UNIVERSIDADE FEDERAL DE ALAGOAS -UFAL
CAMPUS ARAPIRACA
MATEMÁTICA-LICENCIATURA

ELOÁ ROSE MARIA DE OLIVEIRA

TEORIA DOS NÚMEROS: A TECNOLOGIA MATEMÁTICA DO ALGORITMO RSA

ARAPIRACA
2023

Eloá Rose Maria de Oliveira

Teoria dos números: a tecnologia matemática do algoritmo RSA

Trabalho de Conclusão de Curso (TCC), apresentação ao corpo docente do curso de Matemática Licenciatura da Universidade Federal de Alagoas - UFAL, Campus Arapiraca, como requisito parcial para a obtenção do grau de Licenciatura em Matemática.

Orientador: Prof. Dr. Moreno Pereira Bonutti

Arapiraca

2023

Universidade Federal de Alagoas – UFAL
Campus Arapiraca
Biblioteca Setorial *Campus* Arapiraca - BSCA

O48t Oliveira, Eloá Rose Maria de
Teoria dos números [recurso eletrônico]: a tecnologia matemática do algoritmo RSA / Eloá Rose Maria de Oliveira. – Arapiraca, 2023.
53 f.: il.

Orientador: Prof. Dr. Moreno Pereira Bonutti.
Trabalho de Conclusão de Curso (Licenciatura em Matemática) - Universidade Federal de Alagoas, *Campus* Arapiraca, Arapiraca, 2023.
Disponível em: Universidade Digital (UD) / RD- BSCA– UFAL (*Campus* Arapiraca).
Referências: f. 53 -54.

1. Matemática. 2. Teoria dos números. 3. Criptografia RSA. 4. Sistema criptográfico. I. Bomutti, Moreno Pereira. II. Título.

CDU 51

Bibliotecário responsável: Nestor Antonio Alves Junior
CRB-4 / 1557

Eloá Rose Maria de Oliveira

Teoria dos números: a tecnologia matemática do algoritmo RSA

Trabalho de Conclusão de Curso (TCC), apresentação ao corpo docente do curso de Matemática Licenciatura da Universidade Federal de Alagoas - UFAL, Campus Arapiraca, como requisito parcial para a obtenção do grau de Licenciatura em Matemática.

Data de aprovação: 24/04/2023.

Banca Examinadora

gov.br Documento assinado digitalmente
MORENO PEREIRA BONUTTI
Data: 19/10/2023 09:17:34-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Moreno Pereira Bonutti
Universidade Federal de Alagoas - UFAL
Campus de Arapiraca
(Orientador)

gov.br Documento assinado digitalmente
JOSE ARNALDO DOS SANTOS
Data: 19/10/2023 13:43:37-0300
Verifique em https://validar.iti.gov.br

Prof. Me. José Arnaldo dos Santos
Universidade Federal de Alagoas - UFAL
Campus de Arapiraca
(Examinador)

gov.br Documento assinado digitalmente
WAGNER OLIVEIRA COSTA FILHO
Data: 19/10/2023 14:51:26-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Wagner Oliveira Costa Filho (Avaliador)
Universidade Federal de Alagoas - UFAL
Campus de Arapiraca
(Examinador)

Dedico este trabalho ao meu esposo Victor Hugo, pelo incentivo e pela compreensão nas minhas horas de ausência; por ter sido meu sustento em momentos difíceis e me deu condições para continuar a luta e chegar até aqui. E, em memória de minha mãe, também protagonista dessa jornada.

AGRADECIMENTOS

Primeiramente agradeço as boas energias que regem o universo por proporcionar essa oportunidade de ampliar minhas chances na competição da vida, por me dar forças e conquistar mais uma vitória.

Agradeço ao meu orientador Moreno Bonutti, pelo suporte no pouco tempo que lhe coube, pelas correções e incentivo, além de toda a paciência que teve em meio as minhas indecisões.

Aos amigos que fiz dentro do curso e que com carinho os trouxe para fazer parte da minha vida fora do campus, Adriano Ribeiro, Claudia Maria e Gabriela Melo, juntos compartilhamos momentos bons e divertidos, assim como, os momentos de desespero nos estudo. Agradeço a eles pelo apoio e incentivo.

Sou grata a todos que de alguma modo contribuíram na minha trajetória acadêmica.

O impulso para descobrir segredos está profundamente enraizado na natureza humana. Mesmo a mente menos curiosa é estimulada pela perspectiva de compartilhar o conhecimento oculto aos outros.

(John Chadwick).

RESUMO

O presente trabalho busca explorar as técnicas matemáticas que constituem o algoritmo RSA, em específico ao campo da teoria dos números. Portanto, o seu objetivo geral, visa apresentar a criptografia RSA como método prático, sistema ao qual está centrado nos conceitos da Teoria dos Números. Trata-se de uma pesquisa de cunho bibliográfica e documental, que busca explorar os elementos da Teoria dos Números empregados no algoritmo RSA, também, compreender a sintaxe de codificação e decodificação das mensagens, assim como, analisar a confiabilidade do algoritmo. Para contextualizar, será apresentada a evolução criptográfica e curiosidades sobre os matemáticos relacionados. O exemplo prático escolhido busca dar sentido prático aos conceitos, tidos como sem nenhuma praticidade real, e para desconstruir esse juízo, afirma-se que, o advento da RSA, acelerou relativamente a corrida matemática, em busca de um dos prêmios milionários, de grande interesse das empresas da internet. Uma vez que, os números inteiros em geral e, os primos, um dos assuntos que gera prêmio, são alguns dos elementos abstratos da matemática que fundamentam esse algoritmo. E, ao finalizar a pesquisa, ficará entendido como esses tópicos contribuem para a criptografia garantir a permanência de sigilo dos dados.

Palavras-chave: matemática; teoria dos números; criptografia RSA; códigos.

ABSTRACT

The present work seeks to explore the mathematical techniques that constitute the RSA algorithm, specifically in the field of number theory. Therefore, its general objective is to present RSA cryptography as a practical method, a system which is centered on the concepts of Number Theory. This is a bibliographical and documental research, which seeks to explore the elements of Number Theory employed in the RSA algorithm, as well, understand the encoding and decoding syntax of messages, as well as analyze the algorithm reliability. To contextualize, the cryptographic evolution will be presented and fun facts about related mathematicians. The practical example chosen seeks to give practical sense to the concepts, considered without any real practicality, and to deconstruct this judgment, it is stated that the advent of RSA relatively accelerated the mathematical race, in search for one of the millionaire prizes, of great interest to internet companies. Once that inters in general and primes, one of the subjects of mathematics that underlie this algorithm. And, at the end of research, it will be understood how these topics contribute to cryptography guaranteeing the maintenance of data secrecy.

Keywords: mathematics; number theory; RSA encryption; codes.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A matemática se faz presente em diversos cenários, visto que representa uma ciência que abrange variadas aplicações em inúmeros ramos. Dessa forma, a Matemática conta com um forte caráter interdisciplinar e integrador, ou seja, o conteúdo matemático evolui de forma igual no cenário de outras ciências, e isso condiz também com o momento de crescimento cibernético, onde a evolução humana se configura a tecnologia digital, tendo umas das principais atividades transações comerciais e navegação seguras. Contudo, mesmo tendo ciência de que a matemática está conectada a basicamente tudo o que nos cerca, ainda assim, há uma dificuldade em grande escala em assimilar algumas áreas dessa ciência com o nosso cotidiano, principalmente quando refere-se a conceitos puramente abstratos. Segundo Resende e Machado (2012, p. 263) "A teoria dos Números é um importante campo científico de conhecimento e de pesquisa dentro da Matemática". Mediante a essa afirmação, vale ocasionar uma significação dos conteúdos, ou seja, dá um sentido ao seu uso de forma prática.

Neste sentido, ao depararmos com o advento da internet e a frequência de seu uso como forma de trocar informações e como meio de comunicação, notou-se como essas relações estruturam a sociedade. Considerando que, o método prático escolhido, deve-se ao fato de que essa criptografia está estabelecida como um estudo de técnicas matemáticas, além de que, apesar de modesta, ela assume extrema relevância em nossas vidas.

Devido a praticidade e a agilidade no tráfego de dados que a internet assegura, as relações sociais adotaram as tecnologias de redes como o principal meio de transmissão, logo, é preciso a garantia de uma boa tecnologia digital que assegure a confidencialidade dos dados em questão, de modo que, potencialize a cibernética com técnicas cada vez mais avançadas. A antiga estratégia de codificar mensagens, iniciada séculos atrás para fins de segredos de estado, hoje se torna banal, e unificada com a era digital, adaptada às novas tendências para atender a atual demanda, tendo como exemplo, um dos métodos mais utilizados para essa finalidade é o RSA. A base que constitui esse sistema criptográfico é a matemática discreta seus conceitos reflexivos tornaram um casamento perfeito, visto que, no campo da teoria dos números existem complexidades que a favorece como aliada ideal para gerar enigmas, nesse sentido, o sistema criptográfico RSA se estabeleceu, por meio da teoria dos números, criando um emaranhado de problemas, que resultou em um processo difícil de solucionar; é conhecido por ser um método que exprime grande utilidade pela garantia de segurança. Nessa perspectiva, como a Teoria dos Números interage com a realidade por meio da criptografia RSA?.

Sobre a criptografia Diffie e Hellman (1976, p. 644) destaca: “A criptografia é o estudo de sistemas matemáticos”. Seguindo este raciocínio, neste trabalho podemos associar a abstração matemática à aplicação comum a nossa realidade. De modo que, o presente estudo tem como objetivo geral apresentar a criptografia RSA como método prático que está fundamentado na Teoria dos Números. Como objetivos específicos destacam-se explorar como estão empregados os principais conceitos da teoria dos números, os quais, estabelece o algoritmo RSA; assim como, compreender o processo de codificação e decodificação das mensagens, e ainda, analisar a segurança do algoritmo que utiliza elementos da teoria dos números.

A ideia desse sistema de segurança foi oriunda dos matemáticos Ron Rivest, integrante do Departamento de Ciências da Computação do MIT (Instituto de Tecnologia de Massachusetts) pioneiro do invento, Adi Shamir, Leonard Adleman, licenciado no ensino de biologia molecular, e ambos, doutores em Ciências da Computação. Rivest em suas pesquisas descobriu que poderia unir problemas matemáticos com um grau de complexidade para serem solucionados, e juntos descobriram o problema da fatoração, que dependendo da quantidade de algarismos é impossível de calcular, inclusive por computadores, ainda, Du Sautoy em seu livro destaca.

> Ele delineava uma visão ampla do que era a criptografia e do que se poderia tornar. [...] Era um problema com claras implicações práticas no mundo real, mas que também tinha ligações diretas com as preocupações teóricas que tanto ocupavam o pensamento de Rivest. [...] Enquanto exploravam os diversos problemas matemáticos "difíceis", seus sistemas criptográficos embrionários começaram a usar mais ideais da teoria dos números. […] Eles vinham pensando há algum tempo no difícil problema de fatorar número. Não haviam boas propostas de programas que conseguissem decompor números em seus blocos de construção primos. (DU SAUTOY, 2007, p. 694-698).

Parte-se da hipótese de que esse sistema criptográfico computacional garante a segurança eletrônica e está estruturado na área da Teoria dos Números. Esse sistema aborda números inteiros em geral em destaque os números primos, divisibilidade, máximo divisor comum, algoritmo de Euclides, congruência modular, inclusive a linear e inverso multiplicativo, assim como, função de Euler. Esse algoritmo está diretamente ligado a problemas matemáticos de cálculo muito difícil de ser resolvido até mesmo por computador, como o problema da fatoração interna, problema do algoritmo discreto. Todas as tentativas feitas com o intuito de resolver seu problema, foram fracassadas.

A presente pesquisa, vai além de uma mera curiosidade ou demonstração, uma vez que, o assunto é de grande interesse de entidades mundiais importantes, pois ela é responsável

pelo comércio eletrônico, e seu segredo está constantemente ameaçado, esse sistema ainda é um dos mais usados até hoje, para criptografar e para assinatura digital, a descoberta do padrão dos números primos, causaria um colapso globalizado,

> Contudo, à medida que desmistificamos os primos, os códigos se tornam mais inseguros. Esses números são as chaves dos cofres onde estão guardados os segredos eletrônicos do mundo. É por isso que empresas como AT&T e Hewlett-Packard financiam pesquisas para entender as sutilezas dos números primos e da hipótese de Riemann. O conhecimento gerado por essas investigações poderá ajudar a decifrar os códigos de números primos, tornando-os inseguros [...]. Essa razão pela qual teoria dos números e o comércio se tornaram aliados, algo tão inimaginável no passado. (DU SAUTOY, 2007, p. 48-49).

Como visto, o tema proposto tem uma relevância que pode causar grandes impactos em nossa realidade, nessa visão, pode despertar interesses fora das salas de aula, o que contribui muito para a compreensão. Para tanto, fez-se necessário buscar mais conhecimentos sobre o tema proposto, com a finalidade de sair da abstração matemática para um sentido prático, e, portanto, o presente trabalho discute a criptografia RSA como uma aplicação prática da Teoria dos Números.

Com caráter bibliográfico e documental, o trabalho baseia-se em diversos autores como Du Sautoy, Diffie e Hellman, Milies e Coelho, Santos, que tratam o assunto na visão matemática no âmbito da Teoria dos Números, juntamente com o olhar das ciências da computação voltados para criptografia.

Para a confecção deste trabalho foram utilizados dados secundários, como material de apoio livros eletrônicos em pdf, trabalhos de monografias, artigos, trabalhos acadêmicos de conclusão de curso, sites e revistas eletrônicas, vídeos no youtube, pesquisados em plataformas como google e no acadêmico, IEEE Xplore, usando palavras chaves específicas, tais são, criptografia, criptografia RSA, teoria dos números, teoria dos números e criptografia RSA. Trata-se de uma revisão de literatura de pesquisa básica e estratégica, por meio descritivo quali-quantitativo, que, consequentemente, busca realizar uma revisão bibliográfica no sentido de situar o leitor nos conteúdos da Matemática Discreta e nos princípios da criptografia, como, levar a compreensão de como se dá o desenvolvimento para codificar e decodificar das mensagens, apresentando o passo a passo para a construção do algoritmo, mostrando também os motivos aos quais garantem seu funcionamento e a segurança, logo, a pesquisa torna-se de caráter dedutivo. Para melhor contextualização, será abordada uma exposição de fatos históricos importantes acerca da evolução da criptografia e dos matemáticos envolvidos e assuntos relacionados.

O presente estudo justifica-se pela importância do tema, constatou-se a dificuldade em relacionar o quanto a teoria dos números têm influência na nossa realidade. É válido afirmar também que, dentro das paredes das salas de aulas acaba despertando desmotivação dos alunos nessa área, devido às complexidades e abstrações que geram dificuldades de compreensão, comprometendo até mesmo a formação de futuros matemáticos ou de novas descobertas por meio dessa área de atuação. Assim, pode-se também pensar na criptografia RSA como proposta de um ensino didático prático para expor dentro da sala de aula, no ensino da Teoria dos Números, uma vez que, essa criptografia faz uso de muitos de seus conceitos, de forma, a dar destaque a importância desses conhecimentos fora dos muros da instituição de ensino, pois a matemática está atrelada ao nosso dia-a-dia, está presente em todas as ciências. E nessa inclusão, é sabido que, a era digital deu um salto relevante para a evolução da modernidade, mudando inclusive o aspecto da comunicação e do comércio que agora eletrônico, ou seja, os sistemas de computadores cada vez mais assumem um papel central dentro da sociedade, possivelmente a mais ascendente no mercado de trabalho, só é possível devido a matemática nela estabelecida.

No capítulo 2 será apresentada as técnicas matemáticas usadas na criptografia RSA. Tópicos da Teoria dos Números, como centro de nosso estudo, será exposto como uma revisão objetiva, para fins de inteirar o leitor aos conhecimentos básicos necessários à construção do algoritmo, e também para o mesmo fazer a conexão desses conceitos com sua aplicação prática.

Antes de irmos à prática, é importante entender conceitos básicos sobre alguns sistemas criptográficos, assim como, conhecer a evolução histórica da criptografia e de como se deu essa necessidade de codificar mensagens. Essas informações ficam por conta do capítulo 3.

E por fim, o capítulo 4, centro do desenvolvimento deste trabalho, o qual apresenta a aplicação de todos os conceitos matemáticos vistos no capítulo 2 por meio do sistema RSA.

2 REVISÃO À TEORIA DOS NÚMEROS

A Teoria dos Números é o campo dedicado a explicar os princípios matemáticos, ou seja, as origens das ideias matemáticas, como o próprio nome já sugere, embora sendo apenas conceitos reflexivos, é possível aplicá-la na prática, esse campo, relaciona-se em diversas ciências. A teoria dos números tem uma proximidade muito grande com as ciências eletrônicas e da computação, nessa perspectiva, veremos então, a aplicação dos conceitos preliminares para a construção do algoritmo RSA, os tópicos apresentados neste capítulo serão expostos de modo que, o leitor tenha um conhecimento matemático prévio de como está organizada a criptografia RSA. Inicialmente iremos apresentar os elementos matemáticos envolvidos, para por fim, apresentar a aplicação na prática.

2.1 DIVISIBILIDADE

Considerando que o leitor já tenha conhecimento nos conjuntos dos Números Inteiros, $\mathbb{Z}$, e suas propriedades, consideravelmente os positivos, assim como, nos conjuntos dos Naturais, $\mathbb{N}$, para o desenvolvimento deste trabalho, nosso estudo neste capítulo será iniciado com noções de divisibilidade, e algumas de suas propriedades, uma vez que, o sistema criptográfico apresenta uma grande relação com esta.

Definição 2.1.1 Dados dois números inteiros a e b, pertencentes ao conjuntos dos números inteiros, com $a \neq 0$, dizemos que b é múltiplo de a, ainda que, a divide ou é um divisor de b, denotado por a|b, se existir um número c tal que b = ac.

Exemplo 2.1.1 2|2022, pois 2022 = 2 . 1011.

Exemplo 2.1.2 -7|98, pois 98 = (-7) . (-14).

Exemplo 2.1.3 O conjunto S = {..., -12, -8, -4, 0, 4, 8, 12, 16, 20, ...} é a coleção de todos os múltiplos $\mathbb{Z}$ de 4. Podemos descrever S da forma 4s: S = {4s; s $\in \mathbb{Z}$}.

Lema 2.1.1 Se a, b, c, d pertencem ao conjunto $\mathbb{Z}$, valem as seguintes propriedades.

i) Se a|b e b|c, então a|c;

ii) Se a|b e a|c, para todo x e y $\in \mathbb{Z}$, então a|(bx + cy);

iii) Se a|b e c|d, então ac|bd;

iv) Se a|b então b = 0 ou |a| $\leq$ |b|;

Demonstração: (i) Como a|b, existe um x $\in \mathbb{Z}$ tal que b = ax. Como b|c, Existe um y tal que c = by. Então c = (ax) y, ou seja, c = a (xy). Logo a|c.

(ii) Se a|b e a|c, existem m, n $\in \mathbb{Z}$ tais que b = am e c = an. Multiplicando a primeira equação por x e a segunda por y, obtém-se bx = xam e cy = yan. Agora somando bx + cy, tem-se

$$bx + cy = xam + yan = a(xm + yn).$$

E concluímos que, a|(bx + cy).

(iii) Mostremos que se a|b e c|d, então ac|bd. Como a|b e c|d, da definição, existem x e y $\in \mathbb{Z}$ tais que, b = ax e d = cy. Fazendo o produto de b por d, conclui-se que

$$bd = (ax)(cy) = (xy)ac,$$

ou seja, ac|bd.

(iv) Suponha a|b e b $\neq$ 0. Assim, b = an com n $\neq$ 0, logo |n| $\geq$ 1 e |b| = |a| |n| $\geq$ |a|.

□

Haverá situações em que a divisão de b por a deixará um resto, para esses casos diz-se que a não divide b, ou que b não é múltiplo de a, denotamos por $a \nmid$ b.

Exemplo 2.1.4 Observe que 5 $\nmid$ 21, pois a divisão de 21 por 5 deixa resto 1 $\neq$ 0

Euclides foi mais longe, e determinou a existência e unicidade para resolver alguns problemas de divisibilidade, assim a divisão de números inteiros segundo o matemático, fica definido.

Teorema 2.1.1 (Divisão Euclidiana) Dados dois números a e b, com $a \neq 0$, então existem únicos q e r inteiros tais que, b = aq + r, com 0 $\leq$ r < |a|. Chamamos q de quociente e r de resto.

Demonstração: Considere o seguinte conjunto,

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

Provando a existência: Valendo a Propriedade Arquimediana, que nos diz, que existe um número n $\in \mathbb{Z}$ tal que -nb > - a, então, a - nb > 0, isso implica que o conjunto S $\neq \emptyset$. Seguindo, pelo Princípio da Boa Ordem, todo subconjunto não vazio composto por números naturais existe um menor elemento pertencente a ele, que de fato, o conjunto S possui um menor elemento r. Por suposição r = a - bq. Portanto, o valor de r $\geq$ 0. Agora, resta provar que r < |b|. Nesse caso, provaremos por absurdo, r $\geq$ |b|. Logo, admitimos a existência de um s $\in \mathbb{N}$ {0}/ r = |b| + s, e 0 $\leq$ s < r. Porém, se notarmos bem, essa afirmação contradiz a anterior, quando diz que r é o menor elemento dentro de S, pois s = a - (q $\pm$ 1)b $\in$ S, e s < r.

Para provar a unicidade, suponha a = bq + r = bq' + r', onde q, q', r, r' $\in \mathbb{Z}$, 0 $\leq$ r < |b|, com 0 $\leq$ r' < |b|. De modo que, -|b| < r $\leq$ r' - r $\leq$ r' < |b|. Logo, para os módulos |r' - r| < |b|, e, então b(q- q') = r' - r. Observe que, |b| |q- q'| = |r' - r| < |b|, isso só será possível caso q = q', então r = r'.

□

Assim, a divisão de b por a significa encontrar o quociente e resto que satisfaça de acordo com o teorema. Contudo, casos como, 23 = 7. 2 + 9, de acordo com o que foi apontado na proposição, o resto não pode ser maior que o divisor, portanto, o quociente 2 e resto 9 não são considerados resultado da divisão de 23 por 7. Usando a mesma analogia, sendo 3 o quociente e 2 o resto da divisão de 23 por 7, satisfaz o enunciado, pois, 23 = 7. 3 + 2, pois o resto é menor que o divisor.

2.2 MÁXIMO DIVISOR COMUM

O Máximo Divisor Comum (mdc) de um número tem como princípio a divisibilidade, neste a e b, com $a \neq 0$ ou b $\neq$ 0, e ambos pertencem ao conjunto $\mathbb{Z}$, cada um deles pode ser associado à um conjunto finito de divisores e que a interseção entre esses dois conjuntos é, não vazio, pois pelo menos o número 1 é comum entre eles. Caracteriza-se o máximo divisor comum da seguinte forma.

Definição 2.2.1 Dados dois números a e b, chamamos de máximo divisor comum entre a e b um determinado elemento d $\in \mathbb{Z}$, tal que, d divide a e b simultaneamente e é o maior inteiro que satisfaz essa condição, em outras palavras:

i) d|a e d|b, d é divisor comum de a e b;

ii) Se c|a e c|b, então c|d.

Notação: mdc (a, b) = d.

Exemplo 2.2.1 mdc (18, 30), divisores de (18) : 1, 2, 3, 6, 9, 18. Agora os divisores de (30) : 1, 2, 3, 5, 6, 10, 15, 30. Note que, temos um conjunto de intersecção de divisores D = {1, 2, 3, 6}, observe que o maior elemento entre eles é o número 6, logo é o mdc (18, 30) = 6.

Conhecemos o método de decomposição por meio de fatores primos do tipo,

$$a = p_1^{a1}, p_2^{a2}, ..., p_n^{an} \text{ e } b = p_1^{b1}, p_2^{b2}, ..., p_n^{bn},$$

como forma para determinar um mdc entre dois ou mais número, porém, para números imensos, não seria prático e nada fácil para realizar a decomposição. A seguir, demonstraremos um método que torna viável essa decomposição, denominada de Algoritmo de Euclides ou método das divisões sucessivas, essa permite a utilização de uma série finita de divisões.

Em resumo, podemos afirmar que se existe um determinado número que é o máximo divisor comum, aqui, nomeado de d, e esse satisfaz a divisão de a e b, se e somente se, d|a e d|a-b, para qualquer divisor comum entre eles. Tem-se que, o mdc (a,b) = mdc (a,a-b); em outra palavras, d é divisível por todo divisor comum de a e b, o que implica que c $\leq$ d.

2.3 ALGORITMO DE EUCLIDES

Quando falamos em Matemática, dificilmente iremos abordar algum assunto matemático que não esteja relacionado a Euclides, pois suas contribuições foram muitas e constituem na estruturação de muitas outras teorias. Escritor grego, mestre e matemático da escola platônica, Euclides conhecido como Pai da Geometria, viveu em Alexandria, no Egito, nascido em Atenas em meados de 330 a.C. lecionou no Egito durante o reino Ptolomeu.

Seu principal trabalho, o livro Os Elementos, composto por 13 volumes, reuniu todo seu conhecimento em matemática, este livro é dedicado principalmente a geometria do plano e a aritmética, com triângulos, linhas paralelas e círculos, ele também fez provas de teoremas, como o de Pitágoras, além de introduzir as noções de PGCD (maior divisor comum) e repetidas subtrações sucessivas, chamadas divisões euclidianas.

A figura 1 apresenta a imagem de um dos maiores matemáticos já conhecidos, Euclides de Alexandria, tido como pai da Geometria.

Figura 1- Euclides de Alexandria

Fonte: Disponível em: https://www.wikiwand.com/pt/Geometria_euclidiana. Acesso em: 25 jul. 2022.

O Algoritmo de Euclides é um elemento chave para nosso trabalho, pois ele é usado para descobrir números que seja satisfatório em múltiplas congruências ou inverso multiplicativo de um número finito.

Observações feitas, o Algoritmo de Euclides tem o mdc como base, sem que precise nenhum tipo de fatoração, tem como princípio de que o mdc não muda se o menor número for subtraído ao maior, como veremos a seguir.

Lema 2.3.1 (Algoritmo de Euclides) Sejam a, b inteiros, com b $\neq$ 0; e sejam, q e r quociente e o resto da divisão de a por b, respectivamente. Então, D(a, b) = D(b, r), onde D(a, b) é o seguinte conjunto:

$$D(a, b) = \{d \in \mathbb{Z} / d \text{ é divisor de a e b}\},$$

temos também que, mdc (a, b) = mdc (b, r).

Demonstração: Podemos escrever a = bq + r. Seja x $\in$ D(a, b). Então, x|a e x|b, mas r = a -bq e x divide cada um dos somados, logo x|r, Mostramos, assim, que D(a,b) $\subset$ D(b, r). A inclusão contrária segue de forma análoga, donde resulta a igualdade dos conjuntos.

Desse modo, fica provado. Se os conjuntos são iguais, seus máximos também coincidem, isto é, mdc (a, b) = mdc (b, r).

□

Verifique que o teorema acima consiste em determinar que o problema do mdc (a, b) se reduz a achar o mdc (b, r). Vejamos alguns exemplos abaixo.

Exemplo 2.3.1 Por divisões sucessivas:

$$
\begin{aligned}
a &= bq_1 + r, & 0 < r_1 < q_1 \\
b &= r_1q_2 + r_2, & 0 < r_2 < r_1 \\
r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2 \\
&\dots & \dots \\
r_{n-2} &= r_{n-1}\, q_n + r_n, & 0 \leq r_n < r_{n-1}. \\
r_{n-1} &= r_nq_{n-1} + 0
\end{aligned}
$$

Com isso, depois de aplicar finitas vezes o algoritmos da divisão, obtemos uma sequência numérica decrescente, formadas por restos $r_1 > r_2 > r_3 > r_4 > \dots > r_{n-2} > r_{n-1} > r_n > 0$, usando o teorema acima repetidas vezes em algum momento encontramos o resto 0. Assim o mdc (a, b) = r_n, que é o último resto que antecede o 0. E essa sequência de restos como são de números positivos os valores são maiores que 0, e por ser decrescente isso nos garante que em algum momento iremos obter um resto igual a 0.

Exemplo 2.3.2 Vejamos agora um exemplo prático, mdc (414, 662), segue;

$$
\begin{aligned}
662 &= 1 \,.\, 414 + 248 \\
414 &= 1 \,.\, 248 + 166 \\
248 &= 1 \,.\, 166 + 82 \\
166 &= 2 \,.\, 82 + 2 \\
82 &= 2 \,.\, 41 + 0
\end{aligned}
$$

Assim, o mdc (414, 662) = mdc (414, 248) = mdc (248, 166) = mdc (166, 82) = mdc (82, 2) = mdc (41, 0). De acordo com o Teorema 2.3.1, o resto que antecede o número 0 é o valor 2, logo, mdc (414, 662) = 2.

Exemplo 2.3.3 Respectivamente, podemos realizar o Algoritmo de Euclides usando o diagrama. Usaremos os mesmos valores do exemplo anterior; segue mdc (414, 662).

	1	1	1	2	41
662	414	248	166	82	2
	248	166	82	2	0

É válido fazer a observação de que d pode ser escrito como uma combinação linear de a e b, pois d = mdc (a, b), ou seja, nos fornece um meio prático de escrever o mdc entre dois números como a soma de dois múltiplos dos números a, b.

Como mencionado anteriormente, os divisores comuns entre dois ou mais números podendo ser escrito como um conjunto que nunca será vazio, pois o número 1 é divisor de qualquer número pertencente ao conjunto dos inteiros. Dito isso, haverá casos em que o mdc entre a e b será igual a 1, quando isso acontece dizemos que a e b são primos entre si, e para isso, a e b não necessariamente precisam ser números primos. Por exemplo, mdc (9, 14) = 1.

Definição 2.3.2 Dois números inteiros a e b são primos entre si, se o mdc (a,b) = 1

Proposição 2.3.2 Se n e p são números inteiros, com p primo e p∤n, então p e n são primos entre si e mdc (n, p) = 1.

Demonstração: Consideremos d = mdc (n, p), com d $\in \mathbb{Z}$, então d|n e d|p. Nessa relação temos então d|p, assim d = 1 ou d = p. Observe que, isso não é possível para segunda igualdade, uma vez que, p ∤ n, então d ≠ p. portanto d = 1.

□

A definição 2.3.2 é muito relevante para a criptografia RSA, assim como os números primos, que compõem a base inicial para construção do algoritmo, por isso, é imprescindível conhecermos suas características.

2.4 NÚMEROS PRIMOS

Existem números indivisíveis, e os gregos antigos foram os primeiros a entender a importância desses números, denominados de números primos, o matemático Euclide foi o primeiro a provar que os números primos são infinitos, porém ele não conseguiu construir nenhuma fórmula que previsse quais eram esses números, não imaginava ele que, devido a essa ausência, grandes avanços se tornaram possíveis impactando o que chamamos de civilização moderna. Os número primos têm um papel importante nos sistemas computacionais, iremos compreender uma de suas importantes atribuições durante o desenvolvimento deste trabalho.

Definição 2.4.1 Um número inteiro n que possui somente dois divisores positivos n e 1 é chamado número primo. Se n > 1 não é primo, dizemos que n é composto.

Teorema 2.4.1. Dados dois números primos p, q e um outro número inteiro a qualquer. As seguintes propriedades são válidas.

i) Se p|q, então p = q;
ii) Se p $\nmid a$, então mdc (p, a) = 1

Demonstração: (i) Como p|q, sendo que o número q é um primo, temos que por definição, que p = 1 ou p = q. Novamente por definição, sendo p primo, segue-se que p > 1, o que acarreta p = q.

(ii) Se p $\nmid a$, então mdc (p, a) = 1, já foi provado na Proposição 2.3.2.

□

A busca por um padrão que possa dar todos os números primos é um desafio que perpetua até hoje em dia. Durante séculos matemáticos estudam meios, e buscam provar teorias deixadas por grandes mestres do passado, a fim de desvendar o mistério da formação desses números. O maior número primo já encontrado atualmente, só foi possível com a ajuda de computadores, recorrendo a fórmula de Mersenne 2^n- 1, Marin Mersenne foi um padre francês que viveu nos anos de 1588 até o ano de 1648. Com quase 25 mil algarismos, segundo a um projeto de pesquisa global chamado Great Internet Mersenne Prime Search (GIMPS),

que se dedica em descobrir esses primos, o maior número descoberto é $2^{82.589.933}$- 1. A criptografia RSA se beneficia pelo motivo de não haver uma padrão que defina como são gerados os números primos, e por isso a infinidade desses números contribui para a segurança do sistema. Para Du Sautoy sobre esse dilema, diz que:

> felizmente, a natureza foi caridosa com o mundo do comércio eletrônico. O teorema dos números primos de Gauss determina que a quantidade de primos com 60 algarismos é de aproximadamente 10^{60} dividido pelo logaritmo de 10^{60}. Ou seja, existem suficientes primos com 60 algarismos para que cada átomo da Terra tenha seu próprio par de primos. (DU SAUTOY, 2007, p. 261).

Portanto, se um número natural $n > 1$ é composto, existirá um divisor natural n_1 de n tal que $1 < n_1 < n$. Logo, também existirá um número $n_2 \in \mathbb{N}$ tal que, $n = n_1n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$.

Exemplo 2.4.1 Temos, 2, 3, 5, 7, 11 e 13 são números primos, enquanto que 4, 6, 8, 9, 10 e 12 são números compostos.

Com esse enunciado, podemos generalizar os números primos mostrando que qualquer número que pertence ao conjunto dos inteiros, e que seja diferente de 0 e 1, pode ser escrito como sendo um produto de números primos por meio de decomposição e de forma singular, a menos da ordem dos fatores, esse processo foi denominado como Teorema Fundamental da Aritmética. Vejamos em seguida com demonstração.

Teorema 2.4.2 (Teorema Fundamental da Aritmética) Todo número inteiro $n \geq 2$ e que pertence aos naturais, pode ser escrito de modo único, como um produto de números primos, de forma que $n = p_1 ... p_k$, onde $k \geq 1$ é um natural e $p_1 ... p_k$ são primos.

Demonstração: Existência: Sendo n um número primo, não teremos o que demonstrar. Consideremos então, n um número composto, nesse caso, segundo o teorema 2.4.2, nos permite dizer que n tem outros divisores além do 1 e o próprio n, isso implica que, existe um p_1, com $p_1 > 1$ sendo ele primo e o menor positivo diferente de 1 dos divisores de n. Se caso p_1 não for primo, então ele é composto, sendo ele composto, ele poderia ser escrito como produto de pelo menos mais outros dois números, de modo que, haveria um p, tal que, $1 < p < p_1$, ou seja, p seria um divisor de p_1, e assim, p também dividiria n, isso contradiz a

minimalidade de p_1, uma vez, haveria um outro número menor que p_1 e que divide p_1.Como isso não é verdade, temos de fato que, n é um número primo e pode ser escrito $n = p_1 n_1$.

Se n_1 for primo, então a fatoração está concluída; mas tenhamos n_1 como um número composto, logo, existe p_2 o menor divisor de n_1 que é maior que 1. Sendo p_2 o menor dos divisores de n_1. Note que p_2 é primo, e portanto, n pode ser escrito como $n = p_1 p_2 n_2$, pelos mesmos motivos de p_1. O processo continua se repetindo até que encontre um n_r que seja primo.

A continuidade desse método, gera uma sequência de termos decrescente de números inteiros positivos maiores que 1, como, $n_1 > n_2 > n_3 > \ldots > n_r$, observe que,

$$n_1 = p_2 n_2 \text{ e } n_2 = \frac{n_1}{p_2},$$

e assim sucessivamente, sendo um processo finito.

Os primos da sequência $p_1, p_2, p_3, p_4, \ldots, p_k$ não são, necessariamente, distintos, dito isso, p_1 pode ser o próprio p_2, por exemplo, para sanar essa possibilidade, coloca-se potências. Dito isso, colocando os fatores comuns de n será, $n = p_1^{\alpha 1} p_2^{\alpha 2} p_3^{\alpha 3} p_4^{\alpha 4} \ldots p_m^{\alpha m}$.

Unicidade: Mostraremos por meio da indução forte em n. Se n = 2, então, não há nada a ser feito, pois 2 é primo. Desse modo, supondo que a é única para todo k tal que $2 < k < n$. Para que nossa prova não acabe por aqui, n não pode ser primo; logo, n é um número composto e que tem duas fatorações em números primos. Sejam elas, $n = p_1 p_2 p_3 \ldots p_r$ e, também $n = q_1 q_2 q_3 \ldots q_s$.

Assim, temos que p_1 divide $q_1 q_2 q_3 \ldots q_s$, sendo verdade, é sabido que, um número primo que divide um certo produto, ele também divide um de seus fatores. Nesse caso, temos um número primo dividindo outro primo, e para isso acontecer, a única possibilidade é se eles forem iguais. Portanto, como p_1 e q_1 são primos, segue que são iguais.

Seguindo o raciocínio, substituindo q_1 por p_1 por serem iguais, temos, $n = p_1 p_2 \ldots p_r$ e, $n = p_1 q_2 q_3 \ldots q_s$, são iguais. Como $1 < \frac{n}{p_1} <$ n, segue da hipótese de indução que a fatoração de $\frac{n}{p_1}$ é única, pois para valores entre 2 e n a fatoração é única.

E, portanto, as fatorações de $p_2 \ldots p_r$ e $q_2 \ldots q_s$ são iguais (a menos de ordem). Isso acontece porque se $p_1 = q_1$, com a hipótese de indução provamos que todo o resto da fatoração também é igual, logo, podemos concluir que no final, n só tem uma fatoração.

□

2.5 CONGRUÊNCIA MODULAR

A criptografia RSA é composta pelas congruências, tendo-as como ponto central para o processo de codificação e decodificação. O conceito de aritmética modular foi desenvolvido pelo matemático Gauss.

Definição 2.5.1 Se a e b $\in \mathbb{Z}$ dizemos que a é congruente a b módulo m, com m > 0, se a e b têm o mesmo resto na divisão por m, com m fixo, ou se m|(a - b). Notação $a \equiv$ b (mod m).

Em resumo, a definição garante que $a \equiv$ b (mod m) $\Leftrightarrow$ m divide a-b ou b-a. Para nosso trabalho somente nos interessa os casos em que a e b são congruentes, desse modo, nesses exemplos não iremos abordar os casos com incongruência.

Exemplo 2.5.1 Temos 19 ≡ 7 (mod 3), pois 3 divide 12 = 19 - 7. Além disso, a congruência se configura também pelo método dos restos da divisão euclidiana, pois 19 por 3 deixa resto 1, assim como 7 por 3 deixa resto 1, ambos deixam o mesmo resto na divisão por 3.

A relação de congruência (≡) mod m é uma relação (~) de equivalência, pois ela satisfaz as três condições, reflexiva, simétrica e transitiva.

Teorema 2.5.1 Dados a, b, c e m inteiros, m > 0, as seguintes propriedades são verdadeiras.

i) $a \equiv a$ (mod m) para qualquer $a \in \mathbb{Z}$, ou seja, a relação é reflexiva;
ii) Se $a \equiv$ b (mod), então b ≡ a (mod m), para quaisquer a e b $\in \mathbb{Z}$, existe uma simetria nessa relação;
iii) Se $a \equiv$ b (mod m) e b ≡ c (mod m), então $a \equiv$ c (mod m) para quaisquer a, b e c, $\in \mathbb{Z}$, dizemos que, existe transitividade.

Demonstração: (i) segundo a definição **2.5.1,** para a congruência a e b têm-se que, deixar o mesmo resto na divisão por m, ou, m|(a - b). Sendo $a \equiv a$ (mod m), $\forall$ $a \in \mathbb{Z}$, então, essa prova é trivial; pois, a - a = 0, pois 0 é divisível por qualquer número, Isso também implica que, a relação é reflexiva, visto que, todo número é congruente a ele mesmo módulo m. Logo, podemos escrever 0 = m.0, de modo que; m|0 , portanto m|(a-a) = 0.

(ii) Temos $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$. Como $a \equiv b \pmod{m}$, então pela definição m|(a-b), isso significa que se m dividir um outro número inteiro, que chamaremos de k, logo, a - b = k, ele também divide b - a = -k, temos m|- (a-b) = (b-a). E, portanto, b ≡ a (mod m). A simetria é imediata $a \sim b \Rightarrow b \sim a$.

Para a propriedade (iii) verifica-se, se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, sabemos que m|(a-b), segue para a segunda congruência m|(b-c). Logo, existem dois números inteiros d_1 e d_2, tais que, a - b = d_1m e b - c = d_2m, para esse, o módulo divide a soma m|[(d_1) + (d_2)]. Somando-se, membro a membro, estas últimas equações a - b + b - c = d_1m + d_2m, cancelamos os termos semelhantes, fica, a - c = (d_1+ d_2)m, o que implica $a \equiv c \pmod{m}$. Ou seja, a relação é transitiva, observe que os elementos das congruências se relacionam.

□

A relação de congruência se mantém pelas operações de soma e produto, ou seja, em seguida veremos algumas das propriedades válidas.

Teorema 2.5.2 Dados a, b, c, d e m ∈ ℤ, com m > 1. São válidas as seguintes propriedades.

i) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, temos $a + c \equiv b + d \pmod{m}$. (adição)
ii) Sejam $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, logo $ac \equiv bd \pmod{m}$. (multiplicação)

Demonstração: (i) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, pela definição 2.5.1, m|a-b e m|c-d. Tome, a - b = k e c - d = k_1, onde k e $k_1$são os resultados dessa diferença, visto isto, m também divide a soma de ambas congruências, m|[(a-b) + (c-d)], organizando, o sinal negativo pondo em evidência, fica m|[(a+c) - (b+d)], isso implica, a + c ≡ b + d (mod m).

Para (ii) Temos, $a \equiv b \pmod{m}$, então m|(a-b), além de m|c(a-b), pois, m vai dividir qualquer múltiplo de a - b, e assim segue para a segunda congruência $c \equiv d \pmod{m}$. Se m divide as diferenças entre as congruências, ele também vai dividir qualquer múltiplo de ambos, assim, m|c(a-b) e m|b(c-d), e, portanto, m também vai dividir a soma de ambos

$$m|[c(a-b) + b(c-d)] = [(ac-bc) + (bc-bd)],$$

eliminando os termos iguais com sinais opostos, segue que, m|(ac) - (bd). E, portanto, concluímos que, m também divide o produto $ac \equiv bd \pmod{m}$.

□

Com isso, demonstradas as propriedades, fica provada a relação das congruências módulo m, como, reflexiva, simétrica e transitiva. Logo, trata-se de uma relação de equivalência e está definida no conjunto dos inteiros.

Para resolvermos alguns passos da criptografia é preciso resolver problemas de congruências lineares, tal qual, para saber se a congruência é verdadeira, é preciso identificar a existência de um valor para X ∈ ℤ que satisfaça essa relação, isso, define se o problema em questão tem solução ou não. Para tanto, inicialmente é preciso averiguar o critério que aponta se a congruência admite solução.

Definição 2.5.3 (Congruência linear) Dados a, b e m ∈ ℤ, com m > 1. Uma congruência linear em uma variável, é uma expressão do tipo aX ≡ b (mod m), X é a incógnita, e, X ∈ ℤ.

Teorema 2.5.3 (Congruência linear) Dados a,b e m ∈ $\mathbb{N}^*$, com m > 1, as congruências lineares ax ≡ b (mod m) terá solução se, e somente se, mdc (a, m)|b.

Demonstração (⇒) Suponhamos que a relação ax ≡ b (mod m) seja verdadeira, que admite a existência de x ∈ ℤ tal que m|(ax - b), o que equivale à existência de y onde ax - b = my; podemos reescrever da seguinte forma, isolando b, temos ax - my = b, perceba que caímos em uma equação diofantina, em outras palavras, por meio da congruência obtemos uma equação polinomial do primeiro grau, ao qual as duas variáveis x e y assumem valores inteiros que permite verificar possíveis soluções para o problema proposto. Isto é entendido que, a existência de uma solução para a congruência linear, depende de quando a equação diofantina tem solução. Ou seja, ax - my = b admite solução ⇔ d = mdc (a, m) divide b, de modo que, como d = mdc (a, m) então, d|a e d|m, logo, ele também divide qualquer combinação linear de a e m, isso, implica que mdc (a, m)|b.

(⇐) Suponha que mdc (a, m)|b. Logo, as incógnitas da equação x, y são consideradas uma solução da equação diofantina, nesse caso, a equação obtida ax - my = b admite uma solução x, y. Portanto, ax = b + my, e, consequentemente, x é solução dessa congruência, pois, ax ≡ b (mod m).

□

Exemplo 2.5.3 Considere x solução da congruência linear 15x ≡ 9 (mod 6), pois, calculando o mdc (15, 6) = 3|9, isso significa que 6|15x - 9. Temos 15x - 9 = 6y, podemos resolver a

equação diofantina 15x - 6y = 9, com x e y ∈ $\mathbb{Z}$, e determinar os valores que x pode assumir. Pelo Lema 2.3.1, construímos a seguinte equação 15 = 2.6 + 3, onde, 3 é escrito como combinação linear de 15 e 6; reescrevendo, obtemos a igualdade do resto 3 = 15.1- 2.6, que para x_0= 1 e y_0= - 2. Note que, 15.1 ≡ 9 (mod 6), pois 6|15 - 9 = 6. E, portanto x_0= 1 é uma solução de 15x ≡ 9 (mod 6).

Sabe-se que para solucionar a congruência linear antes é preciso analisar as soluções da equação diofantina. Visto isso, a existência de uma solução particular desencadeia possíveis infinidade de soluções, qualquer número congruente a essa solução também será uma solução. De fato, uma vez que x = x_0 e y = y_0 obtemos uma solução particular da equação. Assim, todas as soluções da equação, são dadas por

$$x = x_0 + (-\frac{m}{d})t \text{ e } y = y_0 - \frac{a}{d}\, t,\ t \in \mathbb{Z}$$

Se x_0 e y_0 nos dá a solução da equação diofantina obtida por meio da congruência, então, temos que x_0 é uma solução particular para a congruência.

Nesse caso, como o que nos interessa é a solução da congruência linear, usaremos apenas a incógnita x. Para conseguirmos calcular todos os números que satisfazem a congruência no exemplo exposto acima, utilizamos a seguinte fórmula;

$$x_0 - \frac{m}{d}\, t \Rightarrow 1 - \frac{6}{3}\, t,\ t \in \mathbb{Z}$$

E, portanto x_0= 1 - 2t é uma fórmula geral de uma solução numérica da congruência linear dada, onde para cada valor de t é possível obter uma solução numérica da congruência. Logo, toda solução de x_0 de 15x ≡ 9 (mod 6) será dada por x_0= 1 - 2t, ou seja, por meio dela, pode-se encontrar todos os números que satisfazem a congruência, para isso, é preciso considerar as incongruências, pois é por meio dos restos dos números n ∈ $\mathbb{Z}$ deixados na divisão por 6, que será dados os valores de todos os x.

Atribuímos os valores de t para cada classes de congruência do módulo d = (a, m), como d = 3, os possíveis restos na divisão por 3 são dados pelos inteiros positivos menores que ele, assim, segue 0, 1 e 2. Logo, t assume cada um desses valores, com t ∈ $\mathbb{Z}$, para obter uma solução numérica.

Como mdc (15, 6) = 3, então t_0 = 0, t_1 = 1, t_2 = 2. Substituindo na fórmula.

$x_0 = 1 - 2t \Rightarrow x_0 = 1 - 2 \cdot 0 \Rightarrow x_0 \equiv 1 \pmod 6$;

$x_1 = 1 - 2t \Rightarrow x_1 = 1 - 2 \cdot 1 \Rightarrow x_1 \equiv -1 \equiv 5 \pmod 6$;

$x_2 = 1 - 2t \Rightarrow x_2 = 1 - 2 \cdot 2 \Rightarrow x_2 \equiv 3 \pmod 6$.

Perceba que, a solução para uma congruência linear não é somente um número, e sim, toda uma classe de congruência, é preciso buscar essas classes que verificam a relação. Portanto, todos os n $\in \mathbb{Z}$ que deixam os restos 1, 3 e 5 na divisão por 6, são soluções para a congruência $15x \equiv 9 \pmod 6$. Ou seja, as soluções incongruentes são as classes $\overline{1}$, $\overline{3}$ e $\overline{5}$ módulo 6. Agora, caso a congruência linear tenha o mdc (a, m) = 1, então, ela só admite uma solução, isso não vem ao nosso caso.

Vimos que a congruência é uma relação de equivalência, assim, dados a e b pertencentes ao conjunto dos inteiros, e m inteiro positivo, então $a \sim b \Leftrightarrow a \equiv b \pmod m$. Também vimos que, ao achar um valor para a incógnita x, buscamos validar a relação da congruência $ax \equiv b \pmod m$. Desse modo, podemos dizer que, o conjunto dos inteiros é uma relação de equivalência e, pode-se particionar em conjuntos que não tem intersecção, esses conjuntos são chamados de classes de equivalência módulo m, representamos as classes com uma letra minúscula do alfabeto ou um número com um traço em cima,como por exemplo $\overline{a}$ e $\overline{b}$ ou $\overline{1}$ e $\overline{2}$. As classes são conjuntos, e os elementos que compõe a essas partições são aquelas que são congruentes ao termo, dizemos que, $x \in \overline{a} \Leftrightarrow x \equiv a \pmod m$.

A definição a seguir, caracteriza-se como um conjunto, tais que poderemos observar o comportamento entre seus elementos, vale ressaltar que, trataremos apenas os casos com solução.

Definição 2.5.4 (classes de congruência) Seja $m \in \mathbb{Z}_+^*$. Dado $x \in \mathbb{Z}$ definimos sua classe de congruência módulo m como o conjunto $\overline{a} = \{x \in \mathbb{Z} / a \equiv x \pmod m\}$.

Exemplo 2.5.4 Dado o conjunto da classe de congruência de 3 módulo 7, é o conjunto cujos elementos deixam o mesmo resto que 3 na divisão por 7, de modo $\{y \in \mathbb{Z} / y \equiv 3 \pmod 7\}$. Pòdemos determinar o conjunto das classes $\overline{3}$ por meio da Divisão Euclidiana, tal qual, diz que $b = a \cdot q + r$, com $0 \leq r < |b|$. Assim para a congruência $y \equiv 3 \pmod 7$ temos um q que

multiplicado por 7, será equivalente a 7q = y-3, se isolarmos o y temos a fórmula geral de um elemento da classe de congruência, assim y = 7q+3. Portanto,

$$\overline{3} = \{7q + 3 / q \in \mathbb{Z}\} = \{.., -4, 3, 10, 17, ...\}.$$

Logo, os valores que y pode assumir, são os elementos do conjunto obtido, pois na divisão por 7 deixam resto 3.

Assim sendo, dada uma classe $\overline{a}$ para um número n inteiro qualquer, com n $\in \overline{a}$, então $\overline{n} = \overline{a}$. E portanto, cada elemento pertencente a uma dessas classes é um representante da classe.

O conjunto dos inteiros das classes residuais módulo m, denotado por $\mathbb{Z}_n$, por esta relação, é representado da seguinte forma, $\mathbb{Z} / \sim = \{\overline{0}, \overline{1}, \overline{2},...,\overline{n-1}\}$, ao qual vem do Teorema de Euclides, onde diz que os restos são $0 \leq r < n$.

Exemplo 2.5.5 O conjunto das classes de equivalência módulo 3, denotado por $\mathbb{Z}_3$, será igual a $\{\overline{0}, \overline{1}, \overline{2}\}$, pelas propriedades do Teorema 2.5.1, todos os elementos do conjunto se relacionam entre si, além de, se dois inteiros são congruentes, suas classes são iguais, observe que, quando realizada a multiplicação de $\overline{2} \cdot \overline{2} = \overline{4} = \overline{1}$, pois, 4 = 3.1+1; assim sendo 4 ≡ 1 (mod 3), ou, se pela soma $\overline{2} + \overline{1} = \overline{3} = \overline{0}$, desse modo segue para as demais classes residuais.

Vale observar as operações de $\mathbb{Z}_n$, esses conjuntos possuem todas as operações dos inteiros, comutativa, a associativa, e as operações admitem o elemento neutro, a adição possui o inverso, e a multiplicação é distributiva com relação a adição, logo, o conjunto $\mathbb{Z}_n$ é anel. Um outro exemplo em $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$. Esse conjunto é chamado de corpo dos números binários.

O teorema abaixo nos dá uma caracterização de quais elementos de $\mathbb{Z}_n$ são inverso multiplicativo. Em suma, dizer que um inteiro a é invertível módulo m é o mesmo que dizer que existe em $\mathbb{Z}_n$ um elemento $\overline{b}$ tal que $\overline{a} \cdot \overline{b} \equiv 1$. Ou seja $\overline{a}$ é invertível em $\mathbb{Z}_n$ e que seu inverso é $\overline{b}$.

Teorema 2.5.4 Dados a e m $\in \mathbb{Z}$, com m > 0. Então existe um inteiro b $\in \mathbb{Z}$, tal que ab ≡ 1 (mod m) se, e somente se, mdc (a, m) = 1.

De outro modo, ab ≡ 1 (mod m) ⇔ mdc (a, m) = 1. Neste caso, dizemos que a é invertível módulo m que b é o inverso de a módulo m.

Demonstração: (⇒) Sejam ab ≡ 1 (mod m), segue, o módulo m|ab - 1. Logo, existe q ∈ ℤ de modo que ab - 1 = mq, isso implica, ab - mq = 1. Temos, mdc (a, m) = 1.

(⇐) Reciprocamente, se o mdc (a, m) = 1, sabendo que, a e m ∈ ℤ, com m > 0, então, existem b, q ∈ ℤ, tais que, ab - mq = 1. Assim, fica provado.

□

Exemplo 2.5.6 Considere a seguinte congruência 7x ≡ 1 (mod 4), com x ∈ ℤ, dizemos que 7 é invertível módulo 4. Seja x_0 solução de 7x ≡ 1 (mod 4), para tal, 4|7x - 1. Visto isso, existem x_0 e y_0 ∈ ℤ tais que 7x_0 - 1 =.4y_0. Sabemos que, a solução de uma congruência é determinada por uma solução da equação diofantina, temos 7x_0 - 4y_0 = 1, e, a equação só terá solução em ℤ se mdc (7, 4)|1. Pelo Lema 2.3.1 obtemos x = 3 e y = 5, isso implica, 7. 3 = 21 e 4 . 5 = 20, o que nos dá 21 - 20 = 1. Como 7x ≡ 1 (mod 4), temos 7 . 3 ≡ 1 (mod 4), logo 21 ≡ 1 (mod 4). Observe que, pela definição, o módulo 4|21 - 1, ainda, a divisão de 21 por 20 de fato deixa resto 1. E, portanto, concluímos que x_0 de fato é solução.

Ainda, um elemento $\overline{a}$ ∈ $\mathbb{Z}_n$ será invertível apenas se o mdc (a, m) = 1. Para tanto, todos os elementos de $\mathbb{Z}_n$ - {0} são invertíveis, isso caso m for igual a um número primo p. Para esses casos chamamos os conjuntos $\mathbb{Z}_p$ de corpo.

Exemplo 2.5.7 O conjunto $\mathbb{Z}_4$ {$\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$}. é o conjunto das classes residuais dos restos deixados por n qualquer na divisão por 4. Assim, determine o inverso de $\overline{3}$ em $\mathbb{Z}_4$.
Como mdc (3, 4) = 1, então $\overline{3}$ tem inverso em $\mathbb{Z}_4$.

Armada a congruência 3x ≡ 1 (mod 4), sabendo que, por definição 4|3x - 1. Dada a equação, temos, 3x - 1 = 4y, com x, y ∈ ℤ organizando, 3x - 4y = 1 como combinação linear de 1. Desse modo, 1 = 3 **(-1)** + 4 . 1, segue, 1 = -3 + 4, logo, 1 = 1. Observe, o inverso de $\overline{3}$ em $\mathbb{Z}_4$ é $\overline{-1}$ = $\overline{3}$.

O próximo Teorema é de extremo valor, assim como todos os anteriores; contudo, ele nos ajudará a fazer o teste de primalidade. Para encontrar primos na proporção pedida pelo sistema RSA, por meio do Teorema 2.4.2 (Teorema Fundamental da Aritmética) seria inviável, desse modo, para encontrar primos, Fermat em seu teorema sintetizou por meio da

definição de congruência. Um modo de garantir que todos os elementos sejam invertíveis, logo, $\mathbb{Z}_p$ é corpo. Assim sendo, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_7$,$\mathbb{Z}_{11}$, ….

Com isso, podemos estudar melhor O Pequeno Teorema de Fermat.

2.6 PEQUENO TEOREMA DE FERMAT

Uma curiosidade acerca de Pierre de Fermat, um jurista francês, que também mostrava muito interesse nos estudos matemáticos, nascido em 1601 e falecido no ano de 1665, foi um dos maiores responsáveis em resultados e problemas que motivaram a evolução da matemática, suas contribuições estão fortemente ligadas aos estudos da Teoria dos Números, assim como seus antecessores, Euclides e Eratóstenes.

Em 160, Fermat escreveu uma carta endereçada a seu amigo Frenicle, que também era um amante pelos estudos matemáticos; nesta carta, ele denota por meio da seguinte fórmula $F_n = 2^{2^n} + 1$, que todos eram primos, garantindo com base em suas observações, que os números no formato, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65537$ são todos primos; ele conseguiu calcular o valor de F_5, contudo, ele não aplicou nenhum método de fatoração, certo de que, o mesmo seria também um número primo. Porém, ao calcular F_5, houve um erro que nem mesmo ele ou Frenicle não observaram, e ambos tomaram como verdade a conjectura proposta. Assim, cem anos depois, coube a Euler a tarefa de apresentar a não primalidade deste quinto número. Em seguida a imagem mostra Pierre de Fermat, que em sua época foi apelidado de “o príncipe dos amadores”, matemático francês, e entre suas muitas áreas interessou principalmente na área da física.

Figura 2 - Pierre de Fermat

Fonte: Disponível em: https://pt.wikipedia.org/wiki/Pierre_de_Fermat. Acesso em: 25 jul. 2022.

Teorema 2.6.1 Se p é primo, e a é um número inteiro tal que $a \not\equiv 0 \pmod{p}$, então, temos a congruência $a^{p-1} \equiv 1 \pmod{p}$.

Demonstração: Considere que $a \equiv 0 \pmod{p}$, o que consiste dizer que, todas as potências de a^{p-1} serão congruentes a 0 modulo p. Vamos supor que, a não é múltiplo de p, ou seja, $p \nmid a$, de modo, mdc (a, p) = 1, assim considere o conjunto A= $\{a, 2a, 3a, \ldots, (p-1)a\} \pmod{p}$, A é o conjunto dos múltiplos de a. Existem p - 1 números dos inteiros nesta sequência e todos estão no intervalo [1, p - 1], pelo fato da redução do módulo p. Observe, como, p primo, todos os números desta sequência são diferentes entre si, isso significa que todos os inteiros do intervalo [1, p - 1] aparecem nesta sequência.

Agora, suponhamos que $1 \leq i \leq j \leq p - 1$ e $ia \equiv ja \pmod{p}$. Implica em $(j - i)\, a \equiv 0 \pmod{p}$, isso significa que $p|(j - i)\, a$. Por hipótese, se $p \nmid a$, nos resta que, p|(j - i). Entretanto, observe que $0 \leq j - i < p-1$, neste intervalo 0 é o único número inteiro divisível por p. Assim, temos j - i = 0, o que implica i = j. Em analise, se $i \neq j$, $ia \not\equiv ja \pmod{p}$.

Assim, como a sequência desses números apresentados contém com precisão os inteiros em um intervalo [1, p - 1], logo, o produto de todos os elementos da sequência acima será igual ao produto de todos os inteiros neste intervalo. Deste modo, $\{a, 2a, 3a, \ldots, (p - 1)\, a\} \equiv \{1, 2,3, \ldots, p - 1\}! \pmod{p}$, o que implica $a^{p-1}(p - 1)! \equiv (p - 1)! \pmod{p}$. Como $(p - 1)! \not\equiv$

0 (mod p), multiplicando a igualdade acima pelo seu inverso em ambos os lados, obtemos $a^{p-1} \equiv 1$ (mod p). Assim fica demonstrado.

□

Exemplo 2.6.1 Seja p primo diferente de 2 e 5. Prove que p tem múltiplos da forma 111…1. Sendo a = 10, pelo Teorema de Fermat, e p primo, isso permite dizer que $10^p \equiv 10$ (mod p); também é sabido que, p ≠ 2 e p ≠ 5, logo, p não é divisor de 10, então o mdc (a, p) = 1, esta condição permite afirmar que existe a classe inversa de a (mod p), denotamos a classe inversa com a'. Seguindo o raciocínio temos,

$10^p \equiv 10$ (mod p)

a'. $10^p \equiv a$' . 10 (mod p)

a'. 10. $10^{p-1} \equiv a$'. 10 (mod p)

$10^{p-1} \equiv 1$ (mod p)

10^{p-1} -1 ≡ 0 (mod p)

999 … 9 ≡ 0 (mod p)

Em resumo, podemos escrever 9999.9 como,

9 . 111 … 1 ≡ 0 (mod p)

Se p ≠ 3 então mdc (p, 9) = 1, nesse caso pode-se cancelar o número 9 deste resultado, daí, 111 … 1 ≡ 0 (mod p). Considerando p = 3, temos 3 múltiplo de 9, desse modo, entramos 111 é múltiplo de 3.

Concluímos que, para qualquer p ≠ 2 e p ≠ 5, podemos conseguir um múltiplo dele formado só por números 1.

Agora, uma outra condição. Se p = 13, então, o mdc (10, 13) = 1, isso implica a existência do inverso multiplicativo de 10 (mod 13), assim, continuamos que,

$10^{13} \equiv 10$ (mod 13)

a'. $10^{13} \equiv 10 . a$' (mod 13)

a'. 10. $10^{13-1} \equiv 10 . a$' (mod 13)

$10^{13-1} \equiv 1$ (mod 13)

$$10^{13-1} - 1 \equiv 0 \pmod{13} \Rightarrow 10^{12} - 1 \equiv 0 \pmod{13}$$

Novamente, observe que, para a base 10,qualquer valor que a potência assuma, diferente de 0, resultará em um algoritmo composto de 1 seguidos de um ou mais 0, nesse caso, 10^{12} podemos escrever 1,0 . 10^{12}. Segue-se

$$1{,}0 \cdot 10^{12} - 1 \equiv 0 \pmod{13} \Rightarrow 999 \ldots 9 \equiv 0 \pmod{13}$$
$$9 \cdot 111 \ldots 1 \equiv 0 \pmod{13}$$

Note que, como mdc (13, 9) = 1, logo, 9 pode ser cancelado,ficamos com,

$$111 \ldots 1 \equiv 0 \pmod{13}$$

E, como verificado anteriormente, 111 … 1 é um múltiplo de 13, com isso, fica provado que vale para p = 13.

2.7 FUNÇÃO DE EULER

Vários matemáticos se ocuparam pela busca dos números primos, por achar um padrão. Em XVIII Leonhard Euler foi um grande matemático e físico, nascido na Suíça em 1707, tinha tudo para seguir a carreira de seu pai no clero, contrariando as vontades do pai, seu interesse eram voltados além da matemática, à áreas como construção de navios, hidráulicas, balísticas, e até mesmo passando pela música.

Euler tinha verdadeira paixão pelo estudo da teoria dos números, era um matemático experimental, mesmo assim, em seus trabalhos sempre se preocupou com as demonstrações, até mesmo em provar as de Fermat, que ao contrário, que não se preocupava em provar suas afirmações.

A figura 3 traz a figura do matemático e físico que deixou um grande legado na Matemática. Euler foi considerado um dos mais ilustres matemáticos da sua época, e estende-se até os dias de hoje. Em seguida veremos uma de suas teorias, utilizada na criptografia em questão.

Figura 3 - Leonhard Euler

Fonte: Disponível em: https://pt.wikipedia.org/wiki/Leonhard_Euler. Acesso em: 25 jul. 2022.

Assim como, o Pequeno Teorema de Fermat visa a primalidade dos números, e originou um teste simples e eficiente apontando a não primalidade. Já, o Teorema de Euler é um contraponto do Teorema de Fermat, que associa cada inteiro positivo n a uma quantidade de inteiros positivos menores que ele, e que são coprimos de n, além disso, uma outra aplicação é a descoberta da ordem do grupo multiplicativo de inteiros módulo, Teorema esses fundamentais na definição da criptografia RSA. Pois ajuda a garantir a segurança dificultando a possibilidade de um possível adversário decodificar a mensagem. A função Phi (φ) de Euler. Denotada como φ (n), nos diz que, se um determinado número p é primo, como de 1 a p o único elemento não primo com p é o próprio p, então φ (p) = p - 1. Numa situação mais geral, sendo p primo e n = p^{α} ($\alpha \geq 1$), os elementos serão 1, 2, …, p^{α}, agora, consideramos apenas os que são multiplo com p, temos p, 2p, …, $p^{\alpha-1}$. p. Observe que, o valor 0 jamais fará parte de qualquer conjunto, em resumo, n um número inteiro positivo, a função φ de Euler, será definida como $\mathbb{Z}_{+}^{*} \leq$ n e relativamente primo com n.

Definição 2.7.1 A função φ: $\mathbb{N}^{*} \rightarrow \mathbb{N}^{*}$ que associa a cada n ∈ $\mathbb{N}^{*}$ o número de elementos do conjunto {k ∈ $\mathbb{N}^{*}$ | 1 ≤ k ≤ n e mdc (k, n) =1} é chamada função φ de Euler.

Exemplo 2.7.1 Para φ (n), com n = 8, temos φ (8) = 4 porque, de 1 a 8 (inclusive), os números primos com 8 são; 1, 2, 3, 4, 5, 6, 7, 8. Pela Definição 2.7.1, a função φ associa a cada um dos número inteiros positivos n, ela dará uma quantidade de números inteiros

positivos primos com n. Logo, φ (8) = 4, pois os números inteiros positivos menores e primos com 8 são {1, 3, 5, 7}. Ou seja, pegamos um k ∈ $\mathbb{Z}_+$, 0 < k < 8 tal que o mdc (k, 8) =1.

Teorema 2.7.1 Para todo inteiro n > 1 e para todo $a \in \mathbb{Z}_+^*$, tal que mdc (a, n) = 1, vale a congruência $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Demonstração: Sendo então r_1, r_2, r_3,..., $r_{\varphi(n)}$ um sistema reduzido de resíduos módulo n, assim, o seguinte sistema será também um sistema reduzido de resíduos módulo n, ar_1, ar_2, ar_3,..., $ar_{\varphi(n)}$**.** A demonstração consiste em mostrar que a sequência tem todos os seus elementos primos com n, além de, dois a dois, são incongruentes ao mesmo módulo. Sabendo que mdc (a, n) = 1 assim como, mdc (ar_i, n) = 1, temos ar_i e ar_j são incongruentes módulo n, isso se, i ≠ j. Porém, o mdc (a, n) = 1, uma vez que, $ar_i \equiv ar_j \pmod{n}$, também $r_i \equiv r_j \pmod{n}$, logo i = j. E, portanto r_1, r_2, r_3,..., $r_{\varphi(n)}$, é um sistema reduzido de resíduos módulo n.

□

Exemplo 2.7.2 Se n = kd, com k, d ∈ ℕ, então a quantidade de números naturais m tais que 1 ≤ m ≤ n e mdc (n, m) = d é φ (k). De fato, temos que 1 ≤ m ≤ n e mdc (m, kd) = d, se e somente, se m = λd, com 1 ≤ λ ≤ k e mdc (λ, k) = 1. E, portanto, observe que a quantidade de números naturais m, é igual à quantidade dos λ ∈ ℕ tais que 1 ≤ λ ≤ k e mdc (λ, k) = 1; ou seja, φ (k).

Exemplo 2.7.3 Considere, para todo inteiro n, n^5 - n é divisível por 30. Seja n ∈ ℕ, e n > 0, logo, se fatorarmos n^5 - n, temos M = n (n^4 - 1), observe que, pela fatoração a^2 - b^2 = (a + b) (a + b), assim, (n^4 - 1) = $(n^2)^2$ - 1^2, isso implica, M = n (n^4 - 1) = n (n^2 + 1) (n^2 - 1^2) = n (n^2 + 1) (n + 1) (n - 1). Reescrevendo, M = (n - 1) n (n + 1) (n^2+ 1). Perceba que 30 = 2.3.5, de modo que temos que provar 2|M, 3|M e 5|M. Considerando que 2 divide o produto de dois números naturais consecutivos, assim segue 3 também divide o produto de três números. Logo, mostraremos que 5 também divide M.

n = 5q + r; q, r ∈ ℕ e 0 ≤ r ≤ 4

r = 0 ⇒ n = 5q

$$M = (5q - 1)\, 5q\, (5q + 1)\, [(5q)^2 + 1] \Rightarrow 5|M$$

$$r = 1 \Rightarrow n = 5q + 1$$

$$M = 5q\, (5q + 1)\, (5q + 2)\, [(5q + 1)^2 + 1] \Rightarrow 5|M$$

$$r = 2 \Rightarrow n = 5q + 2$$

$$M = (5q + 1)\, (5q + 2)\, (5q + 3)\, 5\, (5q^2 + 4q + 1] \Rightarrow 5|M$$

$$r = 3 \Rightarrow n = 5q + 3$$

$$M = (5q + 2)\, (5q + 3)\, (5q + 4)\, 5\, (5q^2 + 6q + 2] \Rightarrow 5|M$$

$$r = 4 \Rightarrow n = 5q + 4$$

$$M = (5q + 3)\, (5q + 4)\, 5\, (q + 1)\, [(5q + 4)^2 + 1] \Rightarrow 5|M$$

Com isso concluímos que 5|M para qualquer resto que possa assumir de 0 à 4.

O próximo capítulo, se encarregará de adentrar na construção do algoritmo, o texto será objetivo e direto, onde, poderemos entender melhor seu processo e compreender o porquê o torna tão seguro.

3 CONHECENDO A CRIPTOGRAFIA

Antes de iniciar o processo de construção do algoritmo RSA é preciso uma breve apresentação sobre o que é criptografia, para enfim o leitor conhecer o propósito desta. Com esse afinco, este capítulo traz um pouco do seu contexto histórico junto com algumas das metodologias criptográficas que foram surgindo durante o passar de décadas, assim como sua finalidade e distinção.

3.1 O QUE É CRIPTOGRAFIA E COMO SURGIU?

A criptografia é uma área da criptologia que estuda a prática os princípios e as técnicas que garantem uma comunicação segura, ao qual, reúne técnicas matemáticas que permita escrever uma mensagem de modo cifrada ou em códigos, que possam dificultar o entendimento de uma mensagem, tornando-a incompreensível para pessoas que não estão no ciclo de interesse do remetente, de todo modo, podemos dizer que a criptografia é um conjunto de regras e técnicas utilizadas para cifrar ou codificar o que é escrito, para que impossibilite os adversários de ler a mensagem, ou seja, é a escrita de mensagens por meio de códigos secretos.

A palavra criptografia é composta e vem do grego, onde gráphein é escrita e kripytós quer dizer oculto, portanto escrita oculta. Essa habilidade surgiu da necessidade de proteger informações, os primeiros vestígios criptográficos conhecidos foram os hieróglifos egípcios, porém, há quem diga que não se pode considerar como criptografia, pois seus métodos rudimentares constituem em substituição de letras por símbolos. Com o passar dos anos foram surgindo a necessidade de aprimorar e dificultar as técnicas para ocultar as mensagens, com finalidade de sigilo político e militar, foi a partir daí, que a matemática foi inserida, assim surgiu o método criptográfico sofisticado que conhecemos hoje. Os chineses foram os primeiros a investir nessa criptografia complexa envolvendo processos matemáticos, revoltados após várias derrotas para o acidente, observaram que a criptografia seria uma grande aliada assegurando o sigilo da comunicação sobre as informações das estratégias de guerra.

A confidencialidade de mensagens protagonizou feitos históricos. Há registros de um historiador romano chamado de Heródoto que relatou sobre uma guerra pela liberdade, entre Grécia e Pérsia, segundo ele, os Persas articulou secretamente um exército militar para atacar a Grécia de surpresa, nesta batalha, em defesa, a sua adversária, para comunicar-se com seus

pares, fez-se como uma de suas principais estratégias a escrita escondida. Havia um grego chamado Demarato que morava na Pérsia, este, em comunicação com os seus, escrevia em pares de tabuletas e raspava a cera para formar a mensagem desejada; em seguida, as cobria novamente de forma imperceptível, para poder passar pelos guardas e as mensagens não serem descobertas. Em 3 de setembro de 480 a.C. o líder Persia Xerxes, ordenou o ataque à Grécia que, graças ao seu informante, já estava à espera deste ataque, assim preparando-se, dando a vitória dessa guerra para a Grécia. A mensagem não era codificada e com chaves, como conhecemos atualmente, porém ficou conhecida pela arte de ocultar mensagens, chamada de esteganografia, que vem do grego a palavra steganos e significa coberto e graphein, escrever. De certo, essa forma de comunicação pode ter aberto caminho para novas ideias que futuramente foram surgindo.

Um outro registro de mensagem oculta é a **Cítala Espartana** ou **Bastão de Licurgo**, foi um sistema utilizado para o envio de mensagens secretas pelos éforos espartanos. Esse sistema criptográfico consiste em duas varas com os mesmos diâmetros, e os interlocutores ficavam em posse de uma, a mensagem era escrita em posição longitudinal em uma tira que era enrolada em forma de espiral no bastão. as letras iam sendo escrita a cada volta dada, uma vez escrita a mensagem, a tira era desenrolada e enviada, para conseguir ler a mensagem era preciso enrolar a mensagem novamente no mesmo modo, por esse motivo, o remetente possuía um outro bastão idêntico, era só enrolar a tira e a mensagem original ia se construindo. Ou seja, a chave de decifrar consiste em encontrar a quantidade de colunas conforme o tamanho e espessura do cilindro, uma vez que, é ele que fornece o tamanho de cada bloco que separa a frase a ser codificada.

Figura 4 - Cítala Espartana

Fonte: Disponível em: https://rpm.org.br/cdrpm/89/45.html. Acesso em: 25 jul. 2022.

Posteriormente, as técnicas foram se aprimorando para criptografia codificada por meio de substituição, transposição, com chaves; como por exemplo a Cifra de César, usada

para a comunicação durante a Guerra da Gália, assim como tantos outros que surgiram até chegarmos ao sistema metodológico criptográfico que conhecemos hoje e que silenciosamente faz parte do nosso cotidiano, essa tecnologia só foi possível após a Segunda Guerra Mundial, com o surgimento dos computadores e hoje é a base da ciência da computação moderna.

O processo de sofisticação para a criptografia foi demorado, sobre a dificuldade em garantir uma comunicação secreta , assim como destaca Du Sautoy.

> antes de 1977, quem quisesse enviar uma mensagem secreta se depararia com um problema essencial. Antes que o comunicado fosse transmitido, o emissor e o receptor teriam de se encontrar para decidir qual cifra - o método de codificação - usariam. Os generais espartanos, por exemplo, precisavam concordar sobre as dimensões da cítala. Mesmo com a máquina Enigma, produzida em série, Berlin tinha que enviar agentes para fornecer aos capitães dos barcos U e aos comandantes dos tanques os livros que descreviam as configurações da máquina para codificar as mensagens de cada dia. Naturalmente, se um inimigo pusesse as mãos no livro de códigos, o jogo terminava. (DU SAUTOY, 2007, p. 242).

Atualmente a criptografia está fortemente atrelada a tecnologia, como por exemplo, na área da segurança digital, comumente na segurança da informação, na confidencialidade e integridade de dados, autenticação, dentre outros. Com toda essa modernidade, esse tema requisita a matemática, envolve além da ciência da computação a da comunicação e a engenharia elétrica e física; a qual, se trata na aplicação de tecnologia em uso de cartões com chip, senhas de computadores, comércio eletrônico, bancos digitais e criptomoedas.

3.2 CRIPTOGRAFIA SIMÉTRICA E ASSIMÉTRICA

Além do algoritmo, há um outro elemento essencial para o sistema criptográfico, a chave, e, em alguns sistemas é usado apenas uma chave, a privada, já, em outros são utilizadas duas, uma pública e outra privada. A atribuição da chave é definir o alfabeto cifrado com precisão para que possa ser usado na codificação desejada.

O criptossistema pode-se dividir em duas maneiras distintas, sendo como sistemas simétricos ou assimétricos.

Sistema simétrico Existe apenas uma chave, e é mantida em segredo, pois, a chave de decodificação é a mesma que decodifica, ou seja, o processo de decodificação desfaz o processo de codificação, desse modo retornando a mensagem original.

Sistema assimétrico Existem duas chaves distintas; uma chave é para codificar, essa pode ser de conhecimento público, pois seu conhecimento não compromete o sistema, a segunda chave é para decodificar, apesar de ser diferente ela pertence ao mesmo par criptográfico que a pública mais esta deve ser mantida em segredo. Ainda que ambas pertençam ao mesmo sistema, não é possível descobrir uma chave a partir da outra.

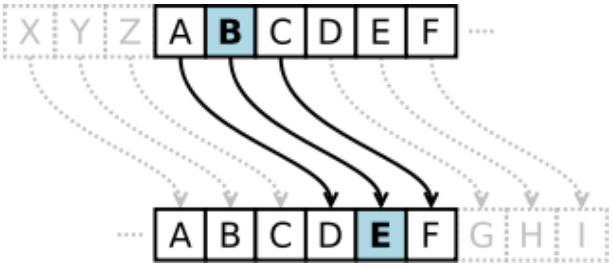
Os recursos matemáticos utilizados para encriptar e decriptar é o que chamamos de chaves de segurança. Com o avanço da comunicação escrita ao longo dos anos também foram surgindo a necessidade de uma comunicação mais segura e que garantisse a privacidade dos interlocutores.

3.3 EVOLUÇÃO

Com o avanço da era cibernética essa nova forma de comunicação trouxe grandes desafios para a criptografia, agora, o modo convencional para a troca de informações foi substituído por uma rede de computadores, onde, a todo momento está sujeito à invasão de terceiros e a quebra de sigilo. Antes de chegar até a criptografia RSA o objeto de estudo deste trabalho, como a aplicação prática dos conceitos matemáticos abordados no capítulo anterior, é importante passar por uma breve apresentação de outros sistemas criptográficos, para assim, compreendermos o processo evolutivo percorrido pela criptografia e os desafios enfrentados até chegarmos a métodos funcionais e eficientes, que correspondem às necessidades da nova comunicação. Assim como Diffie e Hellman (1976, p. 654) afirma que: **"**Antes deste século, os sistemas de criptografia eram limitados a cálculos que podiam ser realizados manualmente ou com dispositivos simples **".**

Cifra de César É um método de substituição de caracteres e de possível reversão de chave simétrica, e consiste em uma regra de posição de três a frente, na qual cada letra do alfabeto é substituída por outra a sua posição a frente, exemplo, se for a letra X seria cifrada pela letra A. A figura abaixo demonstra como funciona esse método de César.

Figura 5- Método de César



Fonte: Disponível em: https://pt.wikipedia.org/wiki/Cifra_de_C%C3%A9sar. Acesso em 04 ago. 2022.

Esse método é facilmente quebrado, basta apenas observar qual letra que mais se repete na mensagem cifrada e analisar qual é a letra mais usada do alfabeto, e assim irá desencadeando outras, e consequentemente é descoberta a técnica de ocultação.

Máquina Enigma Patenteada em 1918 por Arthur Scherbius, era uma máquina eletromecânica com rotores, usada pela Alemanha Narzista durante a Segunda Guerra Mundial. O sistema de chave simétrica tinha como base a substituição de letras por outras de forma aleatória feita pelo misturador, ela quem escolhia para quem iria levar as letras de forma satisfatória, pois a mensagem era cifrada por meio de giros, definido pela quantidade de letras fornecidas na máquina, o que muito dificultou a criptoanálise.

Apesar da sua complexidade, esse método também foi quebrado. Logo abaixo, a figura apresenta a máquina enigma.

Figura 6 - Máquina Enigma

Fonte: Disponível em: https://gizmodo.uol.com.br/maquina-criptografia-nazistas-leiloada/. Acesso em 04 ago. 2022.

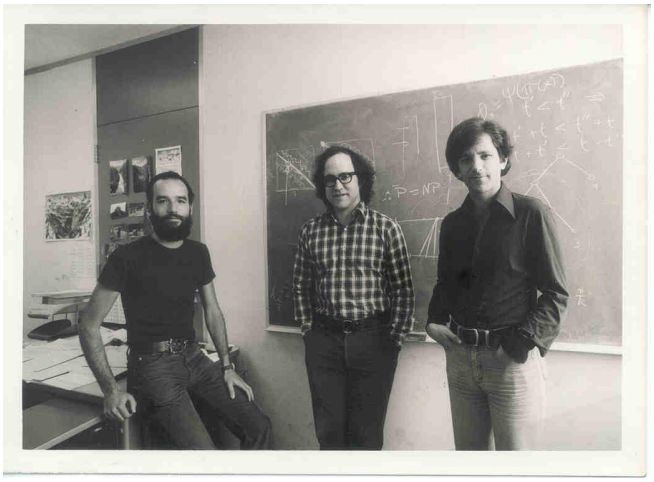
Em 1940, Alan Turing conseguiu solucionar o enigma, desse modo derrubou o principal método de comunicação dos alemães com seus aliados, levando à derrota da Alemanha, pois a partir desse momento todas as suas articulações e seus ataques eram previstos.

Método Diffie-Hellman Como o nome aponta, foi desenvolvido por Whitfield Diffie e Martin Hellman, publicado em 1976. Com chave simétrica, esse sistema é baseado em curvas elípticas (ECC), Como exemplo: $y^2 = x^3 + ax + b$ (y e x são variáveis; a,b constantes), a e b estão em corpos finitos, como, no $\mathbb{Z}_p$ (p é primo). As curvas elípticas buscam por soluções onde pontos de x e y satisfazem uma determinada equação. Esse sistema criptográfico é seguro porque baseia-se em problemas como o de fatoração inteira, problema do logaritmo discreto para curvas elípticas.

Codificação-DES Data Encryption Standard é um um sistema de chave simétrica e cifra de blocos. Esse método trabalha com sistema de 64 bits, o algoritmo cifra o texto usando chaves de 48 bits a partir do texto simples em blocos, porém a chave real é de 56 bits, pois 8 dos 64 são redundantes, fazendo com que 256 chaves diferentes sejam possíveis. O algoritmo executa várias operações para cifrar os dados, dentre eles, combinações e substituições, permutações.

Criptografia RSA Desenvolvida em 1977, e como o próprio nome sugere, os criadores foram Ronald L. **Rivest**, Adi **Shamir** e Leonard **Adleman**, dando nome ao sistema; têm chave assimétrica, e é constituído por três etapas, a pré-codificação, que se trata da geração das chaves pública e privada, criadas pelo destinatário; e a outra etapa é a codificação, onde o emissor usando a chave pública faz a transformação da mensagem para uma versão encriptada, para que esse processo seja eficiente, ele tem que corresponder a uma função bijetora, para assim permitir a volta da mensagem para a versão original; já, a decodificação é o processo reverso, ao qual corresponde ao destinatário que transforma a mensagem encriptada de volta a original. Estes processos serão detalhados mais adiante neste trabalho, uma vez que, é o nosso objeto de estudo. Na figura 6, mostra os três criadores do sistema RSA.

Figura 7 - Ronald L. Rivest, Adi Shamir e Leonard Adleman



Fonte: Disponível em: https://www.chessprogramming.org/Ronald_L._Rivest. Acesso em: 05 ago. 2022.

A criptografia RSA baseia-se nos conceitos matemáticos da Teoria dos Números, é conhecido por seu nível de segurança, que consiste na dificuldade da fatoração de números primos muito grandes.

O capítulo a seguir abordará o processo prático do algoritmo RSA com o uso da tecnologia matemática, explorando a área da Teoria dos Números.

4 RSA DA TEORIA À PRÁTICA

Este capítulo é o ponto central deste trabalho, pois, falar da **Criptografia RSA** é falar da **Teoria dos Números**, a qual ela é totalmente fundamentada. É neste capítulo que será apresentada a aplicação dos conceitos vistos no capítulo 2, aqui o leitor poderá associar a matemática abstrata em uso prático, veremos, não apenas conceitos mas também sua funcionalidade e eficiência, o que o fez se tornar um dos métodos mais utilizados para a segurança de dados.

4.1 ALGORITMO RSA, COMO FUNCIONA?

Tudo começa com uma pré-codificação, é preciso converter a mensagem a ser enviada em uma sequência de números, para essa finalidade é usada uma tabela; de domínio público, geralmente é usada a tabela ASCII (Código Padrão Americano para o Intercâmbio de Informação), porém, será usada neste trabalho, uma tabela simples com efeito apenas para atender o exemplo aqui apresentado. É importante destacar que, todos os números devem corresponder a mesma quantidade de dígitos.

O receptor escolhe aleatoriamente dois números primos muito grandes, ambos distintos; como exemplo, ele é no mínimo da ordem de 10^{100}, que representaremos como números p e q.

A versão cifrada será dividida em blocos b, e cada um desses blocos deverá respeitar a restrição $1 \leq b < n$, sendo n o módulo.

É importante relembrar sobre algoritmos, deste modo, podemos definir da seguinte forma.

Definição 4.1.1 Algoritmo é uma sequência de operações finitas e ordenadas de passos que oferece estabelecer a solução para um determinado problema.

Para a obtenção das chaves, é preciso que o destinatário determine a chave privada para ele, e uma pública para o remetente ou para qualquer outra pessoa que tenha interesse nessa chave.

O destinatário realiza os seguintes passos para a criação das chaves:

1) Escolhe dois números primos distintos p e q;

2) Calcula n = p.q, ao qual, n é o produto dos dois números primos p e q;

3) Determina o número $\varphi(n) = (p-1).(q-1)$;

4) Encontra um número inteiro λ, tal que, mdc $(\lambda, \varphi(n)) = 1$;

5) Obtém um inteiro β / inverso de λ mod $\varphi(n)$, ou seja, resolve-se a congruência $\lambda\beta \equiv 1 \pmod{\varphi(n)}$.

- Chaves pública n e λ.
- Chave privada β.

Os números primos é o grande segredo desse sistema, uma vez que suas chaves de segurança são originadas por meio destes, porém, a cada avanço, o algoritmo adentra na matemática discreta, usando o produto dos números primos para gerar a primeira chave pública, e posteriormente a segunda chave pública é gerada por meio de um número que seja primo com o phi de Euler, e como todo sistema é necessário chave privada, para esta, é obtida através do inverso multiplicativo. Para realizar o processo de codificação e decodificação considera-se a congruência modular, algoritmos de Euclides, teorema dos restos chinês.

4.2 PRÉ-CODIFICAÇÃO

Antes de iniciarmos o passo-a-passo do processo RSA, é importante destacar que a tabela não pode gerar ambiguidade, pois, para que a decodificação seja possível ela precisa permitir a versatilidade, para que haja condições de reversão, e assim, a mensagem volte a forma original, ou seja, para que o método de criptografia dê certo ele têm que corresponder a uma função bijetora, caso a tabela usada não tenha bijeção, então, haverá informações duplicadas, inviabilizando o processo inverso.

A tabela abaixo, representa o meio utilizado para fazer a troca de caracteres, ou seja, no nosso caso, as letras por números, primeira etapa de pré-codificação da mensagem que o remetente faz. A tabela modelo tem objetivo coerente com a proposta, apresentar como funciona a técnica usada no RSA, e portanto, para esta, não haverá necessidade de símbolos, sinais, letras minúsculas e outros.

Tabela 1- Matriz de substituição para a criptografia RSA

Códigos									
A	10	G	16	M	22	S	28	Y	34
B	11	H	17	N	23	T	29	Z	35
C	12	I	18	O	24	U	30	…	99
D	13	J	19	P	25	V	31		
E	14	K	20	Q	26	W	32		
F	15	L	21	R	27	X	33		

Fonte: A autora (2022).

4.3 CODIFICAÇÃO

Exemplo 4.2.1 Mensagem a ser enviada pelo emissor → UFAL

Antes da codificação, o emissor faz um processo de pré-codificação usando uma tabela.

Para este exemplo usamos a tabela 1, dada acima. A mensagem pré-codificada obtida foi, 30151021.

Obtenção das chaves, pré- estabelecidas pelo destinatário;

1) p = 5 e q = 7;

2) n = 5 . 7 = 35;

3) φ (n) = (5-1).(7-1) = 4 . 6 = 24;

4) λ / mdc (λ, φ (24)) = 1;

O valor de λ = 7, pois 7.7 = 49; sabendo que, 48 é um múltiplo de 24, na divisão de 49 por 48 deixa resto 1. Logo, são primos entre si.

- Chaves públicas (35, 7) = (n, λ)

Em seguida separa a pré-codificação em blocos

(b); 30151021 → b_1= 30, b_2 = 15, b_3 = 10, b_4 = 21

Os blocos devem seguir a seguinte regra $1 \leq b < 35$.

Codificação:

$30^7 \equiv \_\_ \pmod{35}$

$30^7 \equiv (-5)^7 \equiv [(-5)^2]^3 (-5) \equiv 25^3 (-5) \equiv 25^2 . 25 (-5) \equiv 625 . 25 (-5) \equiv (-5) 25 (-5) \equiv 125 (-5) \equiv -15 (-5) \equiv 75 \equiv$ **5**

$15^7 \equiv \_\_ \pmod{35}$

$15^7 \equiv [(15)^2]^3 (15) \equiv 15^3 (15) \equiv 15^2 . 15 (15) \equiv 225 (15) \equiv 15 (15) \equiv 225 \equiv$ **15**

$10^7 \equiv \_\_ \pmod{35}$

$10^7 \equiv [(10)^2]^3 (10) \equiv (-5)^3 (10) \equiv 125 (10) \equiv -15 (10) \equiv 150 \equiv$ **10**

$21^7 \equiv \_\_ \pmod{35}$

$21^7 \equiv [(21)^2]^3 (21) \equiv (-14)^3 (21) \equiv (-14)^2 (-14) (21) \equiv -14 (-14) (21) \equiv -14 (21) \equiv -294 \equiv$ **14**

Como se trata de um sistema binário, a palavra codificada fica **05151014**

4.4 DECODIFICAÇÃO

O receptor transforma a versão encriptada de volta à mensagem original.

Considerando as informações anteriores.

A mensagem recebida foi → **05151014**, para decodificar também é preciso separar em blocos, que segue a mesma regra $1 \leq b < 35$. Desse modo,

b_1= 05, b_2 = 15, b_3 = 10, b_4 = 14.

5) Agora encontramos o inverso multiplicativo de λ mod φ (n), ou seja, um número inteiro β / $\lambda\beta \equiv 1 \pmod{\varphi(n)}$.

Sabemos que,

λ [(mod (p-1) (q-1))], p = 5 e q = 7, (5-1) (7-1) = (4.6) = 24; λ = 7.

De modo que, para a congruência temos, $7.\ \beta \equiv 1 \pmod{24}$

O valor de β = 7 também, pois $\lambda = 7$, assim, $\lambda\beta = 49 \equiv 1 \pmod{24}$.

- Chave privada (7) = (β)

Decodificando:

$5^7 \equiv \_\_ \pmod{35}$

$5^7 \equiv [(5)^2]^3\ (5) \equiv 25^3\ (5) \equiv 25^2.\ 25\ (5) \equiv (-5)\ 25\ (5) \equiv -125\ (5) \equiv -625 \equiv$ **30**

$15^7 \equiv \_\_ \pmod{35}$

$15^7 \equiv [(15)^2]^3\ (15) \equiv 15^3\ (15) \equiv 15^2.\ 15\ (15) \equiv 225\ (15) \equiv 15\ (15) \equiv 225 \equiv$ **15**

$10^7 \equiv \_\_ \pmod{35}$

$10^7 \equiv [(10)^2]^3\ (10) \equiv (-5)^3\ (10) \equiv 125\ (10) \equiv -15\ (10) \equiv 150 \equiv$ **10**

$14^7 \equiv \_\_ \pmod{35}$

$14^7 \equiv [(14)^2]^3\ (14) \equiv (196)^3\ 14 \equiv (-14)^3 .\ 14 \equiv (-14)^2\ (-14)\ 14 \equiv -14\ (-14)\ (14) \equiv 196 .\ 14 \equiv (-14)\ 14 \equiv -196 \equiv$ **21**

A mensagem decodificada é **30151021**.

Pela tabela, a versão cifrada corresponde a 30 = **U**, 15 = **F**, 10 = **A**, 21 = **L**.

E portanto, voltamos a mensagem de origem **UFAL**.

4.5 CONFIABILIDADE

A criptoanálise é o estudo dos meios para quebrar as chaves de segurança, e nada melhor do que trabalhar com a Matemática para dificultar esse trabalho, assim, a criptografia RSA se estabeleceu no campo da teoria dos números. Partindo do conhecimento de que os números primos são infinitos e ainda somos incapazes de definir um padrão para eles. Os primos escolhidos inicialmente, darão um produto, e esse produto mesmo sendo de conhecimento público, pelo tamanho dele, é inviável fatorar, até mesmo para um computador, que pode passar dias ou semanas tentando.

Os matemáticos e cientistas da computação Rivest, Shamir e Adleman investiram em problemas matemáticos ainda não resolvidos, relacionado o problema da fatoração interna com os números primos, com o problema do logaritmo discreto, usou outras dificuldades da ciência teórica, e assim, conseguiram garantir a segurança do sistema.

Por curiosidade, é válido mencionar, a definição do problema do algoritmo discreto, é dito que: dados dois elementos R e S de um mesmo grupo, e existindo um p primo, consiste em achar um certo número k de modo que $R = SK \pmod{p}$. E assim, o número K é o logaritmo discreto de R na base S.

Em todo caso, mesmo o adversário sabendo quem é n isso não garante que ele saberá quem são p e q, pois não saberá quem são (p-1) e (q-1), consequentemente não saberá calcular o $\varphi(n)$, sendo assim, também não saberá quem é β expoente aplicado na chave de decodificação. Esse emaranhado, faz com que seja basicamente impossível quebrar as chaves de segurança do método RSA.

5 CONSIDERAÇÕES FINAIS

Quando iniciou-se o trabalho de pesquisa constatou-se a dificuldade em relacionar o quanto a matemática discreta têm influência na nossa realidade, e que por isso, a importância em estudar sobre a Teoria dos Números, a técnica matemática do algoritmo RSA.

Diante disso, a pesquisa teve como objetivo geral apresentar a criptografia RSA como método prático que está fundamentado na Teoria dos Números, à medida que passamos a compreender o processo de construção do algoritmo, constata-se que o objetivo geral foi atendido, porque efetivamente o trabalho conseguiu demonstrar que, os tópicos apresentados no capítulo II, são as técnicas matemáticas que constituem o algoritmo.

Como objetivo específico inicial, buscou-se explorar como estão empregados os principais conceitos da teoria dos números que constitui o algoritmo RSA, que foi atendida pela apresentação no uso de conteúdos referentes, demonstrados neste trabalho.

Um outro objetivo específico foi compreender o processo de codificação e decodificação das mensagens, fica compreendido ao calcular os algarismos que resultam na mensagem codificada, que são obtidos por meio da congruência modular, e o mesmo para o processo de decodificação.

Já o terceiro e último ponto, teve como objetivo específico analisar a segurança do algoritmo que utiliza elementos da teoria dos números, na pesquisa constatou-se que esse algoritmo é eficaz e seguro porque está relacionado a decomposição de números em fatores primos, as suas chaves são geradas pela multiplicação de dois números primos gigantescos, o produto desses primos apesar de ser a chave pública, não é fácil de quebrar, descobrir os números originários é uma tarefa impossível e mesmo computadores poderia levar anos, e isso não seria viável.

A pesquisa partiu da hipótese de que esse sistema criptográfico computacional garante a segurança eletrônica, com base na teoria dos números porque ele aborda conceitos e problemas típicos. Durante o trabalho verificou-se que ele fundamenta-se na dificuldade de fatoração, ou seja, está relacionado ao problema matemático clássico de cálculo muito difícil de ser resolvido por computador, ainda, problema do algoritmo discreto; além de, valer-se da falta de compreensão das pessoas sobre os números primos.

Com caráter bibliográfico e documental, a pesquisa foi realizada por fontes secundárias de revisão literária nacional e internacional, as quais obteve-se uma quantidade significativa de materiais, tendo o critério de avaliação fontes seguras de sites e trabalhos reconhecidos.

Junto a expansão de acesso a internet, um mundo cheio de possibilidades, e com a pouca experiência do usuário, dados pessoais ficaram suscetíveis, com perigo eminente, novas necessidades foram surgindo, como a de achar uma forma segura de manter esses dados em sigilo. Com isso, surge o nascimento da criptografia na rede de forma notória, os matemáticos e cientistas da ciência da computação se dedicaram, nesse propósito, os elementos da clássica matemática interagindo com a realidade por meio da criptografia RSA. Quando passamos um cartão de crédito, realizamos compras online, quando é feita codificação de números de conta, senhas de banco e assinaturas digitais, atividades que nos parecem comuns de se realizar, porém existe toda uma ação por trás para que ao realizar essas tarefas, não sejamos vítimas de golpes. O exemplo prático escolhido, foi ideal, além dele ser um sistema computacional que revolucionou a fase emergente da comunicação global e atua até os dias atuais, também é comprometido com nossa área de estudo. Além do mais, pode abrir a compreensão para o conhecimento matemático, que por meio dele pode-se construir futuro.

REFERÊNCIAS

ARITMÉTICA: aula 9 - divisores e MDC - Algoritmo de Euclides. [*S. l.: s. n.*], 2013. 1 vídeo (40 min). Publicado pelo canal Programa de Iniciação Cientifica da OBMEP. Disponível em: https://youtu.be/o7axIIFY3Ko. Acesso em: 12 dez. 2022.

ARITMÉTICA: aula 56 - outros problemas usando o Pequeno Teorema de Fermat. [*S. l.: s. n.*], 2014. 1 vídeo (9 min). Publicado pelo canal Programa de Iniciação Cientifica da OBMEP. Disponível em: https://youtu.be/9kj-YICjBRI. Acesso em: 30 dez. 2022.

CLASSES de congruência. [*S. l.: s. n.*], 2021. 1 vídeo (17 min). Publicado pelo canal André Costa.Disponível em: https://youtu.be/DLZwAyWWaIE. Acesso em: 20 dez. 2022.

CONGRUÊNCIA. [*S. l.: s. n.*], 2021. 1 vídeo (13 min). Publicado pelo canal André Costa. Disponível em: https://youtu.be/vnPGIq1vURc. Acesso em: 18 dez. 2022.

DIFFIE, Whitfield; HELLMAN, Martin Edward. **New directions in cryptography**. New York: IEEE Xplore, 1976.. Disponível em: https://ieeexplore.ieee.org . Acesso em: 06 ago. 2022.

DOMINGUES, Hygino Hugueros. **Fundamentos de aritmética**. São Paulo: Atual, 1991.

DU SAUTOY, Marcus. **A música dos números primos:** a história de um problema não resolvido na matemática. Rio de Janeiro: Zahar, 2007.

FMDE1 - remoto: introdução à criptografia (parte 1 de 3). [*S. l.: s. n.*], 2020. 1 vídeo (50 min). Publicado pelo canal Robson Ricardo de Araujo. Disponível em: https://youtu.be/1MlylMtD6WI. Acesso em: 09 dez. 2022.

HEFEZ, Abramo. **Elementos de aritmética**. 2. ed. . Rio de Janeiro: SBM, 2005.(Textos Universitários).

LEMOS, Manoel. **Criptografia, números primos e algoritmos**. 4. ed. Recife, PE: IMPA, 2009. (Publicações matemáticas)

MILIES, César Polcino; COELHO, Sônia Pitta. **Números uma introdução à matemática**. 3. ed. São Paulo: Edusp, 2001.

NÚMEROS primos e o teorema fundamental da aritmética. [*S. l.: s. n.*], 2020. 1 vídeo (26 min). Publicado pelo canal André Costa. Disponível em: https://youtu.be/LYlBAOLw5lw. Acesso em: 13 nov. 2022.

OPERAÇÕES com congruência. [*S. l.: s. n.*], 2021. 1 vídeo (12 min). Publicado pelo canal André Costa. Disponível em: https://youtu.be/g8C0YGBvfsQ. Acesso em: 28 nov. 2022.

PROFMAT- MAT1: Prove que 30 divide n^5-n. [*S. l.: s. n.*], 2016. 1 vídeo (8 min). Publicado pelo canal Bruno Glasses Matemática. Disponível em: https://youtu.be/0cS-aMyqDN8. Acesso em: 31 dez. 2022.

RESENDE, Marilene Ribeiro; MACHADO, Sílvia Dias Alcântara. O ensino de matemática na licenciatura: a disciplina teoria elementar dos números. **Revista Educação Matemática Pesquisa**, São Paulo, v. 14, n. 2, p. 257-278, 2012.

SANTOS, José Plínio de Oliveira. **Introdução à teoria dos números**. Rio de Janeiro: IMPA, 1998.

SCHECHTER, Luiz Menasché. **Uma introdução à criptografia de chave pública através do Método El Gamal**. São Carlos,SP: SBMAC, 2014. (Notas em matemática aplicada).

SINGH, Simon. **O livro dos códigos**. Rio de Janeiro: Record, 2002.