**UNIVERSIDADE FEDERAL DE SÃO CARLOS**
**CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA**
**DEPARTAMENTO DE MATEMÁTICA**
**MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT**

**BRUNA SCHWARZ NUNES LUIZ**

# UM ESTUDO EXPLORATÓRIO ENVOLVENDO CRIPTOGRAFIA E NOÇÕES DE COMPUTAÇÃO QUÂNTICA

**SOROCABA**
**JANEIRO/2021**

**UNIVERSIDADE FEDERAL DE SÃO CARLOS**
**CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA**
**DEPARTAMENTO DE MATEMÁTICA**
**MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT**

**BRUNA SCHWARZ NUNES LUIZ**

# UM ESTUDO EXPLORATÓRIO ENVOLVENDO CRIPTOGRAFIA E NOÇÕES DE COMPUTAÇÃO QUÂNTICA

Dissertação apresentada ao Mestrado Profissional em Matemática em Rede Nacional, do Centro de Ciências Exatas e Tecnologia da Universidade Federal de São Carlos, como exigência parcial para obtenção do título de Mestre em Ensino de Matemática.

**Orientação:** Prof.ª Dr.ª Sílvia Maria Simões de Carvalho

**SOROCABA**
**JANEIRO/2021**

Schwarz Nunes Luiz, Bruna

Um estudo exploratório envolvendo criptografia e noções de computação quântica / Bruna Schwarz Nunes Luiz -- 2021.
102f.

Dissertação (Mestrado) - Universidade Federal de São Carlos, campus Sorocaba, Sorocaba
Orientador (a): Silvia Maria Simões de Carvalho
Banca Examinadora: Silvia Maria Simões de Carvalho, Paulo Cesar Oliveira, Mayk Vieira Coelho
Bibliografia

1. Estudo exploratório. 2. Criptografia. 3. Computação quântica. I. Schwarz Nunes Luiz, Bruna. II. Título.

Ficha catalográfica desenvolvida pela Secretaria Geral de Informática (SIn)

DADOS FORNECIDOS PELO AUTOR

Bibliotecário responsável: Maria Aparecida de Lourdes Mariano - CRB/8 6979

**UNIVERSIDADE FEDERAL DE SÃO CARLOS**

Centro de Ciências Exatas e de Tecnologia
Programa de Mestrado Profissional em Matemática em Rede Nacional

## Folha de Aprovação

Defesa de Dissertação de Mestrado da candidata Bruna Schwarz Nunes Luiz, realizada em 07/01/2021.

### Comissão Julgadora:

Profa. Dra. Silvia Maria Simões de Carvalho (UFSCar)

Prof. Dr. Mayk Vieira Coelho (UNIFAL)

Prof. Dr. Paulo Cesar Oliveira (UFSCar)

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

O Relatório de Defesa assinado pelos membros da Comissão Julgadora encontra-se arquivado junto ao Programa de Mestrado Profissional em Matemática em Rede Nacional.

*Dedico este trabalho aos meus pais, Neusa e Hernani, ao meu marido, Alan, e aos meus filhos, Ana Clara e Gabriel, pois sempre me apoiaram, me ajudaram e me incentivaram a não desistir e a concluir esta etapa de estudo com bastante dedicação e apreço.*

# AGRADECIMENTO

Primeiramente agradeço ao meu esposo Alan Nunes Luiz e aos meus filhos Ana Clara e Gabriel pelo apoio, paciência e força pois, desde 2017, não mediram esforços para me ajudar e me impulsionar sempre.

Agradeço também aos meus pais por estarem sempre presentes e por me ampararem em tudo que fosse necessário. Às minhas irmãs Francine e Natália também sou muito grata pelo incentivo em todos os aspectos.

Sem minha família seria impossível continuar a estudar e concretizar o desejo de me tornar mestre.

Do mesmo modo, gostaria de agradecer a todos os professores e professoras do curso na Universidade Federal de São Carlos, campus Sorocaba, por terem ministrado com maestria as aulas no curso do PROFMAT e por terem me proporcionado um avanço ímpar. Aos meus colegas de curso também sou muito grata pelo companheirismo e ajuda sempre.

De uma maneira muito especial, serei eternamente agradecida a minha professora orientadora Doutora Silvia Maria Simões de Carvalho por todo ensinamento passado, por todas orientações dadas e por todo carinho dado a mim e ao meu trabalho.

Por fim, agradeço a Deus por minha saúde, pelo dom da vida e pela maravilhosa oportunidade de me renovar com o estudo nestes últimos anos.

*"Nas grandes batalhas da vida, o primeiro passo para a vitória é o desejo de vencer".*

Mahatma Gandhi

# RESUMO

Neste trabalho, será apresentada um estudo exploratório sobre o ensino da criptografia e a influência do computador quântico na segurança de dados. O objetivo é demonstrar uma forma de como a fatoração e computação quântica pode ser aplicada no ensino regular nos anos finais do Ensino Fundamental. Os estudantes, apesar de terem muito contato com computadores diariamente, não entendem o que é um computador, os quanto seguros estão nas redes sociais e plataformas que usam e, muito menos, conhecem o desenvolvimento da computação quântica que é um tema tão atual e com muito poder de transformação no cotidiano de todos. Com a apresentação das aulas espera-se que os alunos tenham um panorama geral de criptografia e da computação quântica para que, assim, estejam em contato com a Matemática de forma mais aplicada e interessante.

**Palavras-chave:** criptografia; fatoração; computador quântico; estudo exploratório.

## ABSTRACT

In this paper, a proposal for a exploratory study of cryptography and the influence of the quantum computer on data security will be presented. The goal is to demonstrate a way of how factorization and quantum computing can be applied in regular education in the final years of elementary school. Students, despite having a lot of contact with computers on a daily basis, do not understand what a computer is, how safe they are on the social networks and platforms they use, let alone know the development of quantum computing, which is such a current and relevant topic, with a lot of transforming power in everyone's daily life. With the presentation of the classes, students are expected to have an overview of cryptography and quantum computing so that they are thus in contact with mathematics in a more applied and interesting way.

**Keywords:** encryption; factorization; quantum computer; exploratory study.

## Lista de Ilustrações

## Sumário

# 1. INTRODUÇÃO

A criptografia sempre esteve presente nas atividades humanas, porém o que se tem visto recentemente é que ela está inserida no cotidiano de todos pois possibilita a segurança de dados nas operações que envolvem internet, também nas transações bancárias e qualquer outra operação que necessite sigilo. Esta forma de seguridade envolve Matemática e Computação.

Ao longo da história existiram diferentes formas de se codificar mensagens e possibilitar que segredos fossem mantidos em segurança. As técnicas se desenvolveram bastante e hoje estão completamente relacionadas com o progresso da computação e do estudo aprofundado de conceitos matemáticos.

Como a Matemática e a Computação atuam na segurança de trocas de mensagens? Existe, realmente, segurança no sistema de Criptografia RSA usado na atualidade? Será que os jovens, estudantes do ensino regular, já ouviram falar de criptografia e da Computação Quântica, apesar de terem muito contato com internet e redes sociais desde que nasceram?

Estes questionamentos impulsionaram a pesquisa realizada nessa dissertação pois, apesar de estar presente na vida das famílias de forma geral, a proteção de dados confidencias através da criptografia não é conhecida pela grande maioria.

Outro fator que estimulou a exploração do tema foi acreditar que os jovens precisam estudar Matemática Computacional uma vez que a mesma é tema pertinente do seu dia a dia. O estudo de Física Quântica, atrelado a Computação Quântica, pode tornar essa disciplina mais atraente e compreensível. Ricardo Karam, professor e pesquisador da Universidade de Copenhague, Dinamarca, realizou uma pesquisa na qual pretendia mostrar como a Física pode tornar o ensino da Matemática mais atraente. Segundo ele, através da Física a Matemática ganha sentido e desperta o interesse dos estudantes. Explica que *"se o aluno percebe de onde vem esses conceitos matemáticos, a Matemática deixa de ser algo pronto e passa a ter um porquê"* [12].

No capítulo 2, é apresentado o desenvolvimento da criptografia desde a época Medieval até os dias atuais onde o sistema mais utilizado é a Criptografia RSA. Com a investigação feita percebe-se que as formas de codificação se desenvolvem ao passo que a tecnologia avança.

O conjunto dos números inteiros foi explanado no capítulo 3, juntamente com suas proposições e definições até a divisibilidade.

Na sequência os números primos são apresentados no capítulo 4 juntamente com os teoremas e definições necessárias ao entendimento de congruência modular que são aplicados diretamente no desenvolvimento da codificação de mensagens.

A criptografia de uma forma geral e a Criptografia RSA são expostas no capítulo 5 juntamente com as duas técnicas de fatoração estudadas: Fatoração por Fermat e Algoritmo de Shor. Nesta seção da dissertação também é retratada a importância da Computação Quântica na manutenção deste sistema de codificação.

Para que fosse possível esclarecer alguns questionamentos foi apresentado um estudo exploratório com uma sequência ideal dividida em quatro aulas. Foram escolhidos alguns alunos que fazem parte de um seleto grupo de estudos para competições em Olimpíadas de Matemática. Nessas aulas eles responderam um questionário sobre os temas estudados nesta dissertação e para que as dúvidas fossem esclarecidas. O desenvolvimento das aulas e do questionário estão apresentados no capítulo 6.

Por fim, no sétimo capítulo estão as conclusões desta pesquisa

# 2. CRIPTOGRAFIA MEDIEVAL E SUA EVOLUÇÃO ATÉ A CRIPTOGRAFIA RSA

## 2.1 Considerações Iniciais

Neste capítulo será abordada a história do desenvolvimento da criptografia no mundo desde a época medieval até a atualidade, a qual neste momento histórico utiliza-se o sistema RSA.

## 2.2 Desenvolvimento histórico

Criptografia, derivado do grego kryptós, que significa oculto e graphé, que significa escrita, é a "escrita oculta", ou seja, é o estudo das técnicas de ocultação de informações. Esta é uma área tradicionalmente ligada à segurança da informação, remontando a um passado de milhares de anos.

O desenvolvimento da criptografia e da criptoanálise começou com a necessidade de transmissão de mensagens confidenciais, compreendidas apenas pelo emissor e pelo receptor. Isso ocorreu após o aparecimento da escrita com a necessidade de interceptar mensagens e decifrá-las. Aparece por volta de 2000 a.C. no Egito e na Mesopotâmia. O primeiro uso documentado foi no Egito, em 1900 a. C., quando um escriba usou hieróglifos fora do padrão numa inscrição. Este apenas inseriu caracteres fora do padrão no meio do texto original. Os hebreus utilizavam, entre 600 a.C. e 500 a.C., a cifra de substituição simples onde os caracteres são trocados sequencialmente por outros e, após a primeira codificação, repetiam o processo (cifra dupla) [1].

Na antiguidade existia dois métodos de ocultar mensagens de um possível interceptor. O primeiro, chamado de esteganografia, consistia em esconder a mensagem. Neste método, se a mensagem for interceptada será imediatamente decifrada. Exemplos de uso desta técnica são mensagens inscritas em cabeças raspadas e uso de micropontо na Segunda Guerra Mundial. No segundo método foram usados processos mais elaborados nos quais a mensagem mesmo tornada pública, não seria entendida pelo interceptador. A diferença entre a esteganografia e a criptografia é que a primeira tem como objetivo impedir que a mensagem seja descoberta e, na segunda, o objetivo é impedir que seja compreendida [1] e [3].

Por volta do século V a.C., a cidade grega Esparta era dominada por uma rígida cultura de guerra e por uma grande preocupação com a segurança das comunicações militares. Para codificar as mensagens usavam o "Bastão de Licurgo", um bastão de madeira ao redor do qual se enrolava-se, em forma de espiral, uma tira, de couro ou papiro, longa e estreita. O remetente

escrevia a mensagem em colunas, ao longo do bastão e depois desenrolava a tira, que se convertia em uma sequência de letras sem sentido. O mensageiro usava a tira como cinto, com as letras voltadas para dentro. O destinatário, ao receber o cinto, enrolava-o em seu bastão, cujo diâmetro e comprimento eram iguais ao do bastão do remetente. Desta forma, podia ler a mensagem [1].

Este artifício de trocar as letras de posição para codificar as mensagens deu o nome de "Transposição" ao método criptográfico.

A necessidade de ocultar mensagens também sempre esteve presente nas guerras. Júlio César (100 – 44 a.C), imperador romano, usava na correspondência militar com seus generais uma chave de substituição simples, na qual cada letrada mensagem original era substituída pela letra que a seguia em três posições do alfabeto. Em sua homenagem, este código é chamado de Código de César. Substituía a letra A pela D, a B pela E, e assim sucessivamente. A chave de um código de César fica totalmente determinada por um número entre 1 e 24 que corresponde ao deslizamento das letras do alfabeto. Qualquer cifra em que cada letra da mensagem original seja substituída por outra deslocada em um número fixo de posições, não necessariamente três. Um código de César é um método onde uma chave, definida por um número, é usada para cifrar e para decifrar a mensagem. As duas partes, o emissário e o destinatário, conhecem a chave. Este sistema de comunicação coloca toda a segurança do processo sobre a chave e nenhuma sobre o algoritmo. Métodos criptográficos desta natureza são conhecidos como de chave simétrica [1].

Na Idade Média, período que se iniciou em 476 com a queda do Império Romano e terminou em 1453 com a queda de Constantinopla, há poucos sinais históricos do uso da criptografia. Havia muitas perseguições religiosas e, por isso, a correspondência através de mensagens misteriosas e indecifráveis era perigosa e pouco utilizada. Há poucos indícios do uso da criptografia pelos monges apenas para passatempo ou diversão.

Todos os sistemas de códigos utilizados na Idade Média eram de cifras monoalfabéticas, onde cada letra distinta do alfabeto está relacionada a exatamente a um símbolo distinto. De modo geral, o uso de código para a transmissão de mensagens secretas impõe que tanto o remetente quanto o destinatário gravem a chave que gera o código em algum meio (por exemplo escrevendo em um papel) e esconda a anotação em local seguro. O ideal seria a memorização da cifra [1].

Até a primeira metade da Idade Média (até o ano 800), as cifragens monoalfabéticas, como o Código de César, dominavam as trocas de mensagens secretas.

Nesta mesma época, por volta do ano 750, a civilização árabe faz nascer a criptoanálise, com a "análise de frequências". Assim, colocaram os decodificadores na frente dos codificadores.

Na Europa, a Itália foi o país percursor em relação ao tratamento da criptografia com profissionalismo e como questão de estado. O uso da criptografia, criou em 1450, uma secretaria dentro do governo, com o objetivo de lidar com a escrita secreta, solucionando e criando cifras,

a “câmara negra”. Este tempo é também marcado pelo nascimento da Imprensa e a consequente mecanização da escrita. O tratamento de Estado dado à criptografia em Veneza se espalhou, pouco a pouco, por toda a Europa [1].

Na Idade Moderna, em 1580, os criptógrafos continuavam dependentes da cifra monoalfabéticas. Mas, criptoanalistas como Babou, Soro, Viète e Rossignol estavam destruindo as mensagens com a análise de frequências.

A criptografia estava em desvantagem perante a criptoanálise, até que surgiram dois grandes códigos: os códigos de Rossignol (homófona, trabalhava com mais de 500 números e cada grupo de números era associado a uma sílaba da língua francesa) e de Vigenère. A cifragem e decifragem de uma mensagem com uma cifra de Vigenère era muito demorada, dificultando seu uso. Este método usava uma série de diferentes cifras de César baseadas em letras de uma senha. Quando finalmente foi posta em prática, por volta de 1760, teve um curto prazo de validade. A quebra da cifra de Vigenère foi uma realização extraordinária da criptoanálise. Foi o primeiro resultado relevante depois da criação da análise de frequência pelos árabes há mil anos [1].

Em 1844, Samuel Morse desenvolve o código que recebeu seu nome e inventa o telégrafo. O Código Morse é um sistema binário de representação à distância de números, letras e sinais gráficos, utilizando-se de sons curtos e longos, além de pontos e traços para transmitir mensagens. A invenção do telégrafo alterou profundamente a criptografia e tornou a cifragem uma necessidade quase absoluta. Em 1894, o físico italiano Marconi dá os primeiros passos na criação de uma nova e mais poderosa ferramenta de telecomunicação, fazendo necessária uma codificação mais segura: o rádio. “Um sistema de comunicação rápido, eficiente e sem fios, com o sinal viajando magicamente pelo ar a longa distância. Um sistema francamente aberto, impondo imensos desafios à proteção da informação” [1].

A primeira fase no desenvolvimento da criptografia registra as primeiras manifestações históricas e coincide com o advento da escrita, cobrindo as Idades Antiga e Média. No início da Idade Moderna, com a invenção da Imprensa, aparecem os primeiros indícios da fase mecânica da criptografia. A terceira fase, a mecânica, inicia-se com a Revolução Industrial, iniciada na Inglaterra em 1760, seguida da invenção do telégrafo e do rádio no século seguinte. Seu apogeu ocorre com as máquinas de cifragens usadas durante a Segunda Guerra Mundial.

A Primeira Guerra Mundial, 1914 a 1918, iniciou com a grande ofensiva alemã. Neste conflito, a mais famosa cifra em uso foi a ADFGVX, obtida com uma combinação de técnicas de substituição e transposição.

Durante a Segunda Guerra Mundial, de 1939 a 1945, entra em cena a máquina de cifras alemã denominada Enigma. A primeira foi desenvolvida em 1918 e seu objetivo era facilitar a troca de documentos secretos entre comerciantes e homens de negócios. Mais tarde, esta invenção se torna interessante para uso militar. O exército redesenhou a máquina, começou a usá-la em 1930, e a chamou de Enigma I. Para cifrar uma mensagem, o operador teclava uma letra e o comando estimulava o circuito elétrico e as letras cifradas apareciam, uma a uma, no painel luminoso. Eram anotadas para compor a mensagem secreta [1].

A máquina Enigma trabalhava com um processo de cifragem complexo e de chave simétrica e, por questões de segurança, a cada mensagem a chave era trocada. O trabalho de quebra da cifra Enigma foi concluído pela equipe inglesa liderada por Alan Turin, Gordon Welchman e outros pesquisadores, em Bletchley Park, Inglaterra.

Segundo Silva:

> A criptografia é tão antiga quanta a própria escrita, já estava presente no sistema de escrita hieroglífica dos egípcios. Os romanos utilizavam códigos secretos para comunicar planos de batalhas. O mais interessante é que a tecnologia de Criptografia não mudou muito até meados deste século. Depois da Segunda Guerra Mundial, com a invenção do computador, a área realmente floresceu incorporando complexos algoritmos matemáticos. Durante a guerra, os ingleses ficaram conhecidos por seus esforços para decifração de mensagens. Na verdade, esse trabalho criptográfico formou a base para a ciência da computação moderna. (SILVA. 2008. p.137) [2].

Em 1974, a IBM, International Business Machines Corporation, empresa norte americana da área de informática, apresenta a NBS (órgão oficial de segurança em comunicação do governo norte americano) uma nova cifra, o código DES (Data Encryption Standard), que funciona como chave simétrica privada de 56 bits e é extremamente difícil de ser quebrado. A NBS, após avaliar o algoritmo com a ajuda da NSA (National Security Agency), adotou para o governo este código como padrão de cifragem de dados para os Estados Unidos [1].

O código DES foi concebido para implementação em computador. É o algoritmo criptográfico mais usado atualmente no mundo atendendo a bancos, órgãos de defesa, grandes empresas e comércio eletrônico na internet. Com ele, iniciou-se a fase digital da criptografia.

Na atualidade, a criptografia se firmou como uma importante ferramenta para auxiliar a necessidade de troca de informações com segurança.

O código de César na antiguidade, a cifra ADFGVX usada na Primeira Guerra Mundial, a máquina Enigma usada no Segunda Guerra Mundial e a poderosa cifra DES, tem uma característica comum: chave privada. Mas, o processo com chave privada tem uma grande fraqueza pois necessita de um canal de comunicação em paralelo, seguro suficiente para a troca entre remetente e destinatário. A necessidade de uma chave simétrica foi considerada uma verdade necessária durante quase dois mil anos, até que foi contrariada em 1976, com a criação do conceito de chave pública/chave privada (na chave pública, o processo de codificação pode ser conhecido de qualquer um sem comprometer a segurança do código) [1].

A criação do conceito de chave pública surgiu quando dois pesquisadores, Whitfi eld Diffie e Martin Hellman em 1976, conseguiram descobrir que há possibilidade de troca de mensagens no sistema aberto de comunicação através de uma combinação de função exponencial com aritmética modular. Com isso, tivemos a invenção da chave pública/privada, através da famosa cifra RSA, em 1977, que, apesar de não ser a única, é a mais utilizada em aplicações comerciais [1].

### 2.2.1 Sistema criptográfico RSA

Rivest, Shamir e Adleman, três pesquisadores do MIT (Massachussets Institute of Technology), construíram um dos mais poderosos algoritmos criptográficos que o mundo conheceu. O algoritmo foi batizado como RSA, iniciais dos três nomes.

É um método com chave pública que encaminha a mensagem juntamente com sua chave de decodificação. Atua diretamente na internet, por exemplo, em mensagens de e-mails, compras on-line e assinaturas digitais.

O algoritmo RSA tem sua base matemática na teoria dos números primos e a aritmética modular. Trabalha com duas chaves matematicamente ligadas, uma para cifrar (chave pública) e outra para decifrar (chave secreta, particular). A chave privada, usada para decifrar, consiste de dois números primos muito grandes (digamos P e Q). A chave pública, usada para cifrar, é definida por N, onde N é obtido pelo produto N = P x Q. A chave pública N pode ser comunicada a todo mundo. Quebrar o RSA consiste em fatorar N, e neste ponto está sua segurança. Mas, há um problema de natureza tecnológica: não existem computadores rápidos o suficiente, nem algoritmos bons o suficiente, que nos permitam fatorar um número inteiro muito grande que não tenha fatores relativamente pequenos. Atualmente, as implementações comerciais do RSA usam chaves públicas com cerca de 200 algarismos, mas algumas destas implementações chegam a permitir chaves públicas com até 2 467 algarismos [1].

No entanto, ainda assim, os ataques de “hackers” são constantes conforme revela Barbosa (2003, p. 16):

> A segurança desse método se baseia na dificuldade da fatoração de números inteiros extensos. Em 1977, os criadores do RSA achavam que uma chave de 200 bits requereria 1015 anos, porém chaves com 155 bits foram atacadas em menos de 8 meses. A saída é que na medida que os algoritmos se tornem melhores e os computadores se tornem mais velozes, maiores serão as chaves. Atualmente chaves com 300 dígitos (1000 bits) nos dão uma tranquilidade por algum tempo. Em níveis críticos, chaves com 2000 bits começam a ser usadas [4].

Durante algum tempo, o RSA Laboratory, que pertence à empresa que detém os direitos do sistema de codificação RSA, lançou desafios, que consistiam de uma possível chave pública de RSA que deveria ser fatorada. A última destas chaves a ser fatorada tem 193 algarismos e corresponde ao produto dos primos:

1634733645809253848443133883865090859841783670033092312181111085238933
3100104508151212118167511579

e,

19008712816648221131268515739354139754718967899685154936666385390880271038021044989571912614655 71 [1].

A fatoração foi finalizada em novembro de 2005 por F. Bahr, M. Boehm, J. Franke e T. Kleinjung no Escritório Federal de Segurança de Informação da Alemanha. Os cálculos utilizaram 80 computadores de 2.2 GHz cada um e, mesmo assim, foram necessários 5 meses para completar as contas [1].

O algoritmo RSA é classificado como chave assimétrica, uma vez que a chave que cifra a mensagem é diferente da chave que decifra a mensagem e, assim, elimina a necessidade de troca preliminar de chaves e fornece um método para autenticação de mensagens.

# 3. NÚMEROS INTEIROS

A necessidade de contar e relacionar quantidades fez com que o homem desenvolvesse símbolos para expressar as situações vividas. Com isso, sistemas de numerações foram criados em todo o mundo no decorrer dos tempos.

O surgimento dos números naturais revolucionou o método de contagem pois relacionava números a quantidades. Com a expansão comercial na Europa no final da Idade Média, aumentou-se a circulação de dinheiro e, assim, os comerciantes tiveram a necessidade de expressarem situações envolvendo lucros e prejuízos. Assim, foi surgindo o conjunto dos números inteiros, representado pelo símbolo $\mathbb{Z}$.

Assim, tem-se que $\mathbb{Z} = \{...-3, -2, -1, 0, 1, 2, 3...\}$. Neste conjunto destacam-se os seguintes subconjuntos:

- Conjunto $\mathbb{Z}^*$ dos inteiros não nulos: $\mathbb{Z}^* = \{\pm1, \pm2, \pm3, ...\}$;
- Conjunto $\mathbb{Z}_+$ dos inteiros não negativos: $\mathbb{Z}_+ = \{0, 1, 2, 3, ...\}$;
- Conjunto $\mathbb{Z}_-$ dos inteiros não positivos: $\mathbb{Z}_- = \{...-3, -2, -1, 0\}$;
- Conjunto $\mathbb{Z}_+^*$ dos inteiros positivos: $\mathbb{Z}_+^* = \{1, 2, 3, ...\}$;
- Conjuntos $\mathbb{Z}_-^*$ dos inteiros negativos: $\mathbb{Z}_-^* = \{... -3, -2, -1\}$.

Os inteiros positivos são também chamados de naturais e por isso, o conjunto dos inteiros positivos é habitualmente designado pela letra $\mathbb{N}$.

## 3.1 Propriedades dos números inteiros

As propriedades que serão enunciadas são quesitos dos resultados seguintes deste trabalho e bases para a fundamentação teórica do tema principal abordado.

O conjunto $\mathbb{Z}$ munido das operações de adição (+) e multiplicação (.) possui as seguintes propriedades: [5]

**Propriedade 3.1.1:** A adição e a multiplicação são bem definidas.

Para todos a, b, a', b' $\in \mathbb{Z}$, se a = a' e b = b', então:

a + b = a' + b' e a.b = a'.b'.

**Propriedade 3.1.2:** A adição e a multiplicação são comutativas.

Para todos a, b ∈ ℤ, a + b = b + a e a.b = b.a.

**Propriedade 3.1.3:** A adição e a multiplicação são associativas.

Para todos a, b, c ∈ ℤ, (a + b) + c = a + (b + c) e (a.b).c = a. (b.c).

**Propriedade 3.1.4:** A adição e a multiplicação possuem elementos neutros.

Existe 0 ∈ ℤ tal que, para todo a ∈ ℤ, a + 0 = 0 + a = a.

Existe 1 ∈ ℤ tal que, para todo a ∈ ℤ, a.1 = 1.a = a.

**Propriedade 3.1.5:** A adição possui elemento simétrico.

Para todo a ∈ ℤ, existe (-a) tal que a + (-a) = 0.

**Propriedade 3.1.6:** A multiplicação é distributiva com relação à adição.

Para todos a, b, c ∈ ℤ, tem-se a. (a + b) = a.b + a.c.

**Propriedade 3.1.7:** Fechamento de ℕ (conjunto dos números naturais).

O conjunto ℕ é fechado para a adição e para a multiplicação, ou seja, para todos a, b ∈ ℕ, tem-se que a + b ∈ ℕ e a.b ∈ ℕ.

**Propriedade 3.1.8:** Tricotomia.

Dados a, b ∈ ℤ, uma, e apenas uma, das seguintes possibilidades é verificada:

- a = b;
- b – a ∈ ℕ e, assim, diz-se que *a é menor que b*, e representa-se a < b;
- - (b – a) = a – b ∈ ℕ e, assim, diz-se que *a é maior que b*, e representa-se a > b.

## 3.2 Proposições

Nesta seção serão abordadas algumas proposições dos números inteiros necessárias para entender o funcionamento da criptografia de uma maneira geral. Serão usadas nas demonstrações dos principais resultados que possibilitam a segurança de mensagens criptografadas.

**Proposição 3.2.1:** Para todo a ∈ ℤ, a.0 = 0.

Demonstração:

*Temos que a.0 = a. (b + (-b)), para todo b ∈ ℤ. Como a, b ∈ ℤ, então*

*a.b = c ∈ ℤ.*

*Logo, a.0 = c + (-c), com c ∈ ℤ. Pela propriedade 3.1.5, temos a.0 = 0.*

**Proposição 3.2.2:** A adição é compatível e cancelativa com respeito à igualdade. Ou seja, para todos a, b, c ∈ ℤ, a = b se, e somente se, a + c = b + c.

Demonstração:

*(→)*

*Por hipótese temos que a = b (para todo a, b ∈ ℤ). Seja c ∈ ℤ, somando c em ambos os lados da igualdade, temos que a + c = b + c.*

*(←)*

*Por hipótese temos que a + c = b + c, com c ∈ ℤ. Então, existe -c ∈ ℤ. Somando o simétrico de c em ambos os lados temos que a + c + (-c) = b + c + (-c).*

*Pela propriedade 2.1.5, temos que c + (-c) = 0 ∈ ℤ. Logo, a + 0 = b + 0 e, assim, a = b.*

Para a sequência das proposições, será levado em consideração que, dados dois inteiros a e b, define-se o número *b menos a*, denotado por b – a, como sendo o resultado da adição b + (-a). Diz-se que b – a é o resultado da subtração de a de b.

**Proposição 3.2.3:** A relação “menor do que” é transitiva. Portanto, para todos a, b, c ∈ ℤ, a < b e b < c implica que a < c.

Demonstração:

*Sabendo que a < b tem-se que b – a ∈ ℕ e, se b < c, tem-se que c – b ∈ ℕ. Pelo fechamento dos naturais tem-se que (b – a) + (c – b) ∈ ℕ.*

*Pelas propriedades 2.1.3 e 2.1.5:*

*b – a + c – b = c – a.*

*Como c – a ∈ ℕ, então a < c.*

**Proposição 3.2.4:** A adição é compatível e cancelativa com respeito à relação “menor do que”. Ou seja, para todos a, b, c ∈ ℤ, a < b se, e somente se,

a + c < b + c.

Demonstração:

*Suponha que a < b. Logo, b – a ∈ ℕ. Portanto, (b + c) – (a + c) = b – a ∈ ℕ. Isto implica que a + c < b + c.*

*Reciprocamente, suponha que a + c < b + c. Somando (-c) a ambos os lados da desigualdade, tem-se:*

*a + c + (-c) < b + c + (-c)*

*Como a adição é cancelativa, conclui-se que a < b.*

**Proposição 3.2.5:** A multiplicação por elementos de ℕ é compatível e cancelativa com respeito à relação “menor do que”. Ou seja, para todos a, b ∈ ℤ, para todo c ∈ ℕ, a < b implica que a.c < b.c.

Demonstração:

*Suponha que a < b. Logo, b – a ∈ ℕ.*

*Assim, se c ∈ ℕ, como ℕ é fechado, tem-se que b.c – a.c = (b – a).c ∈ ℕ. Logo, a.c < b.c.*

*Reciprocamente, suponha que a.c < b.c, com c ∈ ℕ. Pela 3.1.8, tricotomia, tem-se três possibilidades a analisar:*

1. *Supor a = b.*

   *Isso acarretaria que a.c = b.c, o que é falso.*
2. *Supor b < a.*

   *Isso acarretaria que a.c > b.c, o que é falso pela primeira parte da demonstração.*
3. *Supor a < b.*

   *Única válida, pela tricotomia.*

**Proposição 3.2.6:** A multiplicação é compatível e cancelativa com respeito à igualdade.

Isto é, para todos a, b ∈ Z, para todo c ∈ ℤ \ {0}, a = b se, e somente se,

a.c = b.c.

Demonstração:

*(→)*

*Por hipótese, a = b. Isto implica que a.c = b. c pela propriedade 3.1.1. Também vale quando c = 0.*

*(←)*

*Supor que a.c = b.c.*

*Há duas possibilidades:*

1. *Caso c > 0.*

   *Se a < b, pela proposição 3.2.5, tem-se que a.c < b.c, o que é um absurdo.*

   *Se b > a, pelo mesmo argumento, b.c < a.c, o que é absurdo.*

   *Portanto, a única alternativa válida é a = b.*
2. *Caso –c > 0.*

   *Se a < b, tem-se que a.c > b.c, o que é absurdo.*

   *Se b > a, a.c < b.c, o que é um absurdo.*

   *Portanto, a = b.*

Com essas proposições, tem-se que ℤ é um *domínio de integridade*. Isto significa que, se a e b são números inteiros tais que a.b = 0, então a = 0 ou b = 0 [5].

Demonstração:

*Para todos a, b ∈ ℤ. Sem perda de generalidade, supõe-se que a ≠ 0.*

*Se a.b = 0, a.b = a.0.*

*Como a ≠ 0, tem-se que b =0.*

Neste trabalho serão usadas as notações a ≤ b, para a menor ou igual a b e a notação a ≥ b para a maior ou igual a b.

## 3.3 Valor absoluto de um número inteiro

Seja a ∈ ℤ, define-se que:

$$| a | = \begin{cases} a, \text{se } a \geq 0 \\ -a, \text{se } a < 0. \end{cases}$$

O número inteiro |a| é chamado de módulo ou valor absoluto de a [5].

**Proposição 3.3.1:** Para a, b ∈ ℤ e r ∈ ℕ, tem-se que [5]:

i. |a. b| = |a|. |b|;

Demonstração:

$|a.\ b|^2 = (a.b)^2 = a^2.b^2 = |a|^2.\ |b|^2 = (|a|.\ |b|)^2$

*Logo,* $|a.\ b|^2 = (|a|.\ |b|)^2$ *e, pela definição de módulo,* $|a.\ b| = |a|.\ |b|$.

ii. |a| ≤ r se, e somente se, -r ≤ a ≤ r;

Demonstração:

*(→)*

*Por hipótese,* $|a| \leq r$.

*Sendo* $a > 0$, *temos que* $|a| = a$ *e, assim,* $a \leq r$.

*Sendo* $a < 0$, *temos que* $|a| = -a$ *e, assim,* $-a \leq r$.

*Logo,* $-r \leq a \leq r$.

*(←)*

*Por hipótese,* $-r \leq a \leq r$.

*Como* $a \leq r$, *tem-se que* $|a| \leq |r| = r$, *pois* $r \in \mathbb{N}$.

*Como* $a \geq -r$, *tem-se que* $-a \leq r$. *Isto implica que* $|-a| \leq |r|$ *e, assim,* $|a| \leq r$.

iii. Desigualdade triangular: $|a + b| \leq |a| + |b|$

Demonstração:

$|a + b|^2 = (a + b)^2 = a^2 + 2.a.b + b^2$

*Mas,* $a^2 + 2.a.b + b^2 \leq |a|^2 + 2.\ |a|.|b| + |b|^2 = (|a| + |b|)^2$.

*Logo,* $|a + b|^2 \leq (|a| + |b|)^2$ *e, pela definição de módulo,* $|a + b| \leq |a| + |b|$.

## 3.4 Princípio da Boa Ordenação

O Princípio da Boa ordenação é uma propriedade particular do conjunto dos Números Inteiros diferenciando-o dos Racionais e dos Reais.

Diz que todo subconjunto não vazio formado por números inteiros não negativos possui um menor elemento. Em outras palavras, todo subconjunto não vazio de $\mathbb{Z}_+$ possui o *elemento mínimo*.

Demonstração:

*Nesta demonstração será usado o Princípio de Indução Matemática que está na seção 3.6.1 deste trabalho.*

*Suponha que exista um conjunto $S \subset \mathbb{N}$ que não possua menor elemento. Deve-se mostrar que S é um conjunto vazio.*

*Considerando a afirmação de que n não pertence a S deve-se provar que ela vale para todo $n \epsilon \mathbb{N}$.*

*Tem-se que 1 não pertence a S, pois, do contrário, 1 seria o menor elemento de S. Suponha agora que 1, 2, ..., k não pertençam a S e deve-se mostrar que k + 1 não pertence a S.*

*Se $(k + 1) \epsilon S$ então k + 1 seria o menor elemento de S, pois todos os naturais menores que k + 1 não estão em S, o que seria uma contradição. Logo, k + 1 não pertence a S.*

*Portanto, nenhum elemento de $\mathbb{N}$ está em S. Como $S \subset \mathbb{N}$, S é um conjunto vazio. Assim, pode-se afirmar que se $S \subset \mathbb{N}$ e S não é vazio, então S possui um menor elemento.*

Este princípio tem como principal consequência o Princípio de Indução Finita que é um excelente instrumento para a demonstração de resultados relevantes para o estudo dos Números Inteiros e, consequentemente, da criptografia.

A propriedade enunciada a seguir, é necessária para que que o Princípio da Indução Finita seja aplicado com eficiência e veracidade.

**Propriedade 3.4.1:** Não existe nenhum número inteiro n tal que $0 < n < 1$.

Demonstração:

*Suponha, por absurdo, que exista n tal que $0 < n < 1$.*

*Logo, o conjunto $S = \{x \in \mathbb{Z} / 0 < x < 1\}$ é não vazio e é limitado inferiormente. Portanto, S possui um menor elemento a, com $0 < a < 1$.*

*Multiplicando a desigualdade por a, obtemos $0 < a^2 < a < 1$, logo $a^2 \in S$ e $a^2 < a$. Isto é uma contradição.*

*Logo, S é vazio e, assim, não existe n inteiro tal que $0 < n < 1$ [5].*

**Corolário:** Propriedade Arquimediana

Sejam a, b ∈ ℤ, com b ≠ 0. Então existe n ∈ ℤ tal que n.b > a.

Demonstração:

*Como |b| ≠ 0, pela propriedade 2.4.1, tem-se que |b| ≥ 1. Logo,*

*(|a| + 1). |b| ≥ |a| + 1 > |a| ≥a.*

*Tomando n = |a| + 1, tem-se que n.b > a, se b > 0.*

*E, tomando n = -(|a| + 1), se b < 0, tem-se n.b > a [5].*

## 3.5 Divisibilidade

Sejam a, b ∈ ℤ, com a ≠ 0, diz-se que *a* divide *b* se, e somente se, existe um inteiro q tal que b = a.q.

Se *a* divide *b*, também se diz que *a* é um divisor de *b*, que *b* é um múltiplo de *a*, que *a* é um fator de *b* ou que *b* é divisível por *a*.

Com a notação a|b indica-se que *a* ≠ 0 divide *b*.

E, com a notação a∤b, indica-se que a ≠ 0 não divide b.

Se a é um divisor de b, então –a também é um divisor de b, pois pela igualdade b = a.q implica que b = (-a). (-q), de modo que os divisores de um inteiro qualquer são dois a dois iguais em valor absoluto e de sinais opostos [6].

**Proposição 3.5.1:** Sejam os inteiros a, b e c, tem-se:

i. a|0, 1|a e a|a;
ii. Se a|1, então a = ± 1;
iii. Se a|b e c|d, então a.c|b.d;
iv. Se a|b e b|c, então a|c;
v. Se a|b e b|a, então a = ± b;
vi. Se a|b, com b ≠ 0, então |a| ≤ |b|;

vii. Se a|b e se a|c, então a| (b.x + c.y), para todos x,y ∈ ℤ. [6]

Demonstração:

*i. Decorre das seguintes igualdades:*
*0 = a.0, a = 1.a, a = a.1.*

*ii. Se a|1, então 1 = a.q, com q ∈ ℤ.*
*Isto implica que a = 1 e q = 1 ou a = -1 e q = -1. Logo, a = ± 1.*

*iii. Tem-se que a|b. Logo existe q ∈ ℤ tal que b = a.q.*
*Também, c|d. Assim, existe $q_1$ ∈ ℤ tal que d = c.$q_1$.*
*Portanto: b.d = (a.c). (q.$q_1$).*
*Logo, a.c|b.d.*

*iv. Tem-se que a|b. Logo existe q ∈ ℤ tal que b = a.q.*
*Também, b|c. Assim, existe $q_1$ ∈ ℤ tal que c = b.$q_1$.*
*Portanto: c = a. (q.$q_1$).*
*Logo, a|c.*

*v. Tem-se que a|b. Logo existe q ∈ ℤ tal que b = a.q.*
*Também, b|a. Assim, existe $q_1$ ∈ ℤ tal que a = b.$q_1$.*
*Portanto: a = a. (q.$q_1$). Isto implica que q.$q_1$ = 1 e, assim, $q_1$|1, ou $q_1$ = ± 1 e, assim, a = ± b.*

*vi. Por hipótese, a|b e b ≠ 0.*
*Logo, existe q ∈ ℤ tal que b = a.q, com q ≠ 0 e |b| = |a|. |q|.*
*Como q ≠ 0, segue-se que |q| ≥ 1 e, portanto, |b| ≥ |a|.*

*vii. Por hipótese, a|b. Logo existe q ∈ ℤ tal que b = a.q. E, a|c. Logo, existe $q_1$ ∈ ℤ tal que c = a.$q_1$.*
*Portanto, quaisquer que sejam os inteiros x e y:*
*b.x + c.y = a.q.x + a.$q_1$.y = a. (q.x + $q_1$.y)*

*Isto implica que a| (b.x + c.y)* [6].

**Proposição 3.5.2:** Sejam a, b ∈ ℤ e n ∈ N. Tem-se que a – b divide $a^n – b^n$.

Demonstração:

*Prova por indução sobre n.*

*A afirmação é verdadeira para n =1, pois a – b divide $a^1 – b^1 = a – b$.*

*Suponha, agora, que $a – b|a^n – b^n$.*

*Assim:*

$a^{n+1} – b^{n+1} = a.a^n – b.a^n + b.a^n – b.b^n = (a – b).a^n + b. (a^n – b^n)$.

*Tem-se que a - b|a – b e, por hipótese, $a - b|a^n – b^n$.*

*Logo, pela proposição 2.4.1, item vii, $a - b|a^{n+1} – b^{n+1}$.*

*Assim, o resultado é válido para n ∈ ℕ [5].*

## 3.6 Divisão Euclidiana

Euclides, um dos maiores pensadores da história da ciência matemática, viveu entre os séculos III e II a.C. Seu conhecimento invadiu todo o mundo conhecido à época e foi absorvido pelas civilizações que o sucederam, especialmente a Roma Antiga.

É o autor de *Os Elementos*, escrito por volta de 300 a.C.. Este tratado consiste em 13 livros dedicados a geometria plana (triângulos, linhas paralelas, propriedades do círculo) e aritmética, incluindo números primos, máximo divisor comum e o método das divisões sucessivas repetidas, hoje resumidos sob o nome de divisão euclidiana.

**Teorema 3.6.1:** Sejam a e b dois números inteiros com $b \neq 0$. Existem dois únicos inteiros q e r tais que $a = b.q + r$, com $0 \leq r \leq |b|$ [5].

Demonstração:

*Seja o conjunto $C = \{a – by / y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$.*

*Pela Propriedade Arquimediana, existe* $n \in \mathbb{Z}$ *tal que* $n.(-b) > -a$.

*Assim,* $a - n.b > 0$, *o que mostra que S é um conjunto não vazio.*

*O conjunto S é limitado inferiormente por 0. Então, pelo Princípio da Boa Ordenação, S possui um menor elemento r. Suponha então que* $r = a - b.q$. *Sabe-se que* $r \geq 0$. *Para mostrar que* $r \leq |b|$, *deve-se supor, por absurdo, que* $r \geq |b|$. *Portanto, existe* $s \in \mathbb{N} \cup \{0\}$ *tal que* $r = |b| + s$, *logo* $0 \leq s \leq r$. *Mas, isto contradiz o fato de r ser o menor elemento de S, pois* $s = a - (q \pm 1).\ b \in S$, *com* $s < r$.

*Portanto,* $0 \leq r \leq |b|$.

*Para provar que q e r são únicos deve-se supor que* $a = b.q + r = b.q' + r'$,

*onde* $q, q', r, r' \in Z$, $0 \leq r \leq |b|$ *e* $0 \leq r' \leq |b|$.

*Assim, temos que* $-|b| < -r \leq r' - r \leq r' < |b|$. *Logo,* $|r' - r| < |b|$. *Por outro lado,*

$b.(q - q') = r' - r$,

*e este implica que* $|b|.\ |q - q'| = |r' - r| < |b|$. *E, isto só é possível se* $q = q'$ *e, consequentemente,* $r = r'$.

### 3.6.1. Princípio de Indução Matemática Finita

A indução finita é usada como método de demonstração desde a Antiguidade, e aparece na obra *Os Elementos*, de Euclides (300 a.C.). O nome "indução matemática" surgiu pela primeira vez em 1838, num artigo Augustus De Morgan.

Esse princípio desempenha um papel essencial na fundamentação do número natural devida a G. Peano.

Neste trabalho será usado para demonstrar alguns importantes resultados, como por exemplo, no Teorema Fundamental da Aritmética que será enunciado na seção sobre os números primos.

**Princípio de Indução Matemática [7]:**

Sejam *a* um inteiro dado e S um conjuntos de inteiros maiores ou iguais a *a*, que tem as seguintes propriedades:

(i) $a \in S$.
(ii) Se um inteiro $k \geq a$ pertence a S, então $k + 1$ também pertence a S.

Então S é o conjunto de todos os inteiros maiores ou iguais a *a*.

Demonstração:

*Suponha que a afirmação seja falsa. Então, o conjunto S' dos inteiros maiores ou iguais a a que não pertencem a S é não vazio (e limitado inferiormente por a). De acordo com o Princípio da Boa Ordenação, existe m = min S'.*

*Como a $\epsilon$ S, certamente a < m, logo a $\leq$ m – 1 < m. Temos ainda que*

*m – 1 < m = min S', logo m – 1 não pertence a S', isto é, m – 1 $\epsilon$ S. Conforme (ii), teremos então que m = (m – 1) + 1 $\epsilon$ S, uma contradição, já que m $\epsilon$ S'.*

Segue-se, do Princípio de Indução Matemática, o seguinte importante instrumento usado para demonstrar alguns teoremas:

**Teorema 3.6.1.1:** Prova por Indução Finita:

Seja *a* $\epsilon$ $\mathbb{Z}$ e seja p(n) uma sentença aberta em n. Suponha que:

(i) p(*a*) é verdadeiro, e que

(ii) para todo n $\geq$ a, p(n) é verdadeiro então p(n + 1) é verdadeiro.

Então, p(n) é verdadeiro para todo n $\geq$ *a* [5].

Demonstração:

*Basta considerar o conjunto S dos inteiros n $\geq$ a para os quais p(n) é verdadeira e verificar que está nas condições do Princípio de Indução Matemática citado acima. Assim, S contém todos os inteiros maiores ou iguais a a e segue a tese.*

**Exemplo 3.6.1.1:**

Será mostrado, por Indução Finita, um resultado importante da Geometria plana: "a soma dos ângulos internos de um polígono convexo de n lados é

$S_n = (n – 2).180^o$, com n $\geq$ 3".

De fato, para n = 3 temos que o polígono convexo correspondente é um triângulo e sabe-se da geometria elementar que a soma de seus ângulos é 180º.

Suponha a afirmação válida para $n = k \geq 3$, isto é, que a soma dos ângulos de um polígono convexo com k lados é $S_k = (k – 2).180^o$ e considere o polígono convexo $a_0\ a_1 \ldots a_k$ com k + 1 lados.

O polígono $a_0\ a_2 \ldots a_k$ que se obtém traçando o segmento $a_0\ a_2$ tem k lados. Consequentemente, a soma dos seus ângulos é $S_k = (k – 2).\ 180^o$.

Agora, a soma dos ângulos do polígono original será $S_k$ mais a soma dos ângulos do triângulo $a_0\ a_1\ a_2$, isto é, $S_{k+1} = S_k + 180^o = (k – 2).\ 180^o + 180^o = (k – 1).\ 180^o$.

Logo, pelo Princípio de Indução Finita, a soma dos ângulos internos de um polígono convexo de n lados é $S_n = (n – 2).\ 180^o$.

**Teorema 3.6.1.2:** Prova por Indução Completa:

Seja p(n) uma sentença aberta tal que:

(i) p(a) é verdadeiro, e que
(ii) para todo n, p(a) e p(a + 1) e ... e p(n) então p(n + 1) é verdadeiro.

Então, p(n) é verdadeiro para todo $n \geq a$ [5].

Demonstração:

*Seja $S = \{n \in a + \mathbb{N};\ p(n)\}$.*

*Deve-se provar que o conjunto $S' = (a + \mathbb{N}) \setminus S$ é vazio.*

*Suponha, por absurdo, que vale o contrário. Logo, pelo Princípio da Boa Ordenação, S' teria um menor elemento k, e, como se sabe de (i) que a não pertence a S', segue-se que existe n tal que $k = a + n > a$. Portanto, a, a + 1, ..., k – 1 não pertencem a S'. Logo, a, a + 1, ..., $k – 1 \in S$. Por (ii), conclui-se que*

$$k = k – 1 + 1 \in S,$$

**Exemplo 3.6.1.2:**

Seja a sequência definida da seguinte forma: os dois primeiros termos serão

$a_1 = 1$ e $a_2 = 3$; cada um dos termos subsequentes define-se como a soma dos dois anteriores, isto é, $a_n = a_{n-1} + a_{n-2}$. Assim, os primeiros termos dessa sequência serão: 1, 3, 4, 7, 11, 18, ...

Deve-se demonstrar que, para cada n, vale a desigualdade: $a_n < \left(\frac{7}{4}\right)^n$.

De fato, para n = 1 tem-se que $1 < \frac{7}{4}$ e para n = 2 tem-se que $3 < \left(\frac{7}{4}\right)^2$.

Seja então $k \geq 2$ e suponha agora que ela vale para todo inteiro positivo menor ou igual a k. Deve-se provar que $a_{k+1} < \left(\frac{7}{4}\right)^{k+1}$. Temos então que $a_{k+1} = a_k + a_{k-1}$.

Da hipótese de indução, a afirmação vale, em particular para n = k e n = k – 1.

Logo,

$a_k < \left(\frac{7}{4}\right)^k$ e $a_{k-1} < \left(\frac{7}{4}\right)^{k-1}$ , donde

$a_{k+1} < \left(\frac{7}{4}\right)^k + \left(\frac{7}{4}\right)^{k-1} = \left(\frac{7}{4}\right)^{k-1}.\left(\frac{7}{4} + 1\right) = \left(\frac{7}{4}\right)^{k-1}.\frac{11}{4}$ .

Como ainda, $\frac{11}{4} < \left(\frac{7}{4}\right)^2$, tem-se que:

$a_{k+1} < \left(\frac{7}{4}\right)^{k-1}\left(\frac{7}{4}\right)^2 = \left(\frac{7}{4}\right)^{k+1}$.

Logo, a desigualdade é válida para cada n.

Agora, será definido um conjunto *Ideal* pois em algumas demonstrações, como exemplo proposição de Equações Diofantinas, este conjunto é citado.

**Definição:** Um conjunto não vazio I de números inteiros se diz um *ideal* de $\mathbb{Z}$ se:

(i) $\alpha, \beta \in I \rightarrow \alpha + \beta \in I$;
(ii) $\alpha \in I, a \in Z \rightarrow \alpha a \in I$ [7].

Como exemplo pode-se citar o conjunto dos números pares. De fato, a soma de números pares é par e a multiplicação de um número inteiro qualquer por um número par é par.

### 3.6.2. Máximo Divisor Comum

Diz-se que um número inteiro $d \geq 0$ é um *máximo divisor comum* (mdc) de a e b, sendo $a, b \in \mathbb{Z}$, se possuir as seguintes propriedades:

(i) d é um divisor comum de a e b;
(ii) d é divisível por todo divisor comum de a e b, ou seja, se c é um divisor comum de a e b, então c|d.

**Exemplo:** Sejam dois inteiros a = 16 e b = 24. Os divisores comuns positivos de 16 e 24 são1, 2, 4 e 8, e como o maior deles é 8, segue-se que o mdc (16, 24) = 8.

**Definição 3.6.2.1:** Sejam a e b dois inteiros não conjuntamente nulos. Diz-se que a e b são *primos entre si* se, e somente se, o mdc (a, b) = 1.

**Lema 3.6.2.1:** Se a= b.q + r, então o mdc (a, b) = mdc (b, r), com a, b, q, r ∈ ℤ.

Demonstração:

*Se o mdc (a, b) = d, então d|a e d|b, o que implica que d|(a – b.q) ou d|r. Isto é, d é um divisor comum de b e r.*

*Por outro lado, se c é um divisor comum qualquer de b e r (c|b e c|r), então c|(b.q + r) ou c|a. Isto é, c é um divisor comum de a e b, o que implica que c ≤ d. Assim, o mdc (b, r) = d [6].*

**Teorema 3.6.2.1:** Se a e b são dois inteiros não conjuntamente nulos, então existe e é único o mdc(a,b); além disso, existem inteiros x e y tais que mdc(a,b) = a.x + b.y, isto é, o mdc(a,b) é uma combinação linear de a e b [6].

Demonstração:

*Seja S o conjunto de todos os inteiros positivos da forma que a.u + b.v, com u,v ∈ ℤ, isto é: S = {a.u + b.v / a.u + b.v > 0 e u,v ∈ Z}.*

*Este conjunto S não é vazio porque, se a ≠ 0, então um dos dois inteiros:*

*a = a.1 + b.0 e -a = a. (-1) + b.0 é positivo e pertence a S. logo, pelo Princípio da Boa Ordenação, existe e é único o elemento mínimo de S. E, existem inteiros x e y tais que*

*d = a.x + b.y.*

*Assim, basta mostrar que d = mdc (a, b).*

*Pelo algoritmo da divisão, temos a = d.q + r, com 0 ≤ r < d. Então:*

*$r = a – d.q = a – (a.x + b.y). q = a. (1 – q.x) + b. (-q. y).$*

*Isto é, o resto r é uma combinação linear de a e b. Como $0 \leq r < d$ e $d > 0$ é o único elemento mínimo de S, segue-se que $r = 0$ e $a = d.q$, isto é, $d|a$.*

*Com raciocínio análogo se conclui que também $d|b$. Logo, d é um divisor comum positivo de a e b.*

*Finalmente, se c é um divisor comum positivo qualquer de a e b ($c|a$ e $c|b$, com $c > 0$), então:*

*$c|(a.x + b.y) \rightarrow c|d \rightarrow c \leq d.$*

*Isto é, d é o maior divisor comum positivo de a e b, ou seja:*

*mdc (a, b) = $d = a.x + b.y$, com $x,y \in \mathbb{Z}$ [6].*

### 3.6.3. Mínimo Múltiplo Comum

Sejam a e b inteiros não nulos. Um inteiro c é um múltiplo comum de a e b se a|c e b|c. Sendo M (a, b) o conjunto de todos os múltiplos comuns de a e b e por

$M^+$ (a, b) o conjunto de todos os múltiplos comuns positivos de a e b.

Certamente $M^+$ (a, b) não é um conjunto vazio, pois lal.lbl $\epsilon$ $M^+$ (a, b). Logo, pelo Princípio da Boa Ordenação, esse conjunto contém um elemento mínimo.

Chama-se *mínimo múltiplo comum* de a e b, mmc (a, b), o menor dos seus múltiplos positivos comuns, isto é, mmc (a, b) = min $M^+$ (a, b).

**Exemplo 3.6.3.1:** Sejam os inteiros a = -12 e b = 30. Os múltiplos comuns positivos de a e b são 60, 120, 180, ..., e o menor deles é 60.

Assim, mmc (-12, 30) = 60.

A seguir serão enunciados um lema e teoremas sobre mmc.

**Lema 3.6.3.1:** Sejam a e b inteiros. Então, o mmc (a, b) divide todo outro múltiplo comum de a e b [7].

Demonstração:

*Sejam $\alpha, \beta \in M(a, b)$. Tem-se que $a|\alpha$ e $a|\beta$; logo, $a|(\alpha + \beta)$.*

*Da mesma forma, $b|(\alpha + \beta)$.*

*Sabe-se que M (a, b) deve ser da forma m.Z, em que m é o elemento mínimo de $M^+$ (a, b), isto é, m = mmc (a, b).*

*Assim, se $m' \in M(a, b) = m.Z$, então $m|m'$.*

**Teorema 3.6.3.1:** Sejam a, b $\in$ Z e m um inteiro positivo.

Então, m = mmc (a, b) se e somente se m verifica:

(i) a|m, b|m.
(ii) Se a|m' e b|m', então m|m' [7].

Demonstração:

*Do lema 3.6.3.1 tem-se que mmc (a, b) verifica (i) e (ii).*

*Se m verifica as condições, $m \in M^+(a, b)$ e por (ii), $m = \min M^+(a, b)$, pois $m \leq |m'|$. Logo, m = mmc (a, b).*

Há um resultado importante que relaciona máximo divisor comum e mínimo múltiplo comum entre inteiros a e b, que será enunciado no teorema a seguir. É uma relação importante que permite determinar o mmc de dois inteiros quando se conhece o seu mdc, e vice-versa.

**Teorema 3.6.3.2:** Para todo par de inteiros positivos a e b subsiste a relação:

mdc (a, b). mmc (a, b) = a.b [6].

Demonstração:

*Seja mdc (a, b) = d e mmc (a, b) = m. Como $a|a.(b/d)$ e $b|b.(a/d)$, segue que*

*ab/d é um múltiplo comum de a e b. Portanto, existe um inteiro positivo k tal que*

$$ab/d = m.k,\ k \in \mathbb{N}$$

*o que implica que:*

$$a/d = (m/b).k \text{ e } b/d = (m/a).k$$

*isto é, k é um divisor comum dos inteiros a/d e b/d. Mas, a/d e b/d são primos entre si (definição 3.6.2.1), de modo que k = 1. Assim sendo, tem-se que:*

$$ab/d = m \text{ ou } ab = dm$$

*isto é:*

$$ab = mdc\ (a, b).\ mmc\ (a, b)\ [6].$$

### 3.6.4. Algoritmo de Euclides

É um dos algoritmos mais antigos que se tem conhecimento (data de cerca de 300 a.C.) e pode ser encontrado na obra *Os Elementos*, de Euclides. É um método simples e eficiente de encontrar o máximo divisor comum entre dois números inteiros diferentes de zero.

O algoritmo traz um procedimento também conhecido como processo das divisões sucessivas, pois é a partir de sucessivas divisões que ele é executado.

Algoritmo: Sejam a e b dois inteiros não conjuntamente nulos cujo máximo divisor comum se deseja calcular.

É imediato que:

I. Se $a \neq 0$, então o mdc (a,0) = |a|;

II. Se $a \neq 0$, então o mdc (a, a) = |a|;

III. Se b|a, então o mdc (a, b) = |b|.

Além disso, por ser mdc (a, b) = mdc(|a|,|b|), a determinação do mdc (a, b) reduz-se ao caso em que a e b são inteiros positivos distintos, por exemplo com a > b, tais que b não divide a, isto é: a > b > 0 e b∤a. Nestas condições, a aplicação repetida do algoritmo da divisão fornece as seguintes igualdades:

$$a = b.q_1 + r_1,\ 0 < r_1 < b;$$

$b = r_1.q_2 + r_2,\ 0 < r_2 < r_1;$

$r_1 = r_2.q_3 + r_3,\ 0 < r_3 < r_2;$

$r_2 = r_3.q_4 + r_4,\ 0 < r_4 < r_3;$

..... .....

Como os restos $r_1, r_2, r_3, r_4$, ... são todos inteiros positivos tais que

$b > r_1 > r_2 > r_3 > r_4 > ...$

e existem apenas b – 1 inteiros positivos menores que b, necessariamente se chega a uma divisão cujo resto $r_{n+1} = 0$, isto é, finalmente tem-se:

$r_{n-2} = r_{n-1}.q_n + r_n,\ 0 < r_n < r_{n-1};$

$r_{n-1} = r_n.q_{n+1} + r_{n+1},\ r_{n+1} = 0.$

O último resto $r_n \neq 0$ que aparece nesta sequência de divisões é o máximo divisor comum procurado de a e b, isto é, o mdc (a, b) = $r_n$, visto que, pelo lema 2.5.1. tem-se que:

mdc (a, b) = mdc (b, $r_1$) = mdc ($r_1$, $r_2$) = ... = mdc ($r_{n-1}$, $r_n$) = $r_n$ [6].

Este processo é denominado algoritmo de Euclides e é usual o seguinte dispositivo de cálculo no emprego do algoritmo:

| | $q_1$ | $q_2$ | $q_3$ | | $q_n$ | $q_{n+1}$ |
|---|---|---|---|---|---|---|
| a | b | $r_1$ | $r_2$ | ... | $r_{n-1}$ | $r_n$ |
| $r_1$ | $r_2$ | $r_3$ | $r_4$ | | 0 | |

que se traduz na seguinte *REGRA:* Para se "achar" o mdc de dois inteiros positivos, divide-se o maior pelo menor, este pelo primeiro resto obtido, o segundo resto pelo primeiro, e assim sucessivamente até se encontrar um resto nulo. O último resto não nulo é o máximo divisor comum. [6]

**Exemplo:** Encontrar o mdc (963, 657) pelo algoritmo de Euclides e a sua expressão como combinação linear de 963 e 657.

Tem-se:

| | 1 | 2 | 6 | 1 | 4 |
|---|---|---|---|---|---|
| 963 | 657 | 306 | 45 | 36 | 9 |
| 306 | 45 | 36 | 9 | 0 | |

Portanto, mdc (963, 657) = 9.

Também,

963 = 657.1 + 306

657 = 306.2 + 45

306 = 45.6 + 36

45 = 36.1 + 9

36 = 9.4 + 0

E, pode-se determinar sua expressão como combinação linear de 963 e 657 eliminando os restos 36, 45 e 306 entre as quatro primeiras igualdades anteriores do seguinte modo:

9 = 45 – 36 = 45 – (306 – 45.6) = -306 + 7.45 = -306 + 7. (657 – 306.2) =

= 7.657 – 15.306 = 7.657 – 15. (963 – 657) = 963. (-15) + 657.22

Isto é,

9 = mdc (963,657) = 963. (-15) + 657.22.

### 3.6.5. Equações diofantinas lineares

Diophanto de Alexandria (por volta de 250 d.C.) foi o primeiro a considerar equações indeterminadas que eventualmente admitem infinitas soluções da forma

$$aX + bY = c$$

em que a, b e c são números inteiros e a e b não são ambos nulos.

Tais equações são chamadas *equações diofantinas lineares* em homenagem a Diophanto.

Muito problemas em Aritmética recaem na resolução de equações desse tipo nos números inteiros. Por este motivo, o método de resolução será apresentado nesta seção.

**Proposição 3.6.5.1:** Sejam a, b e c inteiros e d = mdc (a, b). A equação diofantina aX + bY = c tem soluções se e somente se d|c [7].

Demonstração:

*Considere o conjunto I de todos os valores que o primeiro membro pode assumir, ou seja,*

$I = \{ax + by / x, y \in \mathbb{Z}\}$

*Tem-se que I é um ideal e, se d = mdc (a, b) então I = dZ.*

*Logo, a equação tem solução se e somente se c $\epsilon$ I, e isso acontece se e somente se d|c.*

**Teorema 3.6.5.1:** Se d = mdc (a, b) | c, e se o par de inteiros $x_0$, $y_0$ é uma solução particular da equação diofantina linear aX + bY = c, então todas as outras soluções encontradas desta equação são dadas por:

$x = x_0 + \frac{b}{d}.t$ e $y = y_0 - \frac{a}{d}.t$, onde t é um inteiro arbitrário [6].

Demonstração:

*Suponha que $x_0$, $y_0$ uma solução particular da equação considerada e seja $x_1$, $y_1$ uma outra solução qualquer. Assim, $ax_0 + by_0 = ax_1 + by_1 = c$ e, portanto:*

$a.(x_1 - x_0) = b.(y_0 - y_1) = c$

*Como mdc (a, b) = d, existem r, s $\epsilon$ $\mathbb{Z}$ tais que a = dr e b = ds, com r e s primos entre si.*

*Fazendo substituições tem-se que $r.(x_1 - x_0) = s.(y_0 - y_1)$.*

*Assim, $r|s(y_0 - y_1)$ e, e como mdc (r, s) = 1, também $r|(y_0 - y_1)$. Logo,*

*$y_0 - y_1 = rt$ e $x_1 - x_0 = st$, com $t \in \mathbb{Z}$.*

*Portanto,*

$x_1 = x_0 + st = x_0 + \frac{b}{d}.t$

$y_1 = y_0 - rt = y_0 - \frac{a}{d}.t.$

**Exemplo 3.6.5.1:** Determinar todas as soluções da equação diofantina linear

172x + 20y = 1000.

Primeiramente, deve-se determinar o mdc (172, 20) pelo algoritmo de Euclides:

172 = 20.8 + 12

20 = 12.1 + 8

12 = 8.1 + 4

8 = 4.2

Portanto, mdc (172, 20) = 4 e como 4|1000, segue que a equação dada tem solução. Assim, deve-se obter a expressão do inteiro 4 como combinação linear de 172 e 20, para eliminar sucessivamente os restos 8 e 12 entre as três primeiras igualdades anteriores do seguinte modo:

4 = 12 – 8 = 12 – (20 – 12) = 2.12 – 20 = 2. (172 – 20.8) -20 =

= 172.2 + 20. (-17)

Isto é,

4 = 172.2 + 20. (-17).

Multiplicando ambos os lados da igualdade encontrada por 250, obtém-se:

1000 = 172.500 + 20. (-4250).

Portanto, a solução particular encontrada é $x_0 = 500$ e $y_0 = -4250$.

E, assim, todas as soluções são:

x = 500 + 5t

y = -4250 – 43t, onde t é um inteiro arbitrário.

**Proposição 3.6.5.2:** Seja $x_0$, $y_0$ uma solução da equação aX + bY = c, onde mdc(a, b) = 1. Então, as soluções x, y em $\mathbb{Z}$ da equação são:

$X = x_0 + tb$, $Y = y_0 - ta$; $t \in Z$ [5].

Demonstração:

*Sendo x, y uma solução de aX + bY = c tem-se que:*

$ax_0 + by_0 = ax + by = c.$

*Logo,*

$a.(x - x_0) = b.(y_0 - y) = c$ *(i).*

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

*Substituindo a expressão de* $x - x_0$ *na expressão (i), tem-se que* $y - y_0 = ta$ *e isto prova que as soluções são do tipo exibido.*

*Também, x, y é solução pois*

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

# 4. NÚMEROS PRIMOS

Esse capítulo é de extrema importância para este trabalho pois a Criptografia RSA baseia-se em encontrar números primos gigantescos e, ao mesmo tempo, na dificuldade em fatorar o produto de dois números. Por este motivo, nesta seção serão apresentadas os principais teoremas e propriedades destes números que são a base da criptografia na atualidade.

Os números primos são usados em diversas áreas, tais como: arquitetura, eletrônica, teoria musical etc... Mas, na atualidade, sua maior importância está relacionada com a criptografia. Por este motivo, nesta seção será exposto algumas particularidades destes números essenciais para o estudo da Criptografia RSA.

**Definição**: Um inteiro positivo *p* é considerado *primo* se tem exatamente dois divisores positivos, 1 e *p* [7].

Vale notar que a definição exclui o 0, que tem infinitos divisores positivos e o 1, que tem somente um divisor positivo.

Um número inteiro diferente de 0 e 1 que não é primo é chamado de *composto*.

Assim, por exemplo, os inteiros 2, 3, 5 e 7 são todos primos e os inteiros 4, 6, 8 e 10 são todos compostos.

Infelizmente, não existe um conjunto de fórmulas para a identificação de primos, e parece não haver nenhum padrão no aparecimento deles entre os números inteiros. Um dos primeiros métodos para encontrar esses números foi desenvolvido por Eratóstenes de Cirene, em Atenas no ano de 230 a.C.. Este descreveu um método de peneirar números primos entre números inteiros (Crivo de Eratóstenes). Em 1792, Carl Friedrich Gauss sugeriu uma fórmula uma fórmula P(n) para estimar o número de primos menor do que um dado número n (isto é agora chamado o teorema do número primo).

Há algumas proposições e teoremas importantes relacionados a estes números que são necessárias para o desenvolvimento deste trabalho.

**Proposição 4.1:** Seja *p* um número primo, e sejam a e b inteiros, se p∤a, então mdc (p, a) = 1.

Demonstração:

*Se p∤a, o único divisor comum positivo de a e p é 1, donde segue imediatamente a tese.*

**Lema de Euclides:** Sendo p um número primo, e sejam a e b inteiros, se p|ab, então p|a ou p|b.

Demonstração:

*Suponha que p∤ab. Se p∤a, a tese está verificada. Em caso contrário, da proposição 4.1.1 anterior temos que mdc (p, a) = 1, e, do Teorema de Euclides (que diz: Sejam a, b e c inteiros tais que a∤bc e mdc (a, b) = 1, então a∤c), vem que p∤b.*

**Corolário 4.1:** Se um número primo p divide um produto $a_1\ a_2 \ldots a_n$, então $p|a_k$, para algum k, $1 \leq k \leq n$.

***Teorema 4.1:*** Seja p um inteiro diferente de 0, 1 e -1. Então, p é primo se e somente se, toda vez que p divide um produto de dois números, p divide pelo menos um dos fatores [7].

Demonstração:

*Num sentido, o enunciado é a parte (ii) da proposição acima.*

*Para provar a afirmação no outro sentido, usará usada a demonstração por absurdo. Suponha que p tenha a propriedade do enunciado, mas não seja primo. Então, |p| pode ser escrito na forma |p| = a.b, onde a e b são divisores próprios positivos, isto é, verificam*

$1 < a < |p| \quad e \quad 1 < b < |p|$.

*Consequentemente, p|a.b, mas p∤a e p∤b; uma contradição.*

*Logo, p é primo [7].*

O lema a seguir será usado posteriormente para provar que existem infinitos números primos.

**Lema 4.1:** Todo inteiro a > 1 pode ser escrito como produto de números primos [7].

Demonstração:

*Será usado o Princípio de Indução Finita nesta demonstração.*

*Para a = 2 a afirmação é verdadeira pois 2 é, ele próprio, um número primo. Suponha agora que o resultado seja verdadeiro para todo inteiro b, 2 ≤ b < a. Deve-se mostrar que vale também para a.*

*Se a é primo, o lema está demonstrado. Caso contrário, a admite um divisor positivo b tal que 1 < b < a. Isto é, a = b. c, e tem-se que 1 < c < a. Pela hipótese de indução, b e c podem ser escritos como produto de primos, na forma:*

$b = p_1 ... p_s,\ c = q_1 ... q_k$.

*Substituindo, tem-se que a = = $p_1 ... p_s\ q_1 ... q_k$, e o resultado está provado.*

**Corolário 4.2:** Se p, $p_1$, ... ,$p_n$ são números primo se, se $p|p_1...p_n$, então $p = p_i$ para algum i = 1, ..., n.

**Teorema 4.2:** O conjunto dos números primos é infinito [7].

Demonstração:

*Suponha-se que que o conjunto dos primos positivos seja finito e sejam $p_1$, $p_2$, ..., $p_n$ esses primos. Considerar então, o número $P = p_1 p_2 ... p_n + 1$.*

*Conforme o Lema 4.1.1, P admite um divisor positivo primo $p_i$. Como $p_i$ é um dos elementos do conjunto acima, $p_i$ divide o produto $p_1 p_2 ... p_n$. Então, $p_i$ divide também $1 = P - p_1 p_2 ... p_n$, uma contradição.*

*Logo, o conjunto dos números primos é infinito.*

Os números primos são responsáveis por gerar todos os números naturais diferentes de 0 e 1. Esta propriedade é enunciada no Teorema Fundamental da Aritmética e foi publicada nos *Elementos*, de Euclides. A primeira demonstração completa foi feita por Gauss e publicada em 1801.

Esse é um teorema muito importante pois com a decomposição de números em fatores primos pode-se descobrir quantos e quais são os divisores de um número inteiro, fica mais fácil

o cálculo do mínimo múltiplo comum e do máximo divisor comum, e também possibilita a simplificação de radicais e racionalização de denominadores.

A seguir, tem-se o enunciado deste importante teorema.

***Teorema Fundamental da Aritmética***

Todo número natural a > 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como produto de números primos [5].

Demonstração:

*A demonstração será feita pelo Princípio de Indução.*

*Para n = 2 o enunciado é verdadeiro já que 2 é, ele próprio, um número primo. Suponha que o resultado seja verdadeiro para todo natural b,* $2 \leq b < n$.

*Se a é primo, o lema está demonstrado. Caso contrário, a admite um divisor positivo b tal que* $1 < b < n$. *Isto é,* $n = b.c$, *e tem-se também* $1 < c < n$. *Pela hipótese de indução, b e c podem ser escritos como produto de primos, na forma* $b = p_1 \ldots p_s$ *e* $c = q_1 \ldots q_k$.

*Substituindo, temos que* $n = p_1 \ldots p_s.q_1 \ldots q_k.$, *e o resultado também vale para n.*

*Agora deve-se provar a unicidade da escrita. Suponha que* $n = p_1 \ldots p_s = q_1 \ldots q_k$, *onde* $p_i$ *e os* $q_j$ *são números primos. Como* $p_1 | q_1 \ldots q_k$, *pelo corolário 4.1.2 acima, tem-se que* $p_1 = q_j$ *para algum j, que, após o reordenamento de* $q_{1,\ldots,}q_k$, *pode-se supor que seja* $q_1$. *Portanto,* $p_2 \ldots p_s = q_2 \ldots q_s$.

*Como* $p_2 \ldots p_s < n$, *a hipótese de indução acarreta que* $s = k$ *e os* $p_i$ *e* $q_j$ *são iguais aos pares.*

Exemplo 1: A decomposição do inteiro positivo n = 360 num produto de fatores primos é dada pela igualdade:

$$360 = 2.2.2.3.3.5$$

Observa-se que os fatores primos 2 e 3 aparecem repetidos, o primeiro três vezes e o segundo duas vezes. Assim, pode-se escrever $360 = 2^3.3^2.5$.

Exemplo 2: A decomposição do inteiro positivo n = 17460 num produto de fatores primos é dada pela igualdade:

$$17460 = 2^3.3^2.5.7^2$$

Pierre de Fermat enunciou um teorema notável que generaliza um importante resultado a respeito dos números primos conhecido pelos chineses, desde 500 a.C.. Logo será enunciado este teorema, mas, para sua demonstração é necessário o conhecimento do lema abaixo.

**Lema 4.2:** Seja p um número primo. Os números binomiais $\binom{p}{i}$ são todos divisíveis por p, onde $0 < i < p$ [5].

Demonstração:

*Esta demonstração será pelo Princípio de Indução Finita.*

*O resultado vale para i = 1. Pode-se supor, então, que 1 < i < p. Assim,*

$$i! | p(p-1)...(p-i+1).$$

*Como mdc (i!, p) = 1, tem-se que i!|(p – 1)...(p – i + 1), e o resultado se segue, pois* $\binom{p}{i} = p\,\frac{(p-1)\ldots(p-i+1)}{i!}$.

Agora pode-se enunciar e demonstrar o Pequeno Teorema de Fermat. Na seção 4.1 será apresentado novamente na linguagem de congruências.

**Pequeno Teorema de Fermat:** Dado um número primo p, tem-se que p divide número $a^p - a$, para todo $a \in \mathbb{Z}$ [5].

Demonstração:

*Se p = 2, o resultado é válido já que $a^2 - a = a.(a-1)$ é par.*

*Suponha agora que p é ímpar.*

*Nesse caso, basta mostrar o resultado para $a \geq 0$.*

*Esta demonstração será pelo Princípio de Indução Finita sobre a.*

*O resultado vale para a = 0, pois p|0.*

*Supondo o resultado válido para a, deve-se prova-lo para a + 1. Pela fórmula de Binômio de Newton:*

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

*Pelo Lema 4.2 e pela hipótese de indução, o segundo membro da igualdade é divisível por p. Assim, o resultado está provado.*

**Corolário 4.3:** Se p é um número primo e se a é um número natural não divisível por p, então p divide $a^{p-1} – 1$ [5].

Demonstração:

*Pelo Pequeno Teorema de Fermat, $p|a(a^{p-1} – 1)$ e como mdc (a, p) = 1 tem-se que p divide $a^{p-1} – 1$.*

Depois de todos esses lemas, corolários e teoremas sobre os números primos, pode-se ficar um questionamento: dado um inteiro positivo em particular, como decidir se ele é primo ou não?

Um método possível utilizando apenas a definição seria testar se ele é, ou não, divisível por algum dos inteiros positivos menores que ele próprio (excluindo o 1).

Nota-se que se d > 0 é um divisor positivo próprio de um inteiro positivo a então

a = d.c, em que c > 1.

Se acontecesse $d > \sqrt{a}$ e $c > \sqrt{a}$, então:

$a = d.c > \sqrt{a}.\sqrt{a} =$ a, uma contradição.

Assim, todo número composto a tem um divisor primo menor ou igual a $\sqrt{a}$. Ainda, se d é um divisor de a, e p é um divisor primo de d, tem-se que p|a, logo, todo número composto a tem um divisor menor ou igual a $\sqrt{a}$.

Este critério acima simplifica bastante a tarefa de determinar se um inteiro é primo. Por exemplo, o inteiro a = 223. Como $14 < \sqrt{a} < 15$, deve-se testar se a é, ou não, divisível por 2, 3, 5, 7, 11 e 13. Esta verificação mostra que 223 é primo.

Erathósthenes (276 – 194 a. C.) elaborou um método para determinar todos os primos menores que um certo número dado n > 0. Este método é conhecido como *Crivo de Erathósthenes*. É um dos mais antigos métodos para elaborar tabelas de números primos, mas não é muito eficiente para ordens muito elevadas.

Supondo n = 100, por exemplo. Primeiro se escreve todos os inteiros positivos menores ou igual a 100. Depois, deve-se riscar todos os múltiplos de 2, diferentes do 2. O segundo número não riscado é o 3, que é primo. E, em seguida, deve-se riscar todos os múltiplos de 3; e assim sucessivamente com o 5, 7 ... O crivo para n = 100 é o apresentado na figura 1.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ~~1~~ | 2 | 3 | ~~4~~ | 5 | ~~6~~ | 7 | ~~8~~ | ~~9~~ | ~~10~~ |
| 11 | ~~12~~ | 13 | ~~14~~ | ~~15~~ | ~~16~~ | 17 | ~~18~~ | 19 | ~~20~~ |
| ~~21~~ | ~~22~~ | 23 | ~~24~~ | ~~25~~ | ~~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~~ | ~~56~~ | ~~57~~ | ~~58~~ | 59 | ~~60~~ |
| ~~61~~ | ~~62~~ | ~~63~~ | ~~64~~ | ~~65~~ | ~~66~~ | 67 | ~~68~~ | ~~69~~ | ~~70~~ |
| ~~71~~ | ~~72~~ | 73 | ~~74~~ | ~~75~~ | ~~76~~ | ~~77~~ | ~~78~~ | 79 | ~~80~~ |
| ~~81~~ | ~~82~~ | 83 | ~~84~~ | ~~85~~ | ~~86~~ | ~~87~~ | ~~88~~ | 89 | ~~90~~ |
| ~~91~~ | ~~92~~ | ~~93~~ | ~~94~~ | ~~95~~ | ~~96~~ | 97 | ~~98~~ | ~~99~~ | ~~100~~ |

*Figura 1: Crivo de Erátósthenes para n = 100*

Nota-se que, como $\sqrt{100} = 10$, basta riscar os múltiplos dos primos 2, 3, 5 e 7.

Como ocorre a distribuição dos números primos em $\mathbb{N}$ é uma questão importante, bastante misteriosa e está associada a muitos problemas em aberto na atualidade. Um importante problema em aberto é a *Hipótese de Riemann,* uma conjectura que afirma que a distribuição de números primos não é aleatória e pode seguir um padrão descrito por uma equação. Se esta hipótese for provada, muitos mistérios dos números primos serão revelados.

Na próxima seção será feito o estudo de Congruências para que se possa desenvolver, no capítulo 5, o tema principal deste trabalho, a Criptografia RSA.

## 4.1 Congruências

O estudo de congruência foi introduzido por Carl Friedrich Gauss (1777-1885).

Ele observou que, no estudo da Aritmética, frequentemente eram usados os termos "*a* dá o mesmo resto que *b* quando dividimos por *m"* e isto o intrigou. Nas situações em que números diferentes eram divididos por um número distinto dos anteriores e produziam o mesmo resto, ele concluiu que esses números são congruentes, ou seja, "iguais", na divisibilidade por aquele divisor.

O estudo destas situações o levou a desenvolver sua obra intitulada *Disquisitiones Arithmeticae*, em 1801. Este livro é considerado o marco inicial da moderna teoria dos números e ele, é considerado o pai da Aritmética Modular.

A seguir serão tratados alguns conceitos, teoremas e proposições que envolvem a aritmética dos restos para facilitar o entendimento sobre questões algébricas envolvendo "números e contas gigantescas".

**Definição 4.1.1:** Seja $m \neq 0$ um inteiro fixo. Dois inteiros a e b dizem-se congruentes módulos m se m divide a diferença a – b [7].

Neste caso usa-se a notação $a \equiv b \pmod{m}$.

Em sua obra, Gauss escreve que foi induzido a utilizar o símbolo ≡ devido à grande analogia coma igualdade algébrica.

**Exemplo 4.1.1:** $3 \equiv 24 \pmod{7}$, pois 7 divide (3 – 24).

**Proposição 4.1.1:** Seja m um inteiro fixo. Dois inteiros a e b são congruentes módulo m se e somente se eles têm como resto o mesmo inteiro quando divididos por m [7].

Demonstração:

*Sejam*

$a = m.q_1 + r_1$, *com* $0 \leq r_1 \leq m$

$b = m.q_2 + r_2$, *com* $0 \leq r_2 \leq m$.

*Então,* $a - b = m\,(q_1 - q_2) + (r_1 - r_2)$.

*Logo,* $m|(a - b)$ *se e somente se* $m|(r_1 - r_2)$.

*Ainda, como* $0 \leq |r_1 - r_2| < m$, *tem-se que* $m|(r_1 - r_2)$ *se e somente se* $r_1 - r_2 = 0$.

*Consequentemente,* $a \equiv b \pmod m$ *se e somente se* $r_1 = r_2$ *[7].*

**Exemplo 4.1.2:** 5 ≡ 9 (mod 2), pois 5 e 9 tem o mesmo resto quando divididos por 2.

**Proposição 4.1.2:** Sejam m > 0 um inteiro fixo, e a, b, c, d inteiros arbitrários. Então valem as seguintes propriedades:

(i) a ≡ a (mod m).
(ii) Se a ≡ b (mod m), então b ≡ a (mod m).
(iii) Se a ≡ b (mod m) e b ≡ c (mod m), então a ≡ c (mod m).
(iv) Se a ≡ b (mod m) e c ≡ d (mod m), então a + c ≡ b + d (mod m).
(v) Se a ≡ b (mod m), então a + c ≡ b + c (mod m).
(vi) Se a ≡ b (mod m) e c ≡ d (mod m), então a.c ≡ b.d (mod m).
(vii) Se a ≡ b (mod m), então $a^n \equiv b^n$ (mod m), para todo inteiro n positivo.
(viii) Se a + c ≡ b + c (mod m), então a ≡ b (mod m) [7].

Demonstração:

*(i)* *Com efeito,* $m|0$ *ou* $m|(a - a)$. *Então,* $a \equiv a \pmod m$.

*(ii)* *Se* $a \equiv b \pmod m$, *então* $a - b = k\,.m$, *com* $k \in Z$.
*Portanto,*
$b - a = -(k.m) = (-k).m$
*Então,* $b \equiv a \pmod m$.

*(iii)* *Se* $a \equiv b \pmod m$ *e se* $b \equiv c \pmod m$, *então existem inteiros h e k tais que:*
$a - b = h.m \quad e \quad b - c = k.m$
*Logo,*
$a - c = (a - b) + (b - c) = h.m + k.m = (h + k).m$
*e isto significa que* $a \equiv c \pmod m$.

*(iv)* *Como $a \equiv b \pmod m$ e $c \equiv d \pmod m$, tem-se que:*
*$m|(a - b)$ e $m|(c - d)$.*
*Consequentemente, $m|((a - b) + (c - d))$, isto é, $m|(a + c) - (b + d)$.*
*Logo, $a + c \equiv b + d \pmod m$.*

*(v)* *Se $a \equiv b \pmod m$ e $c \equiv c \pmod m$, tem-se, pela propriedade anterior que $a + c \equiv b + c \pmod m$.*

*(vi)* *Se $a \equiv b \pmod m$ e $c \equiv d \pmod m$, então existem inteiros h e k tais que $a - b = h.m$ e $c - d = k.m$. Portanto,*
*$a.c - b.d = (b + h.m).(d + k.m) - b.d = (b.k + d.h + h.k.m).m$*
*o que implica:*
*$a.c \equiv b.d \pmod m$.*

*(vii)* *Usando o Princípio De Indução Finita:*

*A proposição é verdadeira para n = 1. Supondo verdadeira para um inteiro positivo k, tem-se: $a^k \equiv b^k \pmod m$ e $a \equiv b \pmod m$.*

*Portanto, $a^k.a \equiv b^k.b \pmod m$ ou $a^{k+1} \equiv b^{k+1} \pmod m$.*

*Logo, a propriedade é verdadeira para o inteiro positivo k + 1 e, assim, é verdadeira para todo positivo n.*

*(vii)* *Se $a + c \equiv b + c \pmod m$, então $m|(b + c) - (a + c)$ e isto implica que $m|(b - a)$.*
*Logo, $a \equiv b \pmod m$ [5] e [7].*

**Proposição 4.1.3:** Seja m um inteiro fixo e sejam a, b e c inteiros arbitrários.

Se mdc (c, m) = 1, então $a.c \equiv b.c \pmod m$ implica que $a \equiv b \pmod m$ [7].

*Demonstração:*

*Se $a.c \equiv b.c \pmod m$, temos que $m|(a - b).c$.*

*Como mdc (c, m) = 1, vem que $m|(a - b)$, donde $a \equiv b \pmod m$.*

**Exemplo 4.1.3:** Considere a congruência:

$-35 \equiv 45 \pmod 8$ ou $5.(-7) \equiv 5.9 \pmod 8$

Como o mdc (5, 8) = 1, podemos “cancelar” o fator 5 de ambos os membros da congruência, o que dá a nova congruência:

$-7 \equiv 9 \pmod 8$

Pierre de Fermat (1601-1665), magistrado, matemático e cientista francês, afirmou em 1640 que, se *a* é um inteiro não divisível por um primo *p*, então *p* divide $a^{p-1} - 1$. A seguir será enunciado seu teorema, que pode ser usado para provar diversos resultados sobre divisibilidade, e a demonstração desse resultado que já foi exposto neste trabalho como Pequeno Teorema de Fermat.

**Teorema de Fermat:** Sejam *p* um primo e *a* um inteiro tal que *p* não divide *a*. Então, $a^{p-1} \equiv 1 \pmod p$ [7].

Demonstração:

*Considere o conjunto de inteiros A = {a, 2a, 3a, ..., (p – 1). a}.*

*Dados dois elementos quaisquer desse conjunto, eles não são congruentes entre si, módulo p, pois, se x.a ≡ y.a (mod p) com 1 ≤ x, y ≤ p – 1, como mdc (a, p) = 1, “cancelando” teríamos x ≡ y (mod p), o que não acontece, já que os elementos do conjunto B = {1, 2, 3, ..., p – 1} não são congruentes entre si, módulo p.*

*Além disso, nenhum dos elementos de A é congruente a 0 módulo p, já que, se p|x.a, com 1 ≤ x ≤ p – 1, então p|x ou p|a, o que não acontece.*

*Segue-se então que os elementos de A são congruentes aos elementos de B, numa ordem conveniente.*

*Temos, então, p – 1 congruentes da forma*

$a \equiv x_1 \pmod p$

$2a \equiv x_2 \pmod p$

...

$(p - 1).\ a \equiv x_{p-1} \pmod p$,

*onde* $x_1, x_2, ..., x_{p-1}$ *são os inteiros 1, 2, ..., p – 1, eventualmente em uma outra ordem.*

*Multiplicando ordenadamente essas congruências, temos*

$a.2a. \ldots (p - 1).\ a \equiv 1.2. \ldots. (p - 1) \pmod p$,

*ou seja,*

*$(p – 1)!. a^{p-1} \equiv (p – 1)! \pmod{p}$.*

*Como mdc ((p – 1)! p) = 1, pode-se cancelar e obtém-se:*

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

**Corolário 4.1.1:** Sejam p um primo e a um inteiro arbitrário. Então,

$$a^p \equiv a \pmod{p}$$ [7].

Demonstração:

*Se p não divide a, do Teorema de Fermat tem-se que $a^{p-1} \equiv 1 \pmod{p}$; multiplicando os membros dessa congruência por a segue que $a^p \equiv a \pmod{p}$.*

*Se p divide a, então $p|a^p$, e consequentemente $p|(a^p – a)$.*

*Logo, $a^p \equiv a \pmod{p}$.*

### 4.1.1 Congruências Lineares

**Definição 4.1.1.1:** Chama-se congruência linear toda equação da forma

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

onde a e b são inteiros quaisquer e m um inteiro positivo.

Vale notar que se x é uma solução da equação, ax – b deve ser múltiplo de m, ou seja, deve existir y tal que $ax \equiv b – my$, isto é, $ax + my = b$.

Em outras palavras, se x é solução da equação $ax \equiv b \pmod{m}$, existe $y \in \mathbb{Z}$ tal que o par (x, y) é solução da equação diofantina $ax + my = b$.

O teorema a seguir traz a condição de existência de solução de uma congruência linear.

**Teorema 4.1.1.1:** A congruência ax ≡ b (mod m) tem solução se e somente se d = mdc (a, m) divide b [7].

Demonstração:

*(→)*

*Supor que a congruência linear tem como solução o inteiro $x_0$, ou seja,*

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

*Logo, existe um inteiro $y_0$ tal que:*

*$ax_0 - b = my_0$ ou $ax_0 - my_0 = b$.*

*Como d|a e d|m, porque d = mdc (a, m), segue-se que $d|(ax_0 - my_0)$ e, portanto, d|b.*

*(←)*

*Supor agora que d|b, isto é, existe k inteiro tal que b = dk.*

*Como mdc (a, m) = d, existem inteiros $x_0$ e $y_0$ tais que $ax_0 + my_0 = d$.*

*Multiplicando ambos os lados da igualdade acima por k:*

*$a(kx_0) + m(ky_0) = dk = b$*

*$a(kx_0) - b = m(-ky_0)$*

*Isto implica que:*

*$a(kx_0) \equiv b \pmod{m}$*

*Portanto, o inteiro $kx_0$ é a solução da congruência linear [6].*

Se a congruência tem soluções, quantas são? Esta resposta está no teorema enunciado a seguir.

**Teorema 4.1.1.2:** Se d divide b, sendo d = mdc (a, m), então a congruência linear ax ≡ b (mod m) tem precisamente d soluções mutuamente incongruentes módulo m.

*Caso haja interesse, esta demonstração está no livro Teoria Ementar dos Números, de Edgard de Alencar Filho, na página 168 da 3ª edição.*

**Corolário 4.1.1.1:** Se o mdc (a, m) = 1, então a congruência linear ax ≡ b (mod m) tem uma única solução módulo m.

**Exemplo 4.1.1.1:** A congruência linear 18x ≡ 30 (mod 42) tem exatamente 6 soluções incongruentes módulo 42 pois mdc (18, 42) = 6.

Como 18.4 ≡ 30 (mod 42), uma solução da congruência é $x_0 = 4$ e, assim, as suas 6 soluções são dadas pela fórmula x = 4 + (42/6). t = 4 + 7t, onde t = 0, ... ,5.

Logo, x = 4, 11, 18, 25, 32, 39.

**Exemplo 4.1.1.2:** Na congruência linear 11x ≡ 2 (mod 317) há somente uma solução, pois, mdc (11, 317) = 1. Esta solução pode ser obtida com a resolução da equação diofantina

11x – 317y = 2.

Pelo algoritmo de Euclides pode-se concluir que x = -288 ou x = 29 é a única solução módulo 317 da congruência.

É possível resolver equações diofantinas lineares por congruências.

Conforme foi demonstrado anteriormente no Teorema 3.6.5.1, a equação diofantina linear ax + by = c tem solução se e somente se d = mdc (a, b) divide.

Sendo $x_0$, $y_0$ uma solução particular então:

$ax_0 + by_0 = c$ e $ax_0 – c = - by_0$.

Isto implica que:

$ax_0 \equiv c \pmod b$.

Para obter uma solução particular da equação basta determinar uma solução qualquer $x = x_0$ da congruência linear $ax_0 \equiv c \pmod b$ e substituir o valor $x_0$ na equação ax + by = c para encontrar o valor correspondente $y_0$ de y tal que $ax_0 + by_0 = c$ [6].

**Exemplo 4.1.1.3:** Resolver por congruências a equação diofantina linear:

9x + 16y = 35.

Como mdc (9, 16) = 1, a equação tem solução.

A congruência linear 16y ≡ 35 (mod 9) ou 7y ≡ 35 (mod 9) traz que:

$y \equiv 5 \pmod 9$.

Então, $y = 5 + 9t$, onde $t \in \mathbb{Z}$.

Substituindo este valor de y na equação diofantina obtém-se:

$$9x + 16(5 + 9t) = 35$$

$$x = -5 - 16t.$$

Se for preciso resolver um sistema de congruências lineares será usado o Teorema Chinês do Resto enunciado a seguir.

**Teorema Chinês do Resto:** Sejam $n_1, n_2, ..., n_k$ inteiros positivos primos entre si dois a dois, isto é, tais que o mdc $(n_i, n_j) = 1$ se $i \neq j$. Nestas condições, o sistema de congruências lineares:

$x \equiv c_1 \pmod{n_1}$

$x \equiv c_2 \pmod{n_2}$

...

$x \equiv c_k \pmod{n_k}$

tem uma única solução módulo $n = n_1 n_2 ... n_k$ [7].

Demonstração:

*Considere o número $n = n_1 n_2 ... n_k$. Para cada índice i define-se $N_i = n/n_i$. Como $N_i$ é o produto de todos os inteiros $n_1, n_2, ..., n_k$ e eles são relativamente primos com $n_i$, segue que:*

*mdc $(N_i, n_i) = 1$.*

*Pode-se então determinar inteiros $r_i, s_i$ tais que:*

*$r_i N_i + s_i n_i = 1$, com $1 \leq i \leq k$.*

*Agora, será mostrado que o número $x_0$ abaixo é solução do sistema dado.*

*$x_0 = c_1 r_1 N_1 + c_2 r_2 N_2 + ... + c_k r_k N_k$*

*Se $i \neq j$, então $N_i \equiv 0 \pmod{n_i}$, pois $n_i$ é um dos fatores de $N_j$, logo,*

*$c_j r_j N_j \equiv 0 \pmod{n_i}$ e assim:*

*$x_0 = c_1 r_1 N_1 + c_2 r_2 N_2 + \ldots + c_k r_k N_k \equiv c_i r_i N_i \pmod{n_i}$.*

*Ainda, como $r_i N_i \equiv 1 \pmod{n_i}$, logo $x_0 \equiv c_i r_i N_i \equiv c_i \pmod{n_i}$. Isto é, $x_o$ é solução da equação $x \equiv c_i \pmod{n_i}$, para cada i e, consequentemente, é uma solução do sistema.*

*Agora, resta mostrar que toda outra solução é congruente a $x_0$ modulo n.*

*Se x é solução, tem-se que $x \equiv c_i \pmod{n_i}$, $1 \leq i \leq k$.*

*Também, $x_0 \equiv c_i \pmod{n_i}$ e da transitividade da relação de congruência vem que $x \equiv x_0 \pmod{n_i}$. Ainda, como os inteiros $n_i$ são relativamente primos, conclui-se que:*

*$n_1 n_2 \ldots n_k \mid (x - x_0)$. Logo, $x \equiv x_0 \pmod{n}$ [7].*

A seguir há um exemplo de resolução de sistema pelo Teorema Chinês do Resto.

**Exemplo 4.1.1.4:** Resolver o sistema:

$X \equiv 2 \pmod 3$

$X \equiv 3 \pmod 5$

$X \equiv 2 \pmod 7$

Como 3, 5 e 7 são primos dois a dois, o sistema tem solução.

Determina-se primeiramente $n = 3.5.7 = 105$.

Em seguida, $N_1 = 35$, $N_2 = 21$ e $N_3 = 15$.

Tem-se que:

$(2)35 + (-23)3 = 1$, logo $r_1 = 2$.

$(1)21 + (-4)5 = 1$, logo $r_2 = 1$.

$(1)15 + (-2)7 = 1$, logo $r_3 = 1$.

Logo,

$x_0 = 2.(2.35) + 3.21 + 2.15 = 233$ é uma solução.

Como 233 dividido por $3.5.7 = 105$ dá resto 23, vem que $x_0' = 23$ também é uma solução particular e pode-se expressar a solução geral na forma:

$x = 23 + 105t$, $t \in \mathbb{Z}$ .

Também há dois outros importantes teoremas na Teoria dos Números que serão enunciados a seguir.

Mas antes, deve-se definir a função $\phi$ de Euler.

**Definição 4.1.1.2:** Para cada inteiro n ≥ 1, indica-se por $\phi$(n) o número de inteiros positivos, menores ou iguais a n, que são relativamente primos com n. A função assim definida chama-se função $\phi$ de Euler [7].

Por exemplo, se n = 6, os inteiros positivos menores ou iguais a 6, relativamente primos com 6, são 1 e 5, assim $\phi(6) = 2$.

Generalizando, se A = $\{x_1, x_2, ..., x_t\}$ é o conjunto formado pelos inteiros positivos, menores ou iguais a n, relativamente primos com n, $\phi$(n) = t.

Com essa notação tem-se o teorema de Euler a seguir.

**Teorema de Euler:** Sejam a e n inteiros com n ≥ 1, tais que mdc (a, n) =1. Então,

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

Pode-se notar que, se p é primo, $\phi$(p) = p – 1. Assim, o Teorema de Fermat é um caso particular do Teorema de Euler.

Em 1770, John Wilson comunicou a seu professor, o matemático inglês Edward Waring, que todo primo p divide o número (p – 1)! + 1. Na época não passava de uma conjectura, mas Lagrange demonstrou em 1771.

**Teorema de Wilson:** Seja p um inteiro primo. Então:

$(p - 1)! + 1 \equiv 0 \pmod{p}$ [7].

Nos Capítulos 2, 3 e 4 foram explanadas algumas propriedades, alguns teoremas e postulados importantes para a compreensão do que será exposto a seguir.

Agora, há condições de iniciar-se o próximo capítulo que trará um dos principais pilares deste trabalho: a Criptografia RSA. Como funciona este sistema criptográfico? Quanto seguro ele é? Como a Aritmética está envolvida na Criptografia?

Estas e outras questões serão abordadas no Capítulo 5 deste trabalho.

# 5. CRIPTOGRAFIA

Neste capítulo será abordado o tema principal deste trabalho. Primeiramente será desenvolvido o assunto de uma maneira ampla e logo em seguida será dado enfoque a Criptografia RSA.

## 5.1 A criptografia

As pessoas podem até não perceber, mas a criptografia está presente no cotidiano de cada um. Os códigos estão nos celulares, nas redes sociais, nos alarmes de carros e residências, nas transações bancárias, nos computadores e na internet de um modo geral. Em todas as comunicações digitais, a criptografia ajuda na proteção dos conteúdos transmitidos, evitando a intercepção por parte de cyber criminosos e hackers, por exemplo.

A internet é cada vez mais usada pela sociedade de forma geral. É um ambiente que possibilita a comunicação, pesquisa, divulgação e comércio eletrônico. A criptografia tem como principal objetivo tornar uma comunicação segura para todos os envolvidos. Há sempre um remetente, que codifica a mensagem, e um destinatário, que recebe e decodifica a transmissão.

Por isso, a segurança eletrônica é muito discutida atualmente. Existem casos de violação de contas bancárias, invasão e destruição de sistemas e acesso a informações sigilosas. Com o uso de computadores, as informações são transmitidas com muita eficiência e velocidade, mas nem sempre de forma segura.

Atualmente, as informações não são armazenadas somente em papéis, e, sim, em bancos de dados. Assim, como proteger essas informações? Quanto seguro é fazer uma compra pela internet, por exemplo?

Para dar início a essa questão será feita uma breve descrição do desenvolvimento da criptografia ao longo do tempo.

Há indícios de que a criptografia surgiu por volta de 1900 a.C. no Antigo Egito, quando o faraó Amenemhet II governava e decidiu substituir trechos e palavras de documentos por símbolos pois continham importantes informações sobre a localização de tesouros.

Na antiguidade, um dos métodos mais famosos foi um sistema utilizado na Roma antiga, por Júlio César, chamado cifra de César. Neste sistema, cada letra do alfabeto na mensagem original era substituída por outra letra do alfabeto, seguindo um padrão determinado. O padrão está representado na figura seguinte.


*Figura 2: Cifra de César*

Assim, por exemplo, a frase “isto é um segredo” é transformada em JTUP F VN TFHSFEP.

O tipo de sistema usado por César é chamado de cifra por *substituição simples*, onde as letras de um alfabeto são substituídas por outras. Entretanto, esse sistema tem fragilidades. Em um texto de uma determinada língua as letras do alfabeto ocorrem com frequências diferentes e há regras de contato entre elas. Assim, se o interceptor da mensagem tiver bons conhecimentos da estrutura ortográfica da língua, ele pode deduzir qual é a real letra que lhe corresponde.

Para impedir a quebra de um código fazendo a análise das frequências das letras, pode-se usar a *transposição*, que é outra técnica para criptografar mensagens onde forma-se anagramas da mensagem original. Por exemplo, uma mensagem com 50 letras dá origem a 50! permutações das letras, ou seja, aproximadamente $3.10^{64}$ e, assim, torna-se muito mais difícil decifrar a correspondência.

O italiano Leone Battista Alberti, em 1466, propôs um sistema criptográfico mais bem elaborado chamado de *sistema de substituição polialfabética*. Usava o chamado disco de Alberti, ou seja, dois círculos de tamanhos diferentes. Esses discos eram divididos em partes iguais com as letras A, B, C, D, E, F, G, I, L, M, N, O, P, Q, R, S, T, V, X, Z e os numerais 1, 2, 3 e 4.


*Figura 3: Disco de Alberti*

Em 1553, foi introduzida a ideia de chave para cifrar e decifrar uma mensagem. Foi o italiano Giovanni Battista Bellaso, no livro *La cifra del Sig Giovan Belaso*, que introduziu o sistema que utiliza a *tabula recta* e o compartilhamento de uma chave. Neste método, a chave utilizada para cifrar uma mensagem também é utilizada para decifrá-la. Por ser uma cifragem resistente à análise de frequência, era considerada difícil de ser quebrada.

O grande desafio nesse tipo de método é a troca da chave para que somente as partes envolvidas tenham acesso a ela de forma segura.

As cifras polialfabéticas foram usadas na Segunda Guerra Mundial na máquina alemã Enigma. Esta máquina se transformou na ferramenta criptográfica mais importante da Alemanha nazista. Este sistema usado pelos alemães demorou para ser quebrado pelos britânicos através de Alan Turing, considerado um dos pais da computação.

Nestes métodos que foram citados, os sistemas criptográficos usavam as chamadas chaves simétricas, ou seja, a mesma chave usada para cifrar uma mensagem também é usada para decifrar a mesma. E isto não é seguro pois a chave pode ser descoberta. Em contrapartida existe a chave assimétrica (também conhecida como chave pública), baseada em dois tipos de chaves de segurança: uma privada e outra pública. A chave pública é usada para cifrar a mensagem e a privada é usada para decifrar a mesma.

Esse termo “chave” vem do fato de que funciona da mesma maneira que uma chave convencional usada nas portas de lugares fechados de modo a proteger algo. Isso acontece na Criptografia pois para proteger alguma informação deve-se instalar uma fechadura (algoritmo de criptografia). Para operar a fechadura precisa-se da chave que permite decifrar a informação.

E foi com a chegada dos computadores que as trocas de informações ficaram mais seguras. Isso ocorreu porque os computadores utilizam códigos binários e assim foi necessário transformar todas as informações nesse código antes de criptografá-las. Mas, mesmo assim, a questão da privacidade é o grande desafio da computação.

Durante muito tempo acreditou-se que havia uma impossibilidade de trocar senhas sem a mediação de um portador. Mas, três norte-americanos, Whitfield Driffie, Martin Hellman e Ralph Merke, tiveram a ideia de usar a teoria de Números através da noção de congruências e, assim, mostraram ser possível a troca de senhas sem um portador [5].

A seguir será relatado como a Teoria dos Números entrou no campo da Criptografia através dos três americanos.

A invenção deles baseia-se no seguinte: duas pessoas Carlos e Diego precisam trocar informações secretas (chave secreta) por meio de uma comunicação insegura, por exemplo, uma carta.

Primeiramente, eles precisam escolher em comum acordo, um par de números naturais $a$ e $m$ e estes números serão públicos. Carlos escolhe outro número c e o mantém em segredo. Após, calcula o único número s < m tal que $a^c \equiv s \bmod m$, e envia para Diego. Assim, Diego

escolhe um número natural d e o mantém em segredo. Depois, calcula o único número t < m, tal que $a^d \equiv t \bmod m$, como havia feito Carlos.

Posteriormente, Carlos calcula C, sendo:

$C \equiv (a^d)^c \equiv a^{d.c} \equiv a \bmod m$, sendo $\gamma < m$.

Também, Diego calcula D, sendo:

$D \equiv (a^c)^d \equiv a^{c.d} \equiv a \bmod m$, sendo $\gamma < m$.

Assim, está trocada a chave secreta $\gamma$ que apenas Carlos e Diego conhecem. São públicos os números *a*, *m*, s e t e secretas as informações c e d.

Este método é bom porque é relativamente difícil descobrir qualquer um dos três números c, d ou $\gamma$ conhecendo somente *a*, *m*, s e t que são públicos [5].

Este sistema foi denominado DHM (sigla com as inicias dos sobrenomes dos três norte-americanos que inventaram o sistema) e se tornou o primeiro importante passo para solucionar a questão da troca de chaves secretas. No entanto, permite somente a troca de informações entre duas pessoas de cada vez e isso é insatisfatório na atualidade com toda a globalização existente.

O passo suficiente e satisfatório para implementar o primeiro sistema criptográfico com chaves assimétricas foi dado, em 1978, por Ronald Rivest, Adi Shamir e Leonard Adleman. O sistema criado por eles, resumidamente, baseia-se na facilidade de encontrar números primos gigantes e ao mesmo tempo na grande dificuldade em fatorar o produto de dois desses números. O sistema é denominado Sistema RSA e será detalhado a seguir.

## 5.2 O sistema RSA

O sistema RSA foi inventado em 1978 por Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman quando trabalhavam no Massachussetts Institute of Technology (M.I.T) e fundamenta-se nas teorias clássicas dos números.

É o sistema criptográfico mais conhecido e utilizado na atualidade em aplicações comerciais atuando diretamente na internet, como por exemplo, em e-mails e sites para transações bancárias.

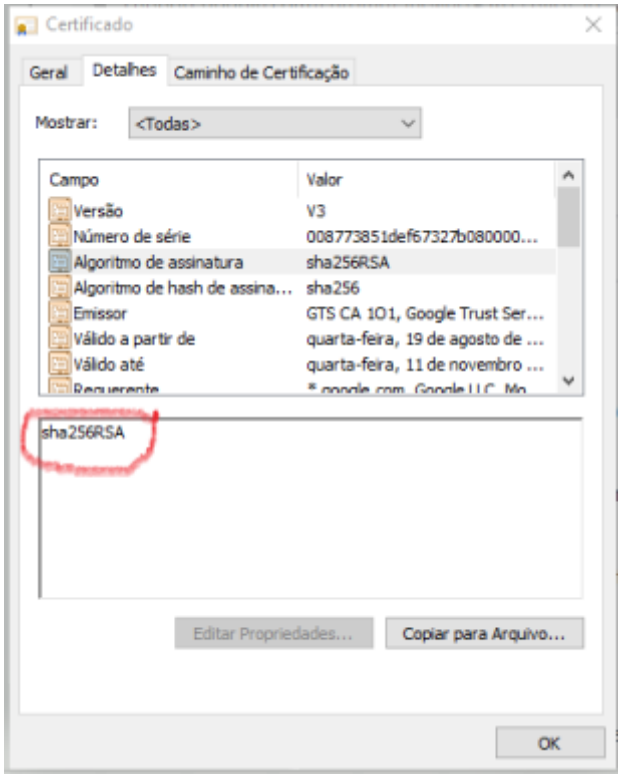



*Figura 4: Certificado no site do Banco Itaú*

Na figura é possível observar a existência criptografia RSA no certificado de segurança do site do Banco Itaú.

É também um dos mais seguros e foi o primeiro algoritmo a possibilitar a assinatura digital.

Por seu um código de chave pública, traz um algoritmo para criptografar e descriptografar através de um par de chaves. A chave é pública e pode ser conhecida por todos; é usada para criptografar os dados que serão enviados, por exemplo: senhas e logins. A outra é privada e deve ser mantida em sigilo. O emissor e o receptor precisam ter, cada um, uma das chaves. Com este sistema, é impraticável decifrar uma mensagem conhecendo apenas uma das chaves.

Para entender o porquê de ser impraticável decifrar apenas com uma das chaves é necessário conhecer como funciona a Criptografia RSA. A seguir, será exposto o funcionamento deste sistema.

### 5.2.1 Funcionamento do sistema RSA

O sistema RSA funciona da seguinte maneira:

1. Escolhe-se dois números primos p e q distintos entre si (a RSA Data Security, que faz a padronização do RSA, recomenda que se utilize chaves de 2048 bits para garantir que a chave não seja quebrada nos próximos 10 anos).

2. Multiplica-se p e q obtendo-se um número N = p.q.

3. Define-se $\varphi(N) = (p - 1).(q - 1)$. A função $\varphi(N)$ é conhecida como função totiente ou de Euler e indica a quantidade de coprimos de um número que são menores que ele mesmo.

4. Escolhe-se um número *e*, que faz parte da chave pública (N, e), de modo que o máximo divisor comum entre ele e $\varphi(N)$ seja 1 e que $1 < e < \varphi(N)$.

5. Resolve-se a seguinte congruência para encontrar o número d (inverso multiplicativo de e) que faz parte da chave privada (N, d): $e.d \equiv 1 \pmod{\varphi(N)}$.

6. É necessário que exista uma tabela pré formulada de domínio público, onde todos os números devem ter a mesma quantidade de dígitos, para que seja feita a transformação dos caracteres da mensagem em números e obter, assim, a mensagem numérica em um único bloco que será dividida em blocos menores b, de forma que, $1 \leq b < N$. Assim, está garantido que irá se obter uma única decodificação resolvendo a congruência do item 5.

7. Tendo a chave pública (N, e) criptografa-se os blocos b de acordo com a congruência $b^e \equiv C(b) \pmod{N}$, sendo C(b) o bloco criptografado.

8. Com a chave privada (N, d) descriptografa-se usando a congruência $C(b)^d \equiv D(C(b)) \pmod{N}$, sendo D(C(b)) o bloco descriptografado, onde $1 \leq D(C(b)) < N$.

9. Para finalizar, cada bloco precisa ser colocado na sequência e deve-se usar novamente a tabela do item 6 para converter os números em caracteres [8].

**Exemplo 5.2.1.1:** Para cifrar e decifrar a palavra TURING deve-se ter uma tabela pré formulada. Neste caso será usada a seguinte tabela:

| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **L** | **M** | **N** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** |

| **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **X** | **Z** |
|---|---|---|---|---|---|---|---|---|---|
| **14** | **15** | **16** | **17** | **18** | **19** | **20** | **21** | **22** | **23** |

Seguindo os passos citados acima tem-se o seguinte:

1. Escolha dos primos p = 17 e q = 41 (escolha de números primos pequenos para que as calculadoras consigam processar).

2. N = p.q
   N = 17.41
   N = 697

3. $\varphi(N) = (p - 1).(q - 1)$
   $\varphi(N) = (17 - 1).(41 - 1)$
   $\varphi(N) = 640$

4. Escolha do valor de e = 13.

   Observação: Com o item 4 fica definida a **chave pública** (N, e) igual a **(697, 13)**.

5. Resolução da seguinte congruência para encontrar o número d que faz parte da chave privada: $13.d \equiv 1 \pmod{640}$.

   Para calcular d será usado o Algoritmo de Euclides (citado neste trabalho no item 3.6.4)

| | | |
|---|---|---|
| | 49 | 4 |
| 640 | 13 | 3 |
| 3 | 1 | |

Após chegar no resto 1 deve-se parar. Agora é necessário isolar o resto:

$3 = 1.640 – 49.13$ (i)

$1 = 1.13 – 4.3$ (ii)

Substituindo (i) em (ii):

$1 = 1.13 – 4.(1.640 – 49.13)$

$1 = 1.13 – 4.640 + 196.13$

$1 = 197.13 – 4.640$

Assim, temos o valor de d = 197, pois na equação acima 197 multiplica 13. Ou seja, $13.197 \equiv 1 \pmod{640}$.

Observação: Com o item 5 fica definida a **chave privada** (N, d) igual a **(697, 197)**.

6. Com o uso da tabela citada acima tem-se o seguinte código para ser criptografado:
   19 – 20 – 17 – 09 – 13 – 07, pois:
   T = 19
   U = 20
   R = 17
   I = 9
   N = 13
   G = 7

7. Com este passo serão criptografados os blocos:
   $b_1 = 19$, $b_2 = 20$, $b_3 = 17$, $b_4 = 09$, $b_5 = 13$ e $b_6 = 07$.

   Usando a chave pública (697, 13) resolve-se a congruência $b^e \equiv C(b) \pmod{N}$, sendo C(b) a mensagem criptografada de cada bloco b.

$19^{13} \equiv C(b_1) \pmod{697} \quad \leftrightarrow \quad C(b_1) = 15$

$20^{13} \equiv C(b_2) \pmod{697} \quad \leftrightarrow \quad C(b_2) = 692$

$17^{13} \equiv C(b_3) \pmod{697} \quad \leftrightarrow \quad C(b_3) = 391$

$9^{13} \equiv C(b_4) \pmod{697} \quad \leftrightarrow \quad C(b_4) = 501$

$13^{13} \equiv C(b_5) \pmod{697} \quad \leftrightarrow \quad C(b_5) = 421$

$7^{13} \equiv C(b_6) \pmod{697} \quad \leftrightarrow \quad C(b_6) = 176$

Assim, a palavra foi cifrada o obteve-se o código 15 – 692 – 391 – 501 – 421 – 176.

8. Com a chave privada **(697, 197)** os blocos do código cifrado serão descriptografados usando a congruência $C(b)^d \equiv D(C(b)) \pmod{N}$, sendo $D(C(b))$ o bloco descriptografado, com $1 \leq D(C(b)) < N$.

$15^{197} \equiv D(15) \pmod{697} \quad \leftrightarrow \quad D(15) = 19$

$692^{197} \equiv D(692) \pmod{697} \quad \leftrightarrow \quad D(692) = 20$

$391^{197} \equiv D(391) \pmod{697} \quad \leftrightarrow \quad D(391) = 17$

$501^{197} \equiv D(501) \pmod{697} \quad \leftrightarrow \quad D(501) = 09$

$421^{197} \equiv D(421) \pmod{697} \quad \leftrightarrow \quad D(421) = 13$

$176^{197} \equiv D(176) \pmod{697} \quad \leftrightarrow \quad D(176) = 07$

9. Para finalizar, o código 19 – 20 – 17 – 09 – 13 – 07 será transformado nas letras utilizando-se a tabela definida e volta-se a mensagem inicial TURING.

Com este algoritmo encontra-se duas grandes dificuldades:

- Lidar com números inteiros muito grandes;
- Descobrir na sequência numérica que deve ser decifrada, quantos números representam cada letra.

Agora, com o funcionamento do sistema RSA definido, este trabalho apresentara como este sistema é usado em sites seguros.

### 5.2.2 Sistema RSA em sites de internet

Pode-se dizer que, atualmente, a internet é fundamental para a vida profissional e pessoal da maioria das pessoas. Desde sua criação até hoje, tem modificado muito o estilo de vida da sociedade de forma geral.

Ela possibilita uma série de facilidades como: compras em sites de produtos, acesso a conta bancária, reuniões de trabalho com pessoas distantes, entre outras situações. Mas essas facilidades precisam estar acompanhadas de segurança para os usuários.

Nesta seção será explanado como que essas ações na internet oferecem segurança ou não.

Primeiramente, o usuário deve estra atento a detalhes que aparecem no browser utilizado. Normalmente, um desenho de “cadeado fechado”, na barra de status, na parte inferior da janela acessada informa a segurança do site visitado. Caso o cadeado esteja aberto, a conexão não é segura. A figura abaixo apresenta exemplos desta figura utilizada me sites no browser Internet Explorer.

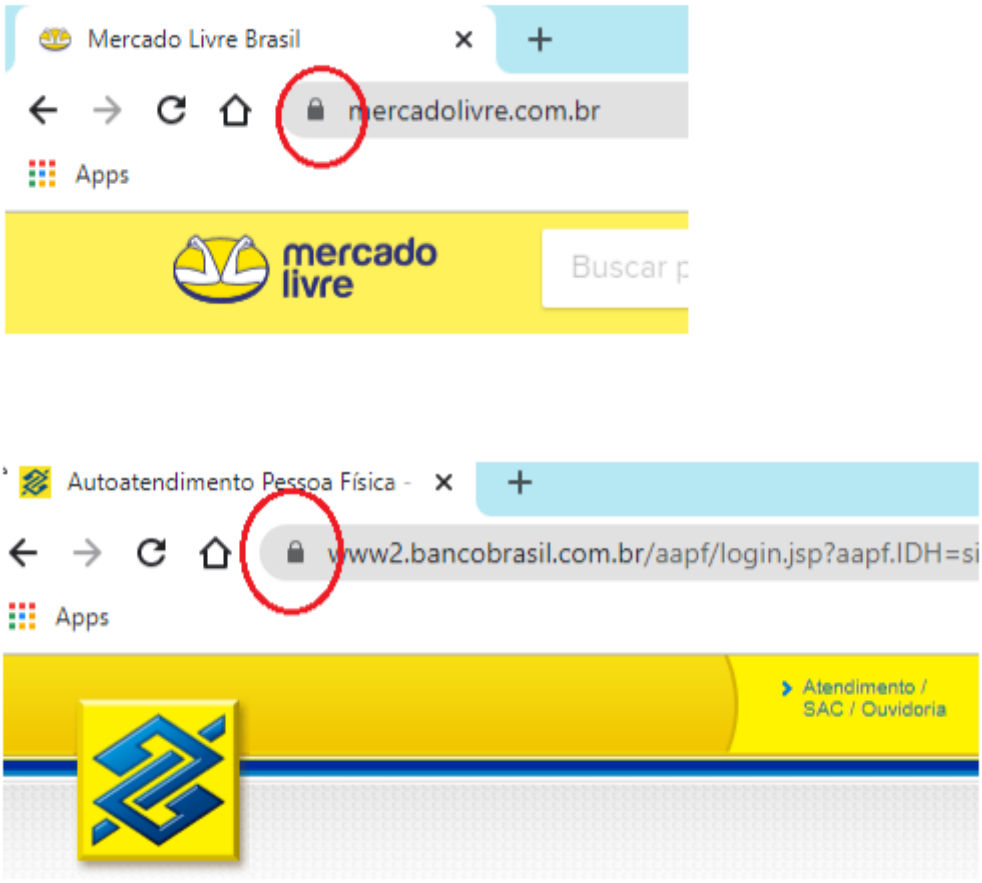



*Figura 5: Segurança em sites*

Também é possível verificar as informações do certificado emitido para a instituição que mantém o site e, também, as informações sobre a chave utilizada para criptografar os dados quando se clica no cadeado. É importante que se verifique o tamanho da chave utilizada; chaves menores que 128 bits podem comprometer a segurança no sigilo dos dados a serem transmitidos.

As informações do certificado aparecem como nas figuras seguintes do certificado do site do Banco do Brasil.

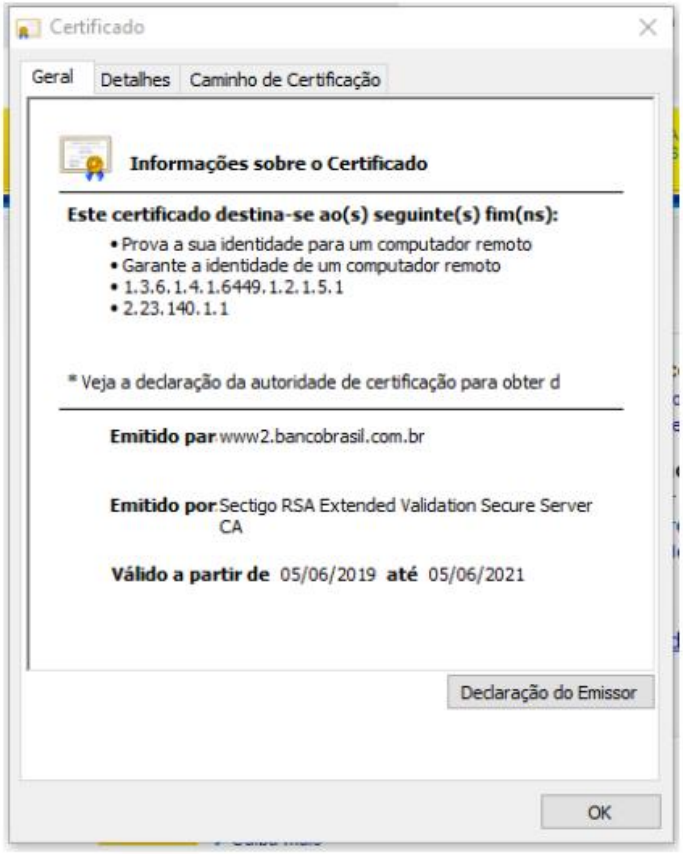



*Figura 6: Certificado no site do Banco do Brasil*

Nesta imagem estão detalhados o órgão emissor do certificado (Sectigo RSA Extended Validation Secure Server CA) e o prazo de validade.

Nas duas imagens abaixo há o detalhamento da chave pública RSA de 2048 bits e a identificação da chave. Estes e todos os outros detalhes podem ser encontrados ao clicar no cadeado dos sites mais seguros.

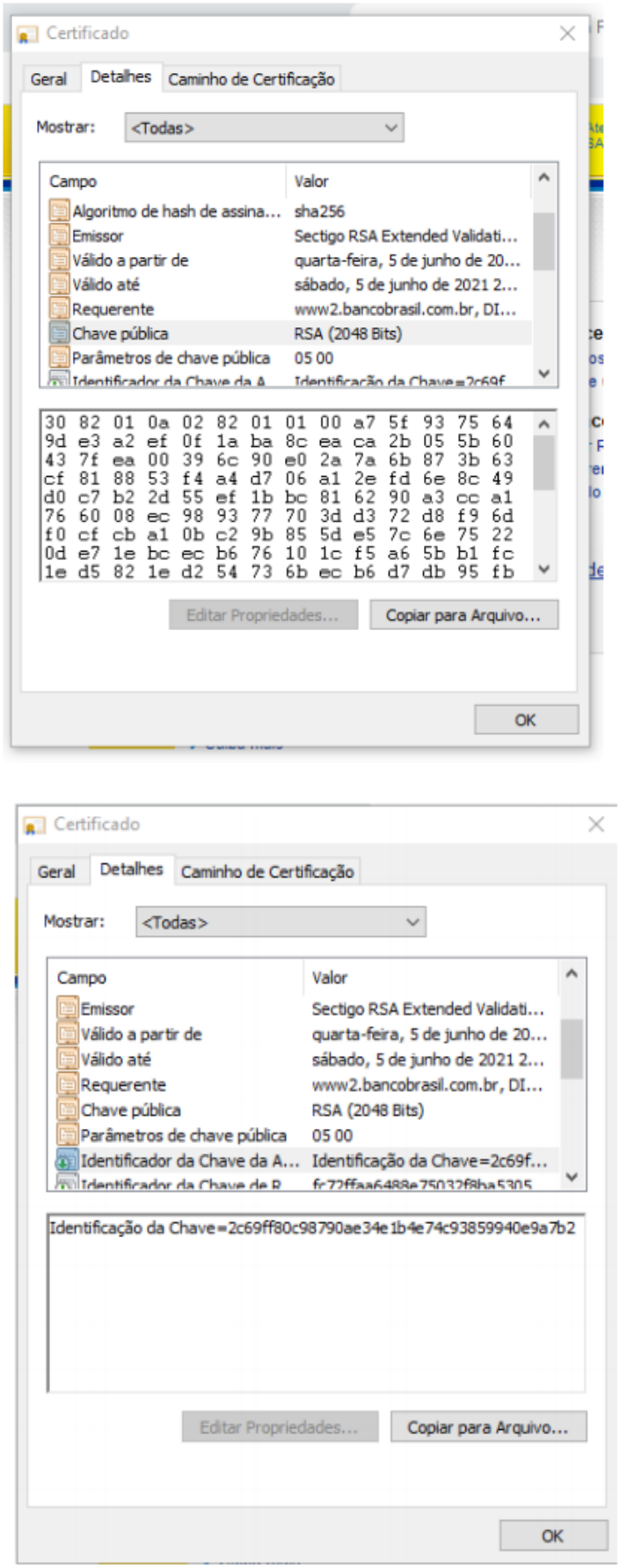



*Figura 7: Chave pública no site do Banco do Brasil*

Estes sites são considerados seguros pois, de acordo com a seção 5.2.1 deste trabalho, para descriptografar as mensagens trocadas é necessário descobrir os números primos p e q que foram multiplicados para gerar N da chave pública.

Para descobrir p e q é necessário fatorar N. Mas, N é resultado da multiplicação de dois números primos muito grandes. E isso demora muito tempo.

Para se ter uma ideia, se considerarmos um "número primo p de 47 algarismos, $p > 10^{46}$ e assim, $\sqrt{p} > 10^{23}$. Pelo algoritmo tradicional de fatoração, aquele por tentativas, precisaríamos testar a divisibilidade de p por todos os primos menores ou iguais à sua raiz quadrada. Há quase $2.10^{21}$ primos menores que $10^{23}$. Para se transformar essa informação em tempo de cálculo, precisamos de quantas divisões um computador é capaz de efetuar em um segundo. O supercomputador inaugurado pela USP em julho de 2015 faz algo em torno de $4{,}6.10^{13}$ operações por segundo. Se utilizássemos esse supercomputador para fazer as divisões, precisaríamos de aproximadamente $\frac{2.10^{21}}{4{,}6.10^{13}} \approx 4{,}348.10^{7}$ segundos, o que equivale a mais de 1 ano e 4 meses." [9].

O método de fatoração utilizado usualmente é inviável para números muito grandes, mesmo sendo utilizado em computadores potentes.

Então, será discutido agora algumas técnicas de fatoração que podem ser utilizadas na tentativa de descriptografar mensagens pois fatorar números é a questão central de segurança na criptografia RSA.

### 5.2.3 Técnicas de fatoração

O matemático francês Pierre de Fermat (1601 – 1665) desenvolveu um método muito eficaz para fatorar números que possuem um fator próximo à sua raiz quadrada chamado de ***Fatoração por Fermat.***

**Fatoração por Fermat**

Para que o algoritmo fique bem entendido é necessário que antes sejam feitas algumas observações.

O método tem como objetivo fatorar n inteiro maior que 1.

Para isso deve-se encontrar inteiros não negativos x e y, com x > y, tais que

$n = x^2 - y^2$, pois $x^2 - y^2 = (x + y).(x - y)$ e, com isso, tem-se uma fatoração de n, não necessariamente em fatores primos, mas com a certeza de que n é um número composto.

Pode-se considerar n ímpar pois, se n fosse par seria escrito como $n = 2^a.b$ para algum a inteiro positivo e algum b inteiro positivo ímpar. Assim, para fatorar n bastaria conhecer a fatoração de b (pois 2 é primo) e, portanto, a questão seria fatorar um número ímpar.

No processo de obter x e y pode-se encontrar números não inteiros. Por isso, será utilizada a notação [k] para indicar a parte inteira de um número real k.

Com essas observações feitas é possível analisar, agora, as etapas da Fatoração por Fermat [9]:

**Etapa 1:** Calcular $\sqrt{n}$.

- Se $\sqrt{n}$ for um número inteiro, n é um quadrado perfeito e o processo termina neste passo pois basta considerar $x = \sqrt{n}$ e $y = 0$.
- Se $\sqrt{n}$ não for um número inteiro, é preciso definir $b = [\sqrt{n}]$.

**Etapa 2:** Calcular $x = b + 1$.

- Se $x = \frac{n+1}{2}$, então n é primo e $y = \sqrt{x^2 - n}$ e esta etapa finaliza o processo.

  Foram obtidos os inteiros x e y com $y = \sqrt{x^2 - n} = \sqrt{\left(\frac{n+1}{2}\right)^2 - n} = \frac{n-1}{2}$.
- Se $x \neq \frac{n+1}{2}$, deve-se seguir para etapa 3.

**Etapa 3:** Calcular $y = \sqrt{x^2 - n}$.

- Se y for um número inteiro, esta etapa finaliza o processo pois n é composto e foram obtidos x e y.
- Se y não for um número inteiro, deve-se desconsiderar o valor anterior de b e definir b = x e voltar para a etapa 2, redefinindo x conforme este novo valor de b.

**Exemplo 5.2.3.1:** Fatorar n = 323.

Considerar n = 323 e $\frac{n+1}{2} = 162$.

Na etapa 1 obtemos $\sqrt{n} \approx 17{,}97$. Então define-se b = $[\sqrt{323}]$ = 17.

Na etapa 2, x = b + 1. Então x = 18. Como 18 ≠ 162 é necessário seguir para a etapa 3.

Nesta etapa, y = = $\sqrt{x^2 - n}$. Logo, y = $\sqrt{324 - 323}$ = 1.

Como 1 é inteiro, conclui-se que 323 é número composto e que x = 18 e y = 1.

Enfim, n = 323 = (x + y). (x – y) = 19.17 [9].

Convém observar que o algoritmo não conclui se os fatores encontrados são primos ou não.

**Exemplo 5.2.3.2:** Fatorar n = 35659.

Considerar n = 35659 e $\frac{n+1}{2} = 17830$.

Na etapa 1 obtemos $\sqrt{n} \approx 188{,}83$. Então, define-se b = $[\sqrt{323}]$ = 188.

Na etapa 2, x = b + 1. Então x = 189.

Nesta etapa, y = = $\sqrt{x^2 - n}$. Logo, y = $\sqrt{189^2 - 35659}$ = $\sqrt{62}$ ≈ 7,874, que não inteiro.

Então é necessária uma próxima tentativa: x = 190.

Assim, y = $\sqrt{190^2 - 35659}$ = $\sqrt{441}$ = 21, que é inteiro.

Como $\frac{n+1}{2} = 17830$, x < 17830 e y é inteiro, conclui-se que 35659 não é primo e x – y = 190 – 21 = 169 e x + y = 190 + 21 = 211.

Logo, 35659 = 169. 211.

Como 169 = $13^2$ e 211 é primo, a decomposição de 35659 em fatores primos é 35659 = $13^2$. 211. Mas, para descobrir que 211 é número primo por esse mesmo algoritmo seriam necessários mais de 90 passos.

É um algoritmo rápido se houver um fator de n não muito distante de $\sqrt{n}$. Este algoritmo pode não ser tão vantajoso quando isso não acontece.

Agora será exemplificado o caso da fatoração de um número maior que os anteriores e como seria a aplicação em uma tentativa de “quebrar” a criptografia RSA.

**Exemplo 5.2.3.3:** Em um algoritmo RSA foi adotado N = 249863005313. Deve-se descobrir a chave privada (N, d).

A variável x é inicializada com a parte inteira da raiz quadrada de N, que neste caso vale 499862. Mas,

$x^2 = 249862019044 < N$

logo passa-se a incrementar x de um em um. Isto deve ser feito até que $\sqrt{x^2 - n}$ seja um número inteiro, ou x ser igual a $\frac{n+1}{2}$, que neste caso vale 124931502657. Com apenas uma repetição de etapa tem-se que x = 499863 e y = 116.

Assim, x + y = 499979 e x – y = 499747 e, com isso, tem-se

$\varphi(N) = (499979 - 1).\ (499747 - 1) = 249862005588,$

e, além disso, deve-se considerar que mdc($\varphi$(N), d) = 1 [10].

Utilizando o algoritmo de Euclides, citado na seção 3.6.4 deste trabalho, percebe-se que para d = 5 a equação mdc($\varphi$(N), d) = 1 é verificada.

| | | | | |
|---|---|---|---|---|
| | 49972401117 | 1 | 1 | 2 |
| 249862005588 | 5 | 3 | 2 | 1 |
| 3 | 2 | 1 | 0 | |

Portanto, a chave privada é (N, d) = (249863005313, 5).

Em 1994, Peter Shor, trabalhando na Bell Labs (uma empresa de pesquisa industrial e desenvolvimento científico, subsidiária da empresa finlandesa Nokia com sede em Nova Jérsia), formulou um algoritmo que resolve o problema da fatoração de números inteiros em primos em computadores quânticos. O ***Algoritmo de Shor*** é a primeira evidência de que os computadores quânticos são inerentemente mais poderosos e pode ser utilizado para quebrar chaves do sistema RSA de criptografia.

## Algoritmo de Shor

Peter Shor formulou esse algoritmo de fatoração que requer uma quantidade em ordem polinomial de passos em um computador quântico para fatorar um número inteiro de tamanho arbitrário. Apresentou um método que não decompõe um número em dois fatores não triviais pelo método direto de divisões sucessivas, e sim, utiliza o problema equivalente de encontrar a ordem de um certo inteiro módulo o número fatorado, onde esse inteiro é escolhido aleatoriamente sendo primo com o número fatorado. O algoritmo calcula essa ordem.

O conceito do algoritmo baseia-se no seguinte: dado um número ímpar composto positivo N, deseja-se fatorá-lo da forma $N = n_1.n_2$, com $1 < n_i < N$. Ou seja, deve-se encontrar um fator não trivial *d* de N diferente de 1 e do próprio N.

Para que fique bem compreendido os passos desse algoritmo são necessárias algumas definições.

**Definição 5.2.3.1:**

Sejam y e N inteiros tais que $1 < y < N$ e mdc (y, N) = 1. Denomina-se a ordem de y módulo N ao menor inteiro positivo r tal que $y^r \equiv 1 \pmod N$.

A ordem de um inteiro y módulo N também é o período de uma certa função definida sobre o conjunto dos números naturais [11].

**Definição 5.2.3.2:**

Sejam y e N inteiros tais que $1 < y < N$ e mdc (y, N) = 1. Considere agora a seguinte função:

$$f_N: \mathbb{N} \rightarrow \mathbb{N}$$

$$a \rightarrow y^a \pmod N$$

Definimos a ordem de y módulo N como o menor inteiro positivo r tal que

$f_N(a + r) = f_N(a)$, para todo $a \in \mathbb{N}$.

Isto é, r é o menor inteiro positivo tal que $f_N(r) = 1$ [11].

Vale observar que os elementos do conjunto imagem de $f_N$ serão, no máximo, todos os restos 0, 1, 2, ..., N – 1 da divisão por N.

O Algoritmo de fatoração de Shor é composto de cinco etapas dentre as quais, somente a segunda (que calcula o período de $f_N$) envolve computação de natureza quântica. As outras etapas necessitam apenas da computação clássica em tempo polinomial.

**Etapa 1:** Escolher aleatoriamente y tal que $1 < y < N$ e calcular mdc (y, N) através do algoritmo de Euclides.

Se mdc (y, N) $\neq 1$ então o processo está finalizado com *d* = mdc (y, N) sendo um fator não trivial de N.

Senão, seguir para a etapa 2.

**Etapa 2:** Com a computação quântica deve-se calcular o período *r* da função

$f_N(a) = y^a \pmod N$.

**Etapa 3:** Se *r* é ímpar, então é necessário voltar a etapa 1. Senão, prosseguir para a etapa 4.

**Etapa 4:** Como *r* é par, tem-se que

$$y^r - 1 = (y^{r/2} - 1).\ (y^{r/2} + 1) \equiv 0 \pmod N.$$

Necessariamente $(y^{r/2} - 1) \not\equiv 0 \pmod N$, pois *r* é a ordem de y módulo N.

Assim, se $(y^{r/2} + 1) \equiv 0 \pmod N$, então é necessário voltar a etapa 1.

Senão, prosseguir para a etapa 5.

**Etapa 5:** Como $(y^{r/2} + 1) \not\equiv 0 \pmod N$, usando o algoritmo de Euclides calcula-se *d* = mdc $(y^{r/2} + 1, N)$. Enfim, o algoritmo é finalizado com *d* sendo um fator não trivial de N.

É importante se observar que o algoritmo depende que o inteiro $1 < y < N$ escolhido aleatoriamente possua uma ordem que satisfaça simultaneamente as duas condições a seguir:

i. *r* par;
ii. $y^{r/2} \not\equiv -1 \pmod N$.

Após a quinta etapa, como $y^r - 1 = (y^{r/2} - 1).(y^{r/2} + 1) \equiv 0 \pmod{N}$, N divide o produto $(y^{r/2} - 1).(y^{r/2} + 1)$ sem dividir qualquer um dos dois fatores. Logo, N pode ser decomposto em dois fatores.

# 6. ESTUDO EXPLORATÓRIO

Neste capítulo será apresentado um plano de estudo exploratório com uma se ideal de quatro aulas para uma abordagem sobre o princípio da sobreposição da mecânica quântica no ensino. Será executada com uma turma selecionada de participantes de Olimpíadas de Matemática de 6º e 7º ano para apresentar o tema criptografia juntamente com fatoração e computação quântica.

## 6.1 Sequência de aulas

As aulas têm como tema principal a fatoração de números e a computação quântica. Estes assuntos serão abordados pois estão totalmente relacionados com a criptografia.

A escola particular escolhida foi o Colégio Dom Aguirre, na cidade de Sorocaba – SP.

O público das aulas será composto de 4 alunos (uma aluna do 6º ano e três do 7º ano) que fazem um curso preparatório para participarem de Olimpíadas de Matemática como a OPM (Olimpíada Paulista de Matemática), a OMU (Olimpíada de Matemática da Unicamp) e a OBMEP. Estes alunos foram escolhidos pois já fazem parte de um grupo selecionado que gosta bastante e se interessa muito por temas relacionados a Matemática, além de terem certa facilidade com esta ciência.

Os objetivos das aulas são:

i. Os alunos devem conhecer a Criptografia RSA e algumas de suas aplicações;
ii. Os alunos devem conhecer as duas técnicas de fatoração apresentadas neste trabalho: Fatoração por Fermat e Algoritmo de Shor;
iii. Os alunos devem entender o que é o computador quântico, suas principais características e sua influência no estudo da criptografia.

Os conteúdos abordados serão a criptografia, a fatoração de números e o computador quântico.

Para que estes temas sejam desenvolvidos, primeiramente os alunos responderão um questionário e após, terão aulas que serão ministradas pela plataforma Microsoft Teams usando recursos do computador como Power Point e outros.

A metodologia será aula expositiva com o desenvolvimento de alguns exemplos e aplicações.

A sequência didática ideal seria composta pelas seguintes aulas:

**1ª aula:** Este encontro tem caráter investigativo. Para realizar a averiguação os alunos responderão um questionário e acontecerá um “bate papo” sobre o que eles entendem por criptografia e computação.

O questionário é composto pelas seguintes questões:

1. Você sabe o que é Criptografia?
2. Você usa Criptografia no dia a dia? Se sim, como?
3. O que é um computador?
4. Caixa eletrônica, videogames e celular são computadores? Por quê?
5. Existem computadores melhores que outros ou todos são iguais? Por que uns são mais caros e outros mais baratos?
6. O que é um computador quântico? É possível construir um? Já existe computador quântico?
7. Quais são as diferenças entre um computador clássico e um quântico?
8. A criptografia pode se tornar mais segura com um computador quântico?
9. Você acredita que a Criptografia corre riscos com os computadores quânticos?
10. Você considera interessante incluir Física Quântica na grade curricular do ensino básico?

**2ª aula:** Esta reunião terá uma especificidade formal onde será ministrada uma aula com apresentação com os seguintes slides e explicações sobre os temas abordados no questionário.

Slide 1:

# A Criptografia, a fatoração e o computador quântico

Slide 2:

**A Criptografia está presente no cotidiano de todos nós!**

**Os códigos estão:**

- **Nos celulares;**
- **Nas redes sociais;**
- **Nos alarmes de carros e residências;**
- **Nas transações bancárias;**
- **E na internet de modo geral.**

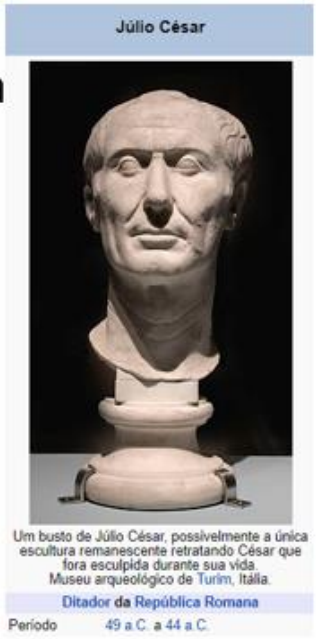
**Ela ajuda na proteção dos conteúdos transmitidos, evitando a interceptação por parte de ciber criminosos e hackers.**

Slide 3:

Há indícios de que a criptografia surgiu por volta de 1900 a.C. no Antigo Egito, quando o faraó Amenemhet II governava e decidiu substituir trechos e palavras de documentos por símbolos pois continham importantes informações sobre a localização de tesouros...

Slide 4:


Cifra de César, usada na Roma antiga




a frase “isto é um segredo” é transformada em JTUP F VN TFHSFEP.

Slide 5:

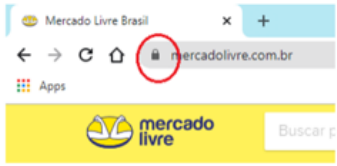
**Máquina Enigma**
**(máquina nazista que quase venceu a Segunda Guerra)**

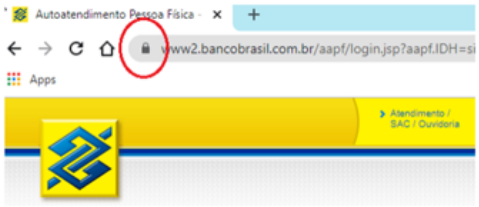
A máquina conhecida como Enigma foi uma das maiores inimigas da humanidade até que Alan Turing inventasse uma máquina ainda melhor para decifrá-la. E sem ele era bem provável que os nazistas vencessem a guerra e o mundo como conhecemos hoje poderia não ter existido.

A criptografia da Enigma era bastante simples, mas sua engrenagem gerava milhares de possibilidades, o que tornava a tarefa em decifrar suas mensagens quase humanamente impossível.

Slide 6:

**Hoje, a criptografia está presente para gerar segurança em sites, por exemplo...**




Slide 7:

E no WhatsApp...


Slide 8:

## Criptografia RSA

- Para cifrar uma mensagem é necessário escolher números primos p e q (MUITO GRANDES) e calcular N = p. q

*(é recomendado que N tenha no mínimo 2048 bits de comprimento, ou seja, é maior que $2^{2047}$ e menor que $2^{2048}$ )*

- N formará a chave pública.
- Acredita-se que para quebrar a criptografia é necessário descobrir p e q, ou seja, é necessário *FATORAR N*.

Slide 9:

E, para fatorar N pode-se utilizar técnicas de fatoração.

Serão apresentadas duas técnicas:

- **Fatoração por Fermat**
- **Algoritmo de Shor**

Slide 10:

## Fatoração por Fermat - Exemplo

**Fatorar n = 35659.**

Considerar n = 35659 e (n+1)/2= 17830.
Na etapa 1 obtemos $\sqrt{n} \approx 188{,}83$. Então define-se b = $[\sqrt{323}]$ = 188.

Na etapa 2, x = b + 1. Então x = 189. Nesta etapa, y = = $\sqrt{x^2 - n}$. Logo, y = $\sqrt{189^2 - 35659} = \sqrt{62} \approx 7{,}874$, que não inteiro.

Então é necessária uma próxima tentativa: x = 190.
Assim, y = $\sqrt{190^2 - 35659} = \sqrt{441}$ = 21, que é inteiro.

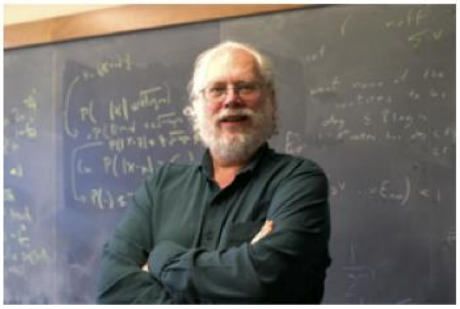
Como (n+1)/2= 17830, x < 17830 e y é inteiro, conclui-se que 35659 não é primo e
x – y = 190 – 21 = 169 e x + y = 190 + 21 = 211.
Logo, 35659 = 169. 211.

Como 169 = $13^2$ e 211 é primo, a decomposição de 35659 em fatores primos é 35659 = $13^2$. 211. Mas, para descobrir que 211 é número primo por esse mesmo algoritmo seriam necessários mais de 90 passos.
É um algoritmo rápido se houver um fator de n não muito distante de $\sqrt{n}$. Este algoritmo pode não ser tão vantajoso quando isso não acontece.

Slide 11:

## Algoritmo de Shor:

é composto de cinco etapas dentre as quais, somente a segunda envolve **computação de natureza quântica**. As outras etapas necessitam apenas da computação clássica em tempo polinomial.



Slide 12:

"O computador de hoje trata-se de uma máquina de cálculos e uma memória que armazena tanto instruções a serem executadas (programa) quanto a entrada para este conjunto de instruções."

## Mas, quanto tempo demora para fatorar nos computadores modernos?

Em uma pesquisa concluída e 2009, foi fatorado um número de 232 dígitos utilizando centenas de máquinas e demorou 3 anos...
Pesquisadores estimam que um módulo RSA de 1024 bits demoraria mais ou menos 3000 anos!

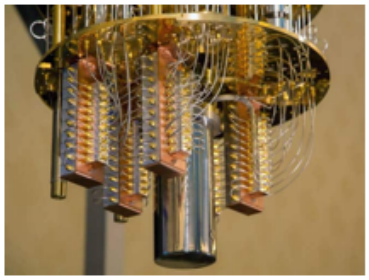
**Com o Algoritmo de Shor demoraria 4,5 minutos...**

Slide 13:

- O que são computadores Quânticos?
- Já existem?

- Com eles a Criptografia não será mais segura?
- A criptografia sobreviverá com a computação quântica?

Slide 14:



Um computador clássico tem uma memória feita de bits. Cada bit guarda um "1" ou um "0" de informação. Um computador quântico mantém um conjunto de qubits. Um qubit pode conter um "1", um "0" ou uma sobreposição destes. Em outras palavras, pode conter tanto um "1" como um "0" ao mesmo tempo. O computador quântico funciona pela manipulação destes qubits.

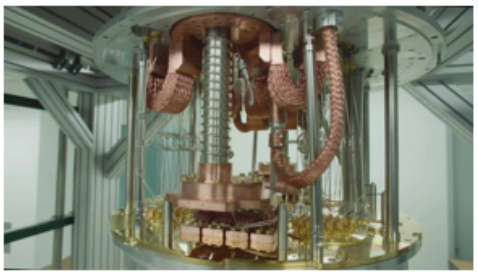
O computador quântico é um dispositivo que executa cálculos fazendo uso direto de propriedades da mecânica quântica, tais como sobreposição e interferência.

Uma moeda, por exemplo, pode ser cara ou coroa. Mas se a moeda seguisse as regras da mecânica quântica, ela estaria girando no ar. Então, até ela cair e olharmos para ela, não sabemos se é cara ou coroa. Efetivamente , é coroa e cara ao mesmo tempo.

Slide 15:

## Já existem?

"Orion. Esse é o nome do primeiro Computador Quântico, que foi apresentado, em 2007, pela empresa canadense D-Wave. Uma máquina de 16 qubits, que custou uma fortuna e funcionou por um período incrivelmente curto. Dez anos mais tarde, a IBM divulgou, durante um evento de produtores de computadores, que estava desenvolvendo um novo processador quântico, dessa vez, de 50 qubits. Conseguiram mantê-lo funcionando por 90 microssegundos."

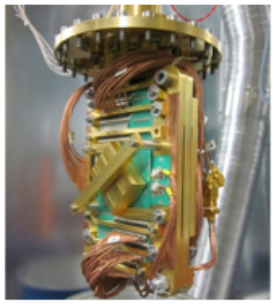


"No mesmo ano, a mesma D-Wave anunciou o 2000Q, com 2000 qubits. Enquanto isso, sistemas de 1000 qubits da empresa já estavam sendo testados pela Google, NASA e Lockheed Martin. No entanto, pouco se sabe sobre qual o desempenho ou a real aplicabilidade desses computadores.

Em 2019, a IBM lança o primeiro computador quântico comercial: o Q System One. Um sistema híbrido de 20 qubits com processamento, em parte quântico e, em parte, clássico. No entanto, a tecnologia só pode ser usada pelo serviço de computação em nuvem da empresa."

Slide 16:

"Quanto à comercialização, a IBM saiu à frente das outras empresas. Mas, enquanto isso, a D-Wave anuncia que seu processador quântico já trabalha com 128 qubits e a Google informa que ela também já tem um computador quântico. Já a Intel construiu um de 49 qubits e a Microsoft está, nesse momento, desenvolvendo seu próprio processador. A China também decide entrar na corrida: no ano que vem deve inaugurar um laboratório estatal de Computação Quântica."



"...cientistas do Google têm trabalhado para criar um processador de computador que pode resolver um problema difícil demais para os melhores supercomputadores do mundo. Na quarta-feira (23), eles anunciaram que foram bem-sucedidos: o computador quântico Sycamore conseguiu resolver em 200 segundos um problema que um supercomputador precisaria de 10.000 anos para resolver, de acordo com suas estimativas. É um problema único e simulado, e o chip falharia em uma competição contra um supercomputador para somar dois mais dois. Mas os cientistas do Google pensam que alcançaram um marco histórico da computação..."

*Reportagem de Outubro de 2019*

Slide 17:

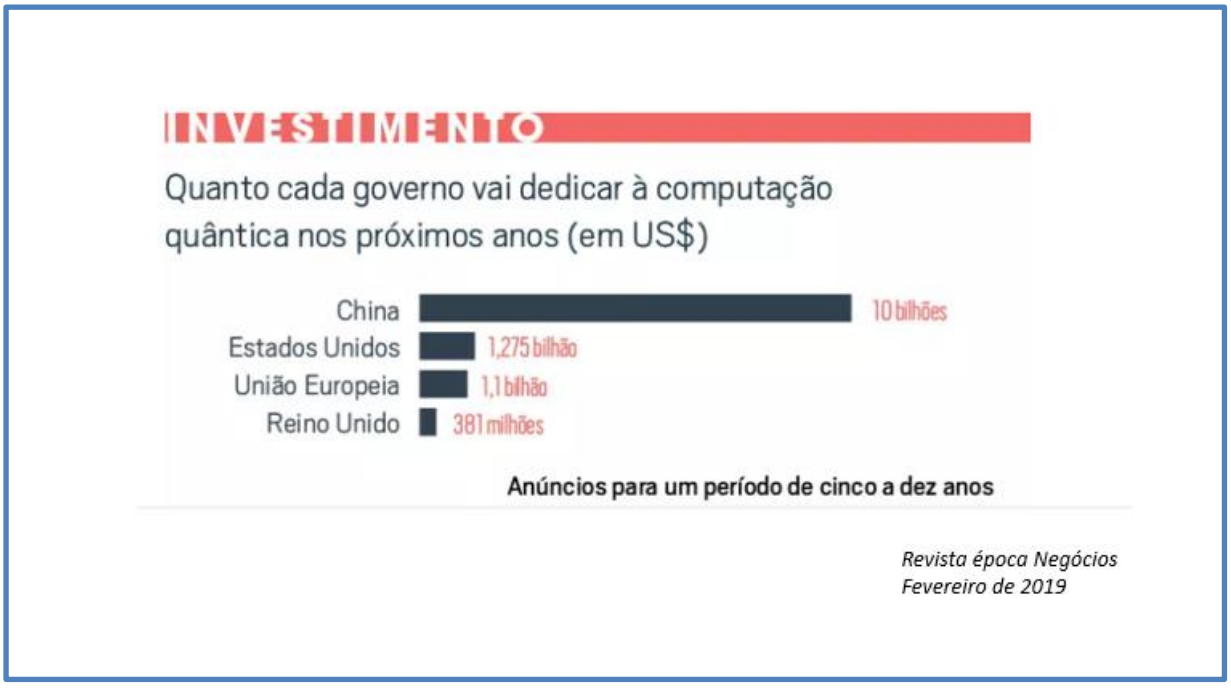
O **algoritmo de Shor** é um marco da computação quântica porque ele foi o primeiro algoritmo a utilizar as funcionalidades particulares de um computador quântico para otimizar a solução de um problema. A publicação do algoritmo de Shor desencadeou uma avalanche de novas pesquisas e experiências na computação quântica. Em dezembro de 2001, cientistas do Centro de Pesquisas da IBM em Almaden conseguiram construir um computador quântico de 7 qubits. Nesse computador foi implementado o algoritmo Shor, que conseguiu realizar corretamente a fatoração do número 15. Obviamente, esse computador não consegue quebrar nenhum sistema de criptografia. A importância desse experimento é que ele comprova a viabilidade da computação quântica. As principais dificuldades enfrentadas nesse primeiro momento são mais tecnológicas do que teóricas, como a alta incidência de erros nos computadores quânticos construídos até agora.

Slide 18:

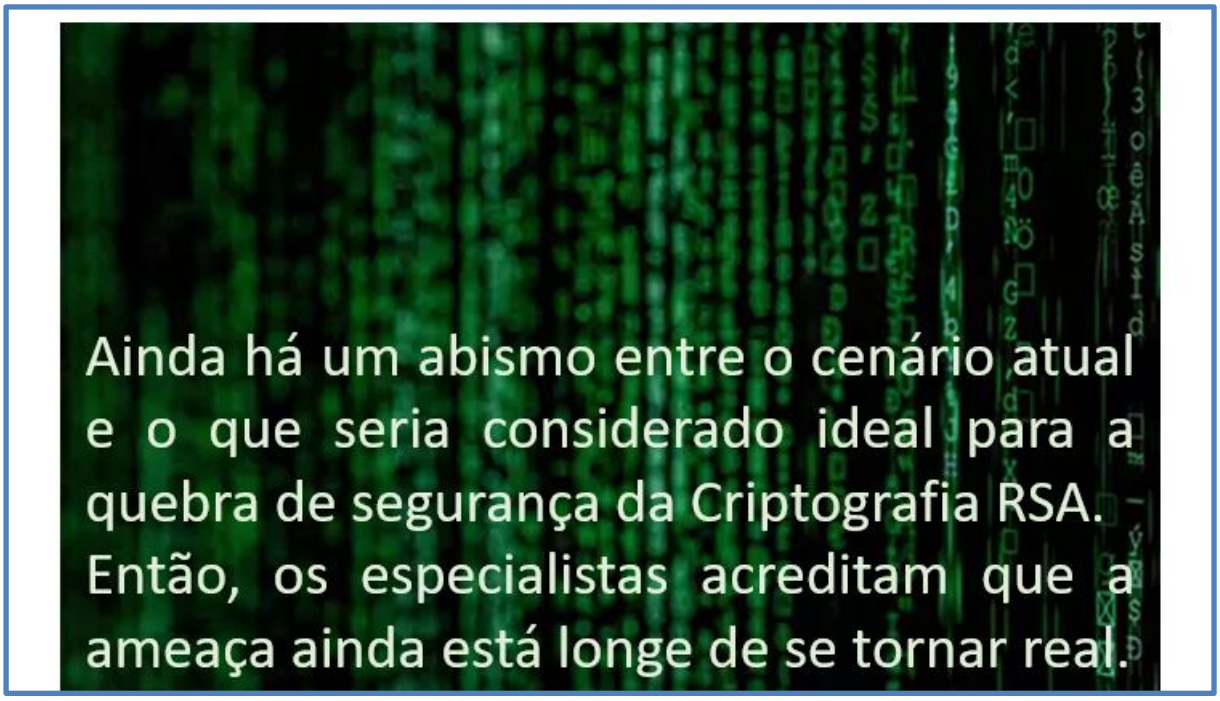
**Mas existem problemas:**

- Alta incidência de erros;
- A operação do computador exige temperaturas baixas (próximas ao zero absoluto: -273,15 °C), a fim de reduzir a incidência de erros;
- a influência do meio sobre o computador quântico pode causar a alteração de qubits;
- se for feita uma leitura dos dados durante a execução de programa em um computador quântico, todo o processamento será perdido. Assim, a maior dificuldade é conseguir corrigir um erro sem de fato medir o sistema. Isso é conseguido através da coerência de fase (utiliza-se ressonância magnética nuclear).

Slide 19:




Slide 20:




**3ª aula:** Nesta aula será solicitado aos alunos que tentem fazer algumas fatorações para possam vivenciar a dificuldade em fatorar números grandes.

Eles devem fazer tentativas de fatoração “na mão” dos seguintes números na ordem apresentada para que possam perceber a complexidade:

(i) 2145 = 3.5.11.13
(ii) 6248 = $2^3$.11.71
(iii) 42598 = 2.$19^2$.59
(iv) 325896 = $2^3$.3.37.367
(v) 154789632 = $2^8$.$3^2$.$23^2$.127

Com os cálculos dos dois últimos números já é possível compreender que é necessário o uso do computador para facilitar o processo.

Após esses cálculos, deve-se apresentar aos alunos calculadoras on-line para que as fatorações sejam feitas no computador de forma muito mais fácil. Sugestão de calculadora on-line: https://www.4devs.com.br/calculadora_fatorar_numero .

Assim, começarão a perceber como o computador agiliza o processo.

Depois, deve-se pedir que fatorem, com o uso do computador números cada vez maiores, por exemplo:

(i) 2354786214524
(ii) 254136987452456

Nestes exemplos os alunos perceberão que a fatoração demora um pouco.

Por fim, pedir que tentem o número 235478965214587562 e, neste, a calculadora não expressa um resultado.

Dessa forma, espera-se que os alunos entendam o quanto é difícil “quebrar” a Criptografia RSA com os computadores modernos e tradicionais e a necessidade da existência de computadores muito mais rápidos como os computadores quânticos.

Com as discussões sobre as fatorações realizadas finaliza-se a terceira aula.

**4ª aula:** Este último encontro será o desfecho da sequência didática no qual será feita uma apresentação sobre Física Quântica e a novamente a aplicação do questionário da 1ª aula para validação do aprendizado.

A apresentação sobre a Física Quântica deve ser introdutória e ilustrativa devido a idade dos alunos. Deverá contemplar os seguintes tópicos:

(i) O que Física Quântica (até o Princípio da S
(ii) obreposição)?
(iii) O que são átomos, moléculas, partículas subatômicas e a quantização de energia?
(iv) Apresentação de alguns dos principais pensadores que contribuíram para o desenvolvimento da Física Quântica como: Planck, Einstein, Rutherford, Bohr...

É interessante mostrar aos alunos algumas animações para ilustrar esta ciência como por exemplo, https://www.youtube.com/watch?v=zKiCEU6P3U0&authuser=0.

## 6.2 Dinâmica das aulas

Primeiramente, foi solicitado aos alunos que respondessem um questionário, no dia 17/11/2020, para que fosse possível analisar o conhecimento em computação e Criptografia. O questionário foi aplicado pelo Google Forms porque os alunos estavam em estudo remoto. Este formulário foi enviado por e-mail e os estudantes enviaram as respostas após três dias.

As respostas foram bem similares, mas um aluno pesquisou um pouco e conseguiu ser um pouco mais técnico.

Dois alunos responderam que não sabiam o que era criptografia, mas que tinham ouvido falar sobre. Uma aluna disse que não tinha certeza, mas achava que tinha a ver com o uso de códigos para deixar a comunicação mais segura. E outro aluno respondeu: “É uma forma de proteção de dados usando grande linhas de código”.

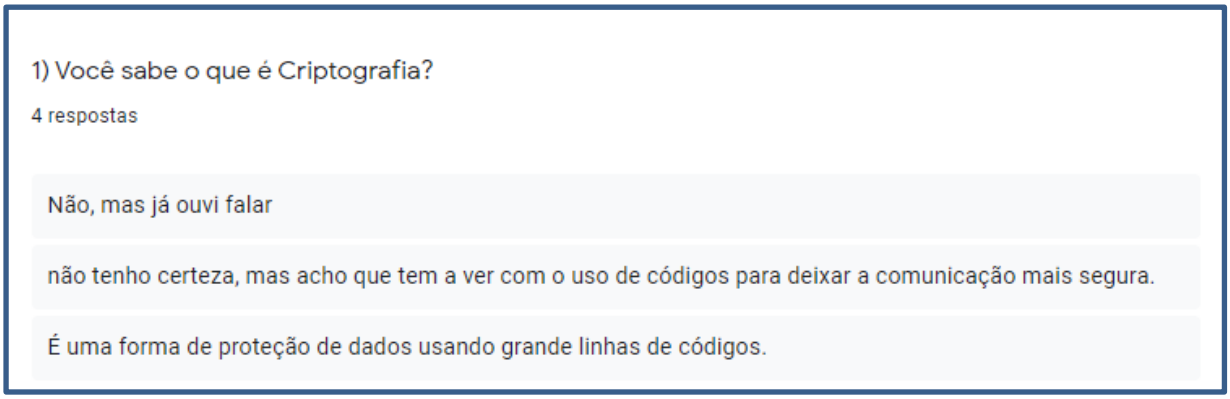



*Figura 8 – Questionário (questão 1)*

Em relação ao uso da criptografia no dia a dia todos responderam que usam no dia a dia quando estão na internet e WhatsApp. O aluno que pesquisou deu a seguinte resposta: “Sim, de várias forma, de acordo com leis a redes sociais que possuem crianças como Youtube e WhatsApp devem ser encriptadas, então ao usar esses serviços eu estou tendo meus dados encriptados, softwares como jogos, editores de data entre outros também costumam ter seu código fonte encriptado para ajudar a se proteger contra a pirataria, e antivírus tendem a usar a

criptografia como um meio de proteção de dados, apesar de eu não usar um atualmente o próprio Windows defender tem uma forma de criptografia".

Sobre o que é um computador, dois alunos responderam que conhecem, mas não sabem bem o que é. Os outros dois responderam que é uma máquina que processa dados transformando-os em informações e que é capaz de seguir ordens e fazer cálculos.

Os quatro alunos responderam que caixas eletrônicos e vídeo games provavelmente são computadores com algumas diferenças como: tamanho e velocidade de processamento e intuito de uso.

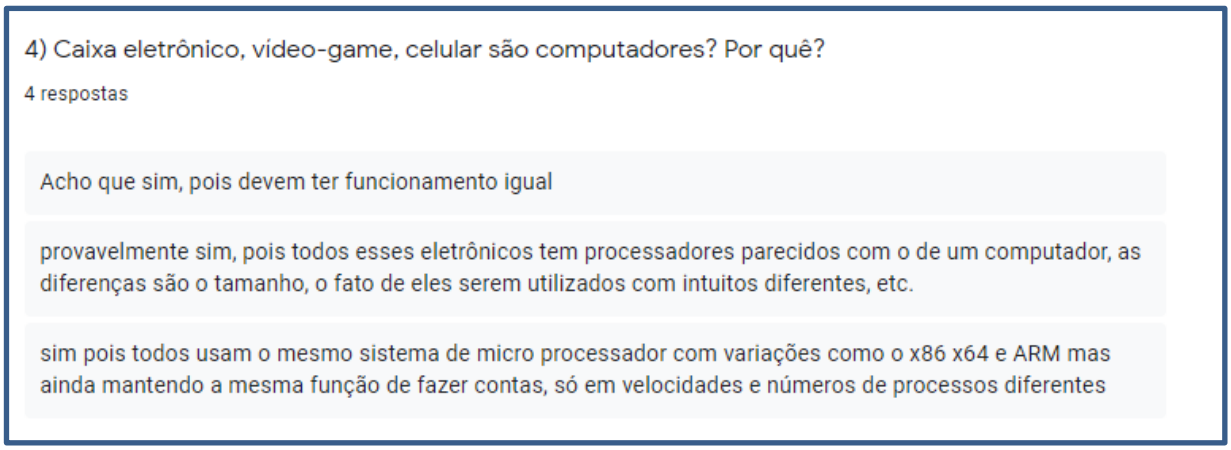



*Figura 9 – Questionário (questão 4)*

Quando questionados sobre haver computadores mais caros e outros mais baratos, todos destacaram que existem diferenças que causam bastante diferença de preços. Dois alunos apontaram a questão da memória como causa de diferença de preços. Outro salientou a velocidade do processador e o design como fatores importantes. E o último, fez o seguinte comentário: "Depende muito da função do computador, mas na área certa um computador pode sim ser melhor que o outro, um aplicativo dependente de single core tipo o cinebench r15 vai ser muito melhor com um computador com um processador de altos clocks e ipcs como o ryzen 9 5950x, mas funcionaria pior em um processador mais caro como um epyc por ter baixos clocks. um computador pode ser mais caro que o outro pelo nível de tecnologias implementadas exemplo: núcleos de processadores podem ser caros por isso um processador com mais núcleos pode ser mais caro pra produzir, isso também conta pra chips, memórias, vrm, mosfetes e etc".

Sobre o computador quântico, três assumiram que não sabem o que é. Uma aluna, após uma breve pesquisa, escreveu: "... é um dispositivo que executa cálculos fazendo uso direto de propriedades da mecânica quântica, tais como sobreposição e interferência. Sim dá para construir um. Sim, o D-Wave Two". Com isso, na questão seguinte, sobre as diferenças entre o computador quântico e o clássico, dois alunos declararam não saber, um citou a diferença de

bits e qubits e o último citou o seguinte exemplo: “Um computador clássico que lê três bits pode fornecer uma possibilidade de combinação, enquanto o computador quântico pode apresentar até oito possibilidades”.

Na oitava pergunta, sobre a segurança da criptografia com o computador quântico, dois responderam que não sabiam e os outros dois que sim, ou seja, que o computador quântico deixaria a criptografia mais segura.

Na nona questão, responderam não saber sobre os possíveis riscos da criptografia com a chegada da computação de natureza quântica.

Por fim, na última pergunta, os quatro responderam que seria muito interessante incluir Física Quântica na grade do ensino básico. Um deles escreveu: “sim, pois o futuro da computação está nos computadores quânticos por isso acho que educação deveria avançar nessa direção”.

O segundo encontro aconteceu no dia 24/11 pela plataforma Microsoft Teams pois os alunos estão com aulas remotas devido a pandemia.

Primeiramente foi explicado o porquê daquele momento e foi feita uma breve apresentação da tese. Após, deu-se início a apresentação dos slides.

A duração da apresentação dos slides e explicação foi de 1h20min.

A aula teve início com a explicação do que é a criptografia e de uma parte de sua história com os slides 1, 2 e 3. Logo após, foi apresentada a Cifra de César e foi feito o seguinte questionamento aos alunos: “O que acham dessa maneira de codificar mensagens? Vocês a acham segura? Se precisassem mandar uma mensagem com um segredo muito importante usariam esta forma de criptografia?”. E todos foram unânimes em responder que não usariam. Falaram que é muito fácil descobrir como ela funciona. Um deles comentou: *“Esse esquema de código não é muito bom porque é só perceber a letra que aparece mais e já se descobre alguma coisa”; outra disse: “É muito fácil perceber que usa a letra seguinte”.* A partir desse comentário foi falado sobre as cifras de substituição monoalfabéticas e sobre a criptografia simétrica e assimétrica.

E partiu-se para o slide da Máquina Enigma. Foi falado sobre u o uso da máquina na Segunda Guerra Mundial e da importância de Alan Turing no desfecho dela.

Com os slides 6 e 7 foram mostrados exemplos de uso da criptografia na atualidade. Neste momento uma aluna disse: *“Professora, eu achei que a Criptografia era um tipo de código e, agora, depois destas explicações vi que está em muitas coisas e desde muito tempo atrás. É muito interessante!”.*

Então, foi apresentada a Criptografia RSA e a importância da fatoração para a quebra de codificações. Foi dado um exemplo de número muito grande e pedido para que tentassem fatorar com a técnica que conheciam.

Tentaram um pouco e logo desistiram pois perceberam que levaria muito tempo para conseguir. Um aluno comentou que poderia ser que não conseguisse terminar se, em algum momento, tivesse um número grande que não poderia ser dividido pelos números primos pequenos. A dúvida dele foi: "*como vou saber se o número que preciso dividir é primo?"* E, a partir deste comentário foram apresentadas as duas formas de fatoração desenvolvidas neste trabalho.

Mas, antes de falar sobre a Fatoração de Fermat e de Shor apresentadas nos slides 9, 10 e 11 foi explicado a eles que estudaram no ensino regular um tipo de fatoração de números (mais apropriada para número não muito grandes) e que estariam vendo, naquele momento, duas outras formas que são mais apropriadas quando se tratam de números muito grandes.

Após a apresentação da técnica de Shor uma aluna comentou que estava ficando muito difícil entender o assunto pois não entendia o que era a computação quântica citada.

E assim, começou a ser falado sobre o computador quântico. Isso foi uma grande novidade para os alunos. Eles comentaram que já haviam escutado este nome, mas desconheciam qualquer fato relacionado à computação quântica.

Para que entendessem melhor o assunto, foi apresentada uma animação através do seguinte link para que tivessem uma introdução sobre a Física Quântica.

https://www.youtube.com/watch?v=zKiCEU6P3U0&authuser=0

Acharam muito interessante, e confessaram que realmente não tinham noção alguma do comportamento de algumas partículas como o elétron. Na verdade, não sabiam nem o que era um elétron; sabiam apenas o que era um átomo. E, a partir disso, começaram a entender o porquê da grande dificuldade existente no sucesso do desenvolvimento e funcionamento de um computador que trabalha com estas micropartículas.

Ficaram um pouco decepcionados ao saber que muitos fatores influenciam no seu bom funcionamento. Ficaram com a impressão de que o uso efetivo deste tipo de computador ainda está muito distante da atualidade mesmo sabendo que existem e que são investidos milhões de dólares no desenvolvimento deles.

Ao finalizar a explanação dos slides foram refeitas algumas perguntas que já haviam respondido no questionário inicial:

- A criptografia pode se tornar mais segura com um computador quântico?
- Você acredita que a criptografia corre riscos com os computadores quânticos?

Todos ficaram na dúvida para responder a primeira pergunta. Uma aluna disse que não sabia a resposta pois ao mesmo tempo que é uma tecnologia inovadora e muito capaz pode fazer com que a Criptografia RSA seja quebrada em minutos. Mas, ela perguntou: "e *se a computação quântica for usada pra desenvolver ainda mais a criptografia?"* E, a partir deste comentário houveram diversas outras indagações e a seguinte dúvida: o uso do computador quântico irá nos deixar mais seguros ou impossibilitará o uso de qualquer forma de criptografia?

Eles disseram que ficaram impressionados porque perceberam que não conheciam nada sobre os assuntos apresentados. Afirmaram que ficaram muito motivados a estudar mais sobre o assunto e comentaram sobre o fato de estarem estudando matemática na prática: *"Gosto muito de Matemática, mas não tinha noção do tamanho da sua importância"*, comentou um aluno. Eles são estudantes que adoram matemática, mas tem somente contato com ela em provas de Olimpíadas e nas aulas regulares. Foi um momento diferente onde perceberam que o estudo desta ciência está em um universo muito maior com suas aplicações.

No final, foi perguntado novamente a eles se achariam interessante estudar Física Quântica no ensino regular e todos responderam que sim. Salientaram que *"é muito legal"* estudar teorias modernas e aplicações da Matemática.

A 3ª e 4ª aulas da sequência didática não foram possíveis de serem aplicadas pois, devido a pandemia deste ano de 2020, os alunos estavam afastados da escola e extremamente sobrecarregados com "novas" demandas. Por isso, estas duas etapas foram condensadas no segundo encontro.

Enfim, foram encontros de muito aprendizado e de muitas novidades que estimulou os alunos a ler mais sobre a criptografia e sobre a computação quântica.

# 7. CONCLUSÃO

O objetivo assumido foi o estudo da criptografia e de formas de fatoração que podem ser usadas para a quebra de codificações. Com isso, desejava-se responder ao questionamento sobre o quanto há de segurança nos sites, nas transações bancárias, nas redes sociais e na internet de forma geral. Além disso, objetivava-se analisar o conhecimento dos alunos no ensino regular dos temas estudados nesta tese e o interesse deles na Física Quântica e em aplicações da Matemática hodiernamente.

Primeiramente, esta análise apoiou-se num estudo teórico da história da criptografia mundial e seu desenvolvimento até a atualidade.

Após a análise da Teoria dos Números, foi feito um estudo aprofundado sobre os números primos pois estes são a base da Criptografia RSA e pelo fato de que criptografar as mensagens é necessário, no início, multiplicar dois números primos muito grandes e, a partir disto, com congruências, é possível codificar informações. Por esse motivo, este trabalho trouxe também o estudo de Congruências Lineares com o intuito de dar suporte ao entendimento do funcionamento do sistema RSA.

Em seguida, o sistema RSA foi apresentado ao leitor.

Com a pesquisa sobre as formas de fatoração para números grandes foi exposta a computação quântica e sua influência na decodificação.

Também foi apresentada uma sequência didática de quatro aulas para alunos do Ensino Fundamental para mostrar uma grande aplicação da Matemática na codificação e a Computação Quântica necessária na Fatoração de Shor. Os alunos gostaram bastante do assunto pois foi mostrada a Matemática, que até então era muito teórica pra eles, aplicada em um tema que envolve proteção de dados, internet e computação. Conclui-se que é muito interessante incluir o estudo de formas de fatoração diferentes, de assuntos atuais e Física Quântica na grade escolar

regular respeitando a idade do grupo de alunos, mas com a possibilidade de aprofundamento conforme o decorrer dos anos.

Enfim, com a pesquisa feita, constata-se que há segurança na Criptografia RSA mesmo sendo possível fatorar com técnicas já existentes e com isso descriptografar mensagens, pois o tempo necessário para isto é relativamente grande com os computadores modernos e o uso do computador quântico para agilizar o processo ainda não está em vigor. Enquanto os problemas enfrentados pela Computação Quântica não forem superados a Criptografia RSA está segura.

## REFERÊNCIAS BIBLIOGRÁFICAS

[1] COSTA, C. Introdução à criptografia. v.1. Rio de Janeiro: UFF/CEP – EB, 2010.

[2] MENEZES, L; CARVALHO, M..Criptografia na sala de aula. In: X Encontro Nacional de Educação Matemática, 2010, Salvador.

[3] PÓVOA, T; Estudo sobre os principais aspectos da criptografia simétrica e assimétrica ao longo da história. 2019. Dissertação (Mestrado Profissional em Matemática). Universidade de Brasília, Distrito Federal.

[4] JÚNIOR, J. L. P Silva; Criptografia RSA e algoritmo AKS. Universidade Federal de São João Del-Rei, Minas Gerais, 2015.

[5] HEFEZ, Abramo; Aritmética. Coleção Profmat. Rio de Janeiro: SBM, 2016.

[6] ALENCAR FILHO, Edgard de. Teoria elementar dos números. 2ª edição. São Paulo. Nobel, 1985.

[7] MILIES, Francisco César Polcino; COELHO, Sônia Pitta; Números: uma introdução à Matemática. 3ª edição. São Paulo. Editora da Universidade de São Paulo, 2001.

[8] BONFIM, Daniele Helena; Criptografia RSA. USP São Carlos, São Paulo, 2017.

[9] SALA de estudo: Fatorando de um jeito diferente (nível avançado). Clubes de matemática da Obmep, 2020. Disponível em: <http://clubes.obmep.org.br/blog/fatorando-de-um-jeito-diferente/>. Acesso em: 07 de setembro de 2020.

[10] CAVALCANTE, André L. B.. Teoria dos Números e criptografia. Revista virtual, 2005. Disponível em: <

https://upis.br/biblioteca/pdf/revistas/revista_informatica/Cavalcante_teoria_numeros_criptografia_2005_UPIS.pdf>. Acesso em: 13 de setembro de 2020.

[11] WATANABE, Mário Sansuke Maranhão; O algoritmo polinomial de Shor para fatoração em um computador quântico. Universidade Federal de Pernambuco, Recife, 2003.

[12] UNIVESP, notícias; Pesquisador explica como a matemática pode ser atraente para os estudantes. Disponível em:

<https://univesp.br/noticias/pesquisador-explica-como-a-matematica-pode-ser-atraente-para-os-estudantes#.X9Yby2hKjIU>. Acesso em 13 de dezembro de 2020.