



Luiz Gustavo Benedito de Sousa

# Criptografia: a arte de ocultar

**Santo André, Novembro de 2015**



**Universidade Federal do ABC**

**Centro de Matemática, Computação e Cognição**

**Luiz Gustavo Benedito de Sousa**

# Criptografia: a arte de ocultar

**Orientador:** Prof. Dr. Daniel Miranda Machado

Dissertação de mestrado apresentada ao Centro de Matemática, Computação e Cognição para obtenção do título de Mestre em Matemática pelo PROFMAT.

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por Luiz Gustavo Benedito de Sousa e aprovada pela comissão julgadora.

**Santo André, Novembro de 2015**

Este exemplar foi revisado e alterado em relação à versão original, de acordo com as observações levantadas pela banca no dia da defesa, sob responsabilidade única do autor e com a anuência de seu orientador.
Santo André, ____de _____ de 20___.
Assinatura do autor: _____
Assinatura do orientador: _____

# Resumo

Este trabalho buscou na criptografia uma nova abordagem para ilustrar e exemplificar os conceitos de funções e aritmética modular no ensino médio. Nesse intuito discorremos sobre as cifras de substituição, César, transposição, colunas, disco de cifras, Poli-alfabéticas, divisibilidade dos números, crivo de Eratóstenes, algoritmo estendido de Euclides, chave simétrica, pública, assimétrica, função de mão única R.S.A, compartilhamento de segredo. Na sequência apresentamos também algumas atividades envolvendo função inversa, aritmética modular, cifra de César, Vigenère, protocolo de compartilhamento de segredos de Shamir para o uso em sala de aula.

**Palavras-chaves:** Aritmética Modular, Função e Criptografia.

# Abstract

This study aimed to present cryptography as a means to illustrate and exemplify the concepts of functions and modular arithmetic in high school using cryptography. To that end we present the substitution ciphers , Caesar, transposition , columns, cipher disk , poly alpha , divisibility of numbers, Eratosthenes sieve the extended algorithm of Euclid , symmetric key , public , asymmetrical, one-way function RSA , sharing secret. Following we present some activities involving inverse function , modular arithmetic, Caesar cipher , Vigenere , Shamir's secret sharing protocol for use in the classroom.

**Keywords:** Modular Arithmetic, Function e Cryptography.

# Agradecimentos


- A Deus em primeiro lugar.
- Ao professor Dr. Daniel Miranda pela paciência.
- A minha querida esposa e filhas, pela paciência dos finais de semana empregados na dedicação desde trabalho.
- Aos colegas do Profmat em especial a colega Marceli que me recebeu em sua casa no curso de verão.
- Nossa senhora de Aparecida pela proteção na estrada no longo caminho percorrido.

# Sumário

# Lista de Figuras

# Lista de Tabelas

# 1 Introdução.

Desde pequeno, me intrigo: como pesquisadores do mundo inteiro descobrem fatos de civilizações antigas, como decifram textos escritos com símbolos? Nessa empolgação em descobrir segredos de textos antigos, de mensagens cifradas é que vou descrever sobre criptografia e sua aplicação em sala de aula, como fonte motivadora. Utilizarei essa fonte inspiradora para surpreender os alunos de forma a tornar a aula de matemática mais agradável e quiçá mais próxima da pratica da matemática corrente.

Em especial, esperamos que a posse de algumas ferramentas apresentadas nesse texto torne o ensino mais coeso. Nesse sentido observamos que o conceito de divisibilidade é trabalhado de forma desconexa, pois ao ensinar a divisão de um número pelo outro, o resto não possui aplicabilidade mas quando utilizamos a congruência esta nos possibilita mostrar critérios de divisibilidade que a maioria dos professores desconhece, e melhor ainda as demostrações feitas utilizando a congruência são de fácil compreensão. Outro conteúdo trabalhado no ensino médio é a função inversa; essa literalmente é transmitida aos alunos, quase sempre sem nenhuma aplicação. Isso poderia ser o contrário se o professor relacionasse como uma função de mão dupla ou seja, quando se utiliza a criptografia para relacionar a aplicação da função inversa os alunos ficam boquiabertos pois uma função que aparentemente não tem aplicação nenhuma transforma-se na diversão da turma em criar textos criptografados e ao mesmo tempo decifrá-los. A análise de frequência é uma outra boa aplicação no ensino médio para trabalhar porcentagem com os alunos pois ao fazer a contagem das letras e comparar com a porcentagem que cada letra aparece no nosso alfabeto os alunos conseguem decifrar mensagens antes impossíveis ao seu olhar.

Assim este trabalho descreve no terceiro e quinto capítulo um pouco de teoria dos números: propriedades da divisão, M.D.C. e critérios de divisibilidade que são mais utilizados no dia a dia do professor e do aluno, uma pequena definição de função afim e inversa e principalmente uma descrição da evolução da criptografia e suas aplicabilidades no ensino fundamental e médio de maneira criativa e quiçá inspiradora.

# 2 Arte de ocultar

A origem do termo criptografia vem do Grego kryptós, significa "escondido", e gráphein, "escrita". A criptografia estuda métodos para codificar uma mensagem de modo que somente seu destinatário legítimo consiga interpretá-la, mesmo quando transmitida em qualquer canal público de comunicação.

Dois conceitos, decifrar e decodificar que serão utilizados no decorrer do texto podem causar alguma confusão logo iremos definir.

**Definição 1.** A **decodificação** é o processo de revelação da mensagem por parte do destinatário, ou usuário legítimo.

**Definição 2.** A **decifração** é processo de revelação da mensagem por outra pessoa que não é destinatário da mensagem.

*Observação* 3. Contudo, a necessidade de se salvaguardar uma mensagem é tão antiga quanto a própria escrita, e foi utilizada para diversas finalidades, tanto para o bem quanto para mal. Nesse sentido, há aproximadamente 4000 anos, surgiram os primeiros registros de criptografia, que consistiam em hieróglifos, os quais eram utilizados por membros da nobreza egípcia, em seus túmulos, no Antigo Egito. Também, em diferentes civilizações, observou-se a utilização da criptografia como a Cifra Atbash, Albam e Atbah pelos hebreus, Bastão de Licurgo ou Cítalo pelos espartanos e Cifra de Políbio, em 200 a.C. (Fiarresga, 2010).

## 2.1 Cifra

**Definição 4.** O processo de **cifragem** é a modificação da mensagem original, sendo que quem a interceptar e não souber como reproduzir a mensagem original, não consiga decifrar.

Existe vários tipos: cifra de substituição ou mono-alfabética, transposição, polialfabética, homofônica e poligrâmicas. Conforme a tabela 2.1, tem-se um texto original, com um algoritmo cifra o texto e com o mesmo ou outro algoritmo dependendo da cifragem retorna-se ao texto original.

## 2.2 Cifra de Substituição.

**Definição 5.** Uma cifra **mono-alfabética** ou cifra de **substituição**, é um processo que consiste em substituir cada carácter de um texto por outras letras, símbolos,

| | **algoritmo** | | **algoritmo** | |
|---|---|---|---|---|
| **texto original** | → | **texto cifrado** | → | **texto original** |

**Tabela 2.1:** Algoritmo de Cifra

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

**Tabela 2.2:** Método da Substituição.

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

**Tabela 2.3:** Cifra de César.[1]

números, figuras, etc.

Um exemplo seria trocar uma letra pela duas próximas letras do alfabeto. A cifra é fundamental na criptografia, ela é um algoritmo e toda a cifra deve ser acompanhada de uma chave que especifica os detalhes exatos da codificação.

Com base na tabela do método da substituição 2.2 iremos codificar a mensagem: " A matemática é a nossa vida" , trocando as letras, fica dessa maneira " L xlepxletnl p l yzddl gtol".

### 2.2.1 Cifra de César

Por volta do século 60 a.C. um dos sistemas criptográficos mais famosos foi utilizado por Júlio César, o qual foi intitulado de Cifra de César.

**Definição 6.** A Cifra de **César** é um processo que consiste na substituição das letras do alfabeto simples por outras letras do próprio alfabeto, sendo que a substituição é feita conforme uma tabela.

Um exemplo de tabela de César é apresentada na Tabela 2.3.

Dessa forma, a comunicação de César com seus generais seguia um padrão bem estipulado. Este método empregado é conhecido como substituição simples.

Assim podemos associar uma função matemática que relaciona cada letra a um número, conforme veremos a seguir.

Iremos utilizar a função $f(x) = x+3$ para criar a cifra de César, pois se relacionarmos $x$ com cada letra do alfabeto transformando-as em números teremos conforme a tabela 2.4.

**Exemplo 7.** Vamos cifrar a mensagem "A matemática".

Utilizando a tabela 2.3 podemos cifrar a mensagem da seguinte forma " D pdwhpd-wlfd"

Para decodificar teremos que utilizar a função inversa para retornar a função original.

**Exemplo 8.** Utilizando a função $f^{-1}(x) = x - 3$ vamos decifrar a mensagem "D pdwhpdwlfd"

| **Alfabeto** | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **valor de cada letra** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| **Alfabeto** | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | $\cdots$ |
| **valor de cada letra** | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | $\cdots$ |
| **APLICANDO A FUNÇÃO** $f(x) = x + 3$ | | | | | | | | | | | | | | | |
| **Alfabeto** | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| **valor de cada letra** | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| **Alfabeto** | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | $\cdots$ |
| **valor de cada letra** | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | $\cdots$ |

**Tabela 2.4:** Função da Cifra de César

| **Aplicando a função inversa retornaremos a mensagem original** | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Alfabeto** | A | B | C | D | E | F | G | H | I | J | K | L | M |
| **cifrado** | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| $f(x)^{-1} = x - 3$ | | | | | | | | | | | | | |
| **decodificado** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| **Alfabeto** | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| **cifrado** | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| $f(x)^{-1} = x - 3$ | | | | | | | | | | | | | |
| **decodificado** | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

**Tabela 2.5:** Função Inversa

| **Entrada** | **valor da letra** | $f(x)^{-1} = x - 3$ | **Saída** | **Decodificado** |
|---|---|---|---|---|
| d | 3 | $f(3)^{-1} = 3 - 3$ | 0 | a |
| | | | | |
| p | 15 | $f(15)^{-1} = 15 - 3$ | 12 | m |
| d | 3 | $f(3)^{-1} = 3 - 3$ | 0 | a |
| w | 22 | $f(22)^{-1} = 22 - 3$ | 19 | t |
| h | 7 | $f(7)^{-1} = 7 - 3$ | 4 | e |
| p | 15 | $f(15)^{-1} = 15 - 3$ | 12 | m |
| d | 3 | $f(3)^{-1} = 3 - 3$ | 0 | a |
| w | 22 | $f(22)^{-1} = 22 - 3$ | 19 | t |
| l | 11 | $f(11)^{-1} = 11 - 3$ | 8 | i |
| f | 5 | $f(5)^{-1} = 5 - 3$ | 2 | c |
| d | 3 | $f(3)^{-1} = 3 - 3$ | 0 | a |

**Tabela 2.6:** Decodificação

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

**Tabela 2.7:** Frequência Relativa das Letras na Língua Portuguesa.[1]

Mas a frente voltaremos a utilizar a cifra de César utilizando a congruência como ferramenta para codificar e decodificar uma mensagem.

No entanto uma das limitações do método de substituição simples é que em boa parte das línguas, algumas letras costumam ser utilizadas em maior frequência em blocos. Isso faz com que a frequência utilizada das palavras seja distinta. Na década de 80, al-Kindi descreveu um método utilizando a análise de frequência, assim com o conhecimento das frequências é possível decifrar qualquer texto sabendo a frequência relativa de cada letra. Contudo, Fiarresga (2010) ressalta que em cada língua, quando se faz a contagem do número de vezes que cada letra aparece em textos longos, observa-se que cada letra tem uma determinada frequência relativa. Deste modo, a língua portuguesa tem conforme a tabela 2.7:

## 2.3 Transposição

**Definição 9.** A **transposição** é um método criptográfico baseado na troca de posição das letras.

A transposição é um método relativamente inseguro pois possui um número limitado de possibilidades para organizar as letras. A transposição sem nenhuma regra específica, tornará a mensagem com uma boa segurança, mas vai gerar um trabalho árduo para o destinatário. Assim deve ser previamente combinado entre o emitente e o destinatário, facilitando a vida de quem organizará a mensagem.

**Exemplo 10.** Vamos cifrar a palavra “ali”.

Utilizando o método da transposição teremos: ila; ial; ail; lai; lia.

**Exemplo 11.** Vamos cifrar a a palavra “Otorrinolaringologista”.

Ela possui nada a menos que 22 letras ou seja para calcular todas as variações teríamos de efetuar o cálculo de $\frac{22!}{5!\cdot 2!\cdot 3!\cdot 3!\cdot 2!\cdot 2!\cdot 2!\cdot 2!}$, que é um número gigantesco (8130792301632000).

A transposição sem nenhuma regra específica, tornará a mensagem com uma boa segurança, mas vai gerar um trabalho árduo para o destinatário. Assim deve ser previamente combinado entre o emitente e o destinatário, facilitando a vida de quem organizará a mensagem.

Citale espartano era um aparelho criptográfico militar para realizar a transposição, criado no séc. V a.C. O Citale era constituído de madeira e à sua volta enrolava-se uma tira de couro conforme a figura 2.1. O funcionamento do Citale era bem simples, bastava o remetente escrever a mensagem ao longo do comprimento do instrumento e depois desenrolava a fita, formando uma mensagem contendo letras sem sentido. Para

**Fig. 2.1:** Citale Espartano [8]

decodificar a mensagem o destinatário deveria possuir um Citale contendo o mesmo diâmetro do que foi usado pelo remetente, e simplesmente enrolava a tira em volta do bastão, formando assim a mensagem. Assim como o método de substituição simples, a transposição tem como principal problema a grande variedade de chaves entre os usuários para se decodificar a mensagem.

**Definição 12. Anagrama** é uma palavra formada pela transposição de uma palavra ou frase..

**Proposição 13.** *O número de permutação de* $\mathsf{k}$ *elementos distintos é* $\mathsf{k!}$

*Demonstração.* Utilizando a formula de arranjo temos que $\mathsf{A(k,k)} = \frac{\mathsf{k!}}{\mathsf{(k-k)!}} = \mathsf{k!}$, o que mostra que a permutação de $\mathsf{k}$ elementos distintos é $\mathsf{k!}$. □

**Proposição 14.** *O numero de anagramas com os caracteres repetidos é* $\frac{\mathsf{k!}}{\mathsf{k_1!\cdot k_2!\cdot\cdots\cdot k_n!}}$, *nos quais* $\mathsf{k_i}$ *são os elementos repetidos.*

**Exemplo 15.** Quantos anagramas possui a palavra " CRIPTOGRAFIA"?

Como criptografia possui 12 letras e duas letras $\mathtt{r}$ repetidas, duas letras $\mathtt{i}$ repetidas e duas letras $\mathtt{a}$ repetidas, assim teremos : $\frac{12!}{2!\cdot 2!\cdot 2!} = \frac{479001600}{8} = 59875200$

### 2.3.1 Transposição das Colunas

**Definição 16.** A **transposição das colunas** é um método de escrever a mensagem em linhas, sendo que a primeira linha utiliza uma chave, sendo esta a que irá orientar a escrita codificada, e as próximas linhas segue a mensagem a ser codificada, conforme o exemplo 2.8.

A escrita deve seguir um critério pré determinado, em nosso exemplo utilizaremos a chave em ordem alfabética para procedermos a codificação. Vamos codificar a mensagem " estamos sendo atacados", observando a tabela 2.8, sendo que a nossa chave será "segredo"

A mensagem codificada "doas esec emoo gtna osta radd sesa" como a cifra de colunas a transposição de colunas é muito simples de ser descoberta.

Em 1466, foi desenvolvido um sistema no qual combinava a substituição de letras e a transposição. Esse método ficou conhecido como Disco de Alberti.

| | | | | | | |
|---|---|---|---|---|---|---|
| s | e | g | r | e | d | o |
| e | s | t | a | m | o | s |
| s | e | n | d | o | a | t |
| a | c | a | d | o | s | a |

**Tabela 2.8:** Transposição de Colunas

| **DISCO MAIOR** | A | B | C | D | E | F | G | I | l | M | N | O | P |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **DISCO MENOR ( já posicionado)** | c | & | b | m | d | g | p | f | z | n | x | y | v |
| **DISCO MAIOR** | Q | R | S | T | V | X | Z | 1 | 2 | 3 | 4 | | |
| **DISCO MENOR ( já posicionado)** | t | o | s | k | e | r | l | h | a | i | q | | |

**Tabela 2.9:** Disco de Cifragem de Alberti

## 2.4 Disco de Cifra

Tal nome se deve ao seu desenvolvedor, o arquiteto italiano Leone Battista Alberti, o qual foi considerado o pai da criptologia ocidental ([1]). Para se utilizar esse método é necessário um disco.

**Definição 17.** O **disco de cifra** é constituído por dois discos concêntricos e de raios diferentes. O disco maior é fixo, e o menor móvel, conforme a figura 2.2.

Dessa forma, tornou-se necessário que tanto o emissor quanto o receptor da mensagem possuíssem os discos. A codificação é realizada de modo que o emissor escolhe uma letra chave do disco maior e a posicione e combine com uma letra qualquer do disco menor. Assim, a letra da mensagem, que está no disco maior será substituída pela letra do disco menor. De forma análoga será realizado em todas as outras letras da mensagem.

**Exemplo 18.** Vamos descrever um método de cifragem utilizando o disco, lembrando que podemos ter varias formas de cifrar pois dependerá da escolha da posição inicial do disco menor.

Vamos cifrar a mensagem, "O traidor é o tenente", vamos observar a tabela 2.9 que facilitará nossa cifragem.

- Eliminando os espaços e acentos obtemos: "Otraidoreotenente"
- cifrando letra a letra temos: "ykocfmyodykdxdxkd".
- Para decodificar a mensagem o destinatário deverá saber a posição inicial para realizar a mesma.

## 2.5 Cifras Poli-alfabéticas

Em 1518 Johannes Trithemius desenvolveu um método em seu livro Poligrafia, de cifras Poli-alfabéticas que consiste em uma tabela quadrada. Essa tabela intitulou-se de Tabula recta. A tabula consiste na inserção do alfabeto completo na primeira

**Fig. 2.2:** Disco de Cifra [5]

linha e na primeira coluna. A partir de então insere-se nas linhas e colunas restantes o alfabeto de modo circular conforme a figura 2.3. Um grande marco na história da criptografia é dado quando o italiano Giovannni Battista Bellaso, introduz o conceito de chaves para se codificar e decodificar uma mensagem. Dessa forma, o método da tabula recta foi utilizado com palavras ou sequência de letras ou frases para se decodificar uma informação. O francês Blaise de Vigenère, em sua publicação, em 1586, descreve o método de Belasso, o qual, acaba inapropriadamente chamado de sistema Vigenère. No entanto, o francês adicionou uma peculiaridade: a auto chave. A auto chave consiste de que o próprio texto é usado como chave, ([1]). Os principais problemas desses sistemas são primeiramente que a codificação/decodificação deverá ser realizada letra a letra, o que torna o processo bastante trabalhoso.

**Definição 19.** Cifra **Poli-alfabética** é a utilização de vários alfabetos para cifrar uma mensagem, dificultando assim a quebra da cifra através da análise de frequência.

A cifra de Vigenère utiliza vários alfabetos para codificar uma mensagem sendo necessário uma chave que combinada com o texto gera aleatoriamente um texto cifrado, assim conforme a figura 2.3, cada letra da mensagem a ser codificada observa-se a linha e cada letra da chave observa-se a coluna a intersecção entre a linha e a coluna é a letra cifrada.

A cifra de Vigenère dificulta a quebra por analise de frequência, ela é conhecida como polialfabética, pois utiliza vários alfabetos. Mas a frente será apresentado uma atividade utilizando a cifra de Vigenère com aritmética modular.

**Exemplo 20.** Vamos utilizar a tabela 2.3 para codificar a mensagem "O traidor é o tenente" e precisamos de uma chave que será "O professor Daniel", para facilitar a compreensão vamos observar a tabela 2.10, assim observamos a tabela 2.3 letra correspondente da mensagem na linha e a letra correspondente na coluna, assim a intersecção será a letra cifrada. Na codificação feita na tabela 2.10 observamos a letra "o" na linha e a letra "o" na coluna assim a intersecção será a letra c, o mesmo acontece letra a letra.

Além da cifra de Vigenère outra cifra é a homofônica esse método de cifragem, cada letra é substituída por vários substitutos, sendo proporcional a frequência da letra.

| | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **mensagem** | o | | t | r | a | i | d | o | r | | e | | o | | t | e | n | e | n | t | e |
| **chave** | o | | p | r | o | f | e | s | s | | o | | r | | d | a | n | i | e | l | o |
| **cifrado** | c | | i | i | o | n | h | g | j | | s | | f | | w | e | a | m | r | e | s |

**Tabela 2.10:** Codificação Utilizando a Cifra de Vigenère

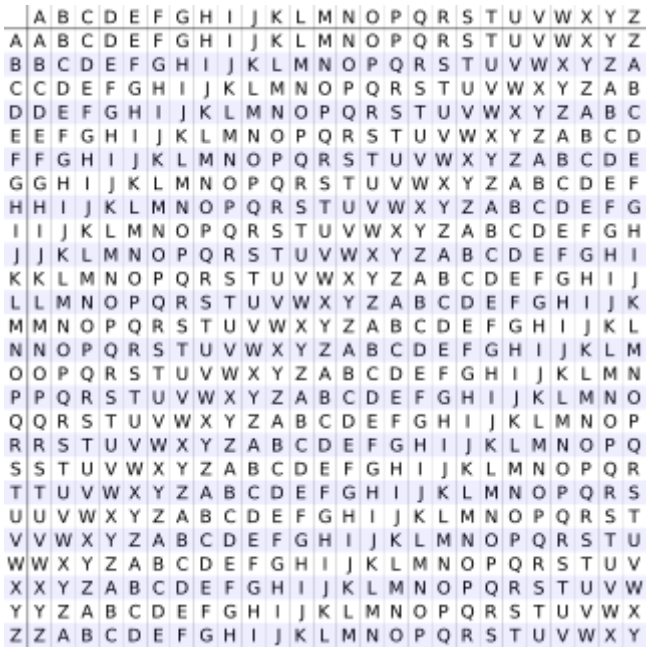


**Fig. 2.3:** Cifra de Vigenère [7]

Por exemplo, a letra "a" corresponde a $14,63\%$ de todas as letras que aparecem num texto em português, logo este possuirá quatorze símbolos para representá-lo. Caso, por exemplo, a letra "e" $12,57\%$ corresponda de um texto em português, este possuirá doze símbolos para representá-lo.

## 2.6 Código

**Definição 21.** O código é um processo que consiste na substituição de uma palavra ou frase, por um símbolo, número ou outra palavra pré fixada.

Na região sudeste quando se joga truco, ( jogo de cartas), combina-se alguns sinais para representar as cartas, sem que o adversário descubra. Um outro exemplo clássico é o código utilizado pelos policiais no radio ao transmitir uma placa para a central, cada letra corresponde a uma palavra ou seja N em uma placa o policial fala navio, M de macaco e assim por diante.

## 2.7 Enigma

Durante a segunda guerra mundial, as cifras ganharam destaques às comunicações e sua quebra foi fundamental para a história mundial. Famosa máquina eletromecânica Enigma inventada pelo alemão Arthur Scherbius e seu amigo Richard Ritter em 1918, fundadores da empresa Scherbius & Ritter. Como o sistema era complexo, os alemães estavam convictos da segurança da troca de informações. A grosso modo, o sistema desenvolvido era bem complexo e de acordo com [1] embaralhava as letras da mensagem original através de um circuito que era ajustado através de uma chave trocada diariamente. A máquina, possuía três elementos básicos ligados por fios, sendo um mostrador contendo várias lâmpadas para indicar a letra cifrada, um teclado para a entrada das letras do texto original, uma unidade misturadora que cifra cada letra. A máquina enigma com três misturadores possuía $26 \cdot 26 \cdot 26$ posições iniciais para cada letra, mesmo uma pessoa com uma máquina enigma, ao interceptar uma mensagem, se não possuísse a disposição inicial seria difícil decifrar.

**Fig. 2.4:** Máquina Enigma [6]

# 3 Fundamentos da Teoria dos Números

Para o estudo matemático da criptografia é fundamental o entendimento de certas propriedades da divisão dos números.

## 3.1 Divisibilidade

Vamos estabelecer algumas propriedades para efetuar a divisão de dois números no conjunto dos inteiros.

**Definição 22.** Dados dois números $a$ e $b \in \mathbb{Z}$, diz-se que $a$ divide $b$, e escreve-se $a|b$, quando existir $q \in \mathbb{Z}$ tal que $b = a \cdot q$, nesse caso diremos também que $a$ é um divisor e $b$ é múltiplo de $a$, então $b$ é divisível por $a$.

Então podemos afirmar que $b$ é múltiplo de $a$, logo $a$ é fator de $b$.

**Proposição 23.** *Se* $a|b$ *e* $b|c$*, então* $a|c$.

*Demonstração.* Se $a|b$ e $b|c$, então existem $f$ e $g \in \mathbb{Z}$, tais que $b = a \cdot f$ e $c = b \cdot g$. O que implica que $c = b \cdot g = (a \cdot f) \cdot g = a \cdot (f \cdot g)$. □

**Proposição 24.** *Sejam* $a, b, c$*, e* $f$ *números inteiros. Se* $a|b$*, com* $a \neq 0$ *então* $a \cdot c | b \cdot c$*, qualquer que seja* $c$.

*Demonstração.* Se $a|b$, então existe um $f \in \mathbb{Z}$ tal que $b = a \cdot f$. Pelo que, $b \cdot c = (a \cdot f) \cdot c = f \cdot (a \cdot c)$.
Se $a|b$ e $b \neq 0$, existe $f \in \mathbb{Z}$ e $f \neq 0$ tal que $b = a \cdot f$. então $| b | = | a \cdot f | \geqslant | a |$. □

**Proposição 25.** *Sejam* $a, b$*, e* $c$ *números inteiros. Se* $a|b$ *e* $a|c$*, então* $a|(x \cdot b + y \cdot c)$*,* $\forall x$ *e* $y \in \mathbb{Z}$.

*Demonstração.* Se $a|b$ e $a|c$, então existem $f$ e $g \in \mathbb{Z}$ tais que $b = f \cdot a$ e $c = g \cdot a$. O que implica que $x \cdot b + y \cdot c = x \cdot f \cdot a + y \cdot g \cdot a = (x \cdot f + y \cdot g) \cdot a$. □

**Exemplo 26.** Sendo $a = 10$, $b = 20$, $c = 30$, $x = 2$ e $y = 3$, assim $10 \mid 20$ e $10 \mid 30$ então $10 \mid (2 \cdot 20 + 3 \cdot 30)$.

No conjunto dos números naturais incluindo o zero a divisibilidade é uma relação de ordem:

1. Reflexiva, ou seja qualquer que seja $a \in \mathbb{N}$ $a|a$.
2. Transitiva, $a \mid b$ e $b \mid c$, assim $a \mid c$ .
3. Antissimétrica, $a \mid b$ e $b \mid a$, logo $a = b$.

Já no conjunto dos inteiros a divisibilidade não é uma relação de ordem, mesmo sendo reflexiva e transitiva ela não é antissimétrica. Exemplificando, temos $2 \mid -2$ e $-2 \mid 2$ mas $2 \neq -2$.

**Proposição 27.** *Sejam* $a$ *e* $b \in \mathbb{Z}$. *e* $n \in \mathbb{N}$ *Temos que* $a - b \mid a^n - b^n$.

*Demonstração.* Para fazer a prova utilizaremos o método de indução.

Para $n = 1$ temos $a-b \mid a^1-b^1$que é verdadeira. Vamos admitir que $a-b \mid a^n-b^n$ é verdadeira para para algum $n \in \mathbb{N}$.

Agora vamos mostrar para $n + 1$. Assim temos $a - b \mid a^{n+1} - b^{n+1} \rightarrow a - b \mid a \cdot a^n - b \cdot a^n + b \cdot a^n - b \cdot b^n = (a - b) \cdot a^n + b \cdot (a^n - b^n)$, o que mostra que $a - b \mid a^{n+1} - b^{n+1}$ pois $a - b \mid a - b$ e por hipótese $a - b \mid a^n - b^n$. □

**Exemplo 28.** Vamos mostrar que $10 \mid 11^n - 1$, $\forall n \in \mathbb{N}$, utilizando a proposição 27 temos $a - b \mid a^n - b^n$,observando temos $a = 11$ e $b = 1$, assim $11 - 1 \mid 11^n - 1$.

Logo quando efetuamos uma divisão possuímos dois números $q$ e $r$ , sendo $q$ e $r \in \mathbb{N}$, chamamos então $q$ de quociente e $r$ de resto, obtendo assim $a = q \cdot b + r$. É importante definir a divisão, pois mais a frente utilizaremos uma poderosa arma para solucionar grandes problemas somente olhando para o resto.

**Exemplo 29.** A divisão de $3 \mid 10$ resulta em um $q = 3$ e $r = 1$, pois $10 = 3 \cdot 3 + 1$.

## 3.2 Máximo Divisor Comum

**Proposição 30.** *Dados dois números não nulos* $m$ *e* $n \in \mathbb{Z}$, se existir um número $p \in \mathbb{N}$ que divide $m$ e $n$ dizemos que $p$ é divisor comum.

*Demonstração.* $p \mid n$ então existe um $k \in \mathbb{Z}$ tal que $n = p \cdot k$ o mesmo acontece com $p \mid m$ existe um $j$ tal que $m = j \cdot p$ , assim $p$ é divisor comum de $m$ e $n$. □

**Exemplo 31.** $\pm 1, \pm 2, \pm 3 \pm 4 \pm 6 \pm 8, \pm 12, \pm 24$ são os divisores comuns de 24 e 48.

**Definição 32.** O máximo divisor comum, "m.d.c", entre dois números inteiros $a$ e $b$, sendo $a$ ou $b$ diferente de zero, é o maior elemento do conjunto dos divisores de $a$ e $b$ e será representado por $(a, b)$

**Proposição 33.** *Se* $a \neq 0$ *e* $d$ *for um divisor comum de* $a$ *e de* $b$*, então* $|d| \leqslant |a|$ *e* $|d| \leqslant |b|$ . *Então o conjunto* $d = (a, b)$ *é limitado superiormente e deve ter um elemento máximo, ou seja, existe um divisor comum de* $a$ *e* $b$ *maior que todos os demais. Dessa maneira para* $b \neq 0$*, o conjunto* $d = (a, b)$ *também tem um elemento máximo. Assim se* $d = (a, b)$ *não é limitado superiormente é o conjunto* $d(0, 0)$*, já que zero é múltiplo de qualquer inteiro não nulo.*

*Demonstração.* Um inteiro, não negativo, $d$ é o máximo divisor comum dos números inteiros $a$ e $b$, se: □

- $d \mid a$ e $d \mid b$ (assim $d$ é um divisor comum);
- Seja $c$ um divisor qualquer de $a$ e $b$, logo $c \mid a$ e $c \mid b$ se $c \mid d$ (assim, $d$ é o maior dos divisores comuns).

- Se $d$ é um m.d.c de $a$ e $b$ e seja $c$ é um divisor comum desses números, então $c < d$. O que nos mostra que $d$ é o máximo divisor comum de $a$ e $b$.

**Exemplo 34.** Qual é o máximo divisor comum entre 9 e 30?

Sendo $W$ o conjunto dos divisores de 9 e $J$ o conjunto dos divisores de 30, temos $W = \{1, 3, 9\}$ e $J = \{1, 3, 5, 6, 10, 15, 30\}$, observando os dois conjuntos temos que o máximo divisor comum de 9 e 30 é 3 , pois 3 é o maior número que divide ao mesmo tempo 9 e 30.

**Proposição 35.** *Seja $d$ o máximo divisor comum de dois números, se existir ele é único.*

*Demonstração.* Vamos supor por absurdo que exista dois valores para o $m.d.c$ de $a$ e $b$ um $d$ é um $d'$, pela definição temos que $d$ é maior de todos logo $d > d'$, mas como $d'$ também é o $m.d.c$ fica que $d' > d$, o que torna numa contradição, então $d$ se existir é único. □

**Exemplo 36.** Os divisores de 8 são $1, 2, 4, 8$ e os divisores de 16 são $1, 2, 4, 8, 16$ assim o maior divisor comum entre 8 e 16 é 8, então ele é único.

## 3.3 Algoritmo Estendido de Euclides

Uma maneira fácil e eficiente de encontrar o máximo divisor comum de dois números é o algoritmo de Euclides, esse algoritmo é um dos mais antigos data por volta de 300 $a.c$, está nos Livros VII e X de sua obra.

**Lema 37.** *(Euclides). Sejam $a$,$b$,$n \in \mathbb{Z}$ tais que $a < na < b$. Então MDC$(a, b) =$ MDC$(a, b - na)$.*

*Demonstração.* Seja $d$= MDC$(a, b-na)$. Como $d/a$ e $d/(b-na)$, segue que $d$ divide $b$ e $b = b - na + na$. Assim $d$ e divisor comum de $a$ e $b$. Suponha agora que $k$ seja um divisor comum de $a$ e $b$, assim $k$ é divisor de $b-na$ consequentemente $k/d$. o que mostra que o MDC $(a, b)$ é igual ao MDC $(a, b - na)$. □

**Teorema 38.** *[Teorema de Divisão de Euclides] Sejam $a$ e $b$ inteiros positivos. Existem números inteiros $q$ e $r$ tais que:*

$$a = b.q + r \text{ com } 0 \leqslant r < b$$

*Além disso, $q$ e $r$ são únicos.*

*Demonstração.* Vamos supor por absurdo que a divisão $a$ por $b$ resulta dois quocientes e dois restos diferentes $q$, $q'$, $r$, $r'$ pertencente aos naturais:

$$a = b \cdot q + r \text{ sendo } 0 \leqslant r < b \tag{3.1}$$

$$a = b \cdot q\prime + r\prime \text{ sendo } 0 \leqslant r\prime < b \tag{3.2}$$

Vamos subtrair 3.1 de 3.2, obtemos:

$$r - r\prime = b \cdot (q\prime - q)$$

mas $0 \leqslant r,\ r\prime < b$ e portanto $0 \leqslant r - r\prime < b$. Ou seja,

$$0 \leqslant b \cdot (q\prime - q) < b$$

Como $b > 0$, temos

$$0 \leqslant q - q\prime < 1,$$

ou seja, $q - q\prime = 0 \to q = q\prime$ e $r = r\prime$. O que é um absurdo, logo $q$ e $r$ são únicos. □

Algoritmo Estendido de Euclides

Vamos apresentar a prova da existência do m.d.c dada por Euclides.

*Demonstração.* Dados $a, b \in \mathbb{N}$, vamos supor $b \leqslant a$. se $b = 1$, ou $a = b$, e se $b/a$, o M.D.C$(a; b) = a$. Supondo que $1 < b < a$ e que $b \nmid a$, podemos escrever pela divisão euclidiana

$$a = b \cdot q_1 + r_1, \text{com } 0 < r_1 < b$$

Temos duas possibilidades $r_1/b$ e $r_1 \nmid b$:

1. $r_1/b$. Nesse caso temos que o M.D.C de $(b, r_1) = r_1$ e pelo lema 37 chegamos a conclusão que:

   $$r_1 = (b, r_1) = (b, a - q_1 \cdot b) = (b, a) = (a, b),$$

   e assim finaliza-se o algoritmo.

2. $r_1 \nmid b$, assim quando efetuamos a divisão obtemos um segundo resto, conforme a equação abaixo:

   $$b = r_1 \cdot q_2 + r_2 \text{ sendo que } 0 < r_2 < r_1.$$

Assim obtemos duas novas possibilidades:

- $r_2/r_1$. Nesse caso temos que o M.D.C de $(r_1, r_2) = r_2$ e pelo lema 37 chegamos a conclusão que:

  $$r_2 = (r_1, r_2) = (r_1, b - q_2 \cdot r_1) = (r_1, b) = (a - q_1 \cdot b, b) = (a, b)$$

  e assim finaliza-se o algoritmo.

- $r_2 \nmid r_1$,assim quando efetuamos a divisão obtemos um novo resto, conforme a equação abaixo:

  $$r_1 = r_2 \cdot q_3 + r_3 \text{ sendo que } 0 < r_3 < r_2.$$

Dessa maneira continuamos até que não possamos mais fazer a divisão nos naturais. Podemos afirmar, pois o princípio da boa ordenação nos garante que existe um menor elemento.

□

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

**Tabela 3.1:** Algoritmo Estendido de Euclides- Procedimento.

**Exemplo 39.** Determinar, pelo Algoritmo de Euclides, o MDC entre 355 e 2450.

Primeiro passo será colocar os dois números na segunda linha, primeira coluna o maior número e na segunda coluna o menor número.

| | |
|---|---|
| 2450 | 355 |
| | |

Segundo passo será fazer a divisão do menor pelo maior e colocar o resto abaixo do maior número e o quociente em cima do menor número.

| | 6 | 1 |
|---|---|---|
| 2450 | 355 | |
| 320 | | |

Terceiro passo será observar o resto, como o resto não é zero copiamos este resto "320" ao lado do 355 e repetimos o processo anterior.

| | 6 | 1 |
|---|---|---|
| 2450 | 355 | 320 |
| 320 | 35 | |

Quarto passo , como o resto ainda não é zero repetimos a divisão novamente.

| | 6 | 1 | 9 |
|---|---|---|---|
| 2450 | 355 | 320 | 35 |
| 320 | 35 | 5 | |

Quinto passo , como o resto ainda não é zero repetimos a divisão novamente.

| | 6 | 1 | 9 | 7 |
|---|---|---|---|---|
| 2450 | 355 | 320 | 35 | 5 |
| 320 | 35 | 5 | 0 | |

Como o resto é 0 terminamos nossa divisão dessa forma temos que o $\mathfrak{m.d.c}$ de $(2450, 355) = 5$.

O algoritmo de Euclides resulta em algumas equações, vejamos:

$5 = 320 - 9 \cdot 35$

$35 = 355 - 1 \cdot 320$

$320 = 2450 - 6 \cdot 355$

Substituindo uma equação na outra obtemos:

$5 = 320 - 9 \cdot 35 = 320 - 9 \cdot (355 - 1 \cdot 320) = 10 \cdot 320 - 9 \cdot 355 = 10 \cdot (2450 - 6 \cdot 355) - 9 \cdot 355 = 10 \cdot 2450 - 69 \cdot 355.$

| | | | | |
|---|---|---|---|---|
| 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 |

**Tabela 3.2:** Primeiros Números Primos.

Que resulta em:
$5 = 10 \cdot 2450 - 69 \cdot 355 = (2450, 355)$, observamos que utilizando o algoritmo de Euclides conseguimos encontrar o $\mathfrak{m.d.c}$. Essa ultima equação é uma representação do algoritmo estendido de Euclides, pois quando escrevemos o $\mathfrak{m.d.c}$ de $(\mathfrak{a}, \mathfrak{b})$ na forma $\mathfrak{a} \cdot \mathfrak{k} + \mathfrak{b} \cdot \mathfrak{j} = (\mathfrak{a}, \mathfrak{b})$, com $\mathfrak{k}$ e $\mathfrak{j} \in \mathbb{Z}$.

## 3.4 Números Primos

**Definição 40.** Um número natural $\mathfrak{p}$ é **primo** se e somente se possui apenas dois divisores 1 e $\mathfrak{p}$.

Quando um número possui mais de dois divisores ele é chamado de composto. Todo número composto pode ser escrito como uma multiplicação de fatores primos.

**Teorema 41.** *Existem infinitos números primos.*

*Demonstração.* (livro de Euclides)
Suponha por absurdo, que existem uma quantidade finita de números primos, que chamaremos de $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_\mathfrak{n}$. Vamos considerar o número $\mathfrak{N} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_\mathfrak{n} + 1$. O número $\mathfrak{N}$ não é divisível por nenhum dos números $\mathfrak{p}_1, \mathfrak{p}_2, ..., \mathfrak{p}_\mathfrak{n}$ (o resto da divisão é sempre 1). Logo, $\mathfrak{N}$ é primo. Isto contradiz a nossa hipótese inicial de que existem somente $\mathfrak{n}$ números primos e portanto existem infinitos números primos.

□

**Exemplo 42.** Conforme a tabela 3.2 temos os primeiros vinte cinco números primos.

**Proposição 43.** *Entre um número* $\mathfrak{n}$*, e seu dobro existe pelo menos um número primo, sendo* $\mathfrak{n} \neq 1 \in \mathbb{N}$*.*

*Demonstração.* Suponha que $\mathfrak{n} = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p} \ldots \mathfrak{p}_\mathfrak{k}$ , sabemos que, $\mathfrak{j} = \mathfrak{p}_1 . \mathfrak{p}_2 . \mathfrak{p}_3 . \cdots . \mathfrak{p}_\mathfrak{k} + 1$ é primo, mas dobro de $\mathfrak{n}$ é $2\mathfrak{n} = 2(\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \cdots \cdot \mathfrak{p}_\mathfrak{K})$ , e $\mathfrak{j} < 2\mathfrak{n}$.
$\mathfrak{j} < 2\mathfrak{n}$, pois $\mathfrak{j} = \mathfrak{n} + 1$ e $\mathfrak{n} + 1 < 2\mathfrak{n}$; dividindo ambos os lados por $\mathfrak{n}$ temos;

- $\frac{\mathfrak{n}+1}{\mathfrak{n}} < \frac{2\mathfrak{n}}{\mathfrak{n}}$
- $1 + \frac{1}{\mathfrak{n}} < 2$, para qualquer valor de $\mathfrak{n} > 1$.

□

**Exemplo 44.** Entre 20 e 40 como $20 = 2 \cdot 2 \cdot 5$ logo pela proposição 43 temos $2 \cdot 3 \cdot 5 + 1$ é primo ou seja 31 , o que verifica que entre um número e seu dobro existe pelo menos um primo.

| | 1 | 1 | 1 | 4 |
|---|---|---|---|---|
| 14 | 9 | 5 | 4 | 1 |
| 5 | 4 | 1 | 0 | |

**Tabela 3.3:** Algoritmo Estendido de Euclides( Exemplo)

**Definição 45.** Dado que o $m.d.c$ de dois números $(a, b) = 1$, dizemos que $a$ e $b$ são primos entre si ou seja coprimos.

**Teorema 46.** *(Teorema de Bézout) Seja* $d = (a, b)$ *assim podemos escrever utilizando o algoritmo estendido de Euclides a seguinte equação* $x \cdot a + y \cdot b = d$ *sendo* $x$ *e* $y \in \mathbb{Z}$.

*Demonstração.* Vamos considerar o conjunto $c$ de todas as combinações lineares de $(a \cdot x + b \cdot y)$ e $n = a \cdot x_0 + b \cdot y_0$, sendo $n$ o menor elemento natural de $c$.

Suponha por absurdo que seja impossível escrever $n \nmid a$ então temos $a = n \cdot q + r$, sendo $0 < r < n$,o que implica que $r = a - n \cdot q \rightarrow r = a - (a \cdot x_0 + b \cdot y_0) \cdot q \rightarrow r = a \cdot (1 - x_0 \cdot q) - b \cdot y_0 \cdot q$. Logo sabemos que $r$ é uma combinação linear de $(a \cdot x + b \cdot y)$, o que um absurdo pois $r < n$ e $n$ é o menor elemento. Assim $n/a$ e analogamente $n/b$, assim $n$ é divisor comum de $a$ e $b$. Resta mostrar que $n = d$, como $d$ é o M.D.C de $a$ e $b$ temos que $d/a$ e $d/b$ assim podemos escrever $a = d \cdot q_1$e $b = d \cdot q_2$ e substituindo na equação $n = a \cdot x_0 + b \cdot y_0 \rightarrow n = (d \cdot q_1) \cdot x_0 + (d \cdot q_2) \cdot y_0 \rightarrow n = d \cdot (q_1 \cdot x_0 + q_2 \cdot y_0)$, assim temos que $d/n$ logo $d \leqslant n$, mas $d$ é o máximo divisor comum ou seja $d = n$. □

**Lema 47.** *(Gauss) Se* $a, b$ *e* $m \in \mathbb{Z}$. *Dessa forma se* $m|a \cdot b$ *e* $(a, m) = 1$ *então* $m|b$

*Demonstração.* Se $m$ divide o produto de $a$ por $b$, logo existe $k \in \mathbb{Z}$ tal que $k \cdot m = a \cdot b$ e se $(a, m) = 1$ sabemos então pelo teorema 46 que existem um $i$ e $j \in \mathbb{Z}$ tais que

$$i \cdot a + j \cdot m = 1$$

Multiplicando ambos os lados por $b$ obteremos a seguinte equação

$$b \cdot i \cdot a + b \cdot j \cdot m = b \cdot 1$$

e como $k \cdot m = a \cdot b$, substituindo $a \cdot b$ por $k \cdot m$ temos

$$k \cdot m \cdot i + b \cdot j \cdot m = b \cdot 1 \rightarrow m \cdot (i \cdot k + b \cdot j) = b$$

o que mostra que $m/b$. □

**Exemplo 48.** $(14, 9) = 1$ utilizando o algoritmo estendido de Euclides temos
logo
$1 = 5 - 4 \cdot 1$
$4 = 9 - 5 \cdot 1$
$5 = 14 - 9 \cdot 1$,
então temos : $1 = 5 - 4 \cdot 1 = 5 - 1 \cdot (9 - 5 \cdot 1) = 2 \cdot 5 - 9 = 2 \cdot (14 - 9 \cdot 1) - 9 = 2 \cdot 14 - 3 \cdot 9 = 1$

### 3.4.1 O Crivo de Eratóstenes

Eratóstenes (a.c. 285-194 a.C.) nasceu em Cyrene estudou filosofia, foi diretor da biblioteca de Alexandria, muito estudioso e exímio matemático, geografo, historiador, filosofo e poeta, conhecido por calcular a circunferência da terra.

**Definição 49.** Uma tabela que contém os números naturais de dois até$\mathfrak{n}$, então marca-se o primeiro número 2 e criva-se seus múltiplos, assim o número 2 é primo, o próximo número que não foi crivado é primo que é o 3, assim ele procede-se da mesma forma até restarem somente primos na tabela.

Esse método é bom até um certo valor, após ele se torna inviável, como qualquer método de força bruta.

**Teorema 50.** *Seja* $\mathfrak{n}$ *um número composto, então* $\mathfrak{n}$ *possui um ou mais divisores primos, tal que qualquer que seja o primo é sempre menor ou igual que a raiz quadrada do próprio número.*

*Demonstração.* Se n é composto logo $\mathfrak{n} = \mathfrak{a}.\mathfrak{p}$ sendo p primo e $\mathfrak{a} \in \mathbb{N}$ dessa maneira $0 < \mathfrak{a} < \mathfrak{n}$ e $0 < \mathfrak{p} < \mathfrak{n}$ . Vamos supor que $\mathfrak{p} \leqslant \mathfrak{a}$, suponhamos também por absurdo que $\mathfrak{p} > \sqrt{\mathfrak{n}}$, mas se $\mathfrak{n} = \mathfrak{a}.\mathfrak{p}$, como $\mathfrak{a} \leqslant \mathfrak{p}$ podemos então trocar a e $\mathfrak{p}$ por $\sqrt{\mathfrak{n}}$ , assim $1524\hat{}\{50\}\mathfrak{n} = \mathfrak{a}.\mathfrak{p} > \sqrt{\mathfrak{n}}.\sqrt{\mathfrak{n}} = \mathfrak{n}$, logo é um absurdo $\mathfrak{n} > \mathfrak{n}$, portanto $\mathfrak{p} \leqslant \sqrt{\mathfrak{n}}$. □

**Exemplo 51.** Vamos determinar os números primos entre 1 e 55.

Determina-se o maior número a ser checado. Ele corresponde à raiz quadrada do valor limite, arredondado para baixo. No caso, a raiz de 55, arredondada para baixo, é 7.

Vamos construir uma tabela com os números até 55

| # | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
| 49 | 50 | 51 | 52 | 53 | 54 | 55 | # |

Encontre o primeiro número da lista. Ele é um número primo, 2. Remova da lista todos os múltiplos do número primo encontrado.

| # | 2 | 3 | # | 5 | # | 7 |
|---|---|---|---|---|---|---|
| 9 | # | 11 | # | 13 | # | 15 |
| 17 | # | 19 | # | 21 | # | 23 |
| 25 | # | 27 | # | 29 | # | 31 |
| 33 | # | 35 | # | 37 | # | 39 |
| 41 | # | 43 | # | 45 | # | 47 |
| 49 | # | 51 | # | 53 | # | 55 |

O próximo número da lista é primo que é o número três, vamos repetir o procedimento.

| # | 2 | 3 | # | 5 | # | 7 |
|---|---|---|---|---|---|---|
| # | # | 11 | # | 13 | # | # |
| 17 | # | 19 | # | # | # | 23 |
| 25 | # | # | # | 29 | # | 31 |
| # | # | 35 | # | 37 | # | # |
| 41 | # | 43 | # | # | # | 47 |
| 49 | # | # | # | 53 | # | 55 |

O próximo número da lista é primo que é o número cinco, vamos repetir o procedimento.

| # | 2 | 3 | # | 5 | # | 7 |
|---|---|---|---|---|---|---|
| # | # | 11 | # | 13 | # | # |
| 17 | # | 19 | # | # | # | 23 |
| # | # | # | # | 29 | # | 31 |
| # | # | # | # | 37 | # | # |
| 41 | # | 43 | # | # | # | 47 |
| 49 | # | # | # | 53 | # | # |

O próximo número da lista é primo que é o número sete, vamos repetir o procedimento, que o ultimo número a ser checado.

| # | 2 | 3 | # | 5 | # | 7 |
|---|---|---|---|---|---|---|
| # | # | 11 | # | 13 | # | # |
| 17 | # | 19 | # | # | # | 23 |
| # | # | # | # | 29 | # | 31 |
| # | # | # | # | 37 | # | # |
| 41 | # | 43 | # | # | # | 47 |
| # | # | # | # | 53 | # | # |

## 3.5 Teorema Fundamental da Aritmética

Nesta secção iremos explanar sobre a composição dos números.

**Corolário 52.** *Se* $p_1$,$p_2 \cdots p_n$ *são números primos e, se* $p/p_1 \cdot p_2 \cdots p_n$*, assim* $p = p_i$*, para algum* $i$ *sendo* $i = 1, 2 \cdots, n$*.*

**Teorema 53.** *Todo número natural maior do que* 1 *ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

*Demonstração.* Vamos utilizar indução para fazer a prova. Seja $n = 2$ o resultado é imediato.

Suponhamos quer seja valido para qualquer número menor que $n$.Vamos mostrar que o resultado é valido para $n$.

Se $n$ é primo nada temos a demonstrar. Se $n$ é composto, logo temos dois números naturais $n_1$e $n_2$, tais que $n = n_1 \cdot n_2$, sendo que $1 < n_1 < n$ e1 $< n_2 < n$ .

Pela hipótese de indução, existem números primos $n_1 = p_1, ..., p_r$, $n_2 = q_1 \cdots q_s$, assim $n = p_1, ..., p_r \cdot q_1 \cdots q_s$. Vamos mostrar que existe somente uma forma de escrever ou seja a unicidade da escrita de $n$.

Suponha, agora, que $n = p_1, ..., p_r = q_1 \cdots q_s$, aonde $p_i$ e $q_s$ são números primos. Como $p/q_1 \cdots q_s$,, pelo corolário 52, temos que $p_1 = p_j$ para algum $j$, que, após reordenamento de$q_i, ..., q_s$, supomos que seja $q_1$,assim: $p_1, ..., p_r = q_1 \cdots q_s$. Como $p_1 \cdots p_r \nmid n$, a hipótese de indução acarreta que $r = s$ e os $p_i$ e $q_j$ são iguais aos pares. □

## 3.6 Pequeno Teorema de Fermat

**Lema 54.** *Seja* $p$ *um número primo. Os números da forma* $\binom{p}{i}$*, onde* $0 < i < p$*, são todos divisíveis por* $p$*.*

*Demonstração.* O resultado vale para $i = 1$. Vamos supor para $1 < i < p$. Assim $i!/p \cdot (p-1) \cdots (p-i+1)$, Como $(i!, p) = 1$, dessa maneira $i!/(p-1) \cdots (p-i+1)$, logo $\binom{p}{i} = i!/p \cdot (p-1) \cdots (p-i+1)$. □

**Teorema 55.** ***(Pequeno Teorema de Fermat)****. Seja um número primo*$p$*, tem-se que* $p$ *divide o número* $a^p - a$*, para todo* $a \in \mathbb{N}$*.*

*Demonstração.* Vamos mostrar por indução, seja $a = 0$, logo $\frac{0^p - 0}{p}$, o que mostra pois $p/$ .

Agora vamos mostrar para $a + 1$,utilizando a fórmula do binômio de Newton, □

## 3.7 Aritmética Modular

Aritmética modular ou aritmética dos restos ou ainda aritmética do relógio, inicialmente criada por Euler em 1750 e posteriormente introduzida por Gauss no seu livro Disquisitiones arithmeticae em 1801. A seguir discorreremos uma pequena parte da aritmética modular, para utilizarmos nas aplicações em sala de aula.

**Proposição 56.** *Dois inteiros* $p$ *e* $q$ *são congruentes modulo* $m$ *com* $m \in \mathbb{Z}$*,* $m > 1$ *se, e somente se,* $p - q$ *for divisível por* $m$ *e representamos* $p \equiv q \mod m$.

*Demonstração.* Suponhamos sem perda de generalidade que $p > q$, assim podemos escrever $p = m \cdot a + r_1$ e $q = m \cdot b + r_2$, com $a, b \in \mathbb{N}$ e com $0 \leqslant r_1 < m$ e $0 \leqslant r_2 < m$, mas $p - q = m \cdot (a - b) + (r_1 - r_2)$, logo para ser congruente temos que ter $r_1 = r_2$, o que implica $m$ divide $p - q$. □

**Exemplo 57.** Seja $8 \equiv 10 \mod 2$, ou seja $10 - 8$ é divisível por 2.

### 3.7.1 Propriedades

O conjunto dos inteiros $\mathbb{Z}$ modulo $m$, é fechado para as operações de multiplicação e soma.

Consideremos $\{a, b, c\} \subset \mathbb{Z}$, as propriedades a seguir fazem uma relação de equivalência da congruência modulo $m$. Se e somente se cada número inteiro corresponde a somente um dos restos da divisão euclidiana por $m$, consequentemente torna o conjunto infinito $\mathbb{Z}$ ao conjunto finito $\mathbb{Z}_m = 0, 1, 2, 3, .....m - 1$.

**Proposição 58.** *Temos algumas propriedades como:*

- Reflexiva: $a \equiv a \mod m$
- Simétrica: $a \equiv b \mod m \iff b \equiv a \mod m$
- Transitiva ou seja $a \equiv b \mod m$, $b \equiv c \mod m \to a \equiv c \mod m$.

Iremos proceder a prova da propriedade transitiva, a reflexiva e a simétrica fica a critério do leitor.

*Demonstração.* $a \equiv b \mod m$, $b - a$ é divisível por $m$, assim temos $b - a = m \cdot q_1 \to b = a + m \cdot q_1$
$b \equiv c \mod m$, $c - b$ é divisível por $m$, assim temos $c - b = m \cdot q_2$.
Substituindo uma equação na outra temos $c - a - m \cdot q_1 = m \cdot q_2 \to (c - a) = m(q_2 + q_1)$, o que mostra que $(c - a)$ é divisível por $m$. □

**Exemplo 59.** Dado $32 \equiv 38 \mod 6$ e $38 \equiv 26 \mod 6 \to 32 \equiv 26 \mod 6$.

**Proposição 60.** *Se* $a \equiv b \mod m$ *e* $c \equiv d \mod m$ *então* $(a + c) \equiv (b + d) \mod m$.

*Demonstração.* Vamos supor sem perda de generalidade, que $b \geqslant a$ e $d \geqslant c$.
$a \equiv b \mod m$, $b - a$ é divisível por $m$, assim temos $b - a = m \cdot q_1$.
$c \equiv d \mod m$, $c - d$ é divisível por $m$, assim temos $d - c = m \cdot q_2$.
Somando ambas as equações temos $(b - a) + (d - c) = m \cdot (q_2 + q_1) \to (b + d) - (a + c) = m \cdot (q_2 + q_1)$, ou seja $(b + d) - (a + c)$ é divisível por $m$. □

**Exemplo 61.** Dado $7 \equiv 9 \mod 2$ e $11 \equiv 13 \mod 2$, logo temos que $7 + 11 \equiv 9 + 13 \mod 2$, ou seja 18 e 22 deixam o mesmo resto quando dividido por ,2.

**Proposição 62.** *Se* $a \equiv b \mod m$ *e* $c \equiv d \mod m$*, então* $(a - c) \equiv (b - d) \mod m$.

*Demonstração.* Suponhamos sem perda de generalidade que $b \geqslant a$ e $d \geqslant c$, sabemos que $b - a$ e $d - c$ é divisível por $m$, logo:
$b - a = m \cdot r_1$
$d - c = m \cdot r_2$
Subtraindo ambas as equações temos:
$(b - a) - (d - c) = m \cdot r_1 - m \cdot r_2$
$b - a - d + c = m \cdot (r_1 - r_2)$
$(b - d) - (a - c) = m \cdot (r_1 - r_2)$
Dessa maneira temos que $(b - d) - (a - c)$é divisível por $m$. □

**Exemplo 63.** Dado $10 \equiv 15 \mod 5$ e $25 \equiv 30 \mod 5$ então pela prova anterior temos que $(15 - 10) - (30 - 25)$ é divisível por 5, que é verdadeiro pois $(15 - 10) - (30 - 25) = 5 - 5 = 0$.

**Proposição 64.** *Se* $a \equiv b \mod m$ *e* $c \equiv d \mod$ *, então* $a \cdot c \equiv b \cdot d \mod m$.

*Demonstração.* Suponhamos sem perda de generalidade que $b \geqslant a$ e $d \geqslant c$, sabemos que $b - a$ e $d - c$ é divisível por $m$, logo:

$b - a = m \cdot r_1$

$d - c = m \cdot r_2$

Vamos multiplicar $b - a = m \cdot r_1$ por $d$ , assim teremos $d \cdot (b - a) = d \cdot (m \cdot r_1)$ e vamos também multiplicar $d - c = m \cdot r_2$ por $a$ , assim teremos $a \cdot (d - c) = a \cdot (m \cdot r_2)$, somando as duas novas expressões temos:

$[d \cdot (b - a)] + [a \cdot (d - c)] = [a \cdot (m \cdot r_2)] + [d \cdot (m \cdot r_1)]$

$d \cdot b - d \cdot a + a \cdot d - a \cdot c = a \cdot (m \cdot r_2) + d \cdot (m \cdot r_1)$

$d \cdot b - a \cdot c = m \cdot (a \cdot r_2 + d \cdot r_1)$, o que mostra que $a \cdot c \equiv b \cdot d \mod m$ é verdadeiro. □

**Exemplo 65.** Dado $10 \equiv 15 \mod 5$ e $25 \equiv 30 \mod 5$, $10 \cdot 25 \equiv 15 \cdot 30 \mod 5$ que resulta em $(15 \cdot 30) - (25 \cdot 10) = 450 - 250 = 200$ e $200/5 = 40$.

Dessa maneira podemos entender que o resto da divisão deixado pelo produto de dois números, quando dividido por $m$, é fornecido pelo resto do produto dos restos deixados por esses mesmos números quando dividido por $m$.

**Proposição 66.** *Se* $a \equiv b \mod m$*, temos que* $a^n \equiv b^n \mod m$*.*

*Demonstração.* Vamos considerar n congruências $a \equiv b \mod m$:

$a \equiv b \mod m$

$a \equiv b \mod m$

$a \equiv b \mod m$

...

...

$a \equiv b \mod m$

Multiplicando todas as congruências temos:

$a \cdot a \cdot \cdots \cdot a \equiv b \cdot b \cdot \cdots \cdot b \mod m = a^n \equiv b^n \mod m$ □

**Exemplo 67.** Dado que $10 \equiv 20 \mod 2$ então $10^2 \equiv 20^2 \mod 2$, pois 100/2 deixa resto 0 e 400/2 também deixa resto 0.

Dessa maneira podemos entender que o resto da divisão deixado pela potência de $n$ de um número, quando dividido por $m$, é fornecido pelo resto da divisão do número por $m$,elevado a $n$.

**Exemplo 68.** Vejamos a expressão $\left(63251 \cdot 36562 + 25623^4\right)$, ao ser dividida por 2 deixa que resto?

$63251 \equiv 1 \mod 2$

$36562 \equiv 0 \mod 2$

$25623 \equiv 1 \mod 2$

Dessa maneira temos $\left(1 \cdot 0 + 1^4\right) = 0 + 1 = 1$

**Proposição 69.** *Para qualquer que seja* $a$*,* $b$*,* $c \in Z$ *valem as seguintes propriedades:*

1. $a \pm b \equiv \mod m = [(a \mod m) \cdot (b \mod m)] \mod m$;

2. $ab \equiv \mod m = [(a \mod m) \cdot (b \mod m)] \mod m$;

| | 1 | 1 | 2 |
|---|---|---|---|
| 5 | 3 | 2 | 1 |
| 2 | 1 | 0 | |

**Tabela 3.4:** Algorítimo Estendido de Euclides ( Aplicação).

**Exemplo 70.** Desenvolvendo a expressão a seguir obtemos:
$(36 \cdot 8 + 54 \cdot 5^4 - 15) \mod 7$.
$= 36 \mod 7 \cdot 8 \mod 7 + 54 \mod 7 \cdot 5^4 \mod 7 - 15 \mod 7$
$= (1 \cdot 1 + 5 \cdot 2 - 1) \mod 7$
$= 10 \mod 7$
$= 3$

### 3.7.2 Equações Modulares

Nesta subseção iremos explanar um pouco sobre resoluções de equações modulares

**Proposição 71.** *Uma equação modular do tipo* $ax + b \equiv k \mod m$*, tem solução se e somente se existe solução se* $mdc$ *de* $(a, m) = 1$,*ou seja existe um inverso para* $a$*, ainda existe solução se* $(a, m) > 1 = j$, $j/k - b$.

**Exemplo 72.** Vamos resolver a equação $5x - 11 \equiv 8 \mod 3$
Como $(5, 3) = 1$, a equação tem solução.
$5x \equiv 11 + 8 \mod 3$
$5x \equiv 19 \mod 3$
$5x \equiv 1 \mod 3$
$x \equiv 1 \cdot 5^{-1} \mod 3$
Vamos determinar o inverso de $5^{-1} \mod 1524^{50}$ 3
Observando a tabela 3.4 temos:

$$1 = 3 - 2 \cdot 1 \tag{3.3}$$

$$2 = 5 - 3 \cdot 1 \tag{3.4}$$

Assim substituindo 3.4 na 3.3 teremos:
$1 = 3 - (5 - 3 \cdot 1) \cdot 1$
$1 = 2 \cdot 3 - 1 \cdot 5$
Aplicando o módulo temos :
$2 \cdot 3 \mod 3 + (-1 \cdot 5) \mod 3 = 1$
$0 + (-1 \cdot 5) \mod 3 = 1 \rightarrow 5^{-1} = -1 \equiv 5 \mod 3$, logo o inverso de $5^{-1} \mod 3$ é próprio 5.
Portanto a solução é: $X \equiv 1 \cdot 5^{-1} \mod 3 \rightarrow 1 \cdot 5 \mod 3$, então $x = 5 + 3 \cdot k$ sendo $k \in \mathbb{Z}$

## 3.8 Critérios de Divisibilidade.

Esse assunto é tratado nas escolas de ensino fundamental como um conjunto de regras, tornando fácil a vida do professor e indiscutivelmente sem fundamentos para os alunos. Dessa maneira vamos mostrar alguns critérios de divisibilidade utilizando as congruências, tornando fácil a vida dos professores.

Para todas as demonstrações iremos utilizar um número com $n$ algarismos, decomposto da seguinte forma: $N = a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + a_1 \cdot 10^1 + a_0$

**Proposição 73.** *Todo número é divisível por* 2 *se e somente se o ultimo algarismo for par.*

*Demonstração.* Sabemos que $10 = 5 \cdot 2$

Seja $N = a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + a_1 \cdot 10^1 + a_0$, assim

$2 \cdot \left(a_{n-1} \cdot 5^{n-1} \cdot 2^{n-2} + a_{n-2} \cdot 5^{n-2} \cdot 2^{n-3} + \cdots + a_1 \cdot 5^1 \cdot 2^0\right) + a_0 \equiv 0 \mod 2 \longleftrightarrow$ $a_0$ for divisível por 2. ou seja $a_0$ tem que ser par. □

**Exemplo 74.** Determine o resto da divisão de $1202^{50}$por 2.

Como 1202 deixa resto 0, na divisão por 2, temos

$1202 \equiv 0 \mod 2$

$1202^{50} \equiv 0^{50} \mod 2$, ou seja deixa resto 0 na divisão .

**Exemplo 75.** Determine o resto da divisão de $1201^{50}$por 2.

Como 1201 deixa resto 1, na divisão por 2, temos

$1201 \equiv 1 \mod 2$

$1201^{50} \equiv 1^{50} \mod 2$, ou seja deixa resto 1 na divisão . Dessa forma qualquer número dividido por 2 deixa dois possíveis resto 0 e 1.

**Proposição 76.** *Todo número é divisível por* 3 *se e somente se a soma de todos os algarismos for divisível por* 3 *.*

*Demonstração.* Seja $N = a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + a_1 \cdot 10^1 + a_0$ e temos das congruências que :

$10 \equiv 1 \mod 3$ ; $10^2 \equiv 1^2 \mod 3$ ; $10^3 \equiv 1^3 \mod 3$ ; $\cdots 10^n \equiv 1^n \mod 3$.

$a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + a_1 \cdot 10^1 + a_0 \equiv x \mod 3$, logo podemos substituir as congruências acima.

$a_{n-1} \cdot 1^{n-1} + a_{n-2} \cdot 1^{n-2} + \cdots + a_1 \cdot 1^1 + a_0 \equiv x \mod 3$

$a_{n-1} + a_{n-2} + \cdots + a_1 \cdot + a_0 \equiv x \mod 3$, assim para verificar se um número é divisível por 3 temos que somar seus algarismos e verificar se essa soma é divisível por 3. □

**Exemplo 77.** Vamos verificar se 1524 é divisível por 3.

$1523 = 1000 + 500 + 20 + 4$

$1 \cdot 10^3 + 5 \cdot 10^2 + 2 \cdot 10 + 4$,

$10 = 1 \mod 3$, temos que:

$1 \cdot 1^3 + 5 \cdot 1 + 2 \cdot 1 + 4 \equiv x \mod 3$

$1 + 5 + 2 + 4 \equiv x \mod 3$

$12 \equiv x \mod 3$

ou seja $x = 0$, pois 12 é divisível por 3, logo 1524 é divisível por 3.

**Exemplo 78.** Determine o resto da divisão de $1524^{50}$por 3.
$1524 \equiv 0 \mod 3$
$1524^{50} \equiv 0^{50} \mod 3$
logo deixa resto 0 na divisão por 3.

**Exemplo 79.** Determine o resto da divisão de $1523^{30}$por 3.
$1523 \equiv x \mod 3$
$1+5+2+3 \equiv x \mod 3$
$11 \equiv x \mod 3 \rightarrow x = 2$ ,
$1523^{30} \equiv 2^{30} \mod 3$, mas $2^4 = 16 \equiv 1 \mod 3$ e $2^{30} = 2^4 \cdot 2^4 \cdot 2^4 \cdot 2^4 \cdot 2^4 \cdot 2^4 \cdot 2^4 . 2^2$
como $2^4 = 16 \equiv 1 \mod 3 \rightarrow 2^{30} = 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 . 2^2 \equiv y \mod 3$
$2^2 \equiv y \mod 3 \rightarrow 4 \equiv y \mod 3 \rightarrow 1 = y$, logo o resto da divisão é 1.

**Proposição 80.** *Todo número é divisível por* 5 *se termina em* 0 *ou* 5.

*Demonstração.* Seja $N = a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + a_1 \cdot 10^1 + a_0$ e temos das congruências que :
$5 \equiv 0 \mod 5$ ; $0 \equiv 0 \mod 5$ ; $10 \equiv 0 \mod 5$ ; $10^2 \equiv 0^2 \mod 5$ ; $10^3 \equiv 0^3 \mod 5$ ; $\cdots 10^n \equiv 0^n \mod 5$.
$a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + a_1 \cdot 10^1 + a_0 \equiv x \mod 5$, logo podemos substituir as congruências acima.
$a_{n-1} \cdot 0^{n-1} + a_{n-2} \cdot 0 + \cdots + a_1 \cdot 0^1 + a_0 \equiv x \mod 5$
ou seja devemos observar somente o ultimo algarismo $a_0$. □

**Exemplo 81.** Verificar se $1523^{20} - 426^{15}$ é divisível por 5.
$1523 \equiv 3 \mod 5$
$3^4 \equiv 1 \mod 5$
Então $1523^{20} \equiv 3^{20} \mod 5 \rightarrow 3^{20} = 3^4 \cdot 3^4 \cdot 3^4 \cdot 3^4 \cdot 3^4 \equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \mod 5$
logo $1523^{20} \equiv 1 \mod 5$
Agora vamos verificar a segunda parcela
$426 \equiv 1 \mod 5$
$426^{15} \equiv 1^{15} \mod 5$
Dessa maneira temos que:
$1523^{20} - 426^{15} \equiv 1 - 1 \mod 5$
Assim $1523^{20} - 426^{15}$ é divisível por 5.

**Proposição 82.** *Todo número é divisível por* 11 *se e somente se o algarismo da unidade somado ao décuplo dos algarismos da ordem ímpar e somado com os algarismos da ordem par o for.*

*Demonstração.* Seja $N = a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + a_1 \cdot 10^1 + a_0$ e temos das congruências que :
$a_0 \cdot 10^0 \equiv 1 \cdot a_0 \mod 11$ ;
$a_1 \cdot 10^1 \equiv 10 \cdot a_1 \mod 11$ ; ou $a_1 \cdot 10^1 \equiv -1 \cdot a_1 \mod 11$ ;
$a_2 \cdot 10^2 \equiv 1 \cdot a_2 \mod 11$ ; ou $a_2 \cdot 10^2 \equiv -10 \cdot a_2 \mod 11$ ;
$a_3 \cdot 10^3 \equiv 10 \cdot a_3 \mod 11$ ; ou $a_3 \cdot 10^3 \equiv -1 \cdot a_3 \mod 11$ ;
$a_4 \cdot 10^4 \equiv 1 \cdot a_4 \mod 11$ ; ou $a_4 \cdot 10^4 \equiv -10 \cdot a_4 \mod 11$ ;
$a_5 \cdot 10^5 \equiv 10 \cdot a_5 \mod 11$ ; ou $a_5 \cdot 10^5 \equiv -1 \cdot a_5 \mod 11$ ;
$a_6 \cdot 10^6 \equiv 1 \cdot a_6 \mod 11$ ; ou $a_6 \cdot 10^6 \equiv -10 \cdot a_6 \mod 11$ ;

$a_7 \cdot 10^7 \equiv 10 \cdot a_7 \mod 11$ ; ou $a_7 \cdot 10^7 \equiv -1 \cdot a_7 \mod 11$ ;
$a_8 \cdot 10^8 \equiv 1 \cdot a_8 \mod 11$ ; ou $a_8 \cdot 10^8 \equiv -10 \cdot a_8 \mod 11$ ;
$a_9 \cdot 10^9 \equiv 10 \cdot a_9 \mod 11$ ; ou $a_9 \cdot 10^9 \equiv -1 \cdot a_9 \mod 11$ ;
$a_{10} \cdot 10^{10} \equiv 1 \cdot a_{10} \mod 11$ ; ou $a_{10} \cdot 10^{10} \equiv -10 \cdot a_{10} \mod 11$ ;
Assim temos : $a_0 + (a_2 + a_4 + a_6 + \cdots) + 10 \cdot (a_1 + a_3 + a_5 + \cdots)$for divisível por 11. □

**Exemplo 83.** Vamos verificar se 649 é divisível por 11, utilizando o critério de divisibilidade.

Logo pelo critério encontrado temos: $9 + 10 \cdot (4) + 6 = 9 + 40 + 6 = 55$ , como 55 é divisível por 11 temos que 649 é divisível por 11.

**Exemplo 84.** Vamos verificar se $785^{10} - 1$ é divisível por 11, utilizando congruência.

Logo pelo critério encontrado temos: $5 + 10 \cdot (8) + 7 = 5 + 80 + 7 = 92$ , logo 785 não é divisível por 11.

Sabemos que $785 \equiv 4 \mod 11$
$785^{10} \equiv 4^{10} \mod 11$
$4^2 \equiv 5 \mod 11$
$\left(4^2\right)^5 \equiv 5^5 \mod 11$
$5^2 \equiv 3 \mod 11$
$5^3 \equiv 4 \mod 11$
$5^3 \cdot 5^2 \equiv 4 \cdot 3 \mod 11$
$5^5 \equiv 12 \mod 11$
$12 \equiv 1 \mod 11$
logo $785^{10} \equiv 1 \mod 11$,
$785^{10} - 1 \equiv 1 - 1 \mod 11$,
$785^{10} - 1 \equiv 0 \mod 11$,
Assim $785^{10} - 1$ é divisível por 11.

# 4 Criptografia Moderna

Com a utilização crescente de computadores pelas empresas e a necessidade do uso da criptografia como medida de segurança, foi necessário proceder uma padronização, de modo que as empresas pudessem trocar mensagens de uma forma segura e eficiente.

Assim, surge a American Stardard Code for Information Interchange (Código Padrão Americano para o Intercâmbio de Informação) que não consiste em uma cifra, mas em linguagem binária (7 dígitos que transformam letras do alfabeto pontuação e algarismos em números binários). Com o sistema binário, percebeu-se a necessidade de obter a segurança das informações lançadas e, portanto, necessitou-se da definição de um sistema criptográfico. Adotaram oficialmente o sistema desenvolvido pela IBM, chamado de Data Encryption Standard (DES). O DES é um sistema complexo, que utiliza uma chave simétrica, ou seja, é concordada entre o codificador e o decodificador. No entanto, o problema da distribuição da chave era grande e embasava-se na confiança mútua. Em 1976, três norte-americanos encontraram a solução para esse problema. Whitfield Driffie, Martin Hellman e Ralph Merkle descobriram uma forma de distribuir a chave sem que os envolvidos precisassem se encontrar. Esses inventores perceberam que as chaves atuais eram funções matemáticas bijetivas – Uma determinada função servia para cifrar uma mensagem, a sua inversa para decifrar (Fiarresga 2010). Assim Driffie considerou a hipótese de se utilizar chaves assimétricas (até então as chaves eram simétricas – a mesma servia para codificar e decodificar a informação). Desta forma, cada usuário teria duas chaves, uma pública para cifragem e outra privada para decifragem (Hefez, 2013). Contudo, Driffie publicou seu artigo revolucionário que utilizado até hoje. Foi então que em 1978, Ronald Rivest, Adi Shamir e Leonard Adleman, no Laboratório de Ciência da Informação do Massachusetts Institute of Technology (MIT) descobriram a forma de como colocar em prática a ideia de Driffie e deram as iniciais de seus próprios nomes a descoberta (RSA). A descoberta parte da proposição de que é necessário encontrar números primos grandes e ao mesmo tempo na enorme dificuldade prática em fatorar o produto de dois desses números (Hefez, 2013).

## 4.1 Chave Simétrica.

**Definição 85.** A chave simétrica é um método que consiste em cifrar e decodificar utilizando uma mesma chave.

Essa chave faz com que o remetente consiga codificar a mensagem, tornando-a em uma mensagem completamente diferente, assim somente o destinatário com a posse da chave consiga decodificar a mensagem. Esse sistema possui uma característica que pode ser inconveniente dependendo da situação, pois se duas pessoas precisam trocar informações e essas informações forem criptografadas eles precisam da chave para cifrar e decodificar, mas como fazê-la sem que uma terceira descubra essa chave.

- Existem dois tipos de chave simétrica: Cifras de fluxo, Cifras de bloco.

| texto original | 010101 |
|---|---|
| códigos aleatórios | 111000 |
| texto criptografado | 101101 |

**Tabela 4.1:** Exemplo da cifra de fluxo

| **texto original** | 0011 | 1010 | 1100 | 1001 |
|---|---|---|---|---|
| **texto criptografado** | 1100 | 0101 | 0011 | 0110 |

**Tabela 4.2:** Exemplo de Cifra de Blocos

**Definição 86.** A cifra de fluxo é um processo que mistura a mensagem original com um outro texto para codificá-lo, sem alterar a quantidade de códigos.

**Definição 87.** A cifra de blocos é um processo que transforma sequências de mesmo tamanho em sequências criptografadas sem alterar a quantidade de códigos de cada bloco.

Vamos construir um exemplo de troca de chaves conforme a tabela 4.3, utilizando aritmética modular.

Esse sistema não é perfeito, pois necessita das duas partes estarem conectas ao mesmo tempo, mas foi uma ideia genial.

### 4.1.1 Alguns Sistemas de Chave Simétrica

- O AES é uma cifra de bloco, usado para criptografia de chave simétrica essa chave possui tamanho de 128 , 192 ou 256 bits , ele é rápido tanto em software quanto em hardware , é relativamente fácil de executar e requer pouca memória.
- DES - 56 bits : O Data Encryption Standard ( DES ).Foi criado pela IBM em 1977 e , apesar de permitir cerca de 72 quadrilhões de combinações , seu tamanho de chave ( 56 bits ) é considerado pequeno , tendo sido quebrado por força bruta em 1997.
- 3DES -112 ou 168 bits : O 3DES é uma simples variação do DES , utilizando o em três cifamentos sucessivos , podendo empregar uma versão com duas ou com três chaves diferentes.
- IDEA 128 bits : O International Data Encryption Algorithm ( IDEA ) foi criado em 1991 por James Massey e Xuejia Lai e possui patente da suíça ASCOM Systec.Mas na maioria dos microprocessadores , uma implementação por software do IDEA é mais rápida do que uma implementação por software do DES.
- Blowfish 32 a 448 bits : Algoritmo desenvolvido por Bruce Schneier , que oferece a escolha , entre maior segurança ou desempenho através de chaves de tamanho variável.
- O Twofish é uma chave simétrica que emprega a cifra de bloco de 128 bits , utilizando chaves de tamanhos variáveis , podendo ser de 128 , 192 ou 256 bits.

| | **Gustavo** | **Daniel** |
|---|---|---|
| **Função** | $3^{a} \equiv x \mod 5$ | $3^{B} \equiv x \mod 5$ |
| **1º passo** | Gustavo escolhe o número $a = 5$ e mantém em segredo | Daniel escolhe o número B =7 e mantém em segredo |
| **2º passo** | Gustavo substitui 5 na função $3^{5} \equiv x \mod 5 \rightarrow x = 3$ | $3^{7} \equiv x \mod 5 \rightarrow x = 2$ |
| **3º passo** | Gustavo atribui o valor de $\alpha = 3$ e envia para Daniel | Daniel atribui o valor de $\beta = 2$ e envia para Gustavo. |
| **Nessa fase acontece a troca de informações, ou seja alguém pode interceptar os números 3 e 2, mas na verdade isso não importa pois 3 e 2 não são chaves.** | | |
| **4º passo** | Gustavo calcula a solução da congruência $B^{\alpha} \equiv x \mod 5$ | Daniel calcula a solução da congruência $\alpha^{B} \equiv x \mod 5$ |
| | $2^{3} \equiv x \mod 5 \rightarrow x = 3$ | $3^{7} \equiv x \mod 5 \rightarrow 2187 \equiv x \mod 5 \rightarrow x = 2$ |
| **chave** | $x = 3$ | $x = 2$ |

**Tabela 4.3:** Troca de Informações

#### 4.1.1.1 Chaves Públicas

**Definição 88.** Chave pública é um processo para codificar uma palavra ou texto que utiliza funções que são difíceis de inverter computacionalmente mas são distribuídas de forma livre, para qualquer meio de comunicação.

Para uma chave pública ser confiável e viável temos pelo menos três possibilidades de abortar esse assunto.

- Alguém de confiança assina a chave pública.
- Rede de confiança de maneira que cada uma assina a chave pública do outro.
- Criptografia baseada em identidades conhecido como IBE. Esse tipo de criptografia não necessita de um repositório para armazenamento de chaves públicas o custo computacional reduzido, permite também a implementação dos modelos hierárquicos e assinaturas em Anel, Curtas e Grupo.

Vamos observar a sequência a seguir:

1. Gustavo envia para Daniel a sua chave pública.
2. Daniel cifra uma mensagem usando a chave pública de Gustavo
3. Gustavo decodifica a mensagem de Daniel com sua chave privada.

Como garantir que a chave pública é realmente de Gustavo?, essa questão é amplamente estudada pois, deve se ter um protocolo para garantir que a chave pública não foi substituída por uma falsa. Assim existe um banco de dados com acesso público que possui todas as chaves públicas. Esse banco de dados é protegido por uma pessoa ou

por um grupo, se não for protegido, qualquer pessoa pode trocar a chave pública de Gustavo e sem saber Daniel cifra a mensagem utilizando essa chave falsa que não é de proprietário e ao enviar para Gustavo ele não conseguirá decodificar, mas a pessoa que trocou a chave sim, ela conseguirá decodificar tornando o sistema inseguro. Supondo que ninguém consiga trocar essa chave no banco de dados ainda pode ocorrer a troca quando Gustavo enviar para Daniel, para evitar esse tipo de constrangimento a pessoa ou grupo que proporciona a segurança do banco de dados "assina" cada uma das chaves que Gustavo envia para Daniel.

## 4.2 Chave Assimétrica

Uma sequência de operações é realizada para a cifragem que é feita por uma chave pública e a decodificação é feita por uma chave privada que não pode ser calculada através da chave pública.

Esse sistema possui duas chaves uma pública e outra secreta.

**Definição 89.** A chave assimétrica é um método que consiste em cifrar utilizando uma chave publica e decodificar utilizando uma chave privada.

Se Gustavo e Daniel desejam se comunicar Gustavo cria duas chaves uma publica e outra privada o mesmo faz Daniel. Quando Gustavo for enviar uma mensagem a Daniel ele criptografa a mensagem utilizando a chave publica de Daniel e quando Daniel recebe a mensagem ele decodifica utilizando a sua chave secreta. As vantagens desse sistema e que não há troca de chaves, o remetente não precisa esperar o recebimento da uma informação para dar sequência a sua cifragem.

### 4.2.1 Alguns Sistemas de Chave Assimétrica

- O RSA é um algoritmo assimétrico que possui este nome devido a seus inventores: Ron Rivest , Adi Shamir e Len Adleman , que o criaram em 1977 no MIT. Atualmente, é o algoritmo de chave pública mais amplamente utilizado, além de ser uma das mais poderosas formas de criptografia de chave pública conhecidas até o momento. A premissa por trás do RSA consiste na facilidade de multiplicar dois números primos para obter um terceiro número, mas muito difícil de recuperar os dois primos a partir daquele terceiro número .Gerar a chave pública envolve multiplicar dois primos grandes; qualquer um pode fazer isto. Derivar a chave privada a partir da chave pública envolve fatorar um grande número .

- O ElGamal é outro algoritmo de chave pública utilizado para gerenciamento de chaves. Sua matemática difere da utilizada no RSA, mas também é um sistema comutativo.

- Diffie-Hellman - Também baseado no problema do logaritmo discreto, e o criptossitema de chave pública mais antigo ainda em uso. O conceito de chave pública, aliás foi introduzido pelos autores deste criptossitema em 1976 .

- Curvas Elípticas-Miller propôs de forma independente a utilização de curvas elípticas para sistemas criptográficos de chave pública. Eles não chegaram a

inventar um novo algoritmo criptográfico com curvas elípticas sobre corpos finitos, mas implementaram algoritmos de chave pública já existentes, como o algoritmo de Diffie-Hellman, usando curvas elípticas .

## 4.3 Resumos Criptográficos

O resumo criptográfico é um método que aplicado a uma informação criptografada de qualquer tamanho e resulta em uma informação de um tamanho fixo (hash). Alguns desses métodos de hash são: SHA-1, SHA-256 e MD5. O hash é criado de forma a não se poder obter a informação original.

## 4.4 Assinatura Digital

Assinatura digital consiste em verificar se uma determinada informação publicada, está correta sem alterações e também verificar se é a mesma pessoa que a publicou. Essa verificação é feita utilizando a chave publica que decodifica a mensagem possibilitando a autenticação. A chave publica apenas decifra, evitando assim a não repudiação da informação publicada. Alguns algoritmos de assinatura digital são RSA, DSA e ELGAMAL .

## 4.5 Protocolos

Os protocolos de segurança visam garantir a integridade a confidencialidade da mensagem. Um protocolo bem detalhado deve fornecer informações necessárias sobre estruturas , em que ponto ele pode ser usado para implementar várias versões e operações de um programa e e representações de dados. Um protocolo tem pelos menos em sua estrutura um acordo de chave ou estabelecimento uma entidade de autenticação Simétrica de encriptação e mensagem de autenticação, transporte de dados em aplicativos de segurança e métodos Não repúdio.Um exemplo de protocolo é Transport Layer Security (TLS) que é usada para proteção da internet.

## 4.6 Sigilo

Uma informação criptografada precisa de sigilo e isso só é possível se qualquer adversário não possa descobrir a informação transmitida, dessa maneira chamamos de sigilo perfeito. Hipoteticamente é quase impossível ter um sistema com sigilo perfeito, mas com a tecnologia atual temos sistemas indecifráveis mas ao mesmo tempo inviáveis. Podemos citar um exemplo de sigilo perfeito a cifra de Vernam. Todo sistema parece bom até ser colocado em prática e alguém o decifrá-lo.

## 4.7 Função de Mão Única

Uma função de mão única é basicamente fácil calcular $f(x)$ dado $x$ mas quase "impossível" ou difícil de calcular $x$ dado $f(x)$. Esse termo utilizado "impossível" se refere

| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** | **N** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **X** | **W** | **Y** | **Z** | | **ESPAÇO** |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | | 37 |

**Tabela 4.4:** Tabela de Pré Codificação do R.S.A

que dado um polinômio de tamanho $p$ , leva um tempo extremamente grande para efetuar seu cálculo.

**Definição 90.** Dizemos que uma função é possivelmente de mão única se e somente se temos um algoritmo que fornece um $f(x)$ em tempo hábil e ao mesmo tempo difícil de inverter computacionalmente dada uma imagem qualquer.

**Exemplo 91.** Produto e decomposição

A função $f(x)$ é gerada a partir do produto de dois números primos $p$ e $q$, essa função pode ser calculada aonde $n$ é o tamanho da entrada e dependendo da quantidade de dígitos da entrada fica difícil de inverter essa função, pois requer encontrar os fatores de um determinado número inteiro $n$.

**Exemplo 92.** A função Rabin $f$ é gerada a partir de dois inteiros positivos $c$ e $n$, sendo $n$ é o produto de dois primos $p$ e $q$, sua saída é $c^2$módulo $n$. O processo inverso requer encontrar as raízes quadradas módulo $n$; que é: dado $y$ e $n$, ache um $x$ que $x^2 \mod n = y$.

## 4.8 R.S.A

O sistema R.S.A, foi criado em cima da teoria dos números baseando-se na dificuldade de se fatorar um número muito grande em especial números formados pelo produto de primos. Como já foi provado todos os números podem ser escritos em forma de produto a menos de uma ordem em fatores primos. Para implementar o R.S.A precisamos de dois parâmetros básicos: dois números primos que vamos chamar de $p$ e $q$. Para codificar uma mensagem usando o R.S.A é suficiente conhecer o produto dos dois primos, que vamos chamar de $n$. Para decodificar uma mensagem precisamos conhecer os primos $p$ e $q$. A chave de codificação do R.S.A é portanto constituída essencialmente pelo número $n = pq$. Esta chave é tornada pública: todos ficam sabendo que, para mandar uma mensagem, deve ser usada a chave $n$. Por isso $n$ também é conhecido como a "chave pública". Já a chave de decodificação é constituída pelos primos $p$ e $q$. Cada usuário tem que manter sua chave de decodificação secreta ou a segurança do método estará comprometida.

### 4.8.1 Matemática do R.S.A

Vamos começar transformando nosso alfabeto em uma sequência de números, chamamos isso de pré codificação, nessa secção iremos adotar a seguinte tabela 4.4.

Observe que o espaço entre duas palavras será substituído pelo número 37, assim por exemplo quando codificarmos a frase "A matemática" teremos a sequência de números 113723113015231130191311.

| **blocos pré codificados** | $c^f$ | $c^f \mod 143$ |
|---|---|---|
| 113 | $113^7$ | 9 |
| 72 | $72^7$ | 19 |
| 31 | $31^7$ | 125 |
| 130 | $130^7$ | 26 |
| 15 | $15^7$ | 115 |
| 23 | $23^7$ | 23 |
| 11 | $11^7$ | 132 |
| 30 | $30^7$ | 134 |
| 19 | $19^7$ | 46 |
| 131 | $131^7$ | 131 |
| 1 | $1^7$ | 1 |

**Tabela 4.5:** Codificação do R.S.A

A vantagem de se escolher dois algarismos é que evitaremos ambiguidades, o que aconteceria por exemplo como o número 12, poderia ser A e B ou outra letra do alfabeto. Agora vamos especificar dois parâmetros ou seja dois números primos $p$ e $q$ e temos $n = p \cdot q$. Para trabalharmos na codificação da frase "A matemática" iremos adotar $p = 11$ e $q = 13$ assim teremos $n = 143$ . O próximo passo da pré codificação é transformar o número acima em blocos da seguinte maneira 113-$72 - 31 - 130 - 15 - 23 - 11$–30–19–131–1, os blocos foram escolhidos da seguinte maneira, nenhum deles é maior que 143 e nenhum deles começa com 0, pois isso traria problemas na hora da decodificação. Outro fator muito importante que os blocos não correspondem as letras da frase pré codificada isso torna o sistema imune ao ataque de frequência.

### 4.8.2 Codificação

Para realizar a codificação necessitamos de $n$ e de um número que seja um inteiro positivo e que seja inversível módulo $\phi(n)$ e torna-se fácil calcular pois conhecemos $p$ e $q$,assim $\phi(n) = (p-1)(q-1)$,

Para codificar a frase "A matemática" utilizaremos $n = 143$, que inversível módulo $\phi(n) = (11-1)(13-1) = 120$, logo o $m.d.c$ de $(143, 120)$ é 1. Assim codificaremos cada bloco separado e teremos uma nova sequência de blocos. A formula para codificar os blocos é a seguinte $K(c)$ =resto da divisão por $c^f$, sendo $f$ o menor número primo que não divide 120 que é 7.

Assim obtemos a nova sequência codificada $9-19-125-26-115-23-132-134-46-131-1$, vejamos agora como refazer o processo para chegar a mensagem original.

### 4.8.3 Decodificação do R.S.A

Para realizar a decodificação teremos que observar $c^f \mod 143$ e o inverso $f$ em $\phi(n)$, assim teremos $t(d)$ o resultado da decodificação. Vejamos que $n = 143$ e $f = 7$, logo pelo algoritmo estendido euclidiano teremos $120 = 7 \cdot 17 + 1$, aonde resulta que $1 = 120 + (-17) \cdot 7$, assim o inverso 7 modulo 120 é $-17$. Como utilizaremos $d$ como expoente teremos $120 - 17 = 103$, que é o menor inteiro positivo módulo 120. Como

| blocos codificados | $(c^f \mod 143)^d$ | $(c^f \mod 143)^d \mod 143$ |
|---|---|---|
| 9 | $9^{103}$ | 113 |
| 19 | $19^{103}$ | 72 |
| 125 | $125^{103}$ | 31 |
| 26 | $26^{103}$ | 130 |
| 115 | $115^{103}$ | 15 |
| 23 | $23^{103}$ | 23 |
| 132 | $132^{103}$ | 11 |
| 134 | $134^{103}$ | 30 |
| 46 | $46^{103}$ | 19 |
| 131 | $131^{103}$ | 131 |
| 1 | $1^{103}$ | 1 |

**Tabela 4.6:** Decodificação do R.S.A

os cálculos são altamente dificultosos com apenas caneta e papel efetuaremos somente um cálculo e o restante fica ao leitor, pois o restante dos cálculos foram usados um sistema computacional.

- $9^{103} = (9^3)^{34} \cdot 9 \mod 143$
- $9^3 = 3^6 \equiv 14 \mod 143$
- $14^3 \equiv 27 \mod 143$
- $9^{103} = (9^3)^{34} \cdot 9 \mod 143 \rightarrow (14)^{34} \cdot 9 \mod 143 \rightarrow (14^3)^{11} \cdot 14 \cdot 9 \mod 143 \rightarrow (27)^{11} \cdot 14 \cdot 9 \mod 143 \rightarrow (3^3)^{11} \cdot 14 \cdot 9 \mod 143 \rightarrow 3^{35} \cdot 14 \mod 143 \rightarrow (3^6)^5 \cdot 3^5 \cdot 14 \mod 143 \rightarrow (14)^5 \cdot 3^5 \cdot 14 \mod 143 \rightarrow 14^6 \cdot 3^5 \mod 143 \rightarrow 14^3 \cdot 14^3 \cdot 3^5 \mod 143 \rightarrow 27 \cdot 27 \cdot 3^5 \mod 143 \rightarrow 3^6 \cdot 3^5 \mod 143 \rightarrow 14 \cdot 3^5 \mod 143 \rightarrow 14 \cdot 243 \mod 143 \rightarrow 3402 \mod 143 = 113$

A questão é esse sistema é seguro?, depende da escolha dos números primos empregados na codificação do sistema que deve ser da ordem de 100 algarismo cada, assim tornando difícil computacionalmente a decomposição de $n$.

Embora esse sistema aparentemente pareça fácil de ser utilizado, não é, pois necessita-se de computadores quando se trabalha com números primos muito grandes. Após essa descoberta, grandes avanços vieram acontecendo. Pode-se mencionar Criptografia as curvas elípticas por Miller e Criptografia Quântica publicada por Charles H. Bennett e Gilles Brassard, dentre outros. No entanto, estudos continuam sendo realizados para maiores avanços no campo da criptografia.

## 4.9 Compartilhamento de Segredos

Parte importante da criptografia é manter um segredo em sigilo como por exemplo, uma senha de um cofre ou número primo importante algo desse tipo, que não seja conhecido apenas por uma pessoa mas por varias e que fosse revelado somente quando todas as partes estiverem decididas a fazê-lo. Nesse caso vamos descrever um método de compartilhamento de segredos chamado protocolo secreto de Shamir. Esse método

consiste em utilizar um polinômio sendo que o termo independente é o segredo, e os coeficientes são distribuídos entre as partes interessadas.

**Definição 93.** O protocolo de Shamir é um sistema que fraciona uma chave (polinômio) entre $n$ usuários e $t$ frações da chave.

Para recuperar a chave temos que ter $t$ sendo $t \leqslant n$ frações necessárias

**Definição 94.** Seja $f$ uma função definida num intervalo $[a; b]$ e conhecida nos pontos.
$a = x_0 < x_1 < \cdots < x_{n-1} < x_n = b$:
Sendo $P$ um polinômio qualquer que satisfaz
$f(x_i) = P(x_i)$ $i = 0, 1, 2, \cdots, n$, é chamado de polinômio interpolador (de Lagrange) def$(x)$ nos pontos dados.

**Proposição 95.** *Sejam* $n+1$ *pontos dados por* $(x_i, L_i)$, $i = 0, ..., n$ $x_i \neq x_i$, *para* $i \neq j$. *Então existe um único polinômio de grau*$n$ *que passa por estes pontos.*

*Demonstração.* Vamos considerar $L(x)$ um polinômio de grau $n$ sendo $L(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + ... + a_nx^n$ e sendo $a_n$ constantes

$$L(x) = \sum_{i=0}^{k} y_i \cdot l_i(x)$$

que passa pelos pontos $L(x_i) = L_i$, $i = 0, ..., n$ , vamos determinar as constantes para depois determinar o $L(x)$.
$l(x_i) = l_i$, $i = 0, ..., n$ é equivalente ao sistema:
$a_0 + a_1x_0 + a_2x_0^2 + a_3x_0^3 + ... + a_nx_0^n = l_0$
$a_0 + a_1x_1 + a_2x_1^2 + a_3x_1^3 + ... + a_nx_1^n = f_1$.
$\vdots$
$a_0 + a_1x_n + a_2x_n^2 + a_3x_n^3 + ... + a_nx_n^n = l_n$
Esse sistema tem solução única se e somente se os coeficientes das incógnitas seja não nulo.

$$\begin{matrix} 1 & x_0 & x_1^2 & \cdots & x_1^n \\ 1 & x_2 & x_2^2 & \cdots & x_2^n \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & x_l & x_l^2 & \cdots & x_l^n \end{matrix}$$

essa é uma matriz Vandermonde, sendo que seu determinante é dado por: $\det(A) = \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i)$
Como $x_i \neq x_j$ para $i \neq j$, temos que $\det(A) \neq 0$, como queríamos demonstrar. □

**Teorema 96.** *(Lagrange) Seja* $f$ *uma função definida num intervalo* $[a, b]$ *e conhecida nos pontos* $(x_i, f_i) i = 0, ..., n$. *Existe somente um Polinômio Interpolador de Lagrange* $p_n$ *de grau menor ou igual a* $n$ *interpolador de* $f$ *nos pontos dados.*

*Demonstração.* Seja o polinômio $p(x) = \sum_{i=0}^{n} F(x_i)l_i(x)$ , aonde $l_i(x) = \prod_{j=0, j\neq i}^{k} \frac{(x-x_j)}{(x_i-x_j)}$, aonde $i = 1, 2, \cdots, n.$, assim cada $l_i$ é um polinômio de grau $n$, e ainda para $l_i(x_j)$ quando $i = j$ temos 1 e $i \neq j$ temos 0. Isto é $l_i(x_j) = \delta_{i;j}$, portanto a função $P_n$ é um polinômio de grau menor ou igual a $n$ verificando as condições de interpolação, provando a existência do polinômio. Agora devemos provar que ele é único. Vamos

supor que $P_n$ e $Q_N$ são dois polinômios de grau menor ou igual a n interpoladores de $f$ nos pontos conhecidos assim o polinômio $M_N(x) = P_n(x) - Q_n(x)$ vai anular pelo menos, nos pontos $x_i$, com $i = 0, 1; \cdots ; n$. dessa maneira $M_N$ é um polinômio de grau menor ou igual a $n$, ele só pode ter $n+1$ zeros se for identicamente nulo. Assim sendo, $P_n(x) = Q_n(x)$, o que mostra que se existir ele é único. □

**Exemplo 97.** Seja os pontos $(0, -5), (1, 1)$ e $(3, 25)$, vamos descobrir o polinômio que passa pelos três pontos.
$l(x_0) = \frac{(x-1)(x-3)}{(0-1)(0-3)} = \frac{x^2-4x+3}{3}$
$l(x_1) = \frac{(x-0)(x-3)}{(1-0)(1-3)} = \frac{-x^2+3x}{2}$
$l(x_2) = \frac{(x-0)(x-1)}{(3-0)(3-1)} = \frac{x^2-x}{6}$ ;
Assim temos: $l(x) = \sum_{i=0}^{n} F(x_i)l_i(x)$ , então $p(x) = f(x_0).l(x_0) + f(x_1).l(x_1) + f(x_2).l(x_2) = (-5) \cdot (\frac{x^2-4x+3}{3}) + 1 \cdot (-x^2 + 3x) + 25 \cdot (\frac{x^2-x}{6}) = 2x^2 + 4x - 5$, encontramos o polinômio que passa pelos três pontos.

**Lema 98.** *Para qualquer* $s, \in \mathbb{Z}p\mathbb{Z}$ *existe exatamente um polinômio* $p^{t-m-1}$ *e* $a, (x) \in \mathbb{Z}p\mathbb{Z}$ *de grau* $\leqslant t - 1$ *com* $a, (0) = s,$ *e* $a'(x_i) = y_i$, $1 \leqslant i \leqslant m$.

O lema 98 mostra que não é possível obter informação nenhuma do segredo desde que as partes, estejam todas separadas, assim a única forma de descobrir o segredo será juntando todas as partes.

**Exemplo 99.** A grande vantagem do compartilhamento de segredo utilizando o método de Shamir é que todas as partes envolvidas devem estar juntas para conseguir revelar o segredo, pois alguns pontos ou coeficientes de um polinômio não revelam informação nenhuma, o que não acontece se dividir por exemplo a senha de um cofre.

Suponhamos que um cofre possui 6 dígitos e que sua senha seja dividida em três partes, e que cada pessoa sabe a posição da sua senha assim se qualquer uma das três pessoas tentar descobrir a senha ela terá $10^4$ possibilidades de descobrir, mas se duas delas juntarem para abrir o cofre o número de possibilidades será de $10^2$, tornando inviável a distribuição de partes da senha.

# 5 Aplicações e Atividades em Sala de Aula

Muitos professores são pegos com a seguinte pergunta, "como e aonde aplicar isso e aquilo", esse questionamento não é especifico de um conteúdo mas de todos, mesmo colegas de outras disciplinas tem uma enorme aspersão a matemática. Devemos então como mediadores do conhecimento mostrar aonde é utilizado esse ou aquele conhecimento e na medida do possível aplicar o conteúdo ensinado. Dessa maneira vamos propor algumas aplicações de funções e aritmética modular.

## 5.1 Funções Inversas

Vamos utilizar uma função polinomial do $1^{o}$ grau para cifrar e a sua inversa decifrar uma determinada mensagem.

### 5.1.1 Atividade para Sala de Aula - Função Inversa

- Objetivo Geral: Desenvolver a compreensão pelos alunos da importância da utilização da função inversa.
- Objetivo específico: Resolver funções determinando seu conjunto solução e suas inversas.
- Público-alvo: Estudantes do ensino médio.
- Recursos Metodológicos: Quadro negro, giz, multimídia.
- Pré-requisito: conhecimento sobre imagem, domínio e contradomínio de como inverter uma função.
- Metodologia: Pode-se trabalhar com apenas três grupos na sala ou vários grupos de apenas três alunos. A atividade deve ser desenvolvida através de um remetente um destinatário um interceptador.
- Duração: Duas aulas de 50 minutos cada.

**Exemplo 100.** Gustavo e Ana Paula desejam trocar uma mensagem pelo telefone e como é uma época de guerra todos os telefones estão grampeados, sem segurança nenhuma. A mensagem a ser decifrada é uma localização para o encontro dos dois. Sabendo que Gustavo está a uma distância considerável de sua amada, ele estipula uma localização para ela, através de uma mensagem criptografada por uma função e de posse de sua inversa sua amada saberá exatamente a posição de encontro dos dois.( previamente eles já estipularam a função )

| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** | **N** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** | **espaço** | |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | |

**Tabela 5.1:** Letras e Números Correspondentes para Cifrar e Decifrar

| **LETRAS** | **VALOR DE CADA LETRA (X) de acordo com a tabela 5.1** | $F(x) = x +$ **2(remetente)-cifra** | $f^{-1}(x) = x -$ **2(destinatário) - decodifica** |
|---|---|---|---|
| D | 14 | $f(14) = 16$ | $f^{-1}(16) = 14$ |
| E | 15 | $f(15) = 17$ | $f^{-1}(17) = 15$ |
| L | 22 | $f(22) = 24$ | $f^{-1}(24) = 22$ |
| F | 16 | $f(16) = 18$ | $f^{-1}(18) = 16$ |
| I | 19 | $f(19) = 21$ | $f^{-1}(21) = 19$ |
| M | 23 | $f(23) = 25$ | $f^{-1}(25) = 23$ |
| espaço | 37 | $f(37) = 39$ | $f^{-1}(37) = 35$ |
| M | 23 | $f(23) = 25$ | $f^{-1}(25) = 23$ |
| O | 25 | $f(25) = 27$ | $f^{-1}(27) = 25$ |
| R | 28 | $f(28) = 30$ | $f^{-1}(30) = 28$ |
| E | 15 | $f(15) = 17$ | $f^{-1}(17) = 15$ |
| I | 19 | $f(19) = 21$ | $f^{-1}(21) = 19$ |
| R | 28 | $f(28) = 30$ | $f^{-1}(30) = 28$ |
| A | 11 | $f(11) = 13$ | $f^{-1}(13) = 11$ |

**Tabela 5.2:** Cifragem e Decodificação Utilizando a Função e sua Inversa.

Gustavo, deseja que o lugar de encontro seja Delfim Moreira, dessa maneira ele utiliza a seguinte função $F(x) = x+2$, de acordo com a tabela 5.2, Gustavo cifrou a mensagem resultando na seguinte sequência "14152216192337232528151928 11", sua amada recebe a sequência e a decodifica sem dificuldade. Observando que foram utilizados números de dois algarismos na tabela 5.1, para evitar ambiguidades.

## 5.2 Aritmética Modular

Descreveremos algumas atividades utilizando aritmética modular como fonte motivadora.

### 5.2.1 Atividade para Sala de Aula - Aritmética Modular (calendário)

- Objetivo Geral: Instigar nos alunos pela descoberta da deliciosa maneira de se criar matemática.

| Dia da semana | resto da divisão por 7 |
|---|---|
| **Quinta-feira** | 0 |
| **Sexta-feira** | 1 |
| **Sábado** | 2 |
| **Domingo** | 3 |
| **Segunda-feira** | 4 |
| **Terça-feira** | 5 |
| **Quarta- feira** | 6 |

**Tabela 5.3:** Dias da Semana

- Objetivo específico: Desenvolver aplicações dos números primos.
- Público-alvo: Estudantes do ensino médio.
- Recursos Metodológicos: Quadro negro, giz, multimídia.
- Pré-requisito: conhecimento sobre, MDC e congruência.
- Metodologia: Desenvolver a atividade em grupos de no máximo 4 alunos.
- Duração: Duas aulas de 50 minutos.

**Exemplo 101.** Em um determinado país comemora-se a sua independência no dia 4 de julho, e o natal no dia 25 de dezembro, sabendo que 4 de julho foi uma quinta feira deseja-se saber que dia da semana irá cair o natal?

Vamos inicialmente enumerar os dias da semana, observe a tabela abaixo.
Vejamos então quantos dias existem entre quatro de julho e 25 de dezembro.

- Julho, 27 dias, agosto, 31 dias, setembro, 30 dias, outubro, 31 dias, novembro, 30 dias, dezembro- 25 dias. Temos um total de dias $27+31+30+31+30+25 = 174$ dias. Agora vejamos quando dividimos 174 por 7 deixa resto 6 , observando a tabela 5.3 o natal será na quarta-feira.

### 5.2.2 Atividade para Sala de Aula - Aritmética Modular - Cifra de César

- Objetivo Geral: Instigar nos alunos pela descoberta da deliciosa maneira de se criar matemática.
- Objetivo específico: Desenvolver aplicações dos números primos e funções .
- Público-alvo: Estudantes do ensino fundamental.
- Recursos Metodológicos: Quadro negro, giz, multimídia.
- Pré-requisito: conhecimento sobre, MDC e congruência.
- Metodologia: Desenvolver a atividade em grupos de no $f(x) \equiv x+3 \mod 26$,máximo 4 alunos.
- Duração: Uma aula de 50 minutos.

| **Alfabeto** | **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** |
|---|---|---|---|---|---|---|---|---|---|
| **valor de cada letra** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| **codificar-** $f(x) \equiv x+3 \mod 26$ | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| **decodificar -** $f(x)^{-1} \equiv (x+3)$**-3** $\mod 26$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| **Alfabeto** | **J** | **K** | **L** | **M** | **N** | **O** | **P** | **Q** | **R** |
| **valor de cada letra** | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| **codificar-** $f(x) \equiv x+3 \mod 26$ | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| **decodificar -** $f(x)^{-1} \equiv (x+3)$**-3** $\mod 26$ | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| **Alfabeto** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** | |
| **valor de cada letra** | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | |
| **codificar-**$f(x) \equiv x+3 \mod 26$ | 21 | 22 | 23 | 24 | 25 | 0 | 1 | 2 | |
| **decodificar -** $f(x)^{-1} \equiv (x+3)$**-3** $\mod 26$ | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | |

**Tabela 5.4:** Codificação e Decodificação

**Exemplo 102.** Vamos cifrar a mensagem "A criatividade é essencial na matemática".

Nesse exemplo utilizaremos a congruência a nosso favor, $f(x) \equiv x+3 \mod 26$, vamos observar a tabela 5.4 .

Assim observando a tabela 5.4verificamos que ao codificar a letra $x$ , trocaríamos ela pela letra $a$. Codificando a mensagem proposta irá ficar da seguinte forma "D fuldwlylgdgh h hvvhqfldo qd pdwhpdwlfd". Esse tipo de cifragem possui 25 possibilidades, pois na função somamos 3, mas poderíamos ter somado 1 até 25, para fazer a cifragem.

### 5.2.3 Atividade para Sala de Aula - Aritmética Modular - Cifra de Vigenère.

- Objetivo Geral: Instigar nos alunos pela descoberta da deliciosa maneira de se criar matemática.
- Objetivo específico: Desenvolver aplicações dos números primos e funções .
- Público-alvo: Estudantes do ensino fundamental.
- Recursos Metodológicos: Quadro negro, giz, multimídia.
- Pré-requisito: conhecimento sobre, MDC e congruência.
- Metodologia: Desenvolver a atividade em grupos utilizando $f(x) \equiv x_N + k_n \mod 26$, (aonde $x$ representa o valor da mensagem a ser codificada e $k$ representa o valor de cada letra da chave), máximo 4 alunos.
- Duração: Uma aula de 50 minutos.

**Exemplo 103.** Para facilitar a compreensão, vamos construir uma tabela 5.5 para codificar a mensagem utilizaremos $a = 0$,$b = 1$ e assim até $z = 25$.

A codificação feita na tabela 5.5, pode ser conferida pelos alunos, sem efetuar cálculos somente observando a figura 2.3.

| **Mensagem a ser codificada** | **Valor da Mensagem** | **Chave** | **Valor** | $f(x) \equiv x_N + k_n \mod 26$ | **Resultado** | **Mensagem cifrada** |
|---|---|---|---|---|---|---|
| **o** | 14 | o | 14 | $f(14) \equiv 14 + 14 \mod 26$ | 2 | C |
| | | | | | | |
| **t** | 19 | p | 15 | $f(19) \equiv 19 + 15 \mod 26$ | 8 | I |
| **e** | 4 | r | 17 | $f(4) \equiv 4 + 17 \mod 26$ | 21 | V |
| **n** | 13 | o | 14 | $f(13) \equiv 13 + 14 \mod 26$ | 1 | B |
| **e** | 4 | f | 5 | $f(4) \equiv 4 + 5 \mod 26$ | 9 | J |
| **n** | 13 | e | 4 | $f(13) \equiv 13 + 4 \mod 26$ | 17 | R |
| **t** | 19 | s | 18 | $f(19) \equiv 19 + 18 \mod 26$ | 11 | L |
| **e** | 4 | s | 18 | $f(4) \equiv 4 + 18 \mod 26$ | 22 | W |
| | | | | | | |
| **é** | 4 | o | 14 | $f(4) \equiv 4 + 14 \mod 26$ | 18 | Q |
| | | | | | | |
| **o** | 14 | r | 17 | $f(14) \equiv 14 + 17 \mod 26$ | 5 | F |
| | | | | | | |
| **t** | 19 | D | 3 | $f(19) \equiv 19 + 3 \mod 26$ | 22 | W |
| **r** | 17 | a | 0 | $f(17) \equiv 17 + 0 \mod 26$ | 17 | R |
| **a** | 0 | n | 13 | $f(0) \equiv 0 + 13 \mod 26$ | 13 | N |
| **i** | 8 | i | 8 | $f(8) \equiv 8 + 8 \mod 26$ | 16 | Q |
| **d** | 3 | e | 4 | $f(3) \equiv 3 + 4 \mod 26$ | 7 | H |
| **o** | 14 | l | 11 | $f(14) \equiv 14 + 11 \mod 26$ | 25 | Z |
| **r** | 17 | o | 14 | $f(17) \equiv 17 + 14 \mod 26$ | 5 | F |

**Tabela 5.5:** Função Modular na Cifra de Vigenère

### 5.2.4 Atividade para Sala de Aula - Abertura do cofre (protocolo de Shamir)

- Objetivo Geral: Instigar nos alunos pela descoberta da deliciosa maneira de se criar matemática.
- Objetivo específico: Desenvolver aplicações sobre funções .
- Público-alvo: Estudantes do ensino médio.
- Recursos Metodológicos: Quadro negro, giz, multimídia.
- Pré-requisito: conhecimento sobre, MDC e congruência e funções.
- Metodologia: Desenvolver a atividade em grupos de no máximo 4 alunos.
- Duração: Uma aula de 50 minutos.

**Exemplo 104.** Sr José é um milionário que já está quase no fim de sua vida. Ele possui três herdeiros em sua família mas nenhum deles é de se confiar, assim o Sr José colocou toda a sua fortuna em um cofre que só poderá ser aberto no dia do seu velório. Pensando nisto forneceu aos seus herdeiros algumas informações . Essas informações sozinhas não tem possibilidade nenhuma de abrir o cofre mas juntas fornecem um polinômio que desvenda o segredo, sendo que o termo independente desse polinômio que é o segredo não é revelado a nenhum de seus herdeiros. Para o primeiro o Sr José lhe deu o primeiro coeficiente 10, para o segundo herdeiro o segundo coeficiente 15 e para o terceiro herdeiro um ponto $(1, 800)$, como era de costume o Sr José adorava misturar funções e aritmética modular e também gostava de um número em especial que erá o 641. Ao falecer os herdeiros se reuniram para tentar abrir o cofre e perceberam que teriam muito trabalho tentando acertar a senha ao acaso, dessa maneira juntaram suas informações para desvendar a função.

Os herdeiros obtiveram a seguinte função, $f(x) = 10x^2 + 15x + c$, como a função deveria ser congruente a 641 e o ultimo herdeiro possuía um ponto, assim substituindo na função eles conseguiram descobrir o valor do termo independente, da seguinte forma: $10 \cdot 1^2 + 15 \cdot 1 + c \equiv 800 \mod 641 \rightarrow c \equiv 800 - 25 \mod 641 \rightarrow c \equiv 775 \mod 641 \rightarrow c \equiv 134 \mod 641$.Assim os herdeiros abriram o cofre.

# A Funções

Neste apêndice discorreremos algumas definições de funções, que são trabalhadas no ensino médio.

**Definição 105.** Uma função de $\mathbb{R} \to \mathbb{R}$, recebe o nome de função **afim**, se e somente se é da forma $f(x) = a \cdot x + b$ , sendo $a$ e $b$ pertencente ao conjunto dos reais. E para cada $x \in \mathbb{R}$ $\exists$ somente um $f(x)$ associado. Chamamos $a$ de coeficiente angular e $b$ de coeficiente linear da função.

**Exemplo 106.** Seja $f(x) = x + 3$ , observamos que o coeficiente linear é igual a 3 aonde o gráfico corta o eixo da ordenada e o coeficiente angular é 1 que é a tangente do ângulo formado pela função com o eixo da abscissa.

**Definição 107.** Uma função é **injetiva** se e somente se quaisquer que sejam $x_1$ e $x_2$ pertencente ao domínio da função e$x_1 \neq x_2$ implica que $f(x_1) \neq f(x_2)$.

**Exemplo 108.** Seja $f(x) = x + 3$, temos que a função é injetiva, pois para $x = 1 \to f(x_1) = 4$ e para $x = 2 \to f(x_2) = 5$.

**Definição 109.** Uma função é **sobrejetiva** se e somente se o contradomínio da função é igual a sua imagem.

**Exemplo 110.** Seja $f(x) = x + 3$, é uma função é sobrejetiva, pois qualquer que seja o valor de $x$ sempre teremos um valor para $f(x)$.

**Definição 111.** Uma função é **bijetora** se e somente se ela é injetiva e sobrejetiva ao mesmo tempo.

Como $f(x) = x + 3$, é injetiva e sobrejetiva, então ela é bijetiva.

# Índice Remissivo

# Referências Bibliográficas


[1] HEFEZ, Abramo. Aritmética. Rio de Janeiro: S.b.m, 2013.

[2] BOYER, Carl Benjamin. Tópicos de HISTÓRIA DA MATEMÁTICA para uso em sala de aula: Cálculo. São Paulo: Atual Editora, 1993.

[3] RONIELTON. Artigo revista segurança digital: publicações. 2012. Disponível em: http://www.ronielton.eti.br. Acesso em: 15 maio 2015.

[4] SINGH, Simon. O livro dos códigos. 7. ed. Rio de Janeiro: Record, 2008.

[5] RODRÍGUEZ, Manuel González. CIFRA DE ALBERTI. Disponível em: http://serdis.dis.ulpgc.es/~ii-cript/PAGINAWEB CLASICA/CRIPTPLOGIA/alberti.htm. Acesso em: 22 nov. 2015.

[6] WINTERBOTHAM, F. W.. Enigma. Disponível em: http://pt.wikipedia.org/wiki/Enigma_(máquina). Acesso em: 22 nov. 2015.

[7] ,A CIFRA de Vigenère. Disponível em: https://pt.wikipedia.org/wiki/Cifra_de_Vigenère. Acesso em: 22 nov. 2015.

[8] , FIARRESGA, Victor Manuel Calhabrês. Criptografia e Matemática. Disponível em: https://pt.wikipedia.org/wiki/Cítala. Acesso em: 22 nov. 2015.

[9] MIRANDA, Daniel; CAPUTI, Armando. Bases Matemáticas. Disponível em: http://gradmat.ufabc.edu.br/disciplinas/bm/livro/. Acesso em: 22 nov. 2015