilizar algoritmos randomizados² que forneçam números primos grandes.

A base desses algoritmos randomizados são testes de primalidade fundamentados no Pequeno Teorema de Fermat/Euler: Teorema 6 e Corolário 2.

2.10 Teste de Primalidade

Para os testes de primalidade, será utilizado o Pequeno Teorema de Fermat:

“Sejam a e n números inteiros tais que $n \nmid a$, se $a^{n-1} \not\equiv 1 \pmod{n}$, então n é composto.”

Na prática, o algoritmo escolhe um número natural n (tão grande quanto for necessário) e um inteiro a , tal que $n \nmid a$, em seguida, analisa-se a congruência $a^{n-1} \pmod{n}$.

Se $a^{n-1} \not\equiv 1 \pmod{n}$, conclui-se que n é composto e passa-se para o próximo número a ser testado. Entretanto, se $a^{n-1} \equiv 1 \pmod{n}$, não pode-se afirmar que n é primo, isso ocorre porque a recíproca do Pequeno Teorema de Fermat não é verdadeira. Um contra exemplo:

$7^{24} \equiv 1 \pmod{25}$, porém 25 é um número composto.

Sempre que um número n não é primo e satisfaz o Pequeno Teorema de Fermat para uma base a , n é chamado de pseudoprimo na base a .

Sempre que $a^{n-1} \equiv 1 \pmod{n}$, é preciso decidir se n é primo ou se é um pseudoprimo na base a , para isso, escolhe-se outra base b e testa-se se $b^{n-1} \equiv 1 \pmod{n}$, caso $b^{n-1} \not\equiv 1 \pmod{n}$, pode-se concluir que n é composto e pseudoprimo na base a , entretanto se $b^{n-1} \equiv 1 \pmod{n}$, repete-se o processo para outra base c .

O problema é que existem números que são pseudoprimos para todas as bases menores que n que são relativamente primas com n , esses números são chamados de números de Carmichael, cujo menor exemplo conhecido é $561 = 3 \cdot 11 \cdot 17$, ou seja, $a^{560} \equiv 1 \pmod{561}$ para todo a relativamente primo com 561. Sendo demonstrado recentemente por Alford, Granville e Pomerance que se $CN(x)$ é considerado a quantidade de números de Carmichael menores que x , então $CN(x) \geq x^{2/7}$, onde x é suficientemente grande, ou seja, existem infinitos números de Carmichael, para a lista destes números de Carmichael menores que 10^6 consulte <ftp://ftp.dpmms.cam.ac.uk/pub/Carmichael>.

Entretanto, pseudoprimos e números de Carmichael são bem raros quando testa-se

¹ Usado em Ciência da Computação, é o nome do algoritmo que sempre produz o mesmo resultado dado determinadas entradas de dados.

² são aqueles que utilizam experimentos randômicos para decidir, em um ou mais momentos durante sua execução, o que fazer ou para onde ir. Por motivo de clareza, algoritmos clássicos (não-randomizados) são também ditos determinísticos. É possível compreender melhor sobre o assunto em http://www.impa.br/opencms/pt/biblioteca/cbm/26_CBM/26CBM07.pdf

números da ordem 10^9 , por exemplo, existem 50.847.534 primos de 1 até 1.000.000.000, mas apenas 5587 pseudoprimos para a base 2 (0,01%), caso sejam utilizadas as bases 2 e 3, esse número cai para 1271 (0,0025%), se houver o teste de outras bases, essa porcentagem cai ainda mais.

A pequena probabilidade de um número ser pseudoprimo, quando testa-se várias bases, é o que fundamenta o teste de primalidade mais utilizado por programas de computação algébrica, o Teste de Miller-Rabin. Rabin provou que quando se testa uma base aleatória a , a probabilidade de que o teste acuse um pseudoprimo é menor que $\frac{1}{4}$, ou seja, se aplica o teste para k bases distintas, a probabilidade de que o teste acuse um pseudoprimo é menor do que $\left(\frac{1}{4}\right)^k$, por exemplo, se o teste for aplicado para 10 bases distintas, a probabilidade de encontrar um pseudoprimo é igual a $\left(\frac{1}{4}\right)^{10} \simeq 0,0000954\%$.

Esse teste está fundamentado na Hipótese de Riemman Generalizada, que afirma ser suficiente testar um número *pequeno* de bases para se garantir a primalidade de um número.

CRIPTOGRAFIA

A criptografia está no cotidiano de cada pessoa. A linguagem de escrever em códigos é usada atualmente em celulares, bancos, computadores, carros, alarmes, na internet para proteger compras on line ou seus dados bancários, dentre outros.

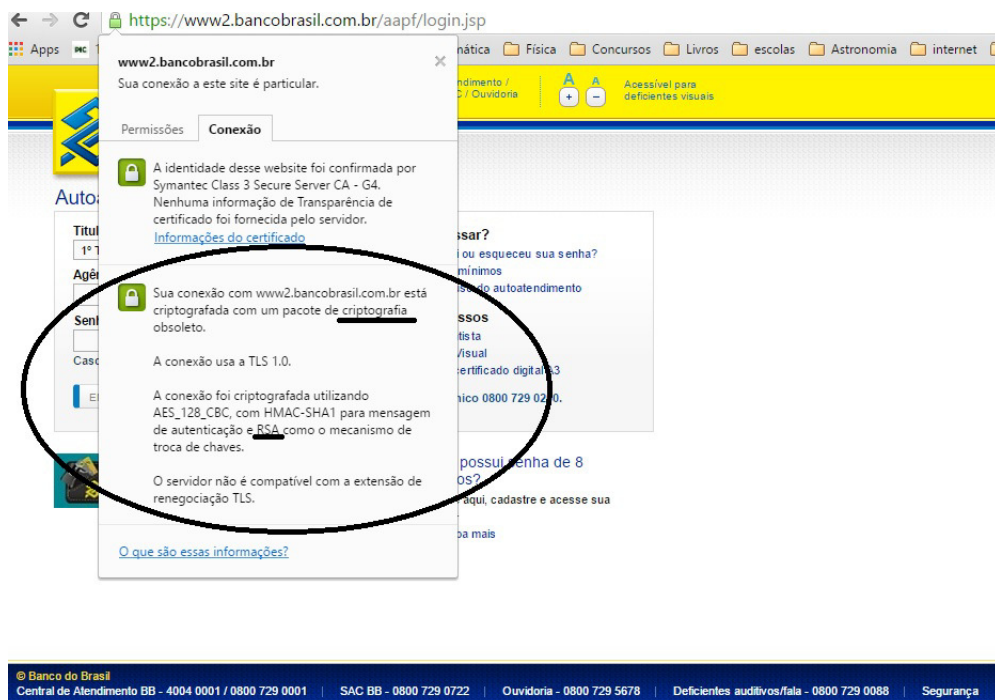


Figura 2 – Criptografia em sites

Nas figuras 2 e 3 é possível observar a criptografia em um site bancário para a proteção dos dados da conta do usuário, bem como a proteção de sua conta e seu dinheiro.

Nos carros também é encontrada a linguagem dos códigos, que pode ser usada no alarme, como na nova chave *keyless* que permitem a partida apenas com o acionamento de um botão (ATMEL, 2016).¹

¹ Fonte disponível em: <http://www.atmel.com>

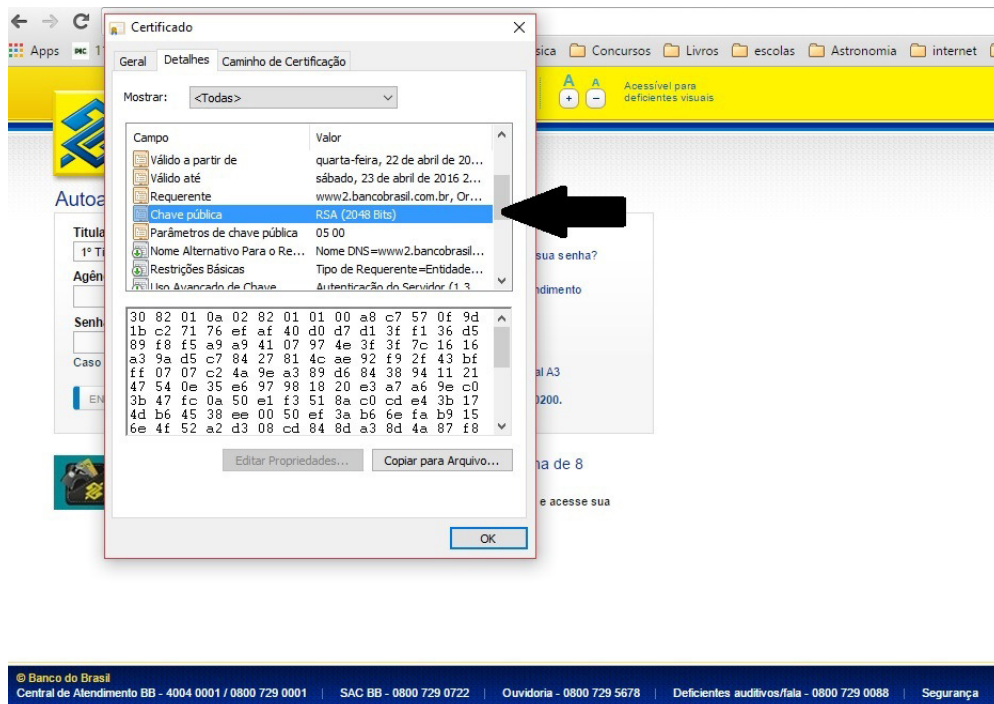


Figura 3 – Criptografia em sites

A natureza humana tem uma necessidade à privacidade, mesmo que seja para guardar simples segredos. É possível observar na história que a linguagem de códigos sempre foi muito usada como recurso militar, político, em questões comerciais, em guerras e até mesmo motivos sentimentais (SINGH, 2005).

Os indícios são que a criptografia começou a ser usada no antigo Egito quando o faraó Amenemhet II governava, por volta de 1900 a.C. pelo arquiteto Khnumhotep II. Em documentos que indicavam a localização de tesouros, o escriba de Khnumhotep II, para dificultar que ladrões os encontrassem, substituiu alguns trechos e palavras de documentos importantes por símbolos estranhos.

O filósofo Heródoto demonstrou que a criptografia já era usada há muito tempo nas guerras, um dos métodos era raspar a cabeça do mensageiro, escrever a mensagem e esperar que o cabelo crescesse novamente, mas dada a facilidade de ser descoberta houve a necessidade de ferramentas que guardassem melhor a mensagem ou de métodos mais difíceis de serem descobertos (LARCHER, 1950).

Nos séculos XVIII e XIX surgiram as *Câmeras Escuras*, onde a arte de quebrar códigos era usada para decifrar mensagens diplomáticas, empregando muitos matemáticos famosos, a de Viena era conhecida como a mais eficiente, quebrando cerca de 100 mensagens internacionais por dia.

Com isso os métodos foram aprimorando: escrita na madeira com cera por cima, embaralhamento das letras, Bastão de Licurgo, método de substituição (como o usado por Júlio César, imperador de Roma), disco de Alberti, máquina Enigma (Segunda Guerra

Mundial), máquina Colossos, criptografia RSA e criptografia quântica.

A criptografia tem sido aprimorada e estado presente desde antes de Cristo, seu desenvolvimento é marcado por três grandes fases: artesanal, mecânica e digital (SINGH, 2005).

A Criptografia artesanal surge paralelamente com o surgimento da escrita, durante as idades antiga e média, onde a utilização das técnicas é fácil com lápis e papel, sendo fáceis de serem quebradas como: a de Heródoto, Bastão de Licurgo, O código de César, Cifrário de Francis Bacon, Criptoanalistas Árabes, A Cifra de Vigenère, Braille, microponto são alguns exemplos.

Inclusive Thomas Jefferson (1743-1826), que foi presidente dos Estados Unidos da América de 1801 a 1809 desenvolveu seu próprio sistema de criptografia chamado de Cilindro de Jefferson, que ele usou durante a revolução americana, onde ele precisava enviar cartas importantes por mensageiros (KAHN, 1996).

A mecânica começa no início da Idade Moderna, a partir da Revolução Industrial as máquinas tomaram conta do mundo e da criptografia, tendo seu apogeu na Segunda guerra Mundial, como o Disco de cifras, o código morse, a máquina Enigma, Colossus, etc.

Segundo Diffie e Hellman (2007, p. 39): “Antes deste século, sistemas de criptografia foram limitados a cálculos que poderiam ser realizadas à mão ou com dispositivos simples”.

Depois da Primeira Guerra Mundial já era possível ver o avanço das máquinas para criptografar mensagens, inclusive como sistemas eletromecânicos, mas foi o desenvolvimento dos computadores digitais que permitiu que métodos mais seguros fossem desenvolvidos (DIFFIE; HELLMAN, 2007).

A criptografia Digital veio com o aperfeiçoamento dos computadores, fazendo cálculos extremamente grandes em pouco tempo, se tornaram uma ferramenta valiosa na criptografia, com códigos mais complicados de serem quebrados, pode-se observar a criptografia simétrica, DES, AES, IDEA, Assimétrica, RSA, ElGamal, Curvas Elípticas, dentre outras (SINGH, 2005).

Do mesmo modo que a arte de criptografar mensagens envolveu a arte de tentar desvendá-las também, um exemplo famoso de decifração é a contagem de frequência, onde a decifração de alguns hieróglifos egípcios feitos por J.F. Champollion no ano de 1822 ficou famoso, a chave para decifrar era a *pedra de Roseta*, atualmente no museu Britânico, em Londres (COUTINHO, 2011).

Alguns destes métodos serão descritos abaixo.

3.1 Tipos

A criptografia é usada quando o remetente pretende escrever mensagens ou textos com o objetivo de que somente a pessoa interessada na mensagem possa lê-la. Um esquema de seu funcionamento segundo Stallings (2008, p. 172):

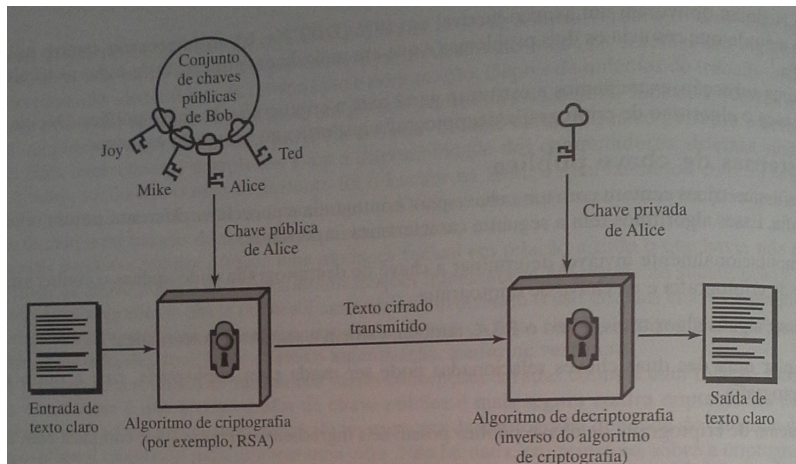


Figura 4 – Como funciona a criptografia

O *texto claro* é aquele que tem informação legível, o *texto codificado* ou texto ilegível, é aquele que foi gerado pela codificação de um texto claro. O ato de codificar ou cifrar é transformar um texto claro em um texto ilegível, e, o ato de decodificar ou decifrar é transformar um texto codificado em um texto claro - uma mensagem pode ser quebrada, ou seja, decodificada, se aplicada as técnicas corretas.

A criptografia pode ser dividida em simétrica (convencional) e assimétrica (de chave Pública), na primeira a mesma chave que criptografa a mensagem é a que descryptografa, desta forma se uma pessoa tem a chave para criptografar uma mensagem automaticamente ela consegue descryptografar. Na segunda há uma chave para criptografar a mensagem: chave pública, e uma para descryptografar: chave privada, logo mesmo que uma pessoa tenha a chave para a criptografia da mensagem ela não consegue decodificar uma sem a outra chave: privada.

Quando há as duas chaves: pública e privada, a primeira pode ser divulgada e deve ser feita de tal forma que mesmo que uma pessoa tenha ela não conseguirá descobrir a privada. A chave privada deve permanecer em segredo, afinal é ela que decodifica a mensagem.

Quando há somente uma chave, no caso da criptografia simétrica, esta deve permanecer secreta e quem a tem pode codificar ou decodificar qualquer mensagem.

O nível de segurança de uma criptografia é medido de acordo com o número de bits, desta forma, quanto mais bits forem usados, mais difícil será quebrar a criptografia usada.

Bit é a sigla para *Binary Digit*, que significa dígito binário, assim 1 bit só pode assumir dois valores: 0 ou 1, essa quantidade de valores é medida de acordo com: 2^n , onde n é o número de bits. Dez bits tem assim 2^{10} possíveis valores.

3.1.1 Heródoto

Heródoto viveu de 484 a.C. a 425 a.C. e adotou alguns métodos para comunicação chamados esteganografia (derivado das palavras gregas *steganos*, que significa coberto, e *graphein*, que significa escrever) arte de ocultar o que está escrito, os que mais se destacaram foram: raspar o cabelo do mensageiro, escrever a mensagem, deixar o cabelo crescer e enviá-lo para o destino; e escrever mensagens em tabletes e cobri-los com cera (LARCHER, 1950).

Existem outros métodos de esteganografia, alguns usam processos físico-químico, como a tinta invisível, basta escrever com suco de limão sobre uma folha de papel branca, para que a mensagem apareça basta colocar a folha em contato com uma fonte de calor.

3.1.2 Bastão de Licurgo

Bastão de Licurgo ou Cítala foi o primeiro aparelho criptográfico militar, presente no século V a.C., foi usado pelos espartanos para envio de mensagens secretas.

Era formada por dois bastões de madeira de espessura semelhante e uma tira de couro (cítala) que era usada como cinto para a transmissão da mensagem.

Cada uma das varas fica em posse de um dos participantes da mensagem: uma com o mensageiro e outra com o destinatário. Para enviar a mensagem era enrolado a tira de couro de forma espiral em um dos bastões, depois se escrevia a mensagem longitudinalmente, aparecendo uma letra em cada parte da volta. Depois da mensagem escrita bastava desenrolar a tira e enviar, de posse da cítala o mensageiro enrolava a tira em seu bastão para ler a mensagem original (OLGIN, 2011).

Esta criptografia também é conhecida como cifra de transposição que pode ser aplicada com uma função bijetiva para cifrar e a sua inversa para decifrar. A figura 5, segundo (FIARRESGA, 2010, p. 47), é um exemplo de Cítale Espartano.

3.1.3 Método de César

O próprio imperador romano, general Júlio César usava a criptografia, mais simples, para se comunicar. Ele trocava cada letra da mensagem original pela terceira letra que a segue no alfabeto, assim quem pegasse a mensagem e não soubesse o código não conseguiria lê-la (MALAGUTTI, 2015).



Figura 5 – Citale Espartano

Contudo esse método não é difícil de ser quebrado, isso é possível aplicando uma análise probabilística de cada letra. No Brasil, por exemplo, a letra mais usada é *a* e a menos usada é *x*, logicamente nem todos os textos tem a letra *a* em maior frequência, como a frase: *O impossível é inexistente*, nela a letra *a* não aparece (COUTINHO, 2008).

Mesmo assim quebrar frases criptografadas com este método são mais simples, mas às vezes pode dar muito trabalho. Observe a Figura 6 que mostra a distribuição de frequência das letras no alfabeto Brasileiro de acordo com Almeida (2015):

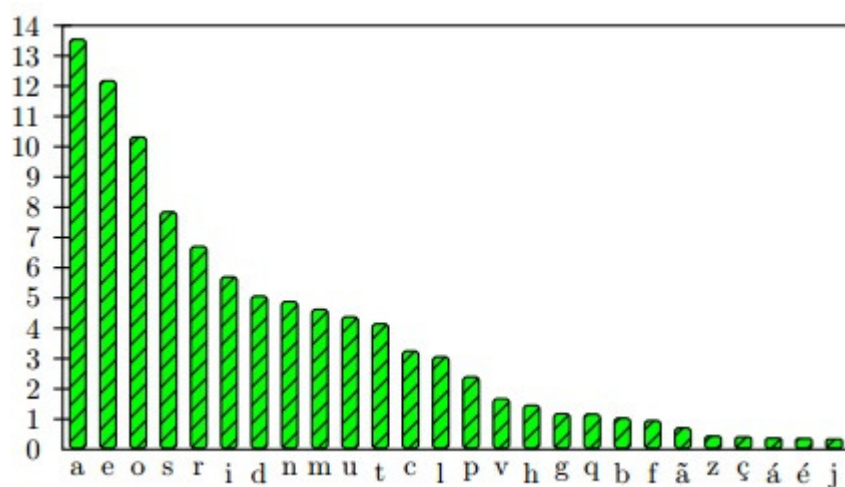


Figura 6 – Frequência das letras no alfabeto (Brasil)

3.1.4 Anagrama

É possível criptografar uma mensagem retirando os espaços entre as palavras e embaralhando as letras (anagrama), ou trocar letras por números, é possível criar vários métodos, quanto mais complexo o método for mais difícil será quebrá-lo (COUTINHO, 2008).

Também conhecida como *cifra de transposição*, é eficaz, pois caso a frase seja muito grande torna-se quase impossível reorganizar sem que se tenha a regra, uma frase com n letras têm $n!$ modos de arranjo (lembrando que este caso é com n letras distintas, pois quando há repetição o cálculo é outro), este tipo de criptografia é interessante para se trabalhar contagem com os alunos.

3.1.5 Blaise de Vigenère

Inventada por Giovan Batista Belaso, em 1553, é um sistema polialfabético, foi conhecida como cifra indecifrável, apesar de ser facilmente decifrada com a aplicação de análise estatística.

A cifra recebe este nome por ter sido atribuída erroneamente a Blaise de Vigenère, contudo apesar de não criá-la, ele criou a noção de auto-chave, que é usado ainda hoje (como no sistema DES).

Para criptografar uma mensagem nesta cifra usa-se a tabela (3), que é uma representação das 26 possibilidades da cifra de César, e uma palavra chave a escolha. Para criptografar repete-se a palavra escolhida em cima ou em baixo da mensagem, a letra da palavra escolhida deve ser localizada na linha e a letra da mensagem na coluna (ou vice-verso), o encontro delas corresponde à letra da mensagem criptografada, como mostrado na tabela 4 que usa a palavra chave *mágica*.

Na tabela 4 para criptografar a mensagem *Cifra de Blaise* com a palavra chave *mágica* relaciona-se pela tabela 3 a letra *C* com a *m*, encontrando a letra *o*, o encontro das letras *i* e *a* é *i*, e assim por diante, obtendo a frase: *oilzc do briksq*.

3.1.6 A cifra de Beale

No ano de 1885 foi publicado um livro chamado *The Beale Papers* por James B. Ward, informando tudo sobre um tesouro que ele havia enterrado juntamente com um grupo, o qual ele chefiou, de 30 pessoas. As imagens abaixo foram tiradas de um documento publicado pela Agência Nacional de Segurança (NSA, 2015).

Beale sumiu em 1822, muitas pessoas desde então, criptoanalistas ou não, tentaram desvendar as três cifras que ele deixou, deixando a especulação de que o tesouro de Beale é uma farsa (KRUH, 1982).

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

Tabela 3 – Tabela para Cifra de Blaise de Vigenère

Mensagem	C	i	f	r	a	d	e	B	l	a	i	s	e
Palavra chave	m	a	g	i	c	a	m	a	g	i	c	a	m
Mensagem	o	i	l	z	c	d	o	b	r	i	k	s	q

Tabela 4 – Criptografando com a Cifra de Blaise

Nas figuras 7, 8 e 9 é possível observar suas mensagens cifradas que ainda não foram decifradas.

É possível encontrar vários documentos sobre este caso no site: www.nsa.gov, em *Declassification and Transparency* (NSA, 2016).

3.1.7 Braille

A linguagem Braille também é uma maneira de codificação, foi desenvolvido como um método de escrita para que as pessoas com deficiência visual possam ler através do sentido do tato. O criador foi Louis Braille, um francês que com três anos de idade perdeu a visão após um ferimento no olho que infeccionou.

Esta linguagem consiste em um arranjo 3×2 de pontos, dispostos como uma pedra de dominó:

De acordo com a localização do ponto ou pontos em auto relevo é possível decodificar a mensagem, na figura 10, por exemplo, é representado a letra A, onde apenas o primeiro ponto da primeira coluna é em relevo. Observe a Figura 10 (Disponível na Apostila 10 - Atividades de contagem a partir da criptografia - do Programa de Iniciação

CODE NO. 1

This code—which a cryptographic team claims it has partially deciphered—describes the exact locality of the vault where the treasure is buried

132	71	194	38	1701	09	76	11	83	1629	40	94	63
213	16	111	95	04	341	975	14	40	64	27	81	139
604	63	90	1120	8	15	3	126	2018	40	74	750	405
486	230	436	654	502	150	251	284	306	231	124	211	
208	225	451	370	11	101	305	139(130?)	189	17	33	03	
117	193	145	1	94	73	416	910	263	28	500	538	356
04	136	219	27	176	130	10	400	25	405	18	436	65
44	200	253	118	320	138	36	416	280	15	71	224	961
246	16	401	39	89	61	304	12	21	24	203	134	92
160	406	682	7	219	104	360	760	18	64	663	474	131
17	79	73	440	95	18	64	581	34	69	128	367	460
471	81	12	103	820	62	116	97	103	062	70	60	1317
120	540	208	121	890	346	36	150	59	560	614	13	
28	63	219	012	2160	1700	99	35	18	21	136	072	15
122	170	68	4	30	44	112	18	147	436	195	320	37
13	113	6	140	8	120	305	42	58	461	44	106	301
89	400	690	93	86	116	530	02	568	9	102	38	416
234	71	216	728	965	810	2	38	121	195	14	326	148
26	18	55	131	234	361	824	5	61	623	48	961	19
36	33	10	1101	365	92	86	101	275	346	201	206	06
919	219	320	829	840	68	326	19	48	122	85	216	284
216	861	326	985	233	64	68	232	431	960	50	29	81
200	321	603	14	612	01	360	36	51	62	194	78	60
464	314	676	112	4	28	18	61	136	247	819	921	1050
294	895	10	6	66	119	38	41	49602*	423	962	302	
34	875	78	14	23	111	109	62	31	501	623	216	280
86	24	150	1000	162	286	19	21	17	340	19	242	31
00	234	140	607	115	33	191	67	104	86	52	08	16
65	121	67	95	122	216	548	96	11	201	77	364	213
71	667	890	226	154	211	10	98	34	119	56	216	119
22	218	1164	1496	1817	51	39	210	36	3	19	540	232
172	141	617	04	290	80	46	207	411	150	29	38	46
931	85	194	36	261	543	697	624	18	212	416	127	
27	19	4	63	96	12	101	418	16	140	230	460	538
84	88	612	1431	90	716	275	74	83	11	426	09	72
04	1300	1706	814	221	132	40	102	34	858	975	1101	
55	16	79	23	16	81	122	324	403	912	227	936	447
203	06	34	43	212	107	95	314	264	1065	323	428	601
213	124	95	216	814	2906	654	820	2	301	112	176	
820	71	87	96	202	35	10	2	41	17	04	221	736
	214	11	60	760								

Figura 7 – Cifra 1

CODE NO. 2

This code, broken by James B. Ward, describes the contents of the vault

15	115	73	24	818	37	52	49	17	31	62	657	22	7
195	140	47	29	107	79	84	56	238	10	26	822	5	
122	308	85	52	159	136	59	210	36	9	46	316	543	
250	106	95	53	58	2	42	7	35	122	53	31	82	77
147	193	56	96	118	71	140	207	20	353	37	994	65	
73	818	24	3	8	12	47	43	59	818	45	316	101	41
78	154	594	122	59	138	195	81	92	77	190	104	273	60
629	85	35	371	106	388	287	63	3	6	190	122	43	233
400	106	290	214	47	48	81	96	26	115	92	157	190	
110	77	85	196	46	10	113	140	353	68	120	106	2	
616	61	420	822	29	125	14	20	37	105	38	248	16	
158	7	35	19	301	125	110	496	287	98	117	520	62	
51	219	37	113	140	810	138	549	8	44	207	398	117	
18	79	344	34	20	59	520	557	107	612	219	37	66	
154	41	20	50	6	584	122	154	240	110	61	52	33	
30	5	38	8	14	84	57	549	216	115	71	29	05	63
42	131	29	138	47	73	230	549	52	53	79	110	51	
44	63	195	12	238	112	3	49	79	353	105	56	371	
566	210	515	125	360	133	143	101	15	284	549	252		
14	204	140	344	7	26	222	138	115	46	73	34	204	
316	616	53	219	7	52	150	44	52	16	40	37	157	
818	37	121	12	95	10	15	35	12	131	62	115	102	810
49	53	133	130	30	31	62	67	41	85	63	10	105	
818	138	8	113	20	32	33	37	333	287	140	47	05	
50	37	49	47	64	6	10	7	71	33	4	43	27	609
207	229	15	190	246	05	94	520	2	270	20	39	7	
33	44	22	40	7	10	3	022	106	44	496	229	393	
210	199	31	10	38	148	297	61	612	520	302	676		
287	2	44	31	33	32	520	557	10	6	250	566	246	53
37	52	03	47	320	30(39?)	33	818	7	44	30	31	250	
10	18	25	106	159	113	31	102	406	229	549	320	29	
84	305	629	15	2	10	8	219	106	353	320	219	37	52
242	72	8	50	204	184	112	125	549	65	106	818	190	
96	110	16	73	33	818	150	409	8	400	50	154	285	96
106	316	270	204	101	822	400	8	44	37	52	40	240	
34	204	30	16	46	47	85	24	44	15	64	73	138	216
85	78	110	33	420	515	53	37	30	22	31	10	110	
106	101	140	15	38	3	5	44	7	90	287	135	150	
96	33	84	125	818	190	96	520	118	459	370	653	465	
106	41	107	612	219	275	30	150	105	49	53	287	250	
207	134	7	53	12	47	85	63	138	110	21	112	140	
495	496	515	14	73	85	584	994	150	199	16	42	5	4
25	42	8	16	822	125	159	32	204	612	818	81	95	
405	41	609	136	14	20	20	26	353	302	246	8	131	
159	140	84	440	42	16	822	40	67	101	102	193	138	
204	51	63	240	549	122	8	10	63	140	47	49	140	

Figura 8 – Cifra 2

CODE NO. 3

This code tells the names of those to whom the treasure belonged, as well as their next of kin

631	317	8	92	73	112	89	67	318	28	96	107	41
12	78	146	397	110	98	114	246	340	116	74	88	
108	65	32	14	81	19	76	121	216	85	33	66	15
11	46	89	18	43	24	122	96	117	36	211	301	15
198	176	310	18	136	68	317	28	90	82	304	71	43
53	20	44	75	98	102	37	85	107	112	64	88	136
48	151	99	175	89	315	326	78	96	214	218	311	43
89	51	90	75	128	96	33	28	103	84	65	26	41
84	270	90	116	32	59	74	66	69	240	15	6	121
77	89	31	11	106	27	81	191	84	224	328	18	75
201	39	23	217	64	55	83	116	251	269	311	96	54
88	1	81	217	64	55	83	116	251	269	311	96	54
32	120	18	132	102	219	211	84	180	219	275	312	64
10	106	87	75	47	21	29	37	01	44	18	126	115
132	160	181	203	76	81	299	314	337	351	96	11	28
97	318	238	106	24	93	3	19	17	26	60	73	88
126	138	234	286	297	321	7	365	264	19	22	84	56
107	98	123	111	214	136	7	33	45	40	13	28	46
107	196	227	344	198	203	247	116	19	8	212	230	
31	6	320	65	48	52	59	41	122	33	117	11	10
71	36	45	83	76	89	92	31	65	70	83	96	27
44	50	61	24	112	136	149	176	180	194	143	171	205
296	87	12	44	31	89	99	34	41	208	173	66	9
16	95	8	113	175	61	56	203	19	177	183	206	187
200	218	260	291	305	618	551	320	18	124	78	65	
19	32	124	48	53	57	84	96	207	244	66	82	119
11	06	77	213	54	02	316	245	303	06	97	106	212
18	37	15	81	89	16	7	81	39	96	14	43	216
29	55	109	136	172	213	64	0	227	304	611	221	364
819	375	128	296	11	18	53	76	10	15	23	19	71
120	134	66	73	89	96	230	48	77	26	101	127	936
210	439	170	171	61	226	230	313	215	102	18	167	262
114	210	66	59	48	27	19	13	82	48	162	119	34
127	139	34	128	129	74	63	120	11	54	61	73	92
180	66	75	101	124	265	89	96	126	274	896	917	434
461	235	890	312	413	328	89	96	105	217	66	110	
22	77	64	42	12	7	55	24	83	67	97	109	121
181	203	219	228	256	21	34	77	319	374	382	673	
684	717	864	203	4	18	92	16	63	82	22	46	55
74	112	135	106	175	119	213	416	312	343	264	119	69
186	218	343	417	845	951	124	209	49	617	856	924	
936	72	19	29	11	35	42	40	66	85	94	112	65
115	118	236	244	106	172	112	85	6	56	38	44	85
72	32	47	73	96	124	217	314	319	221	644	617	621
934	522	416	975	10	22	18	46	137	181	101	39	86
103	116	138	164	212	218	296	815	380(390?)	412	460		
495	675	820	952									

Figura 9 – Cifra 3

Figura 10 – 3×2 - Três linhas por duas colunas

Científica OBMEP, [Malagutti \(2015, p. 45\)](#) :

O Instituto Benjamin Constant oferece cursos e informações sobre o assunto ([BRASIL, 2016](#)).

3.1.8 Disco de Alberti

O disco de Alberti ou Disco de Cifras, foi a primeira máquina criptográfica, criada por Leon Battista Alberti em 1466, que ficou conhecido como “O pai da criptologia Ocidental” por ter criado a substituição polialfabética, método que permite que diferentes símbolos cifrados representem o mesmo símbolo no texto.

Criou também o método de recifragem, onde ele fabricou uma tabela com combinações possíveis dos números 1, 2, 3 e 4, com valores entre 11 e 4444, obtendo 336 grupos. Estes eram utilizados como um dicionário de códigos que correspondia a uma palavra,

$\bullet \circ$ $\circ \circ$ $\circ \circ$	$\bullet \circ$ $\bullet \circ$ $\circ \circ$	$\bullet \bullet$ $\circ \circ$ $\circ \circ$	$\bullet \bullet$ $\circ \bullet$ $\circ \circ$	$\bullet \circ$ $\circ \bullet$ $\circ \circ$	$\bullet \bullet$ $\bullet \circ$ $\circ \circ$	$\bullet \bullet$ $\bullet \bullet$ $\circ \circ$	$\bullet \circ$ $\bullet \bullet$ $\circ \circ$	$\circ \bullet$ $\bullet \circ$ $\circ \circ$
a 1	b 2	c 3	d 4	e 5	f 6	g 7	h 8	i 9
$\circ \bullet$ $\bullet \bullet$ $\circ \circ$	$\bullet \circ$ $\circ \circ$ $\bullet \circ$	$\bullet \circ$ $\bullet \circ$ $\bullet \circ$	$\bullet \bullet$ $\circ \circ$ $\bullet \circ$	$\bullet \bullet$ $\circ \bullet$ $\bullet \circ$	$\bullet \circ$ $\circ \bullet$ $\bullet \circ$	$\bullet \bullet$ $\bullet \circ$ $\bullet \circ$	$\bullet \bullet$ $\bullet \bullet$ $\bullet \circ$	$\bullet \circ$ $\bullet \bullet$ $\bullet \circ$
j 0	k	l	m	n	o > (maior)	p	q	r
$\circ \bullet$ $\bullet \circ$ $\bullet \circ$	$\circ \bullet$ $\bullet \bullet$ $\bullet \circ$	$\bullet \circ$ $\circ \circ$ $\bullet \bullet$	$\bullet \circ$ $\bullet \circ$ $\bullet \bullet$	$\circ \bullet$ $\bullet \bullet$ $\circ \bullet$	$\bullet \bullet$ $\circ \circ$ $\bullet \bullet$	$\bullet \bullet$ $\circ \bullet$ $\bullet \bullet$	$\bullet \circ$ $\circ \bullet$ $\bullet \bullet$	$\bullet \circ$ $\circ \bullet$ $\bullet \bullet$
s	t	u	v	w	x	y	z	
$\bullet \circ$ $\bullet \circ$ $\circ \bullet$	$\circ \bullet$ $\circ \bullet$ $\bullet \circ$	$\circ \circ$ $\circ \bullet$ $\circ \bullet$	$\circ \bullet$ $\circ \circ$ $\circ \bullet$	$\circ \bullet$ $\circ \circ$ $\circ \bullet$	$\circ \bullet$ $\circ \bullet$ $\bullet \bullet$	$\bullet \circ$ $\circ \circ$ $\circ \bullet$	$\circ \bullet$ $\circ \circ$ $\bullet \circ$	
()	Restituidor de Letra	Maiúscula	Número	Expoente	Índice inferior		
$\circ \circ$ $\bullet \bullet$ $\bullet \circ$	$\circ \circ$ $\circ \bullet$ $\bullet \circ$	$\circ \circ$ $\circ \bullet$ $\circ \bullet$	$\circ \bullet$ $\circ \circ$ $\circ \bullet$	$\circ \bullet$ $\bullet \bullet$ $\bullet \bullet$	$\bullet \circ$ $\circ \circ$ $\circ \bullet$	$\circ \bullet$ $\bullet \circ$ $\circ \bullet$		
+	-	\times	\div	=	>	<		
$\circ \circ$ $\bullet \bullet$ $\bullet \circ$	$\circ \circ$ $\circ \circ$ $\bullet \bullet$	$\circ \circ$ $\bullet \circ$ $\bullet \bullet$	$\circ \circ$ $\bullet \bullet$ $\circ \bullet$	$\circ \circ$ $\bullet \bullet$ $\bullet \bullet$	$\bullet \circ$ $\circ \bullet$ $\bullet \circ$	$\circ \bullet$ $\bullet \circ$ $\circ \bullet$		

Figura 11 – Tabela de consulta para letras e números em Braille

quando aparecia em um texto era substituída pelo número e criptografada novamente junto com a mensagem.

O disco é uma das cifras mais seguras, composto por dois anéis concêntricos, onde o externo é fixo e contém 24 casas (20 letras latinas maiúsculas em ordem alfabética e os números 1, 2, 3 e 4) que corresponderá ao texto claro, e o anel interno móvel com 24 letras minúsculas desordenadas para o texto cifrado.

Fixada uma letra maiúscula como índice, o disco deve ser ajustado e a frase cifrada, podendo ser trocada a qualquer momento no texto se escrevendo uma nova letra maiúscula cifrante, indicando ao destinatário que o disco deve ser movido novamente, os números servem de nulos, ou seja, não tem significado prático na mensagem, são apenas para confundir ou dificultar a quebra do código, eles também podem servir para uma nova chave (indicando ao destinatário com antecedência qual deles significaria a nova chave), este método acelerava o trabalho de criptografar ou descriptografar mensagens e reduzia erros (SINGH, 2005).

No site <http://www.numaboa.com.br/criptografia/127-substituicao-polialfabetica/164-alberti> é possível encontrar um aplicativo que cifra mensagens pelo método do Disco de Alberti (TKOTZ, 2016).

3.1.9 Máquina Enigma

Foi uma série de máquinas de cifra, patenteada em 1918 por Arthur Scherbius, desenvolvida quando percebeu-se que o sistema criptográfico da Alemanha estava atrasado, embora não tenha sido atrativa em um primeiro momento, após várias modificações conquistou a marinha alemã em 1926 (Enigma-D), e o exército com sua própria versão (Enigma G) em 1928. Seu funcionamento é baseado em rotores, em uma combinação de sistemas mecânicos e elétricos (WINTERBOTHAM, 1978).

Na Segunda Guerra Mundial, foi usada pela Alemanha, Itália e Japão (Eixo) para enviar mensagens codificadas que eram facilmente interceptadas, mas difícil de serem quebradas, impedindo que Inglaterra, Estados Unidos, França e URSS (Aliados) soubessem de seus planos.

Segundo WINTERBOTHAM (1978) até então era usado um livro de códigos que relacionava palavras ou frases com números, mas não eram considerados completamente secretos, já que se um fosse capturado todas as mensagens podiam ser decifradas.

Havia também o bloco com folhas descartáveis, que era um auxiliar ao livro de códigos, ele indicava números a serem somados na mensagem, cada página usada deveria ser destruída, mas se tornou inviável para ser utilizado em grande escala e com muita frequência.

A máquina Enigma se tornou um grande instrumento de guerra, muitos criptógrafos foram contratados para tentar quebrar seu código, pois isso seria decisivo. Apesar dos esforços o código só foi quebrado em 1933 com a ajuda de uma máquina eletromecânica, desenvolvida por Alan Turing e Gordon Welchman, durante o trabalho em Bletchley Park, juntamente com os poloneses.

Recentemente (2015) foi lançado um filme: *O Jogo da Imitação*, baseado na vida do matemático Alan Turing, mostrando como ele e sua equipe do Bletchley Park deci-

fraram a Máquina enigma na Segunda Guerra Mundial. Foi adaptado de um livro *Alan Turing: The Enigma* escrito por Andrew Hodges, sendo criado um site com notas do autor: <http://www.turing.org.uk/> .

Contudo a vida de Alan Turing já havia sido parcialmente retratada no filme *Breaking the Code* de 1996, dirigido por Herbert Wise, e no filme *Codebreaker* de Clare Beavan e Nic Stacey, lançado em 2011.

3.1.10 *Máquina Colossus*

Projetado em 1943 por Tommy Flowers, engenheiro elétrico, foi um computador digital eletrônico usado na Segunda Guerra Mundial para quebrar códigos da máquina de cifras Lorenz SZ-40, uma das muitas máquinas usadas pelo governo alemão para criptografar suas mensagens. Tinha mais de 1700 válvulas e é referido muitas vezes como o primeiro computador.

Após o fim da guerra muitas destas máquinas foram destruídas, mas em 1991 começou o pensamento de que era possível reconstruir Colossus de modo totalmente operacional.

No site <http://www.cryptomuseum.com/crypto/colossus/index.htm> é possível encontrar uma das poucas fotos tiradas dela.

3.1.11 *Código Morse*

É a representação das letras e números em forma de sinais de pontuação (ponto e traço). Foi desenvolvido por Samuel Morse em 1835, também inventor do telégrafo.

É um código fácil de ser enviado, pois pode ser utilizado pulsos elétricos transmitidos por um cabo, ondas mecânicas, sinais visuais ou ondas eletromagnéticas, o receptor reconhece quatro estados: voltagem-ligada longa (traço), voltagem-ligada curta (ponto), voltagem-desligada longa (espaço entre caracteres e palavras) e voltagem-desligada curta (espaço entre pontos e traços).

3.1.12 *Sistema Binário*

O sistema binário, usado em computadores, é outra forma de codificação, existe uma forma especial para este código chamada de *American Standard Code for Information Interchange*, sendo referida como ASCII (completo ou estendido) muito usada em microprocessadores onde o número x de bits informa a quantidade de caracteres diferentes que podem ser usados aplicando: 2^x (SCOTTI; FERREIRA, 2011).

A ASCII relaciona cada letra do alfabeto com uma sequência de sete dígitos, zeros ou uns, mais um para verificação de erro (paridade), totalizando 8 bits.

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

Tabela 5 – Código Morse

O *Data Encryption Standard* (DES) foi criado pela International Business Machines (IBM) em 1977, permitia 72 quadrilhões de combinações (56 bits) e foi o algoritmo simétrico mais difundido no mundo até que foi padronizado a AES.

A Advanced Encryption Standard (AES) veio a partir de 2001, aplicada nas conexões de Wi-Fi, tem o tamanho de 128 bits, mas suas chaves variam de 128, 192 ou 256 bits, ficou popular por ser rápido, fácil de ser executado e ocupar pouca memória.

Ao se observar a história é possível ver que essa cifra surgiu com Francis Bacon, filósofo do século XVI, contudo ao invés de 0 e 1 ele utilizava as letras *a* e *b*, em um grupo de 5 caracteres (5 bits) que foi publicada no livro VI, capítulo I do *The Advancement of Learning* (ROSS, 1996).

3.2 RSA

O sistema mais usado e mais conhecido atualmente é o de criptografia RSA, que segundo Coutinho (2011, p. 3):

Este código foi inventado em 1978 por R. L. Rivest, A. Shamir e L. Adleman, que na época trabalhavam no Massachusetts Institute of Technology (M.I.T.). As letras RSA correspondem às iniciais dos inventores do código. Há vários outros códigos de chave pública, mas o RSA é, atualmente, o mais usado em aplicações comerciais. Este é o método utilizado, por exemplo, no *Netscape*, o mais popular dos *softwares* de navegação da *Internet* (COUTINHO, 2011, p. 3).

Existe diferença entre a criptografia convencional e a de chave pública (exemplo RSA), segundo Stallings (2008, p. 173) elas estão descritas na tabela 6.

No site <http://demonstrations.wolfram.com> é possível encontrar programas que codificam e decodificam mensagens tanto no método de César quanto no de RSA.

Criptografia convencional	Criptografia de chave pública
<p>Necessário para funcionar: O mesmo algoritmo com a mesma chave é usado para criptografia e descriptografia.</p> <p>O emissor e o receptor precisam compartilhar o algoritmo e a chave.</p> <p>Necessário para a segurança: A chave precisa permanecer secreta.</p> <p>Deverá ser impossível ou pelo menos impraticável decifrar uma mensagem se nenhuma outra informação estiver disponível.</p> <p>O conhecimento do algoritmo, com amostras do texto cifrado precisam ser insuficientes para determinar a chave.</p>	<p>Necessário para funcionar: Um algoritmo é usado para criptografia e descriptografia com um par de chaves, uma para criptografia e outra para descriptografia.</p> <p>O emissor e o receptor precisam ter uma das chaves do par casado de chaves (não a mesma chave).</p> <p>Necessário para a segurança: Uma das duas chaves precisa permanecer secreta.</p> <p>Deverá ser impossível ou pelo menos impraticável decifrar uma mensagem se nenhuma outra informação estiver disponível.</p> <p>O conhecimento do algoritmo, com uma das chaves, e amostras do texto cifrado precisam ser insuficientes para determinar a outra chave.</p>

Tabela 6 – Criptografia convencional e de chave pública

3.2.1 Como Funciona?

O método de criptografia RSA funciona do seguinte modo:

1. Escolhe-se dois primos p e q , distintos entre si.
2. Define-se $N = pq$ e $\varphi(N) = (p - 1)(q - 1)$.
3. Deve-se escolher um número e , que faz parte da chave Pública, de forma que o máximo divisor comum (mdc) entre ele e $\varphi(N)$ seja 1: $(e, \varphi(N)) = 1$ e $1 < e < \varphi(N)$.
4. Resolvendo a congruência $ed \equiv 1 \pmod{\varphi(N)}$ encontra-se d , que faz parte da chave Privada.
5. De acordo com uma tabela pré formulada e de domínio público é feita a transformação de todos os caracteres da mensagem em números (nesta tabela todos os números devem ter a mesma quantidade de dígitos), obtendo-se a mensagem numérica em um único bloco que será dividida em blocos b , de forma que: $1 \leq b < N$. Isso garante que ao utilizar congruência obtenha-se um único resultado na decodificação.
6. De posse da Chave Pública (e, N) criptografa-se os blocos b de acordo com a congruência: $b^e \equiv C(b) \pmod{N}$, onde $C(b)$ é a mensagem criptografada.

7. De posse da Chave Privada (d, N) descriptografa-se de acordo com a congruência: $C(b)^d \equiv D(C(b)) \pmod{N}$, onde $D(C(b))$ é a mensagem descriptografada, $1 \leq D(C(b)) < N$.
8. Cada bloco $D(C(b))$ deve ser colocado em sequência e de acordo com a mesma tabela usada no item 5 os números devem ser convertidos em caracteres.

Exemplo 3. Neste exemplo será usado números primos menores, que facilitem o cálculo com o uso de uma calculadora comum. Dado os primos p e q da forma $6n + 5$, sendo $p = 11$ e $q = 17$, pode-se obter $N = 11 \times 17 = 187$ e $\varphi_N = (11 - 1) \times (17 - 1) = 160$.

Dada a tabela abaixo:

A	B	C	D	E	F	G	H	I	J
21	22	23	24	25	26	27	28	29	31
K	L	M	N	O	P	Q	R	S	T
32	33	34	35	36	37	38	39	41	42
U	V	W	X	Y	Z				
43	44	45	46	47	48				
0	1	2	3	4	5	6	7	8	9
49	51	52	53	54	55	56	57	58	59

Tabela 7 – Tabela Para Conversão

O valor de e deve ser escolhido de modo que $(e, \varphi_N) = 1$, deste modo será escolhido o número 3 e d deverá seguir a congruência $ed \equiv 1 \pmod{\varphi_N}$, assim:

$$3d \equiv 1 \pmod{160}.$$

Deste modo $160k = 3d - 1 \Leftrightarrow 1 = 3d - 160k$, resolvendo pelo método do algoritmo de Euclides:

$$160 = 3 \times 53 + 1 \Leftrightarrow 1 = 160 - 3 \times 53.$$

Como o valor de d não pode ser negativo e as soluções desta equação são: $d = -53 + 160t$ e $k = -1 - 3t$:

$$-53 + 160t > 0 \Leftrightarrow t > \frac{53}{160}.$$

Substituindo $t = 1$ tem-se o menor valor possível para d que é 107. Deste modo já tem-se a chave para Ciptografar $(e, N) = (3, 187)$ e para Descriptografar $(d, N) = (107, 187)$.

A mensagem é “CHAVE”, primeiro é preciso transformar as letras em números de acordo com a tabela, assim tem-se C= 23, H= 28, A= 21, V= 44 e E= 25. Ficando: 23 – 28 – 21 – 44 – 25.

A mensagem deve ser separada em blocos b de modo que cada bloco tenha números menores que 187. Como os primos escolhidos são pequenos, os blocos também devem ser, assim:

$$2328214425 = 2 - 32 - 82 - 14 - 42 - 5$$

Para codificar a mensagem usaremos a chave $(3, 187)$ e a congruência $b^e \equiv C(b) \pmod{N}$:

$$2^3 \equiv C(b_1) \pmod{N} \Leftrightarrow C(b_1) = 8$$

$$32^3 \equiv C(b_2) \pmod{N} \Leftrightarrow 32^3 \equiv 32768 \pmod{N} \Leftrightarrow C(b_2) = 43$$

$$82^3 \equiv C(b_3) \pmod{N} \Leftrightarrow 82^3 \equiv 551368 \pmod{N} \Leftrightarrow C(b_3) = 92$$

$$14^3 \equiv C(b_4) \pmod{N} \Leftrightarrow 14^3 \equiv 2744 \pmod{N} \Leftrightarrow C(b_4) = 126$$

$$42^3 \equiv C(b_5) \pmod{N} \Leftrightarrow 42^3 \equiv 74088 \pmod{N} \Leftrightarrow C(b_5) = 36$$

$$5^3 \equiv C(b_6) \pmod{N} \Leftrightarrow 5^3 \equiv 125 \pmod{N} \Leftrightarrow C(b_6) = 125$$

O bloco codificado será:

$$8 - 43 - 92 - 126 - 36 - 125.$$

Para decodificar é preciso da chave $(107, 187)$ e da congruência:

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

Como 107 é um número primo e usá-lo como expoente faz com que não seja possível usar uma calculadora comum será usado algumas propriedades de congruência citadas na Proposição 14.

Para decodificar o primeiro bloco: 8 deve-se usar:

$$8^{107} \equiv D(C(b)) \pmod{187}$$

Assim como $107 = 3 \times 7 \times 5 + 2$ temos:

$$8^3 \equiv 512 \equiv 138 \pmod{187}.$$

Pelo item 5 da Proposição 14:

$$(8^3)^5 \equiv 138^5 \pmod{187}$$

e

$$138^5 = 138^2 \times 138^2 \times 138 = 19044 \times 19044 \times 138,$$

então:

$$8^{15} \equiv 138^5 \equiv 138^2 \times 138^2 \times 138 \pmod{187}$$

$$\Leftrightarrow 8^{15} \equiv 19044 \times 19044 \times 138 \pmod{187}$$

$$\Leftrightarrow 8^{15} \equiv 157 \times 157 \times 138 \pmod{187},$$

pois

$$19044 \equiv 157 \pmod{187}.$$

Portanto

$$3401562 \equiv 32 \pmod{187}$$

$$\Leftrightarrow 8^{15} \equiv 32 \pmod{187}.$$

Ainda,

$$\Leftrightarrow (8^{15})^7 \equiv 32^7 \equiv 32^3 \times 32^3 \times 32 \pmod{187}$$

$$\Leftrightarrow 8^{105} \equiv 32768 \times 32768 \times 32 \equiv 43 \times 43 \times 32 \pmod{187}$$

$$\Leftrightarrow 8^{105} \equiv 59168 \equiv 75 \pmod{187}.$$

Finalmente conclui-se que

$$\Leftrightarrow 8^{105} \times 8^2 \equiv 76 \times 8^2 \equiv 4864 \equiv 2 \pmod{187}.$$

$$\Leftrightarrow 8^{107} \equiv 2 \pmod{187}.$$

Contudo com este método é gasto muito tempo e deve-se fazer muitos cálculos, um modo mais fácil é usar o Teorema Chinês do Resto.

Assim como sabe-se que $N = 187 = 11 \times 17$, pelo Teorema 2 tem-se que:

$$p|a^{p-1} - 1 \Leftrightarrow a^{p-1} \equiv 1 \pmod{p}.$$

Desta forma:

$$8^{10} \equiv 1 \pmod{11}$$

e

$$8^{16} \equiv 1 \pmod{17}.$$

Assim:

$$(8^{10})^{10} \equiv 1^{10} \pmod{11}$$

$$8^{100} \times 8^7 \equiv 1 \times 8^7 \equiv 2 \pmod{11}$$

$$8^{107} \equiv 2 \pmod{11}$$

e

$$(8^{16})^6 \equiv 1^6 \pmod{17}$$

$$8^{96} \times 8^5 \equiv 1 \times 8^5 \pmod{17}$$

$$8^{101} \equiv 9 \pmod{17}$$

$$8^{101} \times 8^5 \equiv 9 \times 8^5 \equiv 9 \times 9 \equiv 13 \pmod{17}$$

$$8^{106} \times 8 \equiv 13 \times 8 \equiv 2 \pmod{17}$$

$$8^{107} \equiv 2 \pmod{17}$$

Substituindo 8^{107} por x tem-se um sistema de congruências:

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

$$x \equiv 2 \pmod{17}.$$

Pelo Teorema Chinês do Resto:

$$M = 11 \times 17 = 187$$

$$M_1 = \frac{187}{11} = 17$$

$$M_2 = \frac{187}{17} = 11.$$

Assim:

$$17y_1 \equiv 1 \pmod{11}$$

$$\Leftrightarrow y_1 = 2$$

e:

$$11y_2 \equiv 1 \pmod{17}$$

$$\Leftrightarrow y_2 = 14$$

$$X = 17 \times 2 \times 2 + 11 \times 14 \times 2 + t187$$

$$X = 376 + t187.$$

O menor valor de X no conjunto dos naturais para a equação é com $t = -2$, desta forma $X = 2$.

Obtem-se assim o primeiro bloco decodificado. Para obter o segundo bloco decodificado o processo é o mesmo.

Repetindo o processo em todos os blocos será obtido a mensagem decodificada: 2 - 32 - 82 - 14 - 42 - 5. Como é conhecido a Tabela 7, basta reagrupar a mensagem e trocar os números pelas letras voltando à mensagem “CHAVE”.

Exemplo 4. Para resolver este exemplo foi usado o *software* MAXIMA, que é livre e gratuito, pois os cálculos necessários não são feitos por uma calculadora normal e à mão levaria muito tempo.

Dado os primos p e q da forma $6n + 5$, sendo $p = 857$ e $q = 2207$, pode-se obter $N = 857 \times 2207 = 1891399$ e $\varphi_N = (857 - 1) \times (2207 - 1) = 1888336$.

Considere a Tabela 7 já usada no Exemplo 1.

O valor de e deve ser escolhido de modo que $(e, \varphi_N) = 1$. Vejamos algumas opções: 3, 5, 7, 11, 13, 15, 17, 19, 25, 29, 31, 35, 55 ... O valor escolhido será $e = 3$.

Para obter d é preciso utilizar a congruência:

$$ed \equiv 1 \pmod{\varphi(N)}$$

Substituindo, temos:

$$3 \times d \equiv 1 \pmod{1888336},$$

ou seja $3d - 1 = 1888336k \Leftrightarrow 3d - 1888336k = 1$.

Logo recaímos em uma equação diofantina, com solução nos inteiros já que $(3, 1888336) = 1 \mid 1$.

Assim resolvendo a equação diofantina:

$$1888336 = 3 \times 629445 + 1$$

$$\Leftrightarrow 1888336 - 3 \times 629445 = 1.$$

Logo, pela Proposição 9 as soluções para d e k nos inteiros é dada por: $d = -629445 + 1888336t$ e $k = 1 - 3t$. Contudo quer-se números inteiros positivos para d desta forma:

$$-629445 + 1888336t > 0$$

encontra-se que $t > 0,33\dots$. Substituindo t por 1 obtem-se: $d = 1258891$.

A chave Pública

$$(e, N) \Rightarrow (3, 1891399)$$

e a chave Privada

$$(d, N) \Rightarrow (1258891, 1891399).$$

Com a chave Pública será codificada a mensagem:

NÚMEROS D0M1N4M 0 MUNDO.

De acordo com a tabela 7 a mensagem ficará:

3543342539494124493451355434493443352449

será dividida em blocos de três dígitos ficando: 354 - 334 - 253 - 949 - 412 - 449 - 345 - 135 - 543 - 449 - 344 - 335 - 244 - 9.

Bloco 354:

$$354^3 \equiv 859687 \pmod{1891399}$$

Assim o primeiro bloco será: 859687.

Do mesmo modo:

Bloco 334:

$$334^3 \equiv 1323123 \pmod{1891399}$$

Bloco 253:

$$253^3 \equiv 1063085 \pmod{1891399}$$

Bloco 949:

$$949^3 \equiv 1649400 \pmod{1891399}$$

Bloco 412:

$$412^3 \equiv 1844164 \pmod{1891399}$$

Bloco 449:

$$449^3 \equiv 1623096 \pmod{1891399}$$

Bloco 345:

$$345^3 \equiv 1344246 \pmod{1891399}$$

Bloco 135:

$$135^3 \equiv 568976 \pmod{1891399}$$

Bloco 543:

$$543^3 \equiv 1225491 \pmod{1891399}$$

Bloco 449:

$$449^3 \equiv 1623096 \pmod{1891399}$$

Bloco 344:

$$344^3 \equiv 988205 \pmod{1891399}$$

Bloco 335:

$$335^3 \equiv 1658794 \pmod{1891399}$$

Bloco 244:

$$244^{33} \equiv 1286991 \pmod{1891399}$$

Bloco 9:

$$9^3 \equiv 729 \pmod{1891399}$$

Mensagem codificada: 859687 - 1323123 - 1063085 - 1649400 - 1844164 - 1623096 - 1344246 - 568976 - 1225491 - 1623096 - 988205 - 1658794 - 1286991 - 729.

Para decodificar a mensagem é preciso usar a chave Privada (1258891, 1891399).

Para o primeiro bloco:

$$859687^{1258891} \equiv 354 \pmod{1891399}.$$

Fazendo todo o processo inverso volta-se à mensagem criptografada:

354 - 334 - 253 - 949 - 412 - 449 - 345 - 135 - 543 - 449 - 344 - 335 - 244 - 9

⇒ 3543342539494124493451355434493443352449

⇒ 35 - 43 - 34 - 25 - 39 - 49 - 41 - 24 - 49 - 34 - 51 - 35 - 54 - 34 - 49 - 34 - 43 - 35 -
24 - 49

⇒ NÚMEROS D0M1N4M 0 MUNDO

3.2.2 Por que funciona?

Mas por que o método funciona?

A mensagem b deve ser igual à mensagem decodificada $D(C(b))$. De acordo com o processo:

$$b^e \equiv C(b) \pmod{N}, \quad (3.1)$$

$$C(b)^d \equiv D(C(b)) \pmod{N}, \quad (3.2)$$

$$ed \equiv 1 \pmod{\varphi(N)}, \quad (3.3)$$

em que $N = pq$, $\varphi(N) = (p-1)(q-1)$. Como $b < N$, $D(C(b)) < N$, para provar que a criptografia RSA funciona é suficiente verificar que $D(C(b)) \equiv b \pmod{N}$ se verifica. Pela Proposição 14, quinto item e usando as equações (3.1) e (3.2), temos que:

$$(b^e)^d \equiv D(C(b)) \pmod{N}. \quad (3.4)$$

De acordo com a equação (3.3), existe inteiro k tal que

$$ed = k\varphi(N) + 1.$$

Usando (3.4):

$$b^{k\varphi(N)+1} \equiv D(C(b)) \pmod{N}. \quad (3.5)$$

Se $p \mid b$ implica que

$$b \equiv 0 \pmod{p},$$

então:

$$b^{ed} \equiv 0 \pmod{p}.$$

Implicando assim que

$$b^{ed} \equiv b \pmod{p},$$

provando que

$$D(C(b)) \equiv b \pmod{p}.$$

Analogamente se $q \mid b$. Agora, supondo que p e q não dividam b , pelo Pequeno Teorema de Fermat tem-se que

$$b^{p-1} \equiv 1 \pmod{p}, \quad (3.6)$$

e

$$b^{q-1} \equiv 1 \pmod{q}, \quad (3.7)$$

o que implica

$$(b^{(p-1)})^{(q-1)} \equiv 1^{(q-1)} \pmod{p}, \quad (3.8)$$

e

$$(b^{(q-1)})^{(p-1)} \equiv 1^{(p-1)} \pmod{q}. \quad (3.9)$$

Usando (3.8) e (3.9), e o item 2 da Proposição 15, temos que

$$b^{\varphi(N)} \equiv 1 \pmod{pq}$$

e logo

$$(b^{\varphi(N)})^k b \equiv b \pmod{N}.$$

Usando transitividade e (3.5) obtem-se

$$b \equiv D(C(b)) \pmod{N}.$$

Logo a mensagem b é igual à mensagem decodificada $D(C(b))$.

3.2.3 Segurança

Para quebrar o código é preciso ter a chave de decodificação (d, N) , acontece que a chave pública (e, N) já fornece parte do que é preciso, a saber, o número N . Assim é preciso apenas encontrar d e ter a mensagem em mãos.

O número N é igual ao produto de dois números primos p e q que foram escolhidos, assim é preciso encontrar a fatora  o de N para que p e q sejam achados e assim encontrar $\varphi(N) = (p-1)(q-1)$, para que resolva-se a congru  ncia $ed \equiv 1 \pmod{\varphi(N)}$, encontrando d .

Parece simples, mas não é, na realidade é inviável já que não existe computadores rápidos o suficientes, nem algoritmos tão bons que nos permitam fatorar um número inteiro muito grande que não tenha fatores pequenos.

É preciso, neste caso, dar significado à palavra grande: o quão grande deve ser N ? O RSA Laboratory pertence à uma empresa que detém os direitos do sistema de codificação RSA, já lançou desafios para a fatoração de possíveis chaves, uma delas com 193 algarismos foi finalizada no ano de 2005 por F. Bahr, M. Boehm, J. Franke e T. Kleinjung no Escritório Federal de Segurança de Informação da Alemanha. Eles usaram 80 computadores de 2.2 GHz cada um, levando 5 meses para a tarefa.

Há chaves maiores, podendo chegar à 2467 algarismos.

De acordo com [Garrett \(2017\)](#) o novo *Sunway TaihuLight* é um supercomputador da China, o mais poderoso do mundo com mais de dez milhões de núcleos de processamento, sendo assim ele pode fazer 93 quatrilhões de cálculos por segundo, e tudo isso fabricado na China.

Existe uma listagem destes supercomputadores onde China e Estados Unidos lideram, com 167 e 165 computadores cada, respectivamente, no Brasil há 4 deles e o mais poderoso está no 265 lugar.

APLICAÇÕES DA CRIPTOGRAFIA RSA NO PROGRAMA DE INICIAÇÃO CIENTÍFICA OBMEP

A aula foi ministrada aos alunos do 10º Programa de Iniciação Científica Júnior (PIC), Polo Passos - MG, da Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP).

Nesta turma em particular todos os estudantes já haviam feito o curso pelo menos uma vez anteriormente, assim a explicação da matéria podia ser mais aprofundada, pois muitos conteúdos eles já haviam tido uma introdução.

A programação do Grupo 4 deste ano traz Criptografia e Teoria dos Números nos três primeiros encontros, como mostra na figura 12.

Como a turma é misturada, todos os alunos participaram da explanação dos conteúdos programados para os dois grupos, o planejamento do grupo 3 também aborda conhecimentos de Teoria dos Números, como é possível ver na figura 13.

A aula foi ministrada no encontro 6, depois de ter sido abordado todos os conteúdos básicos para se compreender Criptografia RSA.

4.1 Planejamento

Primeiramente foi apresentado um resumo da história da criptografia com a cifra de César, que é mais simples, para isso foi usada as apostilas 7: Criptografia de Severino Collier Coutinho, a apostila 10: Atividades de contagem a partir da Criptografia de Pedro Luiz Malagutti, disponíveis no site <http://www.obmep.org.br/>.

Depois foi falado um pouco sobre os tópicos:

10º PIC (2015) – G4

MÓDULO I – ARITMÉTICA E CRIPTOGRAFIA			
Encontro	Objetivos	Assuntos	Material
1	Estudar as propriedades aritméticas dos números inteiros.	Algoritmo da Divisão. Algoritmo do MDC de Euclides. Aplicações da Relação de Bézout. Equações Diofantinas Lineares.	Apostila 1: Capítulo 3 - Seções 3.4 a 3.10.
2	Apresentar o conceito de congruência de números inteiros e algumas de suas aplicações.	Congruências. Teorema Chinês do Resto.	Apostila 7: Capítulos 2, 3 e 4.
3	Aplicar propriedades de congruências à criptografia RSA.	Criptografia RSA.	Apostila 7: Capítulos 5 e 6.
Material complementar para o PO: Fomin: Capítulo 10.			

MÓDULO II – GEOMETRIA			
Encontro	Objetivos	Assuntos	Material
4	Utilizar propriedades da Geometria Plana em algumas construções geométricas.	Construções Elementares. Lugares Geométricos. Expressões Algébricas.	Apostila 8.
5	Apresentar a Trigonometria do triângulo retângulo.	Trigonometria do Triângulo Retângulo.	Trigonometria e Números Complexos: Capítulos 1 e 2.
6	Apresentar as funções trigonométricas.	Extensões das Funções Trigonométricas. Leis do Seno e Cosseno.	Trigonometria e Números Complexos: Capítulos 3 e 4.
Material complementar para o PO: Tópicos de Matemática Elemental, vol. 2, A. C. Muniz Neto: Capítulos 1 a 4, para o Encontro 4, e Capítulo 7 para o Encontro 6.			

Programação do PIC 2015

Figura 12 – Programação dos Primeiros Encontros do G4

Grupo 3: Programação do PIC 2015 – G3

MÓDULO I – ARITMÉTICA ELEMENTAR				
Encontro	Objetivos	Assuntos	Material	Vídeos do YouTube/DVD do PIC
1	Compreender formalmente o conjunto dos números naturais e as principais propriedades algébricas de seus elementos. Entender o sistema decimal posicional e suas associações com critérios de divisibilidade. Compreender formalmente o conceito de números primos e sua associação com o Teorema Fundamental da Aritmética.	Números naturais. Sistema decimal posicional. Múltiplos e divisores. Critérios de divisibilidade: 2, 3, 5, 9 e 10. Potenciação. Números primos e o Crivo de Eratóstenes. O Teorema Fundamental da Aritmética.	Apostila 1: Capítulos 1 e 2. Fomin: Capítulo 3 - Seção 3.1. OBS: No livro do Fomin, capítulo 8, há vários problemas que envolvem os conteúdos abordados nesse encontro.	2, 10, 33, 34, 40 e 41 (Aritmética)
2	Compreender formalmente o conjunto dos inteiros e propriedades algébricas de seus elementos, em especial os algoritmos da divisão e de Euclides. Modelar e resolver problemas utilizando equações diofantinas lineares.	Números inteiros (múltiplos, divisores, algoritmo da divisão, paridade, MMC, MDC). Algoritmo de Euclides. Relação de Bezout. Equações diofantinas lineares.	Apostila 1: Capítulo 3. Fomin: Capítulo 3 - Seções 3.1, 3.2 e 3.4; Capítulo 10 - Seção 10.3. OBS: No livro do Fomin, Capítulo 8, há vários problemas que envolvem os conteúdos abordados neste encontro.	3, 8, 9, 10, 21, 22, 23, 24, 25, 26, 28, 32, 38 (Aritmética)
3	Entender formalmente o conceito de congruência e suas propriedades operacionais. Utilizar congruência para abordar alguns critérios de divisibilidade: 6, 7, 11 e 13. Determinar restos via congruências. Analisar casos especiais de equações diofantinas não lineares.	Aritmética dos restos e critérios de divisibilidade. Equações diofantinas.	Apostila 1: Capítulo 4. Fomin: Capítulo 10 - Seções 10.1, 10.2 e 10.3. OBS: No livro do Fomin, Capítulo 8, há vários problemas que envolvem os conteúdos abordados neste encontro.	28, 29, 30, 35, 42, 43, 44, 45, 51, 52 e 53 (Aritmética)

Figura 13 – Programação dos Primeiros Encontros do G3

1. a máquina enigma, usada na Segunda Guerra Mundial para as comunicações nazistas, e o site <http://www.numaboa.com.br/criptografia/dispositivos/861-enigma> que

tem um simulador *on line* da máquina enigma onde é possível codificar mensagens, mas não decodificá-las;

2. O código morse;
3. codificação binária ASCII;
4. e, um breve resumo dos outros tipos de criptografia ao longo da história que estão presentes neste trabalho

Foi apresentado a criptografia RSA e um pouco de sua história, assim como onde ela é usada (foi mostrado sites de bancos e de compras), o porque ela funciona, como ela funciona e porque ela é segura, sendo feita as demonstrações necessárias.

Foi discutido também as formas de se encontrar os números primos, onde foi apresentado o site <http://primes.utm.edu/largest.html> e os Problemas do Prémio Millennium (*Hipótese de Riemann*).

4.2 A aplicação

O Exemplo 1 da Seção 2.2 foi feito passo-a-passo com os alunos. A turma então foi dividida em duas equipes e para cada uma foi dada uma mensagem simples para que eles decodifiquem. Com as respostas em mãos foi dada a elas uma segunda mensagem que não pode ser resolvida apenas com calculadora (Exemplo 2), mas sim com algum *software* como, por exemplo, o MAXIMA.

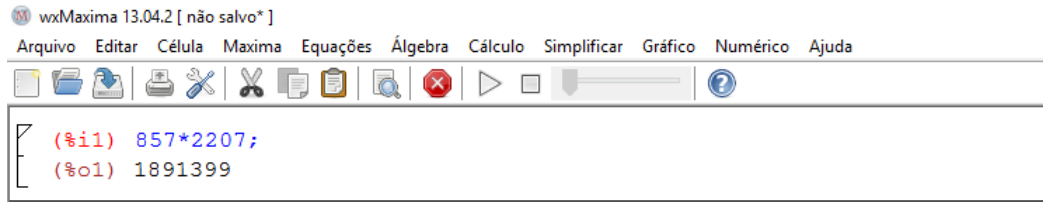
Nesta parte da aula os alunos discutiram a importância dos recursos eletrônicos e foi apresentado o programa MAXIMA. Alguns deles cursam Técnico em Informática integrado ao Ensino Médio no Instituto Federal do Sul de Minas (IFSul), então foi uma conversa muito rica.

4.3 MAXIMA

O programa MAXIMA pode ser baixado gratuitamente, a versão usada foi a 5.30.0. Existe um tutorial em <http://maxima.sourceforge.net>. É possível usá-lo como auxiliar na criptografia RSA, além de outros campos como funções e matriz. Para mostrar como ele é usado será mostrado a resolução do Exemplo 2.

Depois de escolhido os números primos, é possível encontrar o produto com o comando: $p * q$, conforme a figura 14, onde p e q são os números primos escolhidos, depois é só dar enter ou a combinação de teclas [Shift][Enter].

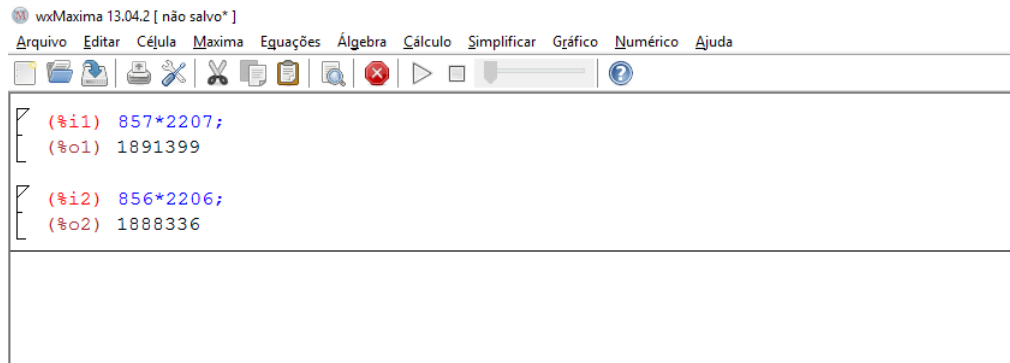
É possível encontrar φ_N de forma parecida como na figura 15.



```

wxMaxima 13.04.2 [ não salvo* ]
Arquivo  Editar  Célula  Maxima  Equações  Álgebra  Cálculo  Simplificar  Gráfico  Numérico  Ajuda
[ (%i1) 857*2207;
  (%o1) 1891399

```

Figura 14 – Encontrando N


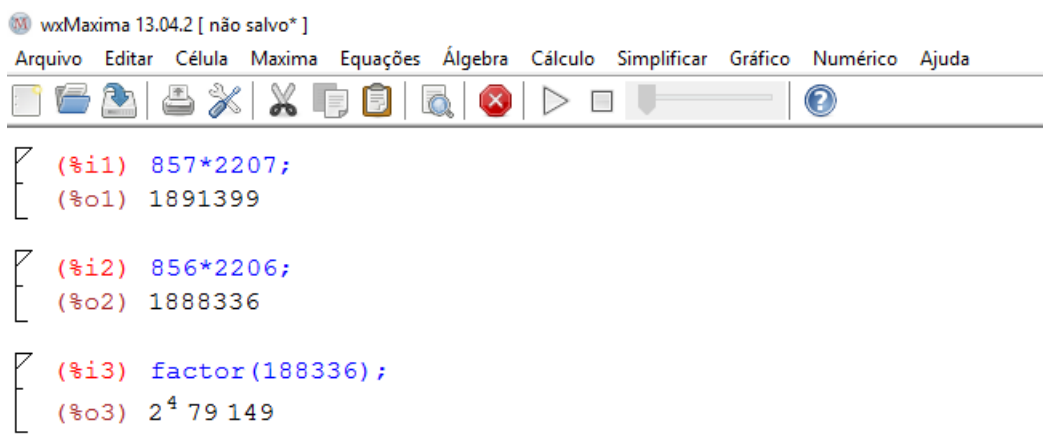
```

wxMaxima 13.04.2 [ não salvo* ]
Arquivo  Editar  Célula  Maxima  Equações  Álgebra  Cálculo  Simplificar  Gráfico  Numérico  Ajuda
[ (%i1) 857*2207;
  (%o1) 1891399
[ (%i2) 856*2206;
  (%o2) 1888336

```

Figura 15 – Encontrando φ_N

Para encontrar e temos que (e, φ_N) , por isso é possível usar o comando $factor(a)$ como na figura 16, onde a é o número a ser fatorado, para garantir que o mdc entre eles seja 1 basta escolher um número primo que não pertença à fatoração de φ_N e seja menor possível. Como os números primos usados são da forma $6k + 5$ isso implica que φ_N nunca será divisível por 3.



```

wxMaxima 13.04.2 [ não salvo* ]
Arquivo  Editar  Célula  Maxima  Equações  Álgebra  Cálculo  Simplificar  Gráfico  Numérico  Ajuda
[ (%i1) 857*2207;
  (%o1) 1891399
[ (%i2) 856*2206;
  (%o2) 1888336
[ (%i3) factor(188336);
  (%o3) 2^4 79 149

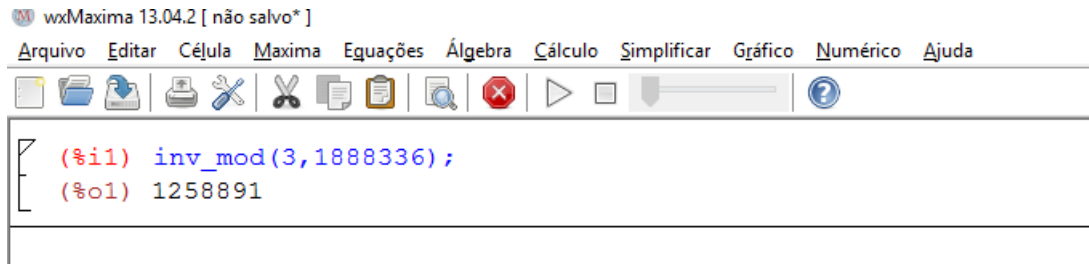
```

Figura 16 – Fatoração de φ_N

Além disso o comando de fatoração, é útil na criptoanálise para descobrir quais números primos estão sendo usados na codificação e assim poder decodificar a mensagem (quando não se tem a chave privada), afinal basta descobrir a fatoração de N para descobrir a Chave Privada.

É possível encontrar d também, que seria o inverso multiplicativo, para isso é

preciso usar o comando $\text{inv_mod}(e, \varphi_N)$ como na figura 17.



```

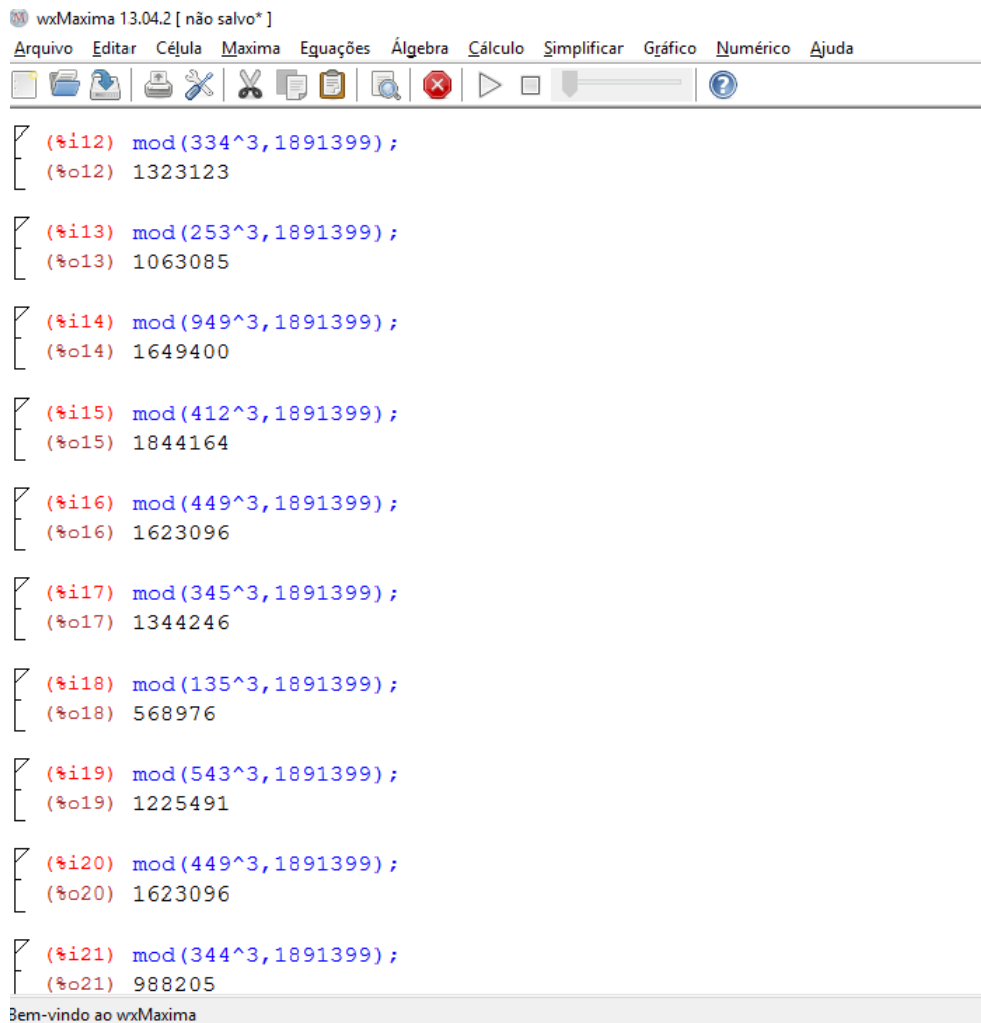
wxMaxima 13.04.2 [ não salvo* ]
Arquivo Editar Célula Maxima Equações Álgebra Cálculo Simplificar Gráfico Numérico Ajuda
[ (%i1) inv_mod(3,1888336);
  (%o1) 1258891

```

Figura 17 – Encontrando d

Para potência é usado \wedge , por exemplo: 10^5 ficaria “ 10^5 ”. O comando $\text{mod}(m, n)$ dá o resto da divisão de m por n , o que é preciso nas congruências usadas.

Assim ao se utilizar as formulas $b^e \equiv C(b) \pmod N$ e $[C(b)]^d \equiv D(C(b)) \pmod N$, basta colocar o comando $\text{mod}(b^e, N)$ e terá o resultado $C(b)$ como nas figuras 18 e 19, o comando $\text{mod}([C(b)]^d, N)$ obtendo $D(C(b))$ como nas figuras 20 e 21.



```

wxMaxima 13.04.2 [ não salvo* ]
Arquivo Editar Célula Maxima Equações Álgebra Cálculo Simplificar Gráfico Numérico Ajuda
[ (%i12) mod(334^3,1891399);
  (%o12) 1323123
[ (%i13) mod(253^3,1891399);
  (%o13) 1063085
[ (%i14) mod(949^3,1891399);
  (%o14) 1649400
[ (%i15) mod(412^3,1891399);
  (%o15) 1844164
[ (%i16) mod(449^3,1891399);
  (%o16) 1623096
[ (%i17) mod(345^3,1891399);
  (%o17) 1344246
[ (%i18) mod(135^3,1891399);
  (%o18) 568976
[ (%i19) mod(543^3,1891399);
  (%o19) 1225491
[ (%i20) mod(449^3,1891399);
  (%o20) 1623096
[ (%i21) mod(344^3,1891399);
  (%o21) 988205
Bem-vindo ao wxMaxima

```

Figura 18 – Codificando a mensagem

The screenshot shows the wxMaxima 13.04.2 interface with the following code and output:

```

(%i22) mod(543^3,1891399);
(%o22) 1225491

(%i23) mod(449^3,1891399);
(%o23) 1623096

(%i24) mod(344^3,1891399);
(%o24) 988205

(%i25) mod(335^3,1891399);
(%o25) 1658794

(%i26) mod(244^3,1891399);
(%o26) 1286991

(%i27) mod(9^3,1891399);
(%o27) 729

```

Figura 19 – Codificando a mensagem

The screenshot shows the wxMaxima 13.04.2 interface with the following code and output:

```

(%i29) mod(859687^1258891,1891399);
(%o29) 354

(%i30) mod(1323123^1258891,1891399);
(%o30) 334

(%i31) mod(1063085^1258891,1891399);
(%o31) 253

(%i32) mod(1649400^1258891,1891399);
(%o32) 949

(%i33) mod(1844164^1258891,1891399);
(%o33) 412

(%i34) mod(1623096^1258891,1891399);
(%o34) 449

(%i35) mod(1344246^1258891,1891399);
(%o35) 345

(%i36) mod(568976^1258891,1891399);
(%o36) 135

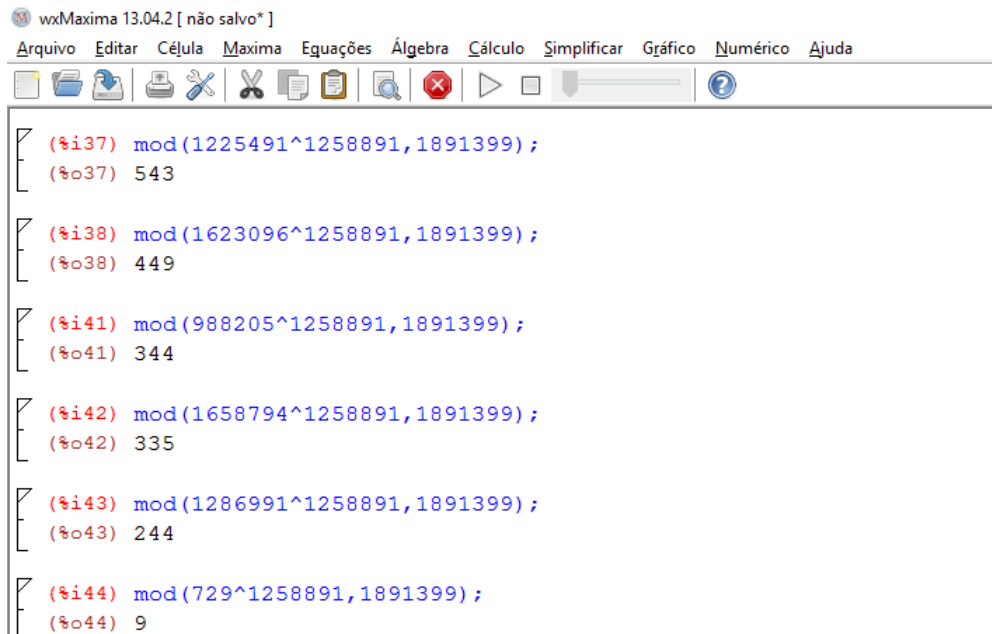
(%i37) mod(1225491^1258891,1891399);
(%o37) 543

(%i38) mod(1623096^1258891,1891399);
(%o38) 449

```

Bem-vindo ao wxMaxima

Figura 20 – Decodificando a mensagem



```

wxMaxima 13.04.2 [ não salvo* ]
Arquivo  Editar  Célula  Maxima  Equações  Álgebra  Cálculo  Simplificar  Gráfico  Numérico  Ajuda

[ (%i37) mod(1225491^1258891,1891399);
  (%o37) 543

[ (%i38) mod(1623096^1258891,1891399);
  (%o38) 449

[ (%i41) mod(988205^1258891,1891399);
  (%o41) 344

[ (%i42) mod(1658794^1258891,1891399);
  (%o42) 335

[ (%i43) mod(1286991^1258891,1891399);
  (%o43) 244

[ (%i44) mod(729^1258891,1891399);
  (%o44) 9

```

Figura 21 – Decodificando a mensagem

4.4 Resultados

Primeiramente foi feita a separação dos dois grupos para o desafio final, ficando cada grupo com 10 alunos. Durante a explanação da história da criptografia, foram feitas muitas observações interessantes por parte dos alunos, como: as maneiras de se interceptar a mensagem, as dificuldades que podiam ser encontradas na decifração, como deixar um código simples mais difícil de ser quebrado, dentre outros, funcionando como uma mesa redonda.

Alguns alunos mostraram que já tinham um código próprio para comunicação com amigos, assim foram desafiados a construir um código único e simples baseado no de César e depois trocar uma mensagem criptografada com este código, foi dado quinze minutos para que eles tentassem quebrar o código, sem nenhum sucesso, então eles pediram mais tempo e com trinta minutos decorridos um grupo já havia quebrado o código.

Quatro dos alunos que fazem o curso também fazem técnico em informática, assim a discussão sobre códigos binários e programas computacionais foi muito aprofundada, um dos alunos mostrou um programa simples que ele havia criado para cálculo de números primos.

Alguns tópicos que foram introduzidos pelos alunos:

1. O assassino em série Zodiaco que escreveu cartas codificadas, onde algumas não foram decifradas até hoje.
2. Cicada 3301, um desafio que surgiu em um site com vários enigmas e códigos a serem decifrados.

3. 11B x 1371, um vídeo onde aparecem mensagens para serem decodificadas, incluindo algumas em código morse.
4. criptografia quântica.

O fato desta aplicação ter sido em um programa de iniciação científica próprio para alunos que gostam de matemática não significa que ela não possa ser aplicada na sala de aula, afinal não é preciso explicar cada teorema com os alunos, porque a criptografia RSA usa restos de divisões (congruência) e potênciação.

REFERÊNCIAS

ALMEIDA, P. Q. de. **Página sobre Criptologia (Criptografia e Criptoanálise)**. Portugal, 2015. Departamento de Matemática - Faculdade de Ciências e Tecnologia - Universidade de Coimbra. Disponível em: <<http://www.mat.uc.pt/~pedro/cientificos/Cripto/>>. Citado na página 54.

ATMEL. **Entrada remota sem chave**. <http://www.atmel.com>: [s.n.], 2016. Disponível em: <<http://www.atmel.com>>. Citado na página 49.

BALLINGER, R.; RODENKIRCH, M. **Proth Search Page**. <http://prothsearch.net/>: [s.n.], 2016. Disponível em: <<http://www.prothsearch.net/>>. Citado na página 45.

BRASIL. **Parâmetros Curriculares Nacionais: matemática**. Brasília: MEC/SEF, 1997. Citado 2 vezes nas páginas 21 e 22.

BRASIL, A. **INSTITUTO BENJAMIN CONSTANT**. <http://www.ibr.gov.br/>, 2016. Disponível em: <<http://www.ibr.gov.br/>>. Citado na página 58.

CALDWELL, C. K. **The Largest Known Primes**. <https://primes.utm.edu/largest.html>: [s.n.], 2016. Disponível em: <<https://primes.utm.edu/largest.html>>. Citado na página 44.

CANTORAL, R. **Desarrollo del pensamiento matemático**. México: Trillas: ITESM, Universidade Virtual, 2003. Citado na página 22.

CARNEIRO, M. J. D.; SPIRA, M.; SABATUCCI, J. **Conteúdo Básico Comum (CBC) de Matemática no Ensino Médio**. 2016. Disponível em: <www.crv.educacao.mg.gov.br>. Citado 3 vezes nas páginas 21, 22 e 43.

CLAY, L. D.; CLAY, L. T. **Clay Mathematics Institute (CMI)**. 2016. [Http://www.claymath.org/](http://www.claymath.org/). Disponível em: <<http://www.claymath.org/>>. Citado na página 87.

COUTINHO, S. C. **Criptografia**. Rio de Janeiro: IMPA, 2008. v. 7. (Programa de Iniciação Científica - OBMEP, v. 7). Citado 4 vezes nas páginas 21, 43, 54 e 55.

_____. **Números Inteiros e Criptografia RSA**. Rio de Janeiro: IMPA, 2011. (Coleção Matemática e Aplicações). Citado 2 vezes nas páginas 51 e 62.

D'AMBROSIO, U. **Educação Matemática: da teoria à prática**. Campinas: Papirus, 1997. (Coleção Perspectiva em Educação Matemática). Citado na página 22.

DIFFIE, W.; HELLMAN, M. E. **New Directions in Cryptography**. New York, 2007. IEEE Xplore. Disponível em: <ieeexplore.ieee.org>. Citado 2 vezes nas páginas 21 e 51.

FIARRESGA, V. M. C. **Criptografia e matemática**. Universidade de Lisboa Faculdade de Ciências, Departamento de Matemática, 2010. Citado na página 53.

FONSECA, M. C. **Por que ensinar Matemática**. Belo Horizonte: Presença Pedagógica, 1995. v. 1. Citado na página 22.

GARRETT, F. **Computador mais poderoso do mundo calcula 93 quatrilhões de dados por segundo**. 2017. Techtudo. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2016/06/pc-mais-poderoso-do-mundo-calcula-93-quatrilhoes-de-dados-por-segundo.html>. Citado na página 72.

HEFEZ, A. **Iniciação à Aritmética**. Rio de Janeiro, 2005. OBMEP. Disponível em: <http://www.obmep.org.br/docs/apostila1.pdf>. Citado na página 43.

KAHN, D. **The codebreakers: The story of Secret Writing**. New York: Scribner, 1996. Citado na página 51.

KRUH, L. **A Basic Probe of the Beale Cipher as a Bamboozlement**. <http://www.tandfonline.com/doi/abs/10.1080/0161-118291857190>: [s.n.], 1982. v. 6 and 12. Citado na página 55.

LARCHER, P. H. **História Heródoto (484 A.C. - 425 A.C.)**. Rio de Janeiro: W. M. Jackson Inc., 1950. XXIII e XXIV. (Clássicos Jackson, XXIII e XXIV). Disponível em: <http://www.ebooksbrasil.org/eLibris/historiaherodoto.html>. Citado 2 vezes nas páginas 50 e 53.

MALAGUTTI, P. L. **Atividades de Contagem a partir da Criptografia**. Rio de Janeiro: IMPA, 2015. v. 10. (Programa de Iniciação científica - OBMEP, v. 10). Disponível em: <http://www.obmep.org.br/docs/apostila10.pdf>. Citado 2 vezes nas páginas 53 e 58.

MALAGUTTI, P. L. **A P versus NP**. 2017. UFSCAR. Disponível em: <http://www.dm.ufscar.br/hp/hp501/hp501001/hp501001.html>. Citado na página 89.

MARTINEZ, F. B.; MOREIRA, C. G.; SALDANHA, N.; TENGAN, E. **Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro**. 3. ed. Rio de Janeiro: IMPA, 2013. (Projeto Euclides). Citado 2 vezes nas páginas 44 e 45.

NSA, N. S. A. **Has The Beale Treasure Code Been Solved**. 2015. Disponível em: <https://www.nsa.gov/news-features/decclassified-documents/beale-papers/assets/files/doc656743.pdf>. Citado na página 55.

_____. **The Beale Papers**. <https://www.nsa.gov/news-features/decclassified-documents/beale-papers/index.shtml>: [s.n.], 2016. Disponível em: <https://www.nsa.gov/news-features/decclassified-documents/beale-papers/index.shtml>. Citado na página 56.

OEIS. **Brier numbers: numbers that are both Riesel and Sierpinski, or odd n such that for all k ≥ 1 the numbers $n \times 2^k + 1$ and $n \times 2^k - 1$ are composite**. <http://oeis.org/A076335>: [s.n.], 2016. Disponível em: <http://oeis.org/A076335>. Citado na página 45.

OLGIN, C. D. A. **Currículo no Ensino Médio: uma experiência com o tema criptografia**. Canoas: Universidade Luterana do Brasil, 2011. Citado na página 53.

RACKSPACE. **PrimeGrid**. <http://www.primegrid.com/>: [s.n.], 2016. The first managed cloud company. Disponível em: [<http://www.primegrid.com/>](http://www.primegrid.com/). Citado na página 45.

RIBENBOIM, P. **Números Primos: Velhos mistérios e novos recordes**. 1. ed. Rio de Janeiro: IMPA, 2012. (Coleção Matemática Universitária). Citado na página 35.

ROSS, T. **The Code that Failed: Testing a Bacon-Shakespeare Cipher**. 1996. The Shakespeare Authorship Page. Disponível em: <http://shakespeareauthorship.com/bacpenl.html>>. Citado na página 62.

SANTOS, J. C. **A hipótese de Riemann 150 anos**. 2017. Disponível em: http://www.fc.up.pt/mp/jcsantos/PDF/artigos/Riemann_150.pdf>. Citado na página 88.

SCOTTI, H. de S.; FERREIRA, R. F. Sistemas de numeração. **UFSC**, 9 2011. Disponível em: <http://www.inf.ufsc.br/~bosco.sobral/extensao/sistemas-de-numeracao.pdf>>. Citado na página 61.

SINGH, S. **O livro dos códigos**. Rio de Janeiro: Record, 2005. Citado 3 vezes nas páginas 50, 51 e 60.

STALLINGS, W. **Criptografia e segurança de redes**. 4. ed. São Paulo: Pearson Prentice, 2008. Citado 2 vezes nas páginas 52 e 62.

TAMAROZZI, A. C. **Codificando e decifrando mensagens**. Brasília: Ministério da Educação, Secretaria de Educação Básica, 2004. Citado na página 22.

TKOTZ, V. **O Disco de Alberti**. 2016. Disponível em: <http://www.numaboa.com.br/criptografia/127-substituicao-polialfabetica/164-alberti>>. Citado na página 60.

TRIVINOS, A. N. **Introdução à pesquisa em Ciências Sociais**. São Paulo: Atlas, 1987. Citado na página 22.

WINTERBOTHAM, F. W. **Enigma: o segredo de Hitler**. Rio de Janeiro: Biblioteca do exército, 1978. Citado na página 60.

WOLTMAN, G.; KUROWSKI, S. **GIMPS (Great Internet Mersenne Prime Search)**. <http://www.mersenne.org/primes/>: [s.n.], 2016. Disponível em: <http://www.mersenne.org/primes/>>. Citado na página 44.

PROPRIEDADE ARQUIMEDIANA

A Propriedade Arquimediana é uma propriedade do conjunto dos números \mathbb{R} que diz que $\forall x \in \mathbb{R}, \exists n \in \mathbb{N}/x < n$. A propriedade arquimediana diz simplesmente que o conjunto \mathbb{N} não admite cota superior.

Proposição 18. (A Propriedade Arquimediana). Dados números reais $0 < a < b$, existe um número natural n tal que $b < na$.

Demonstração. Suponhamos, por contradição, que $na \leq b$, para todo $n \in \mathbb{N}$. Isto implica que o conjunto $A = \{na; n \in \mathbb{N}\}$ é limitado superiormente (b é uma de suas cotas superiores). De acordo com o Postulado de Dedekind, A possui supremo, digamos α . Assim, $na \leq \alpha$, para todo $n \in \mathbb{N}$, de onde $(n+1)a \leq \alpha$, de modo que $n \leq \alpha - a$. Como $a > 0$, $\alpha - a$ seria cota superior de A , menor que o seu supremo α o que é impossível. Então, existe $n \in \mathbb{N}$ tal que $na > b$. \square

OS PROBLEMAS DO PRÊMIO MILLENNIUM

Os *Problemas do Prêmio Millennium* são sete problemas matemáticos. Até o fechamento deste trabalho havia seis problemas que ainda não tinham solução. A solução correta de um destes problemas contempla um prêmio de um milhão de dólares que o Instituto Clay de Matemática em Massachusetts, nos Estados Unidos, oferece. O site do Instituto é <http://www.claymath.org/>.

Este instituto é um fundação privada fundada em 1998 e que não tem fins lucrativos. Seu objetivo é ampliar e disseminar o conhecimento matemático promovendo premiações e patrocinando matemáticos promissores, além de organizar oficinas, conferências, etc.

Seu fundador é o empresário Landon T. Clay com sua esposa Lavinia D. Clay, financiadores (CLAY; CLAY, 2016).

Os Problemas são:

1. P versus NP;
2. A conjectura de Hodge;
3. A conjectura de Poincaré (resolvido por Grigori Perelman);
4. A hipótese de Riemann;
5. A existência de Yang-Mills e a falha na massa;
6. A existência e suavidade de Navier-Stokes;
7. A conjectura de Birch e Swinnerton-Dyer.

A conjectura de Poincaré foi resolvida pelo matemático russo Gregori Perelman no ano de 2006.

B.1 A hipótese de Riemann

Esta conjectura matemática foi publicada pela primeira vez em 1859 pelo matemático Bernhard Riemann. De acordo com Santos (2017) para que seja possível compreender o problema devemos voltar à 1650 quando foi publicado o livro *Novae quadraturae arithmeticae seu se additione fractionum*, de Pietro Mengoli.

Neste livro está presente duas séries:

$$\zeta(1) = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots \quad (\text{B.1})$$

e

$$\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \dots, \quad (\text{B.2})$$

que são importantes para a hipótese de Riemann.

No livro é demonstrado que a primeira série é divergente, levantando o problema: qual é a soma da segunda?

O problema foi proposto depois por Jacob Bernoulli, sendo intitulado na época como *problema de Basileia*, que alguns anos após este questionamento iniciou a estudar séries como:

$$\zeta(n) = 1 + \frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{4^n} + \dots \quad (\text{B.3})$$

para cada $n \in \mathbb{N} \setminus 1$.¹

Euler provou que $\zeta(2) = \frac{\pi^2}{6}$ e calculou $\zeta(n)$ para cada número natural par n , para além de ter obtido o produto euleriano:

$$\zeta(n) = \prod_p (1 - p^{-n})^{-1}, \quad (\text{B.4})$$

para qualquer $n \in \mathbb{N} \setminus 1$. Aqui o símbolo \prod_p denota o produto sobre todos os números primos. Desta forma ele mostrou que existe uma relação entre a função ζ e a distribuição dos números primos.

Assim o problema da hipótese de Riemann se resume à provar que apesar da distribuição de números primos no conjunto dos números naturais não seguir nenhum padrão regular, o matemático alemão GFB Riemann (1826-1866) observou que a frequência de números primos está muito intimamente relacionada ao comportamento da função

$$\zeta(s) = 1 + \left(\frac{1}{2}\right)^s + \left(\frac{1}{3}\right)^s + \left(\frac{1}{4}\right)^s + \dots, \quad s \in \mathbb{C}.$$

¹ \: significa *menos; sem; exceto*.

Esta função é chamada de *função Zeta de Riemann*, e a afirmação de que todas as soluções interessantes da equação $\zeta(s) = 0$ estão sobre a reta vertical $\text{Re}(s) = 1/2$ é conhecida como a famosa hipótese de Riemann. A prova desta hipótese lançará luz sobre muitos dos mistérios em torno da distribuição de números primos.

B.2 P versus NP

É um problema ligado à Ciências da Computação, entrelaçando campos desde a engenharia até a criptografia.

De acordo com [Malagutti \(2017\)](#):

A classe de algoritmos *P* é formada pelos procedimentos para os quais existe um polinômio $p(n)$ que limita o número de passos do processamento se este for iniciado com uma entrada de tamanho n . [...] Os algoritmos *NP* não se referem a procedimentos não polinomiais (na verdade isto é uma conjectura). A leitura correta para procedimentos *NP* é dizer que se referem a algoritmos "não-determinísticos polinomiais" no tempo. [...] A classe dos problemas *NP* é aquela para as quais podemos verificar, em tempo polinomial, se uma possível solução é correta.

Como exemplo: queremos descobrir se um número é primo ou composto, mas não existe um modo rápido para descobrir isso ou descobrir sua fatoração, um dos métodos é o Crivo de Eratóstenes que testa os possíveis divisores, mas isso dá muito trabalho até para um computador, demandando muito tempo, contudo se fosse possível uma certificação que apenas validasse se algo é resposta ou não isso seria mais simples que testar todos os resultados possíveis.

Outro exemplo: suponha que precisaremos dividir um grupo de pessoas em duplas, mas nem todas são compatíveis umas com as outras, tentar todas as possibilidades não é uma alternativa, este é um problema em que há algoritmos eficientes para solucioná-lo e por isso está na classe *P* de "Tempo Determinístico Polinomial". Inclusive foi resolvido por Jack Edmonds em 1965 ajudando a definir o que é computação eficiente.

Agora vamos reformular o mesmo problema: queremos dividir as pessoas em trios nos quais todos os pares delas são compatíveis (partição em triângulos). Neste caso não há um algoritmo eficiente, dada uma solução qualquer, é possível conferir a solução de maneira eficiente: este tipo de problema que possui soluções verificáveis em tempo polinomial define a classe *NP*: de "Tempo Polinomial Não Determinístico". Além disso somente uma Máquina de Turing Não Determinística pode resolvê-lo.

O problema *N versus NP* se refere à prova de que $P \neq NP$ dado as descobertas que foram feitas através do tempo é o que grande parte dos cientistas da computação passou a acreditar, mas é preciso provar. Por isso é um dos problemas mais importantes da ciência da computação e da matemática.

Há a possibilidade de $P = NP$: “O que ganharíamos com $P = NP$ faria com que a Internet inteira parecer apenas um rodapé na história” - Fortnow, L. 2009. Neste caso muitas tarefas de logística se tornariam triviais como: o transporte de pessoas ou produtos seria mais rápido e mais barato, previsões de tempo, terremoto e tsunamis, sem contar que a criptografia não teria mais função, isso porque ela se baseia em problemas difíceis de serem resolvidos, no caso da RSA: a fatoração de números muito grandes em números primos, mas se isso for um problema trivial ela é quebrada facilmente.

Um filme que retrata o impacto deste problema é *Travelling Salesman* ou *O caixeiro viajante*, de 2012, dirigido por Timothy Lanzone, conta a história de quatro matemáticos que descobrem um algoritmo eficiente para o Problema do Caixeiro Viajante, um problema NP -Completo, implicando em consequências drásticas para qualquer sistema de segurança virtual no planeta.

B.3 Curiosidades

Estes problemas já apareceram em alguns seriados famosos, como *NUMB3RS*, produzido pela rede americana CBS, seriado estrelado em 2005 onde um matemático ajuda agentes do FBI a solucionar crimes. Foi produzido somente seis temporadas, representando a matemática e como ela pode ser aplicada.

Em sua primeira temporada, no episódio 5, a filha de um matemático que supostamente havia resolvido a hipótese de Riemann é sequestrada, abordando assim os temas: criptografia, a Hipótese de Riemann e as consequências de sua solução, assim como os problemas do Millennium. Para amantes de números é um seriado interessante, explorando vários campos da matemática.

Também apareceu em *Elementary*, também produzido pela rede americana CBS, iniciada em 2012 ela representa uma nova versão de Sherlock Holmes, criado por Arthur Conan Doyle, contudo desta vez as histórias se passam nos Estados Unidos. Possui até o momento cinco temporadas.

A criptografia aparece no episódio 2 (Solve for X) da segunda temporada, onde o episódio começa com a morte de um matemático, abordando o problema P versus NP , criptografia, suas implicações para a comunidade científica.

Sherlock é outro seriado baseado no detetive criado por Sir Arthur Conan Doyle, sendo uma co-produção da British Broadcasting Corporation (BBC), a segunda temporada tem em seu primeiro episódio uma mensagem aparentemente indecifrável, contudo Holmes a decifra em oito segundos.

No seriado *Bones*, exibido pela FOX nos Estados Unidos, a criptografia é abordada na sétima temporada, episódio 6, onde é preciso decifrar vários códigos deixados por um

assassino em série.

Já no seriado *Hawaii Five-0* o tema é abordado na primeira temporada, episódio 19, onde falam sobre a facilidade em quebrar uma criptografia de 64 bits e novamente na terceira temporada, episódio 7, onde eles lidam com hackers e precisam de uma senha para quebrar uma criptografia de 1024 bits (que levaria meses para ser quebrada e era preciso urgentemente), além de outros.

No seriado *Prison Break*, segunda temporada, episódio 15, um dos protagonistas precisa enviar uma mensagem, então ele codifica-a para que só seu destinatário compreenda, além disso é abordado o código morse.

O livro *Zodíaco* escrito por Robert Graysmith, aborda sobre um serial killer que aterrorizou a cidade de São Francisco em 1968, deixou várias cartas codificadas, algumas não foram decodificadas até hoje, a revista *Mundo Estranho* traz uma reportagem sobre isso: <http://mundoestranho.abril.com.br/cultura/as-outras-cartas-do-serial-killer-zodiaco/>. Um filme também foi feito: *Zodíaco*, lançado em 2007 com direção de David Fincher.

Os clássicos livros sobre o investigador Sherlock Holmes e seu parceiro Watson, escrito por Arthur Conan Doyle, também trazem o tema, no livro *O vale do Terror* os investigadores são chamados à uma casa de campo através de uma mensagem codificada. O investigador Holmes adora quebra-cabeças, outra mensagem assim aparece em *O regresso de Sherlock Holmes*.

A revista *Super Interessante* fez uma reportagem em 31/10/2016 intitulada *O segredo da criptografia*, é possível acessá-la em <http://super.abril.com.br/tecnologia/o-segredo-da-criptografia/>, que traz algumas curiosidades sobre o tema. Em abril de 2016 foi usado 9500 computadores e quatro meses para quebrar um código, mostrando o quanto um bom código é importante para que seja possível guardar um segredo ou algo importante através da criptografia.