UNIVERSIDADE ESTADUAL DO CEARÁ

CENTRO DE CIÊNCIAS E TECNOLOGIA

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

MARIA SUZANA PINHEIRO

CRIPTOGRAFIA RSA, NÚMEROS PRIMOS E UMA SUGESTÃO DE APLICAÇÃO NO ENSINO MÉDIO

QUIXADÁ – CEARÁ

2018

MARIA SUZANA PINHEIRO

CRIPTOGRAFIA RSA, NÚMEROS PRIMOS E UMA SUGESTÃO DE APLICAÇÃO NO ENSINO MÉDIO

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional do Programa de Pós Graduação em Matemática do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial para obtenção do título de mestre em Matemática. Área de concentração: Matemática

Orientador: Prof. Dr. Ulisses Lima Parente

QUIXADÁ – CEARÁ

2018

Dados Internacionais de Catalogação na Publicação

Universidade Estadual do Ceará

Sistema de Bibliotecas

Pinheiro, Maria Suzana .
Criptografia rsa, números primos e uma sugestão de aplicação no ensino médio [recurso eletrônico] / Maria Suzana Pinheiro. - 2018 .
1 CD-ROM: il.; 4 ¾ pol.

CD-ROM contendo o arquivo no formato PDF do trabalho acadêmico com 74 folhas, acondicionado em caixa de DVD Slim (19 x 14 cm x 7 mm).

Dissertação (mestrado profissional) - Universidade Estadual do Ceará, Centro de Ciências e Tecnologia, Mestrado Profissional em Matemática em Rede Nacional, Quixadá, 2018 .
Área de concentração: Matemática .
Orientação: Prof. Dr. Ulisses Lima Parente.

1. Criptografia RSA. 2. Números Primos. 3. Aplicação em sala de aula. I. Título.

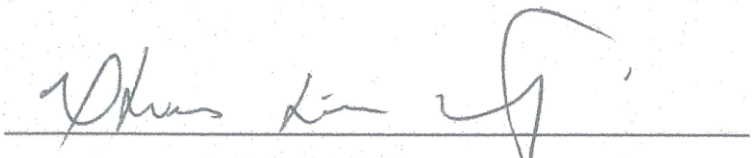
MARIA SUZANA PINHEIRO

CRIPTOGRAFIA RSA, NÚMEROS PRIMOS E UMA SUGESTÃO DE APLICAÇÃO NO ENSINO MÉDIO

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional do Programa de Pós Graduação em Matemática do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial para obtenção do título de mestre em Matemática. Área de concentração: Matemática

Aprovada em: 20 de Setembro de 2018.

BANCA EXAMINADORA



Prof. Dr. Ulisses Lima Parente
Universidade Estadual do Ceará – UECE

Prof. Dr. Jonatan Floriano da Silva
Universidade Federal do Ceará – UFC

Prof. Dr. Jobson de Queiroz Oliveira
Universidade Estadual do Ceará – UECE

Dedico esse trabalho a meu irmão José Leandro Pinheiro (In memorian).

AGRADECIMENTOS

A Deus por ter me dado forças que me permitiram chegar até aqui, por ter me apontado a direção a qual me levou a conquistar esse sonho.

A meu esposo Antônio Glairton Nunes de Lima pela compreensão e o apoio para que eu pudesse concluir este curso.

A minha Mãe e meu Pai pela perseverança e incentivo nos estudos. Por toda a educação, carinho, confiança e paciência que me foram concedidas e que serviram de alicerce para o meu comprometimento e paixão com os estudos.

Aos meus irmãos; José Leandro Pinheiro (In memória) por ser o primeiro a acreditar que isso um dia seria possível e orientar o caminho, Lucas Holanda Pinheiro por todo aconselhamento e ajuda durante o curso em especial no período da dissertação, Mônica Holanda Pinheiro e Fabio Jorge Pinheiro pelo carinho e torcida pela conclusão do curso.

Aos meus colegas de curso pelo companheirismo e apoio durante esta jornada, especialmente a Antonio Alison Pinheiro Martins o qual compartilhei dificuldades, frustrações e vitórias, nossos momentos de estudo tornaram possível chegar até aqui.

Aos meus amigos por acreditarem que eu ira conseguir e não me deixarem desanimar.

A todos os professores que me ajudaram a chegar até aqui, desde mãe que me alfabetizou até aos professores do Curso de Mestrado, Prof. M. Antônio José Melo de Queiroz, Prof. Dr. João Luzeilton de Oliveira, Prof. Dr. Jobson de Queiroz Oliveira e o meu orientador, Prof. Dr. Ulisses Lima Parente, que acompanhou todos os passos na elaboração dessa dissertação.

Agradeço também a CAPES pelo apoio financeiro e me comprometo a ser uma profissional melhor na atuação do ensino de matemática na Educação Básica de nosso país.

Enfim, a todos que participaram direta ou indiretamente deste trabalho.

“No meu fim está o meu princípio.”

(Mary Stuart, Rainha da Escócia)

RESUMO

Este trabalho apresenta o contexto histórico da Criptografia RSA desde sua idealização por Whitfield Diffie a conclusão do trabalho por Shamir, Rivest e Adleman. Demonstra definições, propriedades e teoremas de tópicos de Teoria dos Números. Aborda o contexto histórico, teoremas e definições dos números primos visto a sua importância na garantia da segurança do sistema RSA. Apresenta a descrição do funcionamento do método RSA organizado nas etapas, pré-codificação, codificação e decodificação em seguida demonstra a prova matemática que assegura o seu funcionamento e um breve relato sobre a segurança do método. Propõe sugestões de aplicação em sala de aula na última série do Ensino Médio, demonstrando a matemática que possibilita o funcionamento do sistema RSA através da troca de mensagem e da descrição do método.

Palavras-chave: Criptografia RSA. Números Primos. Aplicação em sala de aula.

ABSTRACT

This paper presents the historical context of RSA Cryptography since its idealization by Whitfield Diffie until the completion of the work by Shamir, Rivest and Adleman. It demonstrates definitions, properties and theorems of Numbers Theory topics. It addresses the historical context, theorems and definitions of prime numbers given their importance in ensuring the safety of the RSA system. It presents the description of the operation of the RSA method organized in the steps, pre-coding, coding and decoding, then demonstrates the mathematical proof that ensures its operation and a brief report on the safety of the method. It proposes suggestions for classroom application in the last grade of High School, demonstrating the mathematics that makes possible the operation of the RSA system through the exchange of message and the description of the method.

Keywords: RSA Encryption. Prime numbers. Application in the classroom.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

O método criptográfico apresentado nesse trabalho é o mais usado nos dias atuais por usuário de internet em todo o mundo. Embora muitos não conheçam essa informação ou como o sistema RSA funciona, ele está garantido à segurança entre a comunicação de quem dele faz uso e, assim, nos consideramos seguros ao enviar uma mensagem através da internet ou digitarmos a senha de contas bancárias em compras online.

A Criptografia RSA surgiu da necessidade da troca de informações secretas e foi necessária a perseverança de homens que buscaram incessantemente um método seguro para realizar essa troca. Baseado no conceito matemático da Aritmética dos Restos e na dificuldade em encontrar um padrão para os números primos desenvolveram uma cifra de mão única, considerada fácil de fazer e difícil de desfazer.

Esse trabalho tem como objetivo principal conhecer e discutir um tema atual que é a Criptografia RSA e sugerir a possibilidade de uma aplicação em sala de aula. O que se dará pela inserção de tópicos matemáticos que permeiam a Criptografia RSA, como por exemplo, o conceito de congruência. Bem como revisar assuntos que já pertencem ao currículo do Ensino Médio como propriedades básicas dos números inteiros, o conceito de números primos e suas propriedades, entre outros.

Os outros objetivos são descritos a seguir. Abordar o contexto histórico da criptografia RSA, a necessidade da troca de informações em um mundo tecnológico e de um método que supra a carência de cifras "fáceis" de quebrar e inacessíveis a grande parte da população. Conhecer os conceitos matemáticos e teoremas que tornam possível a criptografia RSA. Definir o conceito de números primos e sua irregularidade que os tornam ideais para o método RSA. Apresentar a descrição do sistema RSA, sua funcionalidade e segurança e demonstrar um exemplo prático.

Segundo o site G1, "o Brasil fechou 2016 com 116 milhões de pessoas conectadas à internet, o equivalente a 64,7% da população com idade acima de 10 anos." De fato as pessoas estão cada vez mais conectadas. Devido ao grande acesso a tecnologia nos dias atuais um questionamento surge. É possível inserir o conceito de Criptografia RSA no Ensino Médio? Quais contribuições a matemática que permeia o método RSA trará para os alunos do Ensino Médio?

O trabalho se inicia com a definição de criptografia e a descrição de um fato histórico ocorrido no século V antes de Cristo de esteganografia. Até meados da década de 70 todas as formas de criptografia necessitavam da troca de chaves o que era considerado uma

fraqueza, pois, era necessário um encontro ou envio de mensagem para combinar essa chave. O Capítulo 2 relata como esse fato foi enfrentado pelos criptógrafos Whitfield Diffie, Martin Hellman, Ralph Merkle, personagens que antecedem Ronald Rivest, Adi Shamir e Leonard Adleman no contexto histórico da Criptografia RSA.

Para o entendimento da matemática que possibilita a Criptografia RSA é necessário conhecer os conceitos e propriedades básicas dos números inteiros, o capítulo 3 é dedicado a caracterização desses números, os conceitos de divisibilidade, fatorial e congruência, os axiomas de Peano, definição de máximo divisor comum e o mínimo múltiplo comum e o algoritmo Euclidiano Estendido.

Os números primos são os responsáveis por tornar tão difícil a quebra de um código RSA, sua irregularidade e infinitude têm permitido que o código RSA seja considerado seguro até os dias atuais. Por esse motivo o Capítulo 4 é dedicado a relatar o contexto histórico e as principais propriedades desses números.

O capítulo 5 é responsável pela descrição do método de Criptografia RSA, tendo início através da codificação de uma frase simples exemplificando detalhadamente os passos até o momento da decodificação. Logo em seguida é apresentada a prova matemática de como funciona o sistema RSA, a segurança do método e a assinatura digital.

No capítulo 6 são apresentados sugestões de 7 aulas de 50 minutos divididas em 4 planos. O plano é flexível e o professor deve adequá-lo de acordo com a realidade da escola e o nível de aprendizagem dos alunos. Destaca-se a importância da utilização da tecnologia em sala de aula, porque esta é um fator que contribui para a dinâmica da aula a deixando mais atraente e facilitando a organização das informações. Por esse motivo sugere-se a utilização de um software matemático para a codificação e decodificação em sala de aula, não tornando o método entediante e cansativo. No decorrer das aulas os alunos conhecerão a matemática que torna possível a Criptografia RSA e a descrição do método.

2 EM BUSCA DE UMA CIFRA DE MÃO ÚNICA

A preocupação em transmitir uma mensagem de forma secreta que chegue ao destino e somente o receptor de interesse de quem a enviou possa entendê-la é um problema antigo. Esta pode se dar através da esteganografia, comunicação secreta onde a mensagem é ocultada. Um relato de Heródoto, geógrafo e historiador grego que narrou os conflitos entre a Grécia e a Pércia ocorridos no século V antes de Cristo, descreve a história de Histaeu que raspou a cabeça do mensageiro, escreveu a mensagem no couro cabeludo e esperou que o cabelo voltasse a crescer, logo que isso ocorreu enviou o mensageiro que ao chegar ao destino raspou a cabeça e revelou a mensagem ao destinatário, neste episódio somente a ocultação foi suficiente para garantir a transmissão segura da mensagem. Outra forma de esconder uma mensagem é através da criptografia, palavra derivada do grego kriptos que significa oculto, neste caso o objetivo não é ocultar a mensagem e sim esconder o seu significado.

2.1 A NECESSIDADE DA TROCA DE CHAVES

Existem inúmeras formas de criptografar uma mensagem, no entanto, o processo de encriptação é quase sempre um texto misturado de acordo com um protocolo específico que foi estabelecido previamente por transmissor e receptor, onde somente estes têm a **chave** para a decodificação. O termo em destaque refere-se a um código que deixará explícito a mensagem para quem possuí-lo, em caso contrário, será difícil compreender o que é escrito na mensagem.

Enquanto os criptógrafos desenvolvem novos métodos de escrita, é o criptoanalista que luta para encontrar fraquezas nesses métodos de modo a quebrar a mensagem secreta. Durante séculos, uma a uma foram sendo decifradas e os criptoanalistas sempre se destacando.

Todas as ideias criptográficas até meados da década de 1970 necessitavam da troca de chaves, este fato era considerado uma fraqueza. De fato, era necessária como a própria palavra sugere uma “troca”, que poderia ocorrer, entre outras formas, em um encontro pessoal, através do envio de cartas, telegramas ou de um telefonema. No entanto, todas elas envolviam riscos da mensagem ser interceptada ou roubada comprometendo a segurança. Sobre esse assunto ressalta Simon Singh.

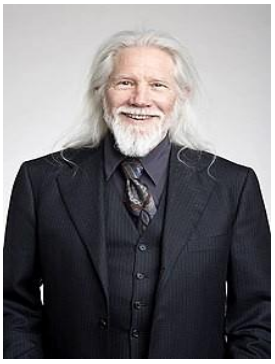
> O problema da distribuição de chaves tem prejudicado a criptografia através da história. Por exemplo, durante a Segunda Guerra Mundial, o alto comando alemão precisava distribuir o livro mensal de chaves diárias para todos os seus operadores da Enigma, o que também era um enorme problema logístico. [...] Em uma época anterior, os usuários da cifra de Vigenère tinham que encontrar um meio de levar a palavra-chave do emissor ao receptor. Não importa o quão segura seja uma cifra em teoria, na prática ela pode ser prejudicada pelo problema da distribuição de chaves (SINGH, 2005, p. 276).

Durante muito tempo o governo e os militares gastaram muito recurso e dinheiro para conseguir transmitir suas chaves e assim fazer com que suas mensagens cheguem ao destino em segurança. Este problema foi considerado de solução impossível até que uma equipe apresentou uma solução brilhante, criando um sistema que desafiava toda a lógica.

2.2 A OBSESSÃO DE WHITFIELD DIFFIE

Era necessário pensar diferente para solucionar o problema que afligia as mentes dos criptoanalistas daquela época, referente a dificuldade relacionada com a troca ou distribuição de chaves. Neste momento surge na história um nome Whitfield Diffie (figura 1), considerado um dos criptógrafos mais entusiasmado de sua geração.

Figura 1 – Whitfield Diffie



Fonte: Site Wikipédia, Artigo Whitfield Diffie (2017)

Diffie nasceu em 1944 e passou a maior parte da infância no Queens, em Nova York. Desde criança era fascinado por matemática e estudou matemática no Instituto de Tecnologia de Massachusetts (MIT), graduando-se em 1965. Segundo a Wikipédia atualmente é vice-presidente e chefe de segurança da Sun Microsystems, fabricante de computadores, semicondutores e software com sede em Santa Clara, Califórnia, no Silicon Valley (Vale do Silício). Diffie foi eleito em 2017 Membro Estrangeiro da Royal Society (Sociedade Real),

uma instituição destinada à promoção do conhecimento científico, título concedido a cientistas notáveis. A possibilidade de uma comunicação sem a troca de chaves não era considerada impossível, "Diffie estava particularmente interessado no problema da distribuição de chaves, e percebeu que aquele que encontrasse uma solução entraria para a história como um dos maiores criptógrafos de todos os tempos" (SINGH, 2005, p. 277). Uma das preocupações envolvia o fato de que não somente empresas e governos tivessem acesso a mensagens criptografadas. "As pessoas comuns um dia teriam seus próprios computadores e seus computadores estariam interligados por linhas telefônicas" (SINGH, 2005, p. 279).

Diffie estava à frente de seu tempo e previa algo comum para os dias de hoje e possível graças aos avanços da criptografia. Os questionamentos sobre como dois estranhos se encontrando via internet poderiam trocar uma mensagem cifrada, ou ainda, uma pessoa querendo comprar um produto pela internet tendo que fornecer dados do cartão de crédito, nessas situações, como isso ocorreria de forma segura? Temendo que a necessidade de distribuição de chaves impedisse que a população tivesse acesso a privacidade digital, Diffie se tornou obcecado com a ideia de procurar uma solução para o problema.

Diffie buscou pessoas que pudessem ajudar a encontrar uma solução para este problema, ao ministrar uma palestra no Laboratório Thomas J. Watson na International Business Machines (IBM) uma empresa dos Estados Unidos voltada para a área de informática, suas ideias foram consideradas experimentais e seu púbico estava cético quanto às perspectivas de se encontrar uma solução. Embora o público não lhe tenha dado crédito o comentário de outra pessoa que havia visitado o mesmo laboratório dias antes com uma palestra abordando o problema de distribuição de chaves deixara Diffie empolgado e naquela mesma noite ele pegou seu carro e percorreu 5 mil quilômetros até a Costa Leste para encontrar a única pessoa que compartilhava de sua obsessão.

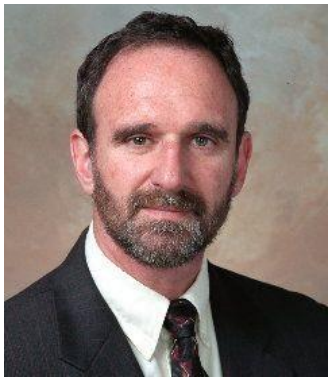
2.3 A FORMAÇÃO DA EQUIPE

O homem procurado era Martin Hellman (figura 2) nascido em 2 de outubro de 1945. Até então Hellman havia trabalhado sozinho e ao conhecer Diffie ele afirma "Foi um tremendo sopro de ar fresco para mim. Trabalhar no vácuo tinha sido muito difícil" (SINGH 2005, p. 280). Os dois iniciaram uma parceria, tentando, de forma desesperada, encontrar uma alternativa para a cansativa tarefa de transportar fisicamente as chaves através de grandes distâncias.

Depois de algum tempo juntou-se a eles Ralph Merkle (Figura 3), nascido em 2 de fevereiro de 1952, era um refugiado intelectual tendo emigrado de outro grupo de pesquisa onde o

professor não tinha simpatias pelo sonho de resolver o problema das chaves. Os três compartilhavam o mesmo desejo e estavam determinados a encontrar uma solução.

Figura 2 – Martin-Hellman.



Fonte: Site Wikipédia, Artigo Martin-Hellman (2017)

Figura 3 – Ralph Merkle.

Fonte: Site Ralph Merkle Home Page

2.4 OS PERSONAGENS ALICE, BOB E EVA

Ao pensar na distribuição de chaves consideremos três personagens Alice, Bob e Eva. Nos episódios que seguem existe o desejo da troca de mensagens entre Alice e Bob. Eva representa o personagem que deseja interceptar a mensagem e decifrá-la. Logo Eva é uma intrusa e o desafio consiste na troca de mensagem sem que ela consiga entendê-la. Imagine que Alice quer mandar uma mensagem para Bob. Ela escreve uma carta secreta e a coloca em uma caixa de ferro com um cadeado no qual só ela tem a chave. Ela a envia para Bob que não pode abri-la, já que não tem a chave. Ao invés disso ele coloca um cadeado no qual somente ele tem a chave e a envia novamente para Alice. Esta, por sua vez, retira o seu cadeado e envia a caixa novamente. Agora Bob pode abri-la, pois só tem o seu cadeado na caixa e ele tem a chave. Por mais que Eva tente interceptar a caixa em suas muitas idas e vindas, não poderá abri-la. Nesse caso o mais importante é que não houve troca de chaves, esse exemplo inspirou Diffie e Hellman a procurarem um método prático de solucionar o problema da distribuição de chaves.

Sua pesquisa concentrou-se em funções matemáticas. Daí, eles observaram que a maioria das funções são de mão dupla, fáceis de fazê-las e desfazê-las. Por exemplo, “triplo” é uma função de mão dupla porque é fácil triplicar um número para obter um novo número e igualmente fácil voltar ao número inicial. No entanto, essas funções de mão dupla não interessavam a Diffie e Hellman, todavia focaram sua atenção em funções de mão única. Como o nome sugere esse tipo de função é fácil de fazer mais muito difícil de desfazer. Vamos

considerar uma situação do cotidiano para ilustrar esse tipo de função. Misturar tinta amarela com tinta azul para produzir tinta verde é uma função de mão única porque é fácil misturar as tintas, mas impossível desfazer a mistura.

Um campo da matemática rico em funções de mão única é a aritmética modular por vezes chamada de aritmética do relógio. Nela é considerado um grupo finito de números, se dispusermos esses números em um círculo como em um relógio ao percorremos todos os números voltamos ao início e não importa quantas voltas dermos os únicos resultados possíveis são os dispostos no círculo. Simon Singh mostra um exemplo,

> A aritmética modular é relativamente simples, e de fato fazemos isso todo dia quando falamos do tempo. Se agora são nove horas e tivermos um encontro daqui a oito horas, podemos dizer que o encontro será às cinco horas e não às 17 horas. Nós calculamos mentalmente 9 + 8 em (mod 12). Imagine o mostrador de um relógio, olhe para o nove e então avance 8 casas, e terminamos no 5: 9 + 8 = 5 (mod 12) (SINGH, 2005, p. 286).

Vamos considerar como outro exemplo a função 3^x, isso significa que vamos multiplicar o número 3 por si mesmo x vezes. Fazendo $x = 2$ temos 3 multiplicado por 3 igual a 9, ou ainda, se o resultado for 81 fica fácil encontramos $x = 4$. Essas afirmações indicam que a função é de mão dupla, pois é bem fácil fazê-la e desfazê-la. No entanto, o comportamento dessa função se estivermos analisando a aritmética modular não é tão sensato. Por exemplo, se nos dizem que 3^x em (mod 7) é 1 não é de imediato que encontramos x. Se fizermos as substituições de x iniciando pelo menor valor possível, no caso 1, e em seguida o 2, assim sucessivamente veremos que o x só será satisfeito quando for igual a 6. "Na aritmética normal, podemos testar números sentir se está ficando frio ou quente. O ambiente da aritmética modular não dá pistas úteis, e a reversão das funções é muito difícil" (SINGH, 2005, p. 288).

Após dois anos estudando a aritmética modular e funções de mão única, surgia uma solução para o problema da distribuição das chaves. Sobre esse episódio Simon Singh descreve

> Depois de meia hora de escrita frenética, ele provou que Alice e Bob podiam estabelecer uma chave sem se encontrar, eliminando portanto um axioma que durara séculos. A idéia de Hellman dependia de uma função de mão única da forma Y^x mod P. Inicialmente Alice e Bob escolhem os valores de Y e P. Quase qualquer valor serve, mas existem algumas restrições tais como Y ser menor que P. Esses valores não são secretos, de modo que Alice pode telefonar para Bob e sugerir, digamos, que Y = 7 e P = 11. Mesmo que a linha telefônica não seja segura e a nefasta Eva ouça a conversação, isso não importa como veremos depois. Alice e Bob agora escolheram uma função de mão única 7^x mod 11. Nesse ponto eles podem iniciar o processo de estabelecer uma chave secreta sem nem se encontrar (SINGH, 2005, p. 289).

A tabela 1 consta em O Livro dos Códigos e descreve o passo a passo de como pode ocorrer essa troca de mensagens.

Tabela 1 – Troca de mensagens Alice e Bob

	Alice	Bob
Fase 1	Alice escolhe um número, digamos 3, e o mantém em segredo. Vamos chamar A o número dela.	Bob escolhe um número, digamos 6, e o mantém em segredo. Vamos chamar de B o número dele.
Fase 2	Alice introduz o 3 na função de mão única e o resultado de 7^A mod 11: 7^3 mod 11 = 343 mod 11 = 2	Bob introduz o 6 na função de mão única e o resultado de 7^B mod 11: 7^6 mod 11 = 117.649 mod 11 = 4
Fase 3	Alice chama o resultado de seus cálculos de alfa e envia o seu resultado, 2, para Bob.	Bob chama o resultado de seus cálculos de beta e envia o seu resultado, 4, para a Alice.
A troca	Normalmente este seria um momento crucial porque Alice e Bob estão trocando informações, e portanto essa é uma oportunidade para Eva escutar e descobrir os detalhes da informação transmitida. Contudo, Eva pode ouvir sem comprometer a segurança final do sistema. Alice e Bob podem usar a mesma linha telefônica através da qual escolheram os valores de Y e P, e Eva pode interceptar esses números que estão sendo trocados, ou seja, 2 e 4. Contudo esses números não são a chave, e por isso não importa que Eva os conheça.	
Fase 4	Alice pega o resultado de Bob e calcula a solução de β^{α} mod 11: 4^3 mod 11 = 64 mod 11 = 9	Bob pega o resultado de Alice e calcula a solução de α^{β} mod 11: 2^6 mod 11 = 64 mod 11 = 9.
A chave	Miraculosamente Alice e Bob terminaram com o mesmo número 9. Esta é a chave!	

Fonte: Simon Singh (2005, p. 290)

Diffie, Hellman e Merkle demonstraram publicamente sua descoberta na Conferência Nacional de Computação, em junho de 1976, assistiam a apresentação um grupo perplexo de especialistas em criptografia. No entanto, o sistema Diffie – Hellman – Merkle, como ficou conhecido, não era perfeito. Embora representasse um gigantesco salto para frente, a situação a seguir poderia prejudicar o método. Considere que Alice deseja enviar uma mensagem para Bob que está em uma cidade distante, onde os horários têm grande diferença e neste momento Bob está dormindo, somente ao acordar ele poderá respondê-la e constituir a chave, só a partir daí Alice poderá cifrar e transmitir a mensagem. Assim, é preferível que os dois Alice e Bob estejam conectados ao mesmo tempo.

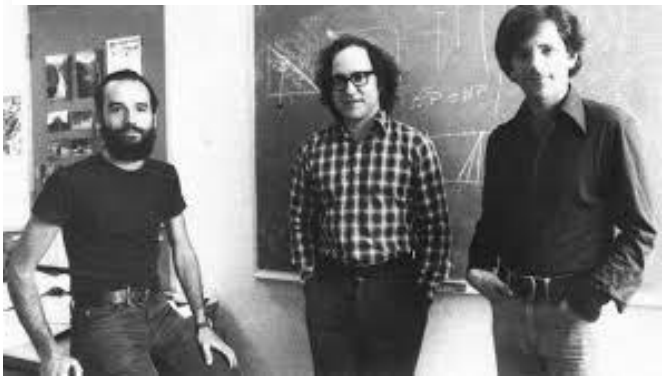
2.5 CHAVE ASSIMÉTRICA

Quando o processo de decifragem é simplesmente o oposto da cifragem dizemos que foram usadas chaves simétricas, nessa situação uma mesma chave é usada para cifrar e decifrar dados. Quando isso não ocorre pode-se dizer que foram chaves assimétricas. Neste caso as chaves de cifragem e decifragem não são idênticas. Diffie idealizou que poderiam existir chaves assimétricas usando funções matemáticas, mas não conseguiu encontrar uma função que tornasse satisfeita a afirmação.

Tal tarefa foi cumprida por um trio de pesquisadores (Figura 4) a cinco mil quilômetros de distância, na Costa Leste dos Estados Unidos. Os responsáveis por tal feito foram Ronald Rivest, Adi Shamir e Leonard Adleman, pesquisadores no oitavo andar do Laboratório de Ciências da Computação do Instituto de Tecnologia Massachussetts (MIT). Simon Singh os descreve.

> Rivest, Shamir e Adleman formavam uma equipe perfeita. Rivest é um cientista da computação com uma tremenda capacidade para absorver ideias novas e aplicá-las nos locais mais improváveis. [...] Shamir, outro cientista da computação, tinha um raciocínio rápido e a capacidade de descartar o que era irrelevante, focalizando o cerne de cada problema. [...] Adleman, um matemático com um enorme vigor, paciência e rigor, foi em grande parte o responsável por detectar as falhas nas ideias de Rivest e Shamir, garantindo que eles não perderiam tempo seguindo pistas falsas (SINGH, 2005, p. 297 - 298).

Figura 4 – Shamir, Rivest e Adleman.



Fonte: Claudio Di Nardo (2013)

Após um ano de tentativas e fracassos Rivest terminou o trabalho em colaboração com Shamir e Adleman, este sistema ficou conhecido como RSA em homenagem aos idealizadores e tornou-se a cifra mais influente da criptografia moderna.

Para entendermos essa nova forma de criptografia precisamos conhecer definições e propriedades dos números inteiros. O próximo capítulo é dedicado à caracterização desses números e a construção de conceitos necessários na utilização do método RSA.

3 CONCEITOS E PROPRIEDADES BÁSICAS DOS NÚMEROS INTEIROS

Nesse capítulo veremos a Caracterização dos Números Inteiros. Conheceremos os Axiomas de Peano com ênfase no Princípio de Indução Finita e o Princípio da Boa Ordem. Estudaremos os Conceitos de Fatorial, Congruência, Divisibilidade e o Algoritmo Euclidiano Estendido.

3.1 CARACTERIZAÇÃO DOS NÚMEROS INTEIROS

Assumiremos do leitor familiaridade com o conjunto dos números inteiros ou apenas inteiros, representado pela $\mathbb{Z}$, são os números a seguir

$$\mathbb{Z} = \{..., -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, ...\}.$$

Assumiremos também que no conjunto $\mathbb{Z}$ dos inteiros estão definidas as operações de soma (+) e produto ($\cdot$) as quais gozam das propriedades fundamentais enumeradas a seguir, que estão no livro Aritmética de Abramo Hefez, (2016, p. 3 - 8), ou em qualquer outro de introdução a álgebra. Para todos $a, b, c \in \mathbb{Z}$,

Propriedade 3.1.1. $(a + b) + c = a + (b + c)$ (associatividade da soma).

Propriedade 3.1.2. Existe $0 \in \mathbb{Z}$ tal que $a + 0 = 0 + a = a$ (existência do elemento neutro).

Propriedade 3.1.3. Existe $-a \in \mathbb{Z}$ tal que $a + (-a) = (-a) + a = 0$ (existência de inverso aditivo de cada elemento $a \in \mathbb{Z}$).

Propriedade 3.1.4. $a + b = b + a$ (comutatividade da soma).

Propriedade 3.1.5. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associatividade do produto).

Propriedade 3.1.6. Existe $1 \in \mathbb{Z}$ tal que $a \cdot 1 = 1 \cdot a = a$ (existência da unidade em $\mathbb{Z}$).

Propriedade 3.1.7. $a \cdot b = b \cdot a$ (comutatividade do produto).

Propriedade 3.1.8. $a \cdot (b + c) = a \cdot b + a \cdot c$ (distributividade do produto em relação à soma).

Propriedade 3.1.9. $a \cdot b = 0$ implica $a = 0$ ou $b = 0$ ($\mathbb{Z}$ não possui divisores de zero).

Observação 1 Apenas a título de completude, por possuir as 9 propriedades acima dizemos que $\mathbb{Z}$ munido da soma e produto é um domínio de Integridade.

As seguintes propriedades decorrem diretamente das 9 apresentadas acima e a demonstração das mesmas ficam como exercício:

Propriedade 3.1.10. Sejam a, b, c, inteiros quaisquer,

(a) Para todo $a, b, c \in \mathbb{Z}$, $a = b$, se e somente se, $a + c = b + c$ (vale a lei do corte);

(b) $0 \cdot a = a \cdot 0 = 0$;

(c) $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$;

(d) $(-a) \cdot (-b) = a \cdot b$;

(e) $a \cdot (b - c) = a \cdot b - a \cdot c$;

(f) $(-1)a = -a$;

(g) $(-1)(-1) = 1$;

(h) $(-1)(-a) = a$.

No conjunto $\mathbb{Z}$ existe a noção de "ordem" (menor do que ou igual) $\leq$, a qual assumiremos com algumas propriedades, a saber:

Propriedade 3.1.11. Para todos $a, b, c \in \mathbb{Z}$,

(a) É reflexiva: $a \leq a$;

(b) É antissimétrica: $a \leq b$ e $b \leq a$, então, $a = b$;

(c) É transitiva: $a \leq b$ e $b \leq c$, então, $a \leq c$;

(d) $a \leq b$, se, e somente se, $a + c \leq b + c$.

Definição 1 Sejam $a, b \in \mathbb{Z}$, dizemos que $a < b$ (lê-se a menor do que b), ou $b > a$ (lê-se b maior do que a) se $a \leq b$ mas a diferente de b.

Assumiremos também que no conjunto $\mathbb{Z}$ vale

Tricotomia: Dados $a, b, \in \mathbb{Z}$, uma, e apenas uma, das seguintes possibilidades é verificada:

i) $a = b$;

ii) $a > b$;

iii) $b > a$.

Definição 2 O módulo ou valor absoluto de um número inteiro a, representado por $|a|$ é definido por:

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

Propriedade 3.1.12. Para a, b, x, inteiros quaisquer, vale

(a) $|a|^2 = |a^2| = a^2$;

(b) $|a \cdot b| = |a| \cdot |b|$;

(c) $|a + b| \leq |a| + |b|$ (Desigualdade Triangular);

(d) Se $x > 0$, $|a| \leq x \iff -x \leq a \leq x$;

(e) $|a| = \sqrt{a^2}$;

(f) $|a| - |b| \leq ||a| - |b|| \leq |a - b|$;

(g) $|a - b| \leq |a - x| + |x - b|$.

Definição 3 Potenciação é uma operação matemática da multiplicação na qual todos os fatores

são o mesmo número real. Podemos escrever assim, para todo $a \in \mathbb{Z}$,

$$a^n = a \cdot a \cdot a \cdot ... \cdot a,$$

em que a repete-se n vezes.

Admite as seguintes propriedades:

Propriedade 3.1.13. Para $a, m, n \in \mathbb{Z}$, $a \neq 0$.

(a) $a^0 = 1$;

(b) $a^1 = a$;

(c) $a^n \cdot a^m = a^{(n+m)}$;

(d) $(a^n)^m = a^{n \cdot m}$;

(e) $(a \cdot b)^n = a^n \cdot b^n$;

(f) $a^{-n} = (\frac{1}{a})^n$;

(g) $a^{\frac{m}{n}} = \sqrt[n]{a^m}$.

3.2 O CONCEITO DE FATORIAL

O fatorial de um número inteiro representado por (!) indica o produto deste número por todos os seus anteriores, assim, para calcular $k!$ faremos,

$$k! = k \cdot (k-1) \cdot (k-2) \cdot (k-3) \cdot ... \cdot 3 \cdot 2 \cdot 1,$$

para $k \geq 2$. Definimos:

- $0!=1$.
- $1!=1$.

Exemplos:

- $3! = 3 \cdot 2 \cdot 1 = 6$.
- $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$.

3.3 OS AXIOMAS DE PEANO

Um subconjunto dos inteiros se destaca, é o conjunto dos Naturais, representado pela letra $\mathbb{N}$, são os números $\mathbb{N} = \{1, 2, 3, 4, 5, ...\}$. Os quatro fatores básicos a seguir são responsáveis pela elaboração de toda a teoria dos números naturais. Devem-se ao matemático italiano Giussepe Peano (1858-1932) do qual levam seu nome e são conhecidos por axiomas de Peano. As propriedades a seguir caracterizam o conjunto dos números naturais. O sucessor de um número natural n será representado por $s(n)$:

Axioma 1. Existe uma função s: $\mathbb{N} \Rightarrow \mathbb{N}$, que associa a cada $n \in \mathbb{N}$ um elemento $s(n) \in \mathbb{N}$, chamado o sucessor de n.

Axioma 2. A função s: $\mathbb{N} \Rightarrow \mathbb{N}$é injetiva.

Axioma 3. Existe um único elemento 1 no conjunto $\mathbb{N}$, tal que $1 \neq s(n)$ para todo $n \in \mathbb{N}$.

Axioma 4. Se X é um subconjunto de $\mathbb{N}$ e é tal que $1 \in X$ e $n \in X \Longrightarrow s(n) \in X$, então $X = \mathbb{N}$.

O conceito de sucessor de um número n, até agora chamado de $s(n)$, é o número que vem imediatamente depois de n na sequência dos números naturais. Assim, 2 é o sucessor de 1, 3 é o sucessor de 2, ..., $n+1$ é o sucessor de n.

3.3.1 O quarto axioma de Peano – O Princípio de Indução Finita (P. I. F.)

O quarto axioma de Peano é responsável por resolver diversas situações problemas em matemática. Através deste muitas generalizações são feitas no conjunto dos naturais. Segundo Coutinho, (2005, p.91) "a palavra indução é usada em matemática em sentido técnico, às vezes qualificado pelo adjetivo finita [...] Mas a palavra também tem um uso vulgar." Em outras palavras o quarto axioma de Peano diz que: se um conjunto de números naturais contém o número 1 e, além disso, contém o sucessor de cada um dos seus elementos, então esse conjunto coincide com o conjunto dos números naturais.

Dada a sua importância chamaremos o quarto Axioma de Peano de Princípio da Indução Finita que abreviaremos para (P. F. I.) e o reescreveremos em linguagem matemática, da forma que segue;

Definição 4 Princípio de Indução Finita (P. I. F.). Seja $P(n)$ uma sentença aberta[1] sobre os naturais. Suponha que são satisfeitas as condições

1. $P(1)$ é verdadeiro, e
2. Para todo $n \geq 1$, se $P(n)$ é verdadeiro, então $P(n+1)$ é verdadeiro.

Portanto, $P(n)$ é verdadeiro para todo natural n. $P(1)$ é a condição inicial, ou passo base. $P(n)$ é a hipótese de indução.

Esta simples propriedade fornece uma das mais poderosas técnicas de demonstração em Matemática.

O Princípio de Indução Finita pode ser aplicado de forma prática como no

[1]Suponha que seja dada uma sentença matemática $P(n)$ nos naturais, passível de assumir valor lógico VERDADEIRO ou FALSO e que dependa de uma variável natural n. Tais sentenças serão ditas sentenças abertas definidas sobre o conjunto dos naturais.

exemplo citado a seguir.

> É como a queda de um dominó. Conhece a brincadeira? Ponha cada peça do dominó, de pé, do lado de outra, a uma pequena distância. Neste caso, A afirmação P(n) é: a n-ésima peça do dominó cai. De fato, se derrubamos a primeira peça (isto é, se P(1) é verdadeira) e se a queda da k-ésima peça derruba a k + 1-ésima (isto é, se P(k) verdadeira implica que P(k + 1) é verdadeira) então caem todas as peças do dominó (COUTINHO, 2005, p. 92).

Alguns cuidados devem ser tomados ao generalizar fórmulas usando indução. Um exemplo deve-se a Fermat, que em uma carta de 1642 afirmou que todos os números da forma

$$2^{2^n} + 1$$

eram primos. Fato que é verdade para $n = \{0, 1, 2, 3, 4\}$, que resultam nos números primos 3,5, 17, 257 e 65537. No entanto, para $n = 5$ temos, $4\,294\,967\,297 = 641 \cdot 6\,700\,417$, um número composto.

3.3.2 Princípio da Boa Ordem – (P. B. O.)

Um subconjunto S dos inteiros é limitado inferiormente se existe $c \in \mathbb{Z}$ tal que $c \leq x$, para todo $x \in$ S. Chamaremos $a \in$ S de menor elemento de S se $a \leq$ x para todo $x \in$ S.

Antes de provar o Teorema da Boa Ordem precisamos da seguinte proposição.

Proposição 1 Se $n \in \mathbb{N}$, não existe p tal que $n < p < n + 1$.

Demonstração: Suponha que exista p tal que $n < p < n+1$. Sendo $p > n$ temos, $p = n + a$, $a \in \mathbb{N}$, e de $n + 1 > p$ temos $n + 1 = p + b$, $b \in \mathbb{N}$. Portanto, $n + 1 = n + a + b$, somando $(-n)$ nos dois lados da igualdade $1 = a + b$. Absurdo, pois, como a e b são naturais, e são no mínimo iguais a 1, mostrando o resultado.

Teorema 1 Todo subconjunto não-vazio A $\subset \mathbb{N}$ possui um menor elemento.

Demonstração: Admitimos, sem perda de generalidade, que $1 \notin$ A pois caso contrário, ele seria o menor elemento de A e a demonstração estaria encerrada.

Queremos provar a existência de um elemento $a \in$ A tal que para todo $x \in$ A, $a \leq x$. Sejam $I_n = \{1, 2, ..., n\}$ e considere o conjunto $X = \{n \in \mathbb{N};\ I_n \subset \mathbb{N} - A\}$, assim todos os elementos de A são maiores que n.

Se valer que $n \in X \Longrightarrow n+1 \in X$ para todo natural n, então pelo axioma de indução X será o conjunto dos naturais, o que não ocorre porque A é não-vazio, portanto, existe um

natural n tal que $n \in$ X e $n + 1 \notin$ X. Logo, $n + 1 \in$ A e como não há $p \in \mathbb{N}$ tal que $n < p < n + 1$, $n + 1$ é o menor elemento de A, chegando ao resultado.

3.3.3 Princípio da Indução Finita - Forte (P. I. F. - Forte)

Uma consequência direta do P.B.O. é a segunda forma de indução, o P.F.I. – Forte. O que este princípio que afirma é apresentado a seguir.

Seja P(m) uma sentença aberta sobre os naturais, suponha que são satisfeitas as condições:

1. P(1) é verdadeiro, e
2. Para cada $m > 0$, P(m) é verdadeira sempre que P(k) for verdadeira para $1 \leq k < m$. Então, P(m) é verdadeiro para todo natural m.

Demonstração: Seja S o conjunto dos $m \in \mathbb{N}$ tais que P(m) seja falsa e suponhamos que S é não vazio. Pelo P.B.O. existe $m_0 \in$ S tal que $m_0 \leq m$ para todo $m \in$ S, e pela hipótese (1) $m_0 > 1$. Assim, P(k) é verdadeira para todo k, $1 \leq k < m_0$. O que por (2) nos dá uma contradição, então não existe m_0 pertencente a S e S é vazio, logo P(m) vale para todo $m \in \mathbb{N}$.

3.4 CONCEITO DE DIVISIBILIDADE

Sejam $n, b \in \mathbb{Z}$, dizemos que b divide n quando existe $q \in \mathbb{Z}$ tal que $n = b \cdot q$, isto é, a divisão de n por b deixa resto zero e escrevemos $b \mid n$ ou ainda que $n = b \cdot q$. A negação dessa sentença é representada por $b \nmid n$, significando que não existe nenhum número inteiro q tal que n = b · q.

Como exemplos, 6 | 18, pois 18 = 6 · 3 e, ainda, 6 ∤ 20, pois não existe $k \in$ Z tal que 20 = 6 · k.

O teorema a seguir recebe o nome de Algoritmo da Divisão Euclidiana.

Teorema 2 Se um número b é um inteiro positivo e não divide um número inteiro n equivale a dizer que a divisão de n por b deixa resto diferente de zero, ou ainda, que existem $q, r \in \mathbb{Z}$ tais que $n = b \cdot q + r$, com $0 < r < b$. Onde q é o quociente e r é o resto da divisão de n (dividendo) por b (divisor).

Existência do quociente q e do resto r.

Demonstração: Considere o conjunto S formado por todos os inteiros não negativos que são da forma, $n - bx$, $x \in \mathbb{Z}$, ou seja, S = $\{n - bx; x \in \mathbb{Z}, n - bx \geq 0\}$. O conjunto S é não vazio, pois $b > 0$ implica $b \geq 1$ e, portanto, para $x = -|n|$ temos que, $n - bx = n + b \mid n \mid \geq n + \mid n \mid \geq 0$.

Assim, pelo Princípio da Boa Ordenação, existe um número inteiro mínimo r de S tal que, $r \geq 0$ e $r = n - bq$ ou $n = bq + r$, $q \in \mathbb{Z}$. Além disso, temos $r < b$, pois, se $r \geq b$, teríamos, $0 \leq r - b = n - bq - b = n - b(q + 1) < n - bq = r$, assim, r não seria o menor elemento de S. Demonstrando o resultado.

Unicidade do quociente q e do resto r.

Demonstração: Suponhamos que existam outros dois números inteiros r_1 e q_1, tais que: $n = bq_1 + r_1$ e $0 \leq r_1 < b$, então $n = bq_1 + r_1 = bq + r$, daí $r_1 - r = (q - q_1) \cdot b$, e, portanto, $|b| \cdot |q - q_1| = |r_1 - r|$. Mas, $-b < -r \leq 0$ e $0 < r_1 < b$, o que implica $-b < r_1 - r < b$, ou seja $|r_1 - r| < b$. Logo, $|b| \cdot |q - q_1| = |r_1 - r| < |b|$, o que só ocorre se $q_1 = q$ e consequentemente, $r = r_1$. Como queríamos demonstrar.

Exemplos do algoritmo de Euclides $11 = 4 \cdot 2 + 3$, $25 = 3 \cdot 8 + 1$, $47 = 9 \cdot 5 + 2$.

3.5 MÁXIMO DIVISOR COMUM

Dados dois números inteiros a e b não simultaneamente nulos, o maior divisor comum de a e b será chamado de máximo divisor comum de a e b e denotado por (a, b).

Definição 5 Diremos que um número $d \geq 0$ é o máximo divisor comum (m.d.c) de a e b se possuir a seguinte as seguintes propriedades:

(1) d é um divisor comum de a e b, e

(2) d é divisível por todo divisor comum de a e b. Podemos escrever assim, se c é um divisor comum de a e b, então $c \mid d$.

Representaremos da seguinte forma (a, b) o (m.d.c) entre a e b.

Proposição 2. Dados dois números inteiros a e b não simultaneamente nulos, existe o (a, b) e é único.

Existência

Demonstração: Seja $D(a, b)$ o conjunto formado pelos divisores comuns de a e b. Como $1 \in D(a, b)$ temos que $D(a, b)$ é não vazio, e como se $d \mid a$ então $|d| \leq |a|$ temos que se $d \in D(a, b)$ então $d \leq$ máximo $\{|a|, |b|\}$ logo possui um elemento máximo e esse elemento é (a, b).

Unicidade

Demonstração: Se d e d' são dois máximos divisores comuns de um mesmo par de números, então, $d \mid d'$ e $d' \mid d$ o que juntamente com as condições $d \geq 0$ e $d' \geq 0$, implicam que $d = d'$. Chegando ao resultado.

3.6 O ALGORITMO EUCLIDIANO ESTENDIDO

Teorema 3 Relação de Bézout

Sejam $a, b \in \mathbb{Z}$. Então existem $x, y \in \mathbb{Z}$ tais que: $ax + by = (a, b)$. Além disso, se $c \mid a$ e $c \mid b$ então $c \mid (a, b)$. Onde (a, b) representa o máximo divisor comum entre a e b.

O caso $a = b = 0$ é trivial (basta tomar $x = y = 0$). Nos outros casos, considere $I(a, b)$ o conjunto de todas as combinações lineares de a e b, isto é,

$$I(a, b) = \{ax + by : x, y \in \mathbb{Z}\}.$$

Pelo Princípio da Boa Ordem o subconjunto dos inteiros descrito acima possui um menor elemento. Seja $d = ax_0 + by_0$ o menor elemento positivo de $I(a, b)$. Afirmamos que d divide todos os elementos de $I(a, b)$. De fato, dado $m = ax + by \in I(a, b)$, sejam $q, r \in \mathbb{Z}$ o quociente e o resto na divisão euclidiana de m por d, de modo que $m = dq + r$ e $0 \leq r < d$. Temos $r = m - dq = a(x - qx_0) + b(y - qy_0) \in I(a, b)$. Mas como $r < d$ e d é o menor elemento positivo de $I(a, b)$, segue que $r = 0$ e, portanto, $d \mid m$.

Em particular, como $a, b \in I(a, b)$ temos que $d \mid a$ e $d \mid b$, logo $d \leq (a, b)$. Note ainda que se $c \mid a$ e $c \mid b$, então $c \mid (ax_0 + by_0) \iff c \mid d$. Tomando $c = (a, b)$ temos que $(a, b) \mid d$, o que juntamente com a desigualdade $d \leq (a,b)$ mostra que $d = (a, b)$.

3.7 MÍNINO MÚLTIPLO COMUM

Definição 6 Diremos que um número inteiro é múltiplo comum de dois números inteiros dados se ele é simultaneamente múltiplo de ambos os números. Em qualquer caso, os números $a \cdot b$ e 0 são sempre múltiplos comuns de a e b. Diremos que um número inteiro $m \geq 0$ é um mínimo múltiplo comum (m.m.c) dos números inteiros a e b se possuir as seguintes propriedades:

(1) m é múltiplo comum de a e b, e

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

Demonstração: Se m e m' são dois mínimos múltiplos comuns de a e b, do item (2) temos que, $m \mid m$' e m' $\mid m$. Como m e m' são dois inteiros não negativos, temos que $m = m$', o que mostra que o mínimo múltiplo comum se existe é único. Por outro lado, se m é o (m.m.c.) de a e b e c é um múltiplo comum de a e b, então $m \mid c$. Portanto se c é positivo, temos $m \leq c$, mostrando que m é o menor dos múltiplos comuns positivos de a e b.

O mínimo múltiplo comum de a e b, se existe, é denotado por $[a, b]$.

Observação 2 Se a e b são números inteiros primos entre si, então $[a, b] = a \cdot b$.

3.8 O CONCEITO DE CONGRUÊNCIA

A congruência entre dois números para a matemática, mais exatamente a aritmética modular, existe quando dois números têm o mesmo resto na divisão por um número inteiro.

Definição 7 Seja m um número natural diferente de zero. Diremos que dois números naturais a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Escreve-se assim, $a \equiv b \bmod m$.

Quando a relação $a \equiv b \bmod m$ for falsa, diremos que a e b não são congruentes, ou que são incongruentes módulo m.

Teorema 4 $a \equiv b \bmod m$ se, e somente se, $m \mid (a - b)$.

Demonstração: Se $a \equiv b \bmod m$, então existem inteiros k_1, k_2 e r tais que $a = k_1m + r$ e $b = k_2m + r$, logo, $(a - b) = m(k_1 - k_2)$ e, consequentemente $m \mid (a - b)$. Reciprocamente, assumimos que $m \mid a - b$. Pela divisão euclidiana, temos que $a = k_1m + r_1$ e $b = k_2m + r_2$ com $0 \leq r_1 < m$ e $0 \leq r_2 < m$, logo $(a - b) = m(k_1 - k_2) + (r_1 - r_2)$. Como $m \mid m(k_1 - k_2)$, segue que $m \mid (r_1 - r_2)$, logo $r_1 = r_2$, pois, $|r_1 - r_2| < m$. Portanto, $a \equiv b \bmod m$.

Da definição de Congruência decorrem as propriedades a seguir.

Propriedade 3.8.1. Sejam $m, n \in \mathbb{N}$. Para todo $a, b, c, d \in \mathbb{Z}$, tem-se que

(a) $a \equiv a \bmod m$.

(b) Se $a \equiv b \bmod m$, então $b \equiv a \bmod m$.

(c) Se $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então $a \equiv c \bmod m$.

Propriedade 3.8.2. Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a + c \equiv b + d \bmod m$.

Demonstração: Suponhamos que $a \equiv b \bmod m$ e $c \equiv d \bmod m$. Logo, $m \mid (b - a)$ e $m \mid (d - c)$. Basta observar que $m \mid [(b - a) + (d - c)]$ e, portanto, $m \mid [(b + d) - (a + c)]$.

Propriedade 3.8.3. Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a \cdot c \equiv b \cdot d \bmod m$.

Demonstração: Suponhamos que $a \equiv b \bmod m$ e $c \equiv d \bmod m$. Logo, $m \mid (b - a)$ e $m \mid (d - c)$. Basta notar que $bd - ac = bd - ad - ac + ad = d \cdot (b - a) + a \cdot (d - c)$. Concluindo que $m \mid (bd - ac)$.

Propriedade 3.8.4. Se $ka \equiv kb \bmod m$ e $(m, k) = 1$, com $k \in \mathbb{Z}$, então $a \equiv b \bmod m$.

Demonstração: Como $m \mid k(a - b)$ e $(m, k) = 1$, segue que $m \mid (a - b)$.

Propriedade 3.8.5. Se $a \equiv b \bmod m$ e $n \mid m$, então $a \equiv b \bmod n$.

Demonstração: Se $a \equiv b \bmod m$, então $m \mid (b - a)$. Como $n \mid m$, segue que $n \mid (b - a)$. Logo, $a \equiv b$

mod n.

Propriedade 3.8.6. Sejam $m_1, m_2, \ldots, m_r \in \mathbb{N}$. Se $a \equiv b \bmod m_i$, para todo $i = \{1, 2, \ldots, r\} \Leftrightarrow a \equiv b \bmod [m_1, m_2, \ldots, m_r]$.

Demonstração: Se $a \equiv b \bmod m_i$, $i = \{1, 2, \ldots, r\}$, então $m_i \mid (b - a)$, para todo i. Sendo $(b - a)$ um múltiplo de cada m_i, segue que $[m_1, m_2, \ldots, m_r] \mid (b - a)$, o que prova que $a \equiv b \bmod [m_1, m_2, \ldots, m_r]$. A recíproca decorre de 3.8.5.

Propriedade 3.8.7. Sejam $(m_1, m_2) = 1$. Se $a \equiv b \bmod m_1$ e $a \equiv b \bmod m_2$, então $a \equiv b \bmod m_1 \cdot m_2$.

Demonstração: Isso decorre da propriedade 3.8.6 juntamente com a observação 2.

Para entendermos a criptografia RSA precisamos conhecer definições e propriedades dos números primos. Portanto o próximo capítulo apresenta um resumo do contexto histórico desses números, o desenvolvimento das descobertas e os recentes recordes de números primos. Enfim, é dedicado a demonstrar a beleza dos números que tornam possível a criptografia RSA.

4 OS NÚMEROS PRIMOS

Antes de entendermos sobre como funciona a criptografia RSA faz-se necessário um estudo sobre os números primos, o comportamento desses números e o contexto histórico de suas descobertas nos mostrarão o quão grande é sua importância nos dias atuais. No livro O Fascínio Dos Números Primos de Jucimar Peruzzo, esta importância é reafirmada.

> Por seu caráter básico na formação de todos os números, os números primos já foram usados, por exemplo, como códigos de contato com seres inteligentes de outros mundos. Nas sondas exploratórias Pioneer e Voyager, entre vozes de pessoas falando em diversas línguas, músicas, sons da natureza e imagens, foram colocados números primos. Há a esperança que algum ser inteligente poderá entender a sequência dos primeiros números primos contidos no disco (PERUZZO, 2012 p. 18) .

Mas afinal, quem são os números primos? Um número inteiro positivo e maior que 1 é chamado *primo* quando possui exatamente dois divisores naturais, 1 e ele mesmo. São exemplos de primos: 2, 3, 5, 7, 11. Um número inteiro positivo é chamado de composto quando possui 3 ou mais divisores. Se um número inteiro positivo não-nulo a é composto, por definição, ele admite um divisor b tal que b seja diferente de 1 e de a, ou seja, um divisor b tal que $1 < b < a$.

Os números primos maiores que 2 são ímpares, pois os números pares maiores que 2 sempre são divisíveis por 2, além de por ele mesmo e por 1.

4.1 CONTEXTO HISTÓRICO

O tempo exato em que a humanidade se deu conta da importância das características dos números primos é impreciso. No entanto, um indicador de tempo se dá através da descoberta de um osso onde estão inscritas três colunas que parecem ter uma natureza matemática, sendo que em uma dessas colunas estão os números primos localizados entre 10 e 20, são eles, 11, 13, 17 e 19. O osso data do ano 6500 a.C e ficou conhecido como

o osso de Ishango, foi encontrado em 1960 nas montanhas da África Central Equatorial. A inscrição no osso nos mostra que naquela época a humanidade já entendia o caráter especial dos números primos.

No livro "Elementos" de Euclides de Alexandria (figura 5) de cerca do ano 300 a.C., contém importantes teoremas sobre números primos, nos quais incluem-se a demonstração de sua infinitude e o teorema fundamental da aritmética. Euclides foi professor, matemático e escritor. Nasceu em 360 a.C. e faleceu em 295 a.C. é considerado o pai da matemática.

Figura 5 - Retrato de Euclides.

Fonte: Site Wikipédia Euclides (2018)

A organização dos números primos através de tabelas foi introduzida por Eratóstenes, (figura 6) no século III a.C., na época em que era diretor da biblioteca de Alexandria. Este método passou a ser chamado de crivo de Eratóstenes, pois cada novo primo gerava um crivo que Eratóstenes utilizava para eliminar os números não primos.

Figura 6 – Retrato de Eratóstenes.

Fonte: Blogger Biografias e Curiosidades Eziel Vieira (2013)

Neste método, os números são colocados até N em uma lista na sua ordem natural e vão sendo eliminados caso sejam múltiplos de um primo menor que ele. Ao final desse processo, os números que sobraram são os números primos dessa lista. A tabela 2 apresenta o Crivo de Eratóstenes com os números primos até o número 100 em destaque.

Este método simples serve para determinar números primos no intervalo de 1 até N. No entanto, quando N é muito grande o método se torna ineficaz, pois demanda muito tempo para a sua execução.

Tabela 2 – Crivo de Eratóstenes

	02	**03**	04	**05**	06	**07**	08	09	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

Fonte: Elaborada pela autora

4.2 TEOREMA FUNDAMENTAL DA ARITMÉTICA

Estabeleceremos alguns resultados que serão usados para entender os mistérios que envolvem estes números.

Teorema 5 (Lema de Euclides**)** Sejam $a, b, p \in \mathbb{N}$, com p primo. Se $p \mid a \cdot b$, então $p \mid a$ ou $p \mid b$.

Demonstração: É suficiente provar que se $p \mid a \cdot b$, e $p \nmid a$, então $p \mid b$. Pelo Teorema de Bézout, existem $m, n \in \mathbb{Z}$ tais que $a \cdot m + p \cdot n = (a, p) = 1$ multiplicando os dois lados da igualdade por b, temos $a \cdot m \cdot b + p \cdot n \cdot b = b$. Como $p \mid a \cdot b$ por hipótese e $p \mid p$, então $p \mid b$, como queríamos demonstrar.

Teorema 6 (Teorema fundamental da aritmética) Um número natural maior que 1, ou é primo,

ou se escreve de maneira única como um produto de primos, a menos de ordenação.

Existência

Demonstração: Prova pelo princípio de indução finita forte em n.

Passo base - Para $n = 2$, o teorema é valido, pois 2 é primo.

Hipótese de indução - Suponha agora que o teorema é válido para todo número natural maior que 2 e menor que n.

Passo indutivo - Provaremos que também é válido para n.

Se n é primo, a afirmação está demonstrada. Consideramos que n não é primo e, portanto, existe $2 \leq n_1 < n$ que divide n e, então, escrevemos $n = n_1 \cdot k$, sendo $2 \leq k < n$. Dessa forma por hipótese de indução, temos que n_1 e k podem ser escrito como produto de primos. Seja, $n_1 = p_1 \cdot ... \cdot p_n$ e $k = q_1 \cdot ... \cdot q_n$, com p_i e q_j números primos, como $n = n_1 \cdot k$, podemos escrever $n = p_1 \cdot ... \cdot p_n \cdot q_1 \cdot ... \cdot q_n$. Desta forma o resultado também é válido para n, finalizando a demonstração.

Unicidade

Demonstração: Se n é primo não há nada a ser determinado. Considere que n seja composto. Prova por indução em n.

Passo base – Considere $n = 4$, que só pode ser escrito como $2 \cdot 2$.

Hipótese de indução - Todo número natural maior que 1 e menor que n se fatora de modo único como produto de primos.

Passo indutivo - Provaremos que n também se fatora de modo único. Suponha por absurdo que n possa ser escrito de duas maneiras diferentes ao menos da ordem de seus fatores, assim, $n = p_1 \cdot p_2 \cdot ... \cdot p_r$ e $n = q_1 \cdot q_2 \cdot ... \cdot q_s$, com p_i e q_j números primos, sendo $i \in \{1, 2, ..., r\}$ e $j \in \{1, 2, ..., s\}$. Vamos provar que r = s e que cada p_i é igual a algum q_j. Como p_i divide o produto $q_1 \cdot q_2 \cdot ... \cdot q_s$, ele divide pelo menos um dos fatores q_j. Suponhamos, sem perda de generalidade, que $p_1 \mid q_1$. Como são ambos primos, isto implica que $p_1 = q_1$.

$$\frac{n}{p_1} = p_2 \cdot ... \cdot p_r = q_2 \cdot ... \cdot q_s$$

Como $1 < \frac{n}{p_1} < n$, constatamos que as duas fatorações são idênticas, ou seja, r = s e, a menos da ordem, as fatorações $p_1 \cdot p_2 \cdot ... \cdot p_r$ e $q_1 \cdot q_2 \cdot \cdot ... \cdot q_s$ são iguais. Provando assim, que n se escreve como produtos de primos de maneira única, finalizando a demonstração. “O Teorema Fundamental da Aritmética já aparece no livro Elementos de Euclides” (PERUZZO, 2012, p. 27). Exemplos:

- $= 2 \cdot 3$
- $8 = 2 \cdot 2 \cdot 2 = 2^3$

- $10 = 2 \cdot 5$
- $20 = 5 \cdot 2 \cdot 2 = 5 \cdot 2^2$
- $28 = 7 \cdot 2 \cdot 2 = 7 \cdot 2^2$
- $102 = 2 \cdot 3 \cdot 17$
- $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^3 \cdot 3^2 \cdot 5$

4.3 TESTE DE RAIZ

Para achar os números primos até um certo número *n*, é necessário eliminar os múltiplos dos números primos até *n*, como no Crivo de Eratóstenes.

Teorema 7 Se *n* é composto ele tem um divisor primo *p* menor que ou igual a $\sqrt{n}$, p $\leq \sqrt{n}$.

Demonstração: Sendo *n* composto, existem n_1 e n_2 tais que $n = n_1 \cdot n_2$, onde $1 < n_1 < n$ e $1 < n_2 < n$. Suponha que $n_1 \geq n_2$ (o caso $n_1 \leq n_2$ é análogo). Daí, temos que $n \geq n_2 \cdot n_2$ ou ainda $n \geq n_2^2$. Sendo assim, $n_2 \leq \sqrt{n}$. Seja *p* um fator primo de n_2 ou $p = n_2$. Como $n_2 \leq \sqrt{n}$ e $p \mid n_2$ então $p \leq n_2 \leq \sqrt{n}$. E, como $p \mid n_2$ e $n_2 \mid n$, então $p \mid n$. Logo *p* é o fator primo de *n* menor que igual a *n*, como queríamos demonstrar.

Na prática esse resultado tem muita importância, pois, para determinarmos se um número *n* é primo, é suficiente testarmos a divisibilidade pelos primos *p* tais que $p \leq \sqrt{n}$.

Essa é uma condição que simplifica bastante a tarefa de determinar se um número é primo. Como exemplo, observe o número 89. Temos que $9 < \sqrt{89} < 10$. Os números primos menores que 9 são: 2, 3, 5, 7. Dividindo 89 por cada um destes primos constatamos que ele próprio é primo, pois nenhum quociente é inteiro.

Para números muito grandes o teste da raiz não tem grande utilidade. Segundo Jucimar Peruzzo (2012, p. 29), "se *n* tiver uns 100 algarismos, para descobrir se ele é primo teria que testar a sua divisibilidade pelos primos que tenham até 50 algarismos, o que não é muito viável."

4.4 PRINCIPAIS PROPRIEDADES DOS NÚMEROS PRIMOS

4.4.1Teorema de Euler

Leonhard Paul Euler (figura 7) foi um matemático e físico suíço, fez importantes

descobertas em várias áreas da matemática. A função $\varphi(n)$ é muito importante no estudo dos números primos. Ela está definida como sendo o número de inteiros positivos que não excedem um inteiro positivo n, que são relativamente primos com n.

A tabela 3 apresenta os valores de $\varphi(n)$ para $1 \leq n \leq 10$.

Tabela 3 – Exemplo de valores de $\varphi(n)$

n	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4

Fonte: Elaborada pela autora

Figura 7 – Leonhard Euler

Fonte: Site Grupo Escolar. Biografias Leonard Euler. Juliana Miranda.

Observe que se p é primo, então todos os inteiros positivos menores que p são primos com p, ou seja, $\varphi(p) = p - 1$ e, ainda, se p e q primos $\varphi(p \cdot q) = \varphi(\mathrm{p}) \cdot \varphi(q)$. O teorema de Euler afirma que,

Teorema 8 (Teorema de Euler) Se n é um inteiro positivo e a é um inteiro tal que o máximo divisor comum entre a e n é 1, então $a^{\varphi(n)} \equiv 1 \bmod n$.

Chamaremos de sistema completo de resíduos módulo n a todo conjunto de números inteiros cujos restos pela divisão por n são os números de 0, 1, ..., $n - 1$, sem repetições e numa ordem qualquer.

Portanto, um sistema completo de resíduos módulo n possui nelementos.

Um sistema reduzido de resíduos módulo n é um conjunto de números inteiros r_1, $..., r_s$ tais que

(a) $(r_i, n) = 1$, para todo $i = 1, ..., s$;

(b) $r_i \not\equiv r_j \bmod n$, se $i \neq j$.

(c) Para cada $m \in \mathbb{Z}$ tal que $(m, n) = 1$, existe i tal que $m \equiv r_i \bmod n$.

Teorema 9 Seja $r_1, ..., r_{\varphi(n)}$ um sistema reduzido de resíduos módulo n e seja $a \in \mathbb{Z}$ tal que $(a, n) = 1$. Então, $ar_1, ..., ar_{\varphi(n)}$ é um sistema reduzido de resíduos módulo n.

Demonstração: Seja $a_1, ..., a_n$ um sistema completo de resíduos módulo n do qual foi retirado o sistema reduzido de resíduos $r_1, ..., r_{\varphi(n)}$. Do fato de que $(a, n) = 1$, tem-se que $(a_i, n) = 1$ se, e somente se, $(aa_i, n) = 1$, o resultado segue disso.

Com essa demonstração estamos prontos para provar o Teorema de Euler.

Demonstração: Seja $r_1, ..., r_{\varphi(n)}$ um sistema reduzido de resíduos módulo n. Logo pela demonstração acima $ar_1, ..., ar_{\varphi(n)}$ é um sistema reduzido de resíduos módulo n e, portanto, $ar_1 \cdot ar_2 \cdot ... \cdot ar_{\varphi(n)} \equiv r_1 \cdot r_2 \cdot ... \cdot r_{\varphi(n)} \mod n$. Consequentemente, $a^{\varphi(n)} \cdot r_1 \cdot r_2 \cdot ... \cdot r_{\varphi(n)} \equiv r_1 \cdot r_2 \cdot ... \cdot r_{\varphi(n)} \mod n$. Como $(r_1 \cdot r_2 \cdot ... \cdot r_{\varphi(n)}, n) = 1$, segue da propriedade 3.8.4 que $a^{\varphi(n)} \equiv 1 \mod n$.

4.4.2 Pequeno Teorema de Fermat

Pierre de Fermat (figura 8) foi um dos fundadores da teoria dos números. Um dos mais importantes teoremas demonstrados por ele é conhecido por Pequeno Teorema de Fermat, e afirma que:

Teorema 10 (Pequeno Teorema de Fermat) Seja p um primo. Se p não divide a, então $a^{(p-1)} \equiv 1 \mod p$. Além disso, para todo inteiro a, $a^p \equiv a \mod p$.

Demonstração: Considere o conjunto de inteiros $B = \{a, 2a, 3a, ..., (p-1)a\}$ onde a é um inteiro satisfazendo $(a, p) = 1$. Nenhum deles é divisível por p e quaisquer dois deles são incongruentes módulo p, em virtude da propriedade 3.8.4. Assim, o conjunto dos restos dos elementos de B coincide com o conjunto dos restos não nulos na divisão por p, a saber, $\{1, 2, 3, ..., p-1\}$. Portanto, $a \cdot 2a \cdot 3a \cdot ... \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) \mod p$, logo, $a^{(p-1)} \cdot (p-1)! \equiv (p-1)! \mod p$.

Figura 8 – Pierre de Fermat.

Fonte: Site Wikipédia Artigo Pierre de Fermat (2018)

Em virtude da propriedade 3.8.4 podemos cancelar o termo $(p-1)!$ em ambos os lados, pois, $((p-1)!, p) = 1$, concluindo assim a demonstração do teorema.

4.4.3 Teorema de Wilson

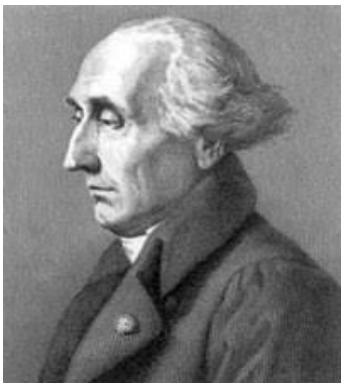
Antes de demonstrarmos o Teorema de Wilson precisaremos do seguinte resultado, este se encontra na Proposição 10.1. Abramo Hefez, (2016, p. 194).

Teorema 11 Sejam $a, m \in \mathbb{Z}$, com $m > 1$. A congruência $a\mathrm{X} \equiv 1 \bmod m$ possui solução se, e somente se, $(a, m) = 1$. Além disso, se $x_0 \in \mathbb{Z}$ é uma solução, então se x é uma solução da congruência se, e somente se, $x \equiv x_0 \bmod m$.

Demonstração: A congruência acima tem uma solução x_0 se, e somente se, $m \mid (ax_0 - 1)$, o que equivale a dizer que a equação diofantina $a\mathrm{X} - m\mathrm{Y} = 1$ possui solução em números inteiros. O que pela Relação de Bézout ocorre se, e somente se, $(a, m) = 1$. Por outro lado, se x_0 e x são soluções da congruência $a\mathrm{X} \equiv 1 \bmod m$, então $ax \equiv ax_0 \bmod m$ e $(a, m) = 1$, o que propriedade 3.8.4. implica que $x \equiv x_0 \bmod m$. Observe que, se x_0 é solução da congruência $a\mathrm{X} \equiv 1 \bmod m$, e $x \equiv x_0 \bmod m$, então x é também solução da mesma congruência, pois $ax \equiv ax_0 \equiv 1 \bmod m$.

O Teorema de Wilson foi provado, pela primeira vez, por Joseph Louis Lagrange (figura 9) matemático italiano.

Figura 9 – Joseph Louis Lagrange.



Fonte: Site Wikipédia Artigo Joseph-Louis Lagrange (2018)

Teorema 12 (Teorema de Wilson) Se p é um número primo, então $(p-1)! \equiv -1 \bmod p$.

Demonstração: O teorema é válido para $p = 2$, pois, 2 divide $[(2-1)! + 1] = 2$, e para $p = 3$, pois 3 divide $[(3-1)! + 1] = 3$. Suponhamos $p \geq 5$, primo. Para todo $i \in \{1, \ldots, p-1\}$, como vimos anteriormente a congruência $i\mathrm{X} \equiv 1 \bmod p$ possui uma única solução módulo p, ou seja,

dado $i \in \{1,...,p-1\}$ existe um único $j \in \{1,...,p-1\}$ tal que $ij \equiv 1 \bmod p$. Por outro lado, se $i \in \{1,...,p-1\}$ é tal que $i^2 \equiv 1 \bmod p$, então $p \mid (i^2 - 1)$, o que equivale a $p \mid (i - 1)$, ou $p \mid (i + 1)$, o que só pode ocorrer se $i = 1$ ou $i = p - 1$. Logo, $2 \cdot ... \cdot (p - 2) \equiv 1 \bmod p$, e, portanto, $2 \cdot ... \cdot (p - 2) \cdot (p - 1) \equiv (p - 1) \equiv -1 \bmod p$.

Vale a recíproca do Teorema de Wilson, como veremos a seguir.

Proposição 3 Seja $p \geq 2$ um inteiro. Se $(p-1)! \equiv -1 \bmod p$, então p é primo.

Demonstração: O resultado vale trivialmente para $p = 2$, $p = 3$ ou $p = 4$. Suponhamos que $p > 4$ e não é primo. Veremos que $p \mid (p-1)!$ Como p é composto suponha que $p = p_1 \cdot p_2$ com $1 < p_1 < p$ e $1 < p_2 < p$. Se $p_1 \neq p_2$ podemos supor, sem perda de generalidade, que $1 < p_1 < p_2$ e, portanto, $(p-1)! = 1 \cdot ... \cdot p_1 \cdot ... \cdot p_2 \cdot ... \cdot (p-1)$ o que mostra que $p \mid (p-1)!$ nesse caso. Se $p_1 = p_2 > 2$, temos $(p-1)! = 1 \cdot ... \cdot p_1 \cdot ... \cdot 2p_1 \cdot ... \cdot (p-1)$ como $p = p_1 \cdot p_1$ ele divide $(p-1)!$. Assim, p não divide $(p-1)! + 1$ e $(p-1)! \not\equiv -1 \bmod p$. Demonstrando que se o teorema é válido então p é primo.

4.5 EXISTEM INFINITOS NÚMEROS PRIMOS

A existência de infinitos primos já era considerada certa no ano 300 a.C, estando resolvida no livro Elementos de Euclides. É considerada uma das mais belas e elegantes soluções para um problema de matemática. Hoje existem outras demonstrações que reafirmam a sua infinitude.

Neste trabalho apresentarei duas delas, a demonstração de Euclides e a demonstração de Goldbach / Hurwitz.

Teorema 13 Existem infinitos números primos.

4.5.1 A demonstração de Euclides

Suponhamos que exista uma quantidade finita de números primos e sejam eles $p_1 = 2$, $p_2 = 3$, ..., p_r. Façamos $P = p_1 \cdot p_2 \cdot ... \cdot p_r + 1$ e seja p um número primo que divide P. Esse número p não pode ser igual a qualquer dos números p_1, p_2, ... , p_r porque então ele dividiria a diferença $P - p_1 \cdot p_2 \cdot ... \cdot p_r = 1$, o que seria impossível. Assim, p é um número primo que não pertence à sucessão e, por consequência, p_1, p_2, ..., p_r não podem formar o conjunto de todos os números primos. Essa demonstração se encontra no livro Números Primos, Velhos Mistérios e Novos Recordes de Paulo Ribenboim, (2012, p.1).

4.5.1 A demonstração de Goldbach / Hurwitz.

De acordo com Paulo Ribenboim (2012, p.4), "a demonstração que será apresentada encontra-se numa carta de C. Goldebach a Euler (datada de 20/31 julho 1730); independentemente, a mesma demonstração foi descoberta por Hurwitz em um exercício de 1891."

Dados dois números primos entre si, qualquer primo que divida um deles, certamente não dividirá o outro. Assim, basta construir uma lista infinita de números que são dois a dois primos entre si. Uma lista que satisfaz essa propriedade pode ser obtida pelos números de Fermat dados, para $n \geq 0$, por $2^{2^n}+1$. Inicialmente provaremos, por indução em m, a seguinte afirmação.

Teorema 14 Se F_m é um número de Fermat vale a seguinte propriedade $F_m - 2 = F_0 \cdot F_1 \cdot F_2 \cdot \ldots \cdot F_{m-1}$.

Demonstração:

Passo base – Para $m = 2$ temos $F_2 - 2 = 2^{2^2}+1-2 = (2^4+1)-2 = 17-2 = 15$.

$F_0 \cdot F_1 = (2^{2^0}+1)\cdot(2^{2^1}+1) = 3 \cdot 5 = 15$.

Hipótese de indução – Suponha que vale para $m = k-1$. $F_{k-1} - 2 = F_0 \cdot F_1 \cdot F_2 \cdot \ldots \cdot F_{k-2}$.

Passo indutivo – Se $F_k - 2 = 2^{2^k}+1-2 = 2^{2^k}-1 = (2^{2^{(k-1)}})^2 - 1^2 = (2^{2^{(k-1)}}-1)(2^{2^{(k-1)}}+1) = (F_{k-1}-2)\cdot F_{k-1} = F_0 \cdot F_1 \cdot F_2 \cdot \ldots \cdot F_{k-2} \cdot F_{k-1}$.

Sendo assim, temos, para $n < m$, F_n divide $F_m - 2$. Se um número primo p divide simultaneamente F_n e F_m, ele divide $F_m - 2$ e, portanto, divide o 2. Logo $p = 2$, o que é impossível porque F_m é ímpar.

Concluímos que, da mesma forma que os números de Fermat são infinitos, os números primos também são.

4.6 O TEOREMA DOS NÚMEROS PRIMOS

O matemático alemão Carl Gauss (figura 10) com apenas 15 anos, ao analisar uma tabela de números primos organizada pelo matemático J. H. Lambert, em 1792, desenvolveu um método para encontrar o número de primos existentes abaixo de um dado inteiro x. Sautoy descreve sobre a descoberta de Gauss.

> O grande avanço de Gauss foi fazer uma pergunta diferente. Em vez de tentar prever a localização precisa do próximo primo, ele buscou ao menos descobrir quantos primos haveria entre os primeiros 100 números, os primeiros 1.000 e assim por diante. Se tomássemos o número *N*, haveria alguma maneira de estimar quantos primos encontraríamos entre os números 1 e *N*? Por exemplo, existem 25 primos até o número 100. Portanto, temos uma chance de um em quatro de encontrar um primo se escolhermos um primo aleatório entre 1 e 100. Como se altera essa proporção se buscarmos os primos de 1 a 1.000 ou de 1 a 1.000.000? Armado com tabelas de números primos, Gauss iniciou sua busca. Ao observar a proporção de primos no universo de números, notou o surgimento de um padrão à medida que a contagem se elevava. Apesar da aleatoriedade desses números, parecia ser possível entrever uma regularidade estonteante. Se observarmos a tabela a seguir, que indica a quantidade de primos que encontramos até diversas potências de dez com base em cálculos mais modernos, torna-se fácil perceber essa regularidade (SAUTOY, 2003, p.56 - 57).

Figura 10 – Carl Gauss.

Fonte: Site Wikipédia Artigo Carl Friedrich Gauss (2018)

A tabela 4 apresenta o que foi citado no texto.

Tabela 4 – Número de primos em um intervalo.

N	Número de primos de 1 a N, frequentemente chamado de π(N)	Em média, quantos números precisamos contar até atingir um número primo?
10	4	2,5
100	25	4
1.000	168	6
10.000	1.229	8,1
100.000	9.592	10,4
1.000.000	78.498	12,7
10.000.000	664.579	15,0
100.000.000	5.761.455	17,4
1.000.000.000	50.847.534	19,7
10.000.000.000	455.052.511	22,0

Fonte: Sautoy, 2008, p.57.

A função $\pi(x)$dos números primos representa a quantidade dos números primos

menores ou iguais a x. Para todo $x \geq 0$ e $x \in \mathbb{Z}$ define-se a função $\pi(x)$ por $\pi(x) = \{p \in \mathbb{Z} \mid p \leq x\}$.

Por exemplo, o número de primos menor ou igual a 14 é 6, são eles: 2, 3, 5, 7, 11, 13. Por isso tem-se que, $\pi(14) = 6$. Para valores maiores de x, Gauss constatou que $\pi(x) \sim \frac{x}{lnx}$.

À medida que x tende ao infinito, temos $\lim_{x\to\infty} \frac{\pi(x)}{x/lnx} = 1$.

O Teorema dos Números Primos foi provado, de maneira independente, por Charles de La Vallée Poussin e Jacques Hadamard em 1896 utilizando novos e poderosos métodos analíticos da teoria das variáveis complexas.

4.7 RECORDES

Os maiores números primos encontrados atualmente são os chamados Primos de Mersenne. "Marin Mersenne era um monge francês que não se interessava somente por questões linguísticas. Ele adorava música e foi o primeiro a desenvolver uma teoria coerente sobre os harmônicos. Também adorava os números" (SAUTOY, 2003, p. 48).

Um número que satisfaz a relação $M_p = 2^p - 1$, com p primo, é um número de Mersenne. Entre esses números uns são primos, por exemplo, $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$ outros compostos, como exemplo, $M_{11} = 2047 = 23 \cdot 89$. Paulo Ribenboim afirma que,

> Em 1640, MERSENNE afirmou que M_q era primo para q = 13, 17, 19, 31, 67, 127 e 257; estava ele enganado em relação a 67 e 257; também não incluíra 61, 89 e 107 (entre os inferiores a 257) que também fornecem números de MERSENNE primos. Sua afirmação era extraordinária, em face da grandeza dos números envolvidos (RIBENBOIM, 2012, p.73).

O maior número primo descoberto atualmente no dia 26 de dezembro de 2017 tem mais de 23 milhões de dígitos, mas precisamente 23.249.425 e foi batizado de "$M_{77232917}$". O responsável pela descoberta foi o engenheiro elétrico de 51 anos, Jonathan Pace, morador de uma cidade de 40 mil habitantes no sudeste americano. Jonathan Pace é voluntário de um projeto criado em 1996 representado pela sigla GIMPS, em que o objetivo é a busca por números de Mersenne primos.

A tabela 5 apresenta os maiores números primos conhecidos até hoje em ordem crescente. M_n é um número de Mersenne primo com expoente n. Tabela retirada da Wikipédia.

Tabela 5 – Maiores números primos encontrados atualmente.

(Continua)

Número	Dígitos	Ano em que foi encontrado
M_{127}	39	1876
$180 \cdot (M_{127})^2 + 1$	79	1951
M_{521}	157	1952
M_{607}	183	1952
M_{1279}	386	1952
M_{2203}	664	1952
M_{2281}	687	1952
M_{3217}	969	1957
M_{4423}	1332	1961
M_{9689}	2917	1963
M_{9941}	2993	1963
M_{11213}	3376	1963
M_{19937}	6002	1971
M_{21701}	6533	1978
M_{23209}	6987	1979
M_{44497}	13395	1979
M_{86243}	25962	1982
M_{132049}	39751	1983
M_{216091}	65050	1985
$391581 \cdot 2216193 - 1$	65087	1989
M_{756839}	227832	1992
M_{859433}	258716	1994
$M_{1257787}$	378632	1996
$M_{1398269}$	420921	1996
$M_{2976221}$	895932	1997
$M_{3021377}$	909526	1998
$M_{6972593}$	2098960	1999
$M_{13466917}$	4053946	2001
$M_{20996011}$	6320430	2003
$M_{24036583}$	7235733	2004
$M_{25964951}$	7816230	2005
$M_{30402457}$	9152052	2005
$M_{32582657}$	9808358	2006
$M_{43112609}$	12978189	2008
$M_{57885161}$	17425170	2013
$M_{74207281}$	22338618	2016
$M_{77232917}$	23249425	2017

(Conclusão)

Fonte: Site Wikipédia Maior número primo conhecido (2018)

Os números primos, especialmente os gigantescos, são os principais responsáveis por garantir a segurança da troca de informações pela internet através do algoritmo criptográfico RSA. Quanto maiores forem estes, mais difícil será quebrar o

código. Estas descobertas passam ser uma vantagem não puramente acadêmica, mas com um valor econômico significativo.

No próximo capítulo compreenderemos detalhadamente o sistema RSA, como funciona e sua importância para a segurança da comunicação nos dias atuais.

5 A CRIPTOGRAFIA RSA

Neste capítulo apresentaremos como se obtém as chaves de codificação e decodificação do sistema RSA. Estudaremos como o método funciona e por que é seguro além de conhecer quais os números mais adequados para garantir essa segurança.

5.1 PRÉ-CODIFICAÇÃO

Nesta primeira etapa converteremos as letras em números usando a seguinte tabela de conversão.

Tabela 6 – Conversão de letras em números

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

Fonte: Elaborada pela autora

O número 99 aparecerá representando um espaço entre duas palavras. Cada letra do alfabeto corresponde a um número de dois algarismos. A escolha se dá dessa forma para evitar o seguinte problema. Considere o caso em que A corresponda ao 1, B ao 2, e assim por diante. Nesse caso ao surgir o número 12 teríamos dúvida se corresponderia a AB ou ao L, que é a décima segunda letra do alfabeto.

Usando a tabela de conversão, a frase “MATEMÁTICA NA UECE” é convertida no número 22102914221029181210992310993014121 4.

A seguir devemos escolher dois primos distintos extremamente grandes (geralmente com mais de 100 dígitos), representaremos por p e q. A diferença entre esses números primos não pode ser pequena para que seja difícil e até inviável a fatoração de $n = p \cdot$

q. O valor n é utilizado para codificar e decodificar a mensagem. No nosso caso escolherei primos pequenos somente para ilustrar o método. Suponha $p = 11$, $q = 13$. Assim $n = 11 \cdot 13 = 143$.

Antes de iniciarmos a codificação devemos quebrar a sequência de números em blocos, de maneira que cada bloco produzido seja menor que o número n. Tendo atenção para que os blocos não se iniciem com 0 a fim de evitar problemas no momento da decodificação.

Existem muitas maneiras de separar a mensagem convertida acima em blocos. Uma delas está apresentada a seguir.

22 - 102 - 91 - 42 - 2 - 10 - 29 - 18 - 12 - 109 - 92 - 3 - 10 - 99 - 30 - 14 - 12 - 14

5.2 CODIFICAÇÃO E CHAVE PÚBLICA

Vimos no capítulo anterior que a função φ de Euler para números primos $\varphi(p) = p - 1$. Assim, $\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p - 1) \cdot (q - 1)$.

O próximo passo é escolher um número $e \in \mathbb{Z}$, $1 < e < \varphi(n)$ que seja invertível módulo $\varphi(n)$, ou seja, $(e, \varphi(n)) = 1$.

Seja b um bloco da mensagem convertida, lembre-se que b é menor que n. Definimos por $C(b)$ o bloco codificado. $C(b)$ é o resto da divisão de b^e por n. Logo, $C(b) \equiv b^e \bmod n$. Obtemos assim, a chave de codificação $C(b) = (n, e)$. No exemplo em que estamos considerando temos, $\varphi(n) = 10 \cdot 12 = 120$. Precisamos escolher e de tal forma que $(e, \varphi(n)) = 1$. O menor primo que satisfaz é 7, assim, consideremos $e = 7$.

A tabela a seguir mostra a codificação de todos os blocos. Para o cálculo das congruências a seguir foram usados recursos computacionais algébricos.

Tabela 7 – Codificação da frase - Matemática na UECE

Bloco Numérico Inicial	b^7	$C(b) \equiv b^e \bmod n$	**Bloco Numérico Resultante**
22	22^7	$C(22) \equiv 22^7 \bmod 143$	22
102	102^7	$C(102) \equiv 102^7 \bmod 143$	119
91	91^7	$C(91) \equiv 91^7 \bmod 143$	130
42	42^7	$C(42) \equiv 42^7 \bmod 143$	81
2	2^7	$C(2) \equiv 2^7 \bmod 143$	128
10	10^7	$C(10) \equiv 10^7 \bmod 143$	10
29	29^7	$C(29) \equiv 29^7 \bmod 143$	94

18	18^7	$C(18) \equiv 18^7 \bmod 143$	138
12	12^7	$C(12) \equiv 12^7 \bmod 143$	12
109	109^7	$C(109) \equiv 109^7 \bmod 143$	21
92	92^7	$C(92) \equiv 92^7 \bmod 143$	27
3	3^7	$C(22) \equiv 22^7 \bmod 143$	42
10	10^7	$C(10) \equiv 10^7 \bmod 143$	10
99	99^7	$C(99) \equiv 99^7 \bmod 143$	44
30	30^7	$C(30) \equiv 30^7 \bmod 143$	134
14	14^7	$C(14) \equiv 14^7 \bmod 143$	53
12	12^7	$C(12) \equiv 12^7 \bmod 143$	12
14	14^7	$C(14) \equiv 14^7 \bmod 143$	53

Fonte: Elaborada pela autora

Obtemos as seguintes sequências de blocos.

22 - 119 - 130 - 81 - 128 - 10 - 94 - 138 - 12 - 21 - 27 - 42 - 10 - 44 - 134 - 53 - 12 - 53

5.3 DECODIFICAÇÃO E CHAVE PRIVADA

Para obter a chave de decodificação determinamos $d \in \mathbb{Z}$, $0 < d < \varphi(n)$, tal que $d \cdot e \equiv 1 \bmod \varphi(n)$ ou seja, d é o inverso multiplicativo de e módulo $\varphi(n)$.

Para determinar d usaremos o algoritmo euclidiano estendido. Como $\varphi(143) = 120$ e, $120 = 7 \cdot 17 + 1$, temos, $1 = 120 + 7 \cdot (-17)$, logo o inverso de 7 módulo 120 é -17, precisamos que d seja positivo, assim $d = 120 - 17 = 103$, que é o menor inteiro positivo congruente a -17 módulo 120. Seja a um bloco da mensagem convertida, lembre-se que a é menor que n. Definimos por $D(a)$ o bloco decodificado. $D(a)$ é o resto da divisão de a^d por n. Logo, $D(a) \equiv a^d \bmod n$.

Obtemos assim a chave de decodificação $D(a) = (n, d)$.

Tabela 8 – Decodificação da mensagem da tabela anterior

Bloco Numérico Resultante	$\mathbf{a^{103}}$	$\mathbf{D(a) \equiv a^d \bmod n}$	**Bloco Numérico Inicial**
22	22^{103}	$D(22) \equiv 22^{103} \bmod 143$	22
119	119^{103}	$D(119) \equiv 119^{103} \bmod 143$	102
130	130^{103}	$D(130) \equiv 130^{103} \bmod 143$	91
81	81^{103}	$D(81) \equiv 81^{103} \bmod 143$	42
128	128^{103}	$D(128) \equiv 128^{103} \bmod 143$	2
10	10^{103}	$D(10) \equiv 10^{103} \bmod 143$	10
94	94^{103}	$D(94) \equiv 94^{103} \bmod 143$	29
138	138^{103}	$D(138) \equiv 138^{103} \bmod 143$	18
12	12^{103}	$D(12) \equiv 12^{103} \bmod 143$	12
21	21^{103}	$D(21) \equiv 21^{103} \bmod 143$	109

27	27^{103}	$D(27) \equiv 27^{103} \bmod 143$	92
42	42^{103}	$D(42) \equiv 42^{103} \bmod 143$	3
10	10^{103}	$D(10) \equiv 10^{103} \bmod 143$	10
44	44^{103}	$D(44) \equiv 44^{103} \bmod 143$	99
134	134^{103}	$D(134) \equiv 134^{103} \bmod 143$	30
53	53^{103}	$D(53) \equiv 53^{103} \bmod 143$	14
12	12^{103}	$D(12) \equiv 12^{103} \bmod 143$	12
53	53^{103}	$D(53) \equiv 53^{103} \bmod 143$	14

Fonte: Elaborada pela autora

Organizando os valores encontrados teremos:

22 - 102 - 91 - 42 - 2 - 10 - 29 - 18 - 12 - 109 - 92 - 3 - 10 - 99 - 30 - 14 - 12 - 14

Os organizando novamente, mas, formando blocos com dois algarismos e relacionando os valores encontrados com os da tabela 6 teremos.

Tabela 9 – Relação "frase exemplo" e tabela de conversão

22	10	29	14	22	10	29	18	12	10	99	23	10	99	30	14	12	14
M	A	T	E	M	A	T	I	C	A		N	A		U	E	C	E

Fonte: Elaborada pela autora

Exatamente a frase que havíamos criptografado no início do capítulo. A justificativa explicando matematicamente por que o método funciona, segue no próximo tópico.

5.4 PROVA MATEMÁTICA DE COMO FUNCIONA O SISTEMA RSA

A codificação de cada bloco se dá através da congruência $C(b) \equiv b^e \bmod n$, onde $C(b)$ é um número menor que n. Para decodificar os blocos usamos a congruência $D(a) \equiv a^d \bmod n$, onde $D(a)$ é um número menor que n. Observe também que na etapa de decodificação usamos $a = C(b)$. Assim, $D(a) \equiv a^d \bmod n = D(C(b)) \equiv (C(b))^d \equiv (b^e)^d = b^{e \cdot d} \bmod n$. De onde temos que

$$(C(b)) \equiv b^{e \cdot d} \bmod n. \qquad (5.1)$$

Lembrando que a escolha de d se deu de tal forma que $d \cdot e \equiv 1 \bmod \varphi(n)$, assim, $e \cdot d = 1 + k \cdot \varphi(n)$, $k \in \mathbb{Z}$. Segue que $b^{e \cdot d} = b^{1 + k \cdot \varphi(n)} = b^1 \cdot b^{k \cdot \varphi(n)} = b^1 \cdot b^{k \cdot (p-1)(q-1)} = b^1 \cdot (b^{(p-1)})^{k(q-1)} = b^1 \cdot (b^{(q-1)})^{k(p-1)}$.

Acrescentando essa informação a 5.1 temos, $D(C(b)) \equiv b^{e \cdot d} \equiv b^1 \cdot (b^{(p-1)})^{k(q-1)}$

mod *n*. Ou ainda, $D(C(b)) \equiv b^{e \cdot d} \equiv b^1 \cdot (b^{(q-1)})^{k(p-1)} \mod n$.

Se p divide b temos que $b^{e \cdot d} \equiv b \mod p$. Suponhamos que p não divide b, pelo Pequeno Teorema de Fermat sabemos que, $b^{(p-1)} \equiv 1 \mod p$, daí, $D(C(b)) \equiv b^1 \cdot (b^{(p-1)})^{k(q-1)} \equiv b^1 \cdot 1^{k(q-1)} = b \mod p$.

Analogamente, se q divide b temos que $b^{e \cdot d} \equiv b \mod q$. Suponhamos que q não divide b, pelo Pequeno Teorema de Fermat sabemos que, $b^{(q-1)} \equiv 1 \mod q$, daí, $D(C(b)) \equiv b^1 \cdot (b^{(q-1)})^{k(p-1)} \equiv b^1 \cdot 1^{k(p-1)} = b \mod q$.

Como $(p, q) = 1$, temos pela propriedade 3.8.7. que $D(C(b)) \equiv b \mod p \cdot q$. Concluímos que $D(C(b)) \equiv b \mod n$.

5.5 A SEGURANÇA DO MÉTODO

Vimos que o algoritmo funciona e assim pode ser usado por quem deseja enviar mensagens em segurança, para transações bancárias, entre outros fins. No entanto, não é somente a funcionalidade do sistema que precisa ser garantido. O método tem que ser seguro e confiável.

Algo muito importante na utilização do método é a escolha dos primos p e q.

> Um ponto muito importante refere-se à escolha dos primos p e q. É claro que se forem pequenos, o sistema será fácil de quebrar. Mas não basta escolhê-los grandes. De fato, se p e q são grandes, mas $| p - q |$ é pequeno, então é fácil fatorar $n = p \cdot q$ usando o algoritmo de Fermat (COUTINHO, 2005, p.187).

A seguir o algoritmo de Fermat citado pelo autor.

5.5.1 Algoritmo de Fermat

Existem alguns métodos para fatorar *n*. O algoritmo de Fermat sugere a seguinte estratégia. A ideia do algoritmo é tentar achar números inteiros positivos tais que $n = x^2 - y^2$, que é o mesmo que $n = x^2 - y^2 = (x - y) \cdot (x + y)$. Assim, $(x - y)$ e $(x + y)$ são os fatores de *n*. Representaremos por [r] a parte inteira de r.

Iniciamos supondo que *n* é inteiro positivo e ímpar. E queremos concluir encontrando um fator de *n* ou uma mensagem indicando que *n* é primo. Para isso seguiremos as seguintes etapas:

Etapa 1: Comece com $x = [\sqrt{n}]$; se $n = x^2$ então *x* é um fator de *n* e podemos parar.

Etapa 2: Caso contrário incremente x de uma unidade e calcule $y = \sqrt{(x^2 - n)}$.

Etapa 3: Repita a Etapa 2 até encontrar um valor inteiro para y, ou até que x seja igual a $\frac{(n+1)}{2}$: no primeiro caso n tem fatores $x + y$ e $x - y$ no segundo n é primo.

A seguir um exemplo numérico para ilustrar o método. Seja n = 7081 o número que desejamos fatorar. O primeiro valor de x é a parte inteira da raiz quadrada de n, que nesse caso vale $x = [7081] = 84$. Mas, $84^2 = 7056 < 7081$, assim não podemos parar na primeira etapa.

Vamos para a Etapa 2. Consideramos x o número anterior (84) somado um e substituindo em $y = \sqrt{(x^2 - n)}$ temos, $y = (85^2 - 7081) = 144 = 12$. Encontramos os valores de $x = 85$ e $y = 12$. No caso de não encontrarmos um número inteiro o processo deverá se repetir até encontrar um y que seja pertencente aos inteiros. Nesse caso temos $(x - y) = 85 - 12 = 73$ e $(x + y) = 85 + 12 = 97$, a fatoração de n está completa.

A demonstração do Algoritmo de Fermat pode ser encontrada em Números Inteiros e Criptografia RSA, Coutinho, (2005, p.41).

5.5.2 Fatorando *n* por meio de φ(*n*)

O método a seguir consiste em tomar $n = p \cdot q$, com p, q primos, assim, $\varphi(n) = (p-1)\cdot(q-1)$. Daí vem que $\varphi(n) = p \cdot q + 1 - (p + q) = n + 1 - (p + q)$, assim,

$$(p + q) = n + 1 - \varphi(n). \tag{5.2}$$

Temos também que

$$(p - q)^2 = (p + q)^2 - 4 \cdot p \cdot q. \tag{5.3}$$

Substituindo 5.2 em 5.3 temos que $(p - q)^2 = (n + 1 - \varphi(n))^2 - 4\, p \cdot q$, logo

$$(p - q) = \sqrt{(n + 1 - \varphi(n))^2 - 4\, n}. \tag{5.4}$$

De 5.2 e 5.4 temos que, $p = \frac{n + 1 - \varphi(n) + \sqrt{(n + 1 - \varphi(n))^2 - 4\, n}}{2}$ e temos também que

$q = \frac{n + 1 - \varphi(n) + \sqrt{(n + 1 - \varphi(n))^2 - 4\, n}}{2}$.

Nesse caso os valores de p e q ficam em função de n, que é conhecido, e de $\varphi(n)$ que é desconhecido permanecendo a dificuldade de fatorar n.

Ainda sobre a importância da escolha dos números primos Coutinho ressalta que

> Isso não é papo furado. Em 1995 dois estudantes de uma universidade americana quebraram uma versão do RSA em público. O feito só foi possível porque a escolha

> dos primos usada neste sistema era inteiramente inadequada. Por outro lado, o RSA está em uso há anos e, se os primos forem bem escolhidos, o sistema tem-se mostrado muito seguro. Portanto, uma receita para escolher primos bons é essencial para a "caixa de ferramentas" de qualquer um que deseje programar o RSA (COUTINHO, 2005, p.187).

No sistema RSA são conhecidos o par (n, e), chamados de chave pública e acessível a qualquer usuário. Para quebrar o código precisamos de d, é então que precisamos conhecer $\varphi(n)$ já que d é o inverso multiplicativo de e módulo $\varphi(n)$, mas $\varphi(n)$ também é desconhecido, a menos que consigamos fatorar n descobrindo os valores de p e q, o que se torna muito difícil se n for grande o suficiente, já que não existem até o momento algoritmos rápidos de fatoração, tornando o método de Criptografia RSA seguro.

5.6 ASSINATURAS DIGITAIS INTENSIFICANDO A SEGURANÇA

A assinatura digital surge como uma solução para o seguinte problema. Suponha que uma empresa deseje enviar uma mensagem a um banco e a mensagem será certamente codificada. No entanto, ao recebê-la qual garantia terá o banco de que a mensagem é realmente da empresa e não de um *hacker*, por exemplo? A assinatura digital garante isso.

Funciona assim: sejam C_a e D_a as funções de codificação e decodificação da empresa e C_b e D_b as funções de codificação e decodificação do banco. Seja c um bloco da mensagem que a empresa deseja enviar ao banco. Ao invés de usar a função de codificação do banco, C_b, e enviá-la, a empresa aplica a sua função de decodificação, D_a, a c seguida da função de codificação do banco, C_b. Assim, ao receber a mensagem o banco aplica a sua função de decodificação, D_b, ao resultado aplica a função de codificação da empresa, C_a, para obter c que é a mensagem original.

Resumindo para codificar $C_b(D_a(c))$, para decodificar D_b seguido de C_a. Desse modo o banco pode ter certeza que a mensagem foi enviada pela empresa, já que D_a só é conhecido por ela.

As assinaturas digitais merecem atenção para não tornarem vulnerável o sistema RSA. Sobre isso Coutinho descreve um caso onde as mensagens assinadas e o tempo que o sistema leva para confirmar a assinatura ajudaram a quebrar um código RSA.

> Recentemente descobriu-se que o uso pouco cuidadoso da técnica de autenticação de assinaturas torna vulneráveis certos métodos de chave pública como o RSA. No final de 1995, um consultor em assuntos de segurança de computadores (mas formado em biologia!) descobriu que é possível usar o sistema de assinaturas para quebrar o RSA. O método consiste em enviar uma mensagem assinada e marcar o tempo que o sistema leva para confirmar a assinatura. Fazendo isto para mensagens de tamanhos ligeiramente diferentes, é possível obter informações suficientes para encontrar a

> chave de decodificação do sistema RSA que esteja sendo usado. Portanto, a segurança do RSA não depende exclusivamente da nossa capacidade de inventar novos algoritmos de fatoração. Há muitos outros fatores importantes, que não têm um caráter puramente matemático (COUTINHO, 2005, p. 190).

A criptografia RSA tem possibilitado uma comunicação segura e acessível a todas as pessoas que dela desejarem fazer uso, como antes sonhado por Diffie. Pessoas que nada entendem de criptografia fazem uso e confiam na segurança dos seus diálogos nas redes sociais, o que é possível graças ao sistema RSA. A conquista do método RSA é citada por Singh.

> Durante dois mil anos os criadores de códigos lutaram para preservar seus segredos enquanto os decifradores de códigos faziam o possível para descobri-los. Esta sempre foi uma corrida apertada, com os decifradores contra-atacando sempre que os criadores de códigos pareciam estar ganhando, e estes inventando novas formas de cifragem, mais poderosas, quando os métodos anteriores não eram mais confiáveis. A invenção da criptografia de chave pública e o debate político que cerca o uso da criptografia mais forte nos leva aos dias de hoje, e está claro que os criptógrafos estão vencendo a guerra da informação (SINGH, 2005, p. 345).

Uma vitória que depende dos números primos e da dificuldade do surgimento de um padrão que localize esses números.

Vimos que a criptografia RSA está diariamente em nossa vida, através de nossas comunicações, transações bancárias ou para outros fins e dependemos dela para garantir a segurança em cada uma dessas ações. Por esse motivo, é interessante o conhecimento desse tipo de criptografia por todos que dela fazem uso.

Buscando suprir essa necessidade o próximo capítulo apresenta sugestões de como introduzir este conceito em sala de aula.

6 A CRIPTOGRAFIA RSA APLICADA EM SALA DE AULA

Este capítulo é dedicado a aplicação de atividades sobre a Criptografia RSA em sala de aula, apresentando aos alunos o contexto histórico, revisando conceitos e informando onde é usada e como essa forma de criptografia é importante para a segurança na troca de informações hoje em dia.

6.1 ESTRUTURA DO CAPÍTULO

São apresentadas sugestões de 7 aulas de 50 minutos distribuídas em 4 planos. O plano é flexível e o professor deve adequá-lo de acordo com a realidade da escola e o nível de aprendizagem dos alunos.

Antes de iniciar as aulas o professor deverá solicitar dos alunos que instalem em seus notebooks ou laptop um software matemático, neste trabalho a sugestão é que faça a utilização do programa MAXIMA[2], onde os alunos possam fazer uso do celular para baixar o aplicativo Maxima on Android, solicitar que levem esses dispositivos no dia da aula. Outra sugestão é baixar a versão do programa no laboratório de Informática da escola e levar os alunos até esse ambiente.

A aula 1 seção 6.2.1é dedicada à apresentação da criptografia RSA, destacando sua importância para a segurança nas comunicações pela internet e em transações bancárias. É necessário relembrar o conceito de números primos e sua infinitude, além de mostrar que o sistema se afirma na dificuldade em encontrar uma regularidade para o surgimento desses números. No decorrer da aula é sugerido que os alunos realizem uma troca de mensagem secreta

[2] O programa MAXIMA pode ser baixado gratuitamente, a versão usada foi a 5.41.0. Existe um tutorial em http://maxima.sourceforge.net.

usando o Sistema RSA. Embora não conheçam detalhadamente os passos da criptografia RSA podem fazer uso, como citado acima, do programa MAXIMA.

A sugestão de iniciar demonstrando o funcionamento do método busca despertar a curiosidade do aluno em criptografar e descriptografar a mensagem. Nas aulas seguintes serão apresentados os conteúdos matemáticos que tornam possível essa forma de criptografia e a descrição detalhada do funcionamento do sistema RSA.

A aula 2 seção 6.2.2 é dedicada a descrever os conceitos matemáticos envolvidos na troca de mensagem realizada nas primeiras aulas. Iniciando com o conceito que torna possível a codificação e faz com que a decodificação chegue ao texto original.

A aula 3 seção 6.2.3 é dedicada a apresentar algumas propriedades do conjunto dos inteiros que tornam possível a Criptografia RSA.

Concluiremos as aulas sobre Criptografia RSA com a demonstração do seu funcionamento descrito no Capítulo 5, tópico 5.4. Na aula 4 seção 6.2.4 optei por não apresentar a função φ de Euler, em seu lugar, neste caso, o professor pode usar $(p-1)\cdot(q-1)$, sendo p e q os primos escolhidos, juntamente com o Pequeno Teorema de Fermat são suficientes para a demonstração.

6.2 PLANOS DE AULA

6.2.1 Aula 01

Série: 3ª série / Ensino Médio
Disciplina: Matemática
Tema: Uma troca de mensagens secretas através da Criptografia RSA.
Pré -requisito: Divisibilidade, Máximo Divisor Comum, Múltiplos, Números Primos e Coprimos e noções de computação.
Duração: 100 minutos (2 aulas de 50 minutos)
01 - Objetivo(s)

- Conhecer a importância da Criptografia RSA na atualidade;
- Recordar o conceito de números primos e discutir sua infinitude;
- Motivar os alunos através da troca de informações secretas usando números;
- Propiciar aos alunos uma troca de mensagens usando a Criptografia RSA.

02 - Conteúdo(s)

- A importância da Criptografia RSA na atualidade;

- Números Primos;
- Troca de mensagens usando o Sistema RSA.

03 – Desenvolvimento

- Fazer uma breve apresentação da importância da Criptografia RSA na atualidade destacando, mesmo que de forma superficial, o que é criptografia, o significado da sigla RSA, o que a diferencia das demais formas de criptografia e destacar onde é usada essa segurança;
- Revisar o conceito de números primos apresentando em slide o crivo de Eratóstenes, tabela 2, capítulo 4, e explicar como o crivo foi construído;
- Dividir a sala em dois grupos com a mesma quantidade de alunos, os que irão receber as mensagens e os que irão enviá-la;
- Realizar uma troca de mensagem usando a Criptografia RSA, seguindo os passos apresentados no APÊNDICE A com o auxilio do instrumental sugerido no APÊNDICE B.

04 – Materiais necessários

- Data show;
- Celulares;
- Pincel;
- Caderno;
- Lápis;
- Borracha.

05 - Avaliação

05 - Avaliação

Avaliar se os objetivos foram atingidos, as dificuldades encontradas pelos alunos, o envolvimento e a empolgação em enviar e receber uma mensagem criptografada.

06 - Sugestão de mídia Portal da Matemática OBMEP. Vídeo aulas:

- Aritmética – Aula 64 - Introdução a criptografia;
- Aritmética – Aula 65 - Apresentação do método RSA;
- Aritmética – Aula 66 - Codificando uma mensagem;
- Aritmética – Aula 67 - Decodificando uma mensagem.

Link[3]

07 - Fontes

- Livro, Números Inteiros e Criptografia RSA, S. C. Coutinho.

[3] https://portaldosaber.obmep.org.br/index.php/modulo/ver?modulo=81

- Livro, O Fascínio dos Números Primos, Jucimar Peruzzo.

6.2.2 Aula 02

Série: 3ª série / Ensino Médio

Disciplina: Matemática

Tema: Congruência, a Aritmética do Relógio.

Pré-requisito: Noções de Divisão Euclidiana. Duração: 100 minutos (2 aulas de 50 minutos)

01- Objetivo(s)

- Compreender o conceito de Congruência;
- Conhecer as propriedades de reflexão, simetria e transitividade em Congruência;
- Definir a existência ou não de inversos modulares.

02 - Conteúdo(s)

- Congruência;
- Inversos modulares.

03 - Desenvolvimento

- Definir o conceito de congruência apresentando fenômenos periódicos comuns, como os dias da semana, meses do ano, as horas em relógio entre outros. Em seguida, apresentar as propriedades do Capítulo 3 tópico 3.8;
- Definição de Inversos Modulares e demonstração de exemplos;
- Solicitar a resolução dos Exercícios no Anexo A.1.

04 - Materiais necessários

- Data show;
- Pincel;
- Caderno;
- Lápis;
- Borracha.

05 - Avaliação

Avaliar se os objetivos foram atingidos retirando as dúvidas ainda existentes.

06 - Sugestão de mídia Portal da Matemática OBMEP. Vídeo aulas:

- Aritmética - Aula 42 - 6 + 7 = 1. Aritmética modular;
- Aritmética - Aula 44 - Cuidado! Cortes nem sempre valem em congruências. Classe inversa módulo n;
- Aritmética - Aula 45 - Tabelas de multiplicação da Aritmética Modular;

- Aritmética - Aula 46 - Existência de inverso módulo n;
- Aritmética - Aula 47 - Caso em que vale a lei do corte;
- Aritmética - Aula 48 - Unicidade da classe inversa.

Link[4].

07 – Fontes

- Livro Aritmética, Abramo Hefez;
- Criptografia, S. C. Coutinho. Estilo OBMEP.

6.2.2 Aula 03

Série: 3ª série / Ensino Médio

Disciplina: Matemática

Tema: O Teorema Fundamental da Aritmética e o Pequeno Teorema de Fermat.

Pré-requisito: Números Primos, Propriedades das Potências e o Conceito de Fatorial.

Duração: 100 minutos (2 aulas de 50 minutos)

01 - Objetivo(s)

- Enunciar o princípio de Indução Finita;
- Apresentar o Teorema Fundamental da Aritmética;
- Provar o Pequeno Teorema de Fermat.

02 - Conteúdo(s)

- Princípio de Indução Finita;
- Teorema Fundamental da Aritmética;
- Pequeno Teorema de Fermat.

03 - Desenvolvimento

- Enunciar o Princípio de Indução Finita usando como base o Capítulo 3, tópico 3.3.1.
- Relembrar o conceito de número primo definido na AULA 01 e enunciar o Teorema Fundamental da Aritmética usando como base o Capítulo 4, tópico 4.2;
- Apresentar o Pequeno Teorema de Fermat descrito no capítulo 4, teorema 10 e mostrar exemplos.
- Solicitar a resolução dos exercícios no ANEXO A.2.

04 - Materiais necessários

- Data show;
- Pincel;

[4] https://portaldosaber.obmep.org.br/index.php/modulo/ver?modulo=63

- Caderno;
- Lápis;
- Borracha.

05 - Avaliação

Avaliar se os objetivos foram atingidos, a participação e o interesse dos alunos nas aulas.

06 - Sugestão de mídia Portal da Matemática OBMEP.Vídeo aula:

- Indução Matemática - Aula 1 - Princípio de Indução Matemática.

Link[5].

Portal da Matemática OBMEP. Vídeo aula:

- Aritmética - Aula 10 - Números primos - Teorema Fundamental da Aritmética; Link[6].

  Portal da Matemática OBMEP. Vídeo aula:

- Aritmética - Aula 54 - Pequeno Teorema de Fermat.

  Link[7].

07 - Fontes

- Teoria dos Números, Rubens Vilhena Fonseca.

6.2.4 Aula 04

Série: 3ª série / Ensino Médio

Disciplina: Matemática

Tema: Como funciona o Sistema RSA.

Pré-requisito: As aulas anteriores.

Duração: 50 minutos

01- Objetivo(s)

- Estudar como o Sistema RSA funciona.

02- Conteúdo(s)

- O Sistema RSA.

03 - Desenvolvimento

- Apresentar a demonstração do capítulo 5.4.

04- Materiais necessários

[5] https://portaldosaber.obmep.org.br/index.php/modulo/ver?modulo=48
[6] https://portaldosaber.obmep.org.br/index.php/modulo/ver?modulo=52
[7] https://portaldosaber.obmep.org.br/index.php/modulo/ver?modulo=63

- Data show;
- Quadro;
- Pincel.

05- Avaliação

Observar se os objetivos foram alcançados.

06- Sugestão de mídia Portal da Matemática OBMEP. Vídeo aula:

- Aritmética - Aula 69 – Por que o método de criptografia RSA funciona.

Link[8].

07- Fontes

- Livro, Números Inteiros e Criptografia RSA, S. C. Coutinho

[8] https://portaldosaber.obmep.org.br/index.php/modulo/ver?modulo=81

7 CONCLUSÃO

Muitos dos conceitos apresentados neste trabalho são conhecidos pelos alunos desde os anos iniciais de estudo como, por exemplo, divisibilidade, máximo divisor comum e mínimo múltiplo comum. O professor de Matemática que busca associar os conteúdos da disciplina a fatos reais do dia a dia tem a oportunidade na Criptografia RSA de debater um tema atual e presente no cotidiano de quem faz uso da internet.

Respondendo as questões iniciais que nortearam o trabalho, vimos no capítulo 6 que é possível aplicar a Criptografia RSA em sala de aula nos anos finais do Ensino Médio com pequenas adaptações e a utilização de um software matemático para a codificação e decodificação, visto que a matemática usada para aplicação do método RSA pode ser compreendida e demonstrada nessa série de ensino. O outro questionamento é relacionado à relevância de conhecermos o método que garante a segurança das comunicações na rede, o método RSA. Embora não seja de caráter obrigatório aos usuários de internet conhecê-lo, este se torna importante, pois, através da matemática que se constrói o método é possível provar sua segurança, o que dará ao usuário maior confiabilidade no uso da internet.

No decorrer do trabalho foi demonstrada a importância dos números primos para a criptografia RSA. Multiplicá-los é uma tarefa considerada "fácil" já o processo inverso, a fatoração, é bem mais difícil, até mesmo para o cálculo com o auxílio de computadores. Pois quanto maior forem os números escolhidos, mais difícil será determinar os primos envolvidos.

Durante o trabalho conhecemos a matemática envolvida na criptografia RSA, o contexto histórico, conceitos matemáticos e teoremas que a tornam possível. Vimos que todos os números ou são primos ou podem ser fatorados em um produto de primos através do Teorema Fundamental da Aritmética. Ainda sobre os números primos conhecemos várias propriedades como Teorema de Euler, Pequeno Teorema de Fermat e o Teorema de Wilson. Estas são importantes na Criptografia RSA para que a decodificação chegue à mensagem original. Vimos também que existem infinitos números primos, conhecemos os recordes mais recentes e o maior deles, descoberto no dia 26 de dezembro de 2017 com mais de 23 milhões de dígitos. Ressaltando que os maiores primos conhecidos atualmente são os Primos de Mersenne da forma $2^p - 1$, com p primo.

Uma mensagem que será codificada no sistema RSA percorrerá as seguintes fases; pré-codificação, onde associamos o alfabeto a uma tabela de conversão e a codificação, onde é usada a chave pública e a aritmética modular para transformar os números da tabela iniciais

em outros. Quem receber a mensagem irá decodificá-la usando também a aritmética modular inversa a usada para codificar e chegará à mensagem inicial. Verdadeiramente o método tem base matemática que assegura voltar à mensagem original e estar feita no capítulo 5 seção 5.4. Quanto à segurança tivemos conhecimento que devem ser tomados alguns cuidados em relação à escolha dos números primos. Mas se forem escolhidos números grandes em que a diferença entre eles não seja pequena o método se torna seguro por não existir métodos rápidos de fatoração.

No último capítulo foi apresentada uma proposta didática visando à aplicação em sala de aula dos conteúdos, conceitos e aplicações estudados ao longo dessa dissertação para alunos do ensino médio, mas especificamente para a 3ª série, com o intuito de despertar o interesse em aprender matemática debatendo um tema atual através de uma abordagem experimental, colocando o aluno para construir o conhecimento através da vivência de uma troca de mensagem secreta.

A matemática que envolve a Criptografia RSA surge como opção para revisar assuntos importantes que estão no currículo da educação básica, como por exemplo, o conceito de divisibilidade, números primos e o teorema fundamental da aritmética. É também uma oportunidade para apresentar o conceito de congruência e suas propriedades. Através das aulas sugeridas no trabalho o aluno pode perceber a importância da matemática para a nossa realidade, possibilitando e garantido a segurança das comunicações pela internet.

Conhecer e entender o conteúdo apresentado neste trabalho nos mostra o quanto a matemática facilita diariamente a vida de quem necessita fazer uso da internet, possibilitando a troca de informações e garantindo a segurança. Não sabemos até quando a Criptografia RSA será considerada um método seguro, mas são notáveis as possibilidades que ela proporciona a nossa geração.

REFERÊNCIAS

COUTINHO, S. C. **Números inteiros e Criptografia RSA, Série de Computação e Matemática.** 2. ed. Rio de Janeiro: IMPA, 2005.

COUTINHO, S. **Criptografia, Estilo OBMEP.** Rio de Janeiro: IMPA, 2016.

DIFFIE, Whitfield. **WIKIPÉDIA, a enciclopédia livre**. Flórida: Wikimedia Foundation, 2017. Disponível em:<https://pt.wikipedia.org/w/index.php?title=Whitfield_ Diffie&oldid=50826860>. Acesso em: 25 maio 2018.

EUCLIDES. **WIKIPÉDIA, a enciclopédia livre**. Flórida: Wikimedia Foundation, 2018. Disponível em:<https://pt.wikipedia.org/w/index.php?title=Euclides&oldid=52130087>. Acesso em: 25 maio 2018.

FONSECA, Rubens V. **Teoria dos números**. Belém: UEPA, 2011.

GAUSS, Carl Friedrich. **WIKIPÉDIA, a enciclopédia livre**. Flórida: Wikimedia Foundation, 2018. Disponível em:<https://pt.wikipedia.org/w/index.php?title=Carl_Friedrich_ Gauss&oldid=51949644>. Acesso em: 25 maio 2018.

GOMES, Helton S. Brasil tem 116 milhões de pessoas conectadas à internet, diz IBGE. **G1.globo**. 21 fev. 2018. Disponível em:<https://g1.globo.com/economia/tecnologia/noticia/ brasil-tem-116-milhoes-de-pessoas-conectadas-a-internet-diz-ibge.ghtml>. Acesso em: 12 maio 2018.

HEFEZ, A. **Aritmética.** 2. ed. Rio de Janeiro: SBM, 2016.

HEFEZ, A. **Iniciação à Aritmética**. Rio de Janeiro: IMPA, 2015.

LAGRANGE, Joseph-Louis. **WIKIPÉDIA, a enciclopédia livre**. Flórida: Wikimedia Foundation, 2018. Disponível em:<https://pt.wikipedia.org/w/index.php?title=Joseph-Louis_ Lagrange&oldid=52106723>. Acesso em: 25 maio 2018.

WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2018. Disponível em: < https://pt.wikipedia.org/wiki/Maior_n%C3%BAmero_primo_conhecido> Acesso em: 25 maio 2018.

HELLMAN, Martin. **In: WIKIPÉDIA, a enciclopédia livre**. Flórida: Wikimedia Foundation, 2017. Disponível em:<https://pt.wikipedia.org/w/index.php?title=Martin_ Hellman&oldid=49854407>. Acesso em: 25 maio 2018.

MERKLE, Ralph. **Ralph Merkle**. Disponível em: <http://www.merkle.com/>.Acesso em: 25 maio 2018.

MIRANDA, J. **Leonhard Euler**. Grupo escolar. Disponível em:<https://www.grupoescolar. com/pesquisa/leonhard-euler.html>Acesso em: 25 maio 2018.

NARDO, Claudio Di. **Rivest Shamir Adleman, também conhecido como "A (in) solidão dos números primos"**. 2013. Disponível em:<https://claudiodinardo.com/2013/ 11/14/rivest-shamir-adleman-aka-the-in-solitude-of-prime-numbers/>. Acesso em: 25 maio 2018.

PERUZZO, Jucimar. **O Fascínio dos Números Primos**. Irani, SC: [s.n.], 2012.

FERMAT, Pierre de. **WIKIPÉDIA, a enciclopédia livre**. Flórida: Wikimedia Foundation, 2017. Disponível em:<https://pt.wikipedia.org/w/index.php?title=Pierre_de_ Fermat&oldid=49076253>. Acesso em: 25 maio 2018.

RIBENBOIM, P. **Números primos:** Velhos Mistérios e Novos Recordes. Rio de Janeiro: IMPA, 2012. (Coleção Matemética Universitária)

SAUTOY, Marcus du. **A música dos números primos:** a história de um problema não resolvido na matemática. tradução de Diego Alfaro. Rio de Janeiro: Jorge Zahar, 2008.

SINGH, Simon. **O livro dos códigos:** A ciência do sigilo - do antigo Egito à criptografia quântica, tradução de Jorge Calife. 5. ed. Rio de Janeiro: Record, 2005.

VIEIRA, Eziel. **Biografia de Eratóstenes Bibliografias e Curiosidades.** 2013.<http: //biografiaecuriosidade.blogspot.com.br/2013/09/biografia-de-eratostenes.html>. Acesso em: 28 maio 2018.

APÊNDICES

APÊNDICE A – Troca de mensagem em sala de aula

A.1 Primeira responsabilidade de quem vai receber a mensagem

1º Cada aluno escolhe dois números primos, de forma secreta, e os multiplica. Sejam p e q os primos escolhidos. Chamaremos de n o produto entre p e q. (Sugerir aos alunos que a princípio escolham números pequenos.)
2º Subtrai o número 1 de cada número primo e os multiplica também de forma secreta. Chamaremos o resultado de $\varphi(n)$. (Os passos 1 e 2 podem ser feitos sem o auxílio da calculadora MAXIMA. Caso desejem usá-la é possível encontrar o produto com o comando $(*)$, assim o valor de n no 1º passo é obtido fazendo $p * q$.)
3º Cada aluno deve escolher um número que seja primo com o número encontrado no 2º passo. Chamaremos de (e) este número. (Como sugestão usar o programa MAXIMA para fatorar $\varphi(n)$ usando o comando factor($\varphi(n)$) e escolher o menor primo que não faz parte dessa fatoração.)
4º Destacar em uma tabela o número escolhido no 3º passo (e), o produto encontrado no 1º passo (n) e o nome do aluno, de forma que seja acessível a todos da sala. Formando o par (n, e). (Nesse momento é importante que o professor explique aos alunos que formamos a chave pública.)

A.2 Responsabilidade de quem vai enviar a mensagem

5º Cada aluno escolhe um colega para enviar uma mensagem. O professor deve conduzir de forma que haja uma conexão biunívoca entre quem vai enviar e quem vai receber a mensagem.
6º Escrever a mensagem. (Sugerir uma mensagem curta, como por exemplo; Bom dia! Ti amo! Atacar! Venha!)
7º Converter a mensagem escrita anteriormente de acordo com a tabela 5.1 do Capítulo 5.
8º Localizar a chave do colega para quem deseja enviar a mensagem.
9º Dividi-la em blocos de acordo com as orientações da seção 5.1 capítulo 5. Chamaremos cada bloco de (b).
10º Calcular o resto da divisão de b^e por n. É possível encontrar o resultado usando o MAXIMA com o código (mod (b^e, n). Fazer todos os blocos. Encontramos novos blocos, chamaremos de (a).

11º Enviar.

A.3 Segunda responsabilidade de quem vai receber a mensagem

(Ao recebermos a mensagem codificada estamos curiosos para saber o que nos foi enviado. Chegou o momento de decodificar!)

12º Para descobrir precisamos de um novo número, que chamaremos de (d). Para encontrá-lo usaremos o programa MAXIMA e o código (inv_mod (e, $\varphi(n)$)).

13º Calcular o resto da divisão de a^d por n. Mais uma vez usaremos o MAXIMA com o código (mod ($a\hat{}d$, n)). Fazer todos os blocos. Os números que encontramos devemos separá-los de dois em dois algarismos.

14º Associar o resultado à tabela de conversão 5.1 do Capítulo 5.

APÊNDICE B – Instrumental para aplicação da troca de mensagens em sala de aula usando o sistema rsa

B.1 Primeira responsabilidade de quem vai receber a mensagem

1º $n = p \cdot q =$ _____

2º $\varphi(n) = (p-1) \cdot (q-1) =$ _____ factor($\varphi(n)$). _____

3º $e =$ _____

4º (n, e) = _____

B.1.2 Responsabilidade de quem vai enviar a mensagem

5º O nome da pessoa para quem deseja enviar a mensagem _____

6º Mensagem _____

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

Escrever a frase convertida aqui _____

8º Chave pública do colega $(n, e) =$ _____

9º Dividir a mensagem em blocos _____

10º (mod (b^e, n). _____

11º Enviar

B.3 Segunda responsabilidade de quem vai receber a mensagem

12º $d =$ inv_mod $(e, \varphi(n)) =$ _____

13º mod $(a\hat{}d, n)$ _____

14º Escrever os números encontrados no 13º ponto em blocos de dois algarismos. _____

Associar à tabela de conversão do 7º ponto. Escrever a frase _____

ANEXOS

ANEXO A – Sugestões de atividades

Sugestão de atividades sobre os temas em estudo. Foi usado como referência para as questões a seguir o material didático encontrado no Portal da Obmep > Módulos > Tópicos adicionais > Aritmética dos Restos: Divisibilidade e resto e Aritmética Modular > Caderno de exercícios.

A. 1 Aritmética dos restos e divisibilidade

1. Em cada item, encontre o menor inteiro positivo x que satisfaz as congruências:
   (a) $x \equiv -5 \bmod 7$.
   (b) $x \equiv -3 \bmod 11$.
   (c) $x \equiv -1 \bmod 13$.
2. Encontre o resto de $100 \cdot 103 \cdot 104$ na divisão por 7.
3. Encontre o resto de $100^2 \cdot 102$ na divisão por 9.
4. Encontre o resto da divisão do número
   (a) $101 \cdot 102 \cdot 103 + 1$ na divisão por 4.
   (b) $73 \cdot 74 \cdot 75 + 2$ na divisão por 4.
5. Observe os restos das potências de 2 na divisão por 3:

	2^0	2^1	2^2	2^3
Resto	1	2	1	2
	2^4	2^5	2^6	2^7
Resto	1	2	1	2

   (a) Seguindo o padrão da tabela, qual deve ser o resto de 2^{2016} na divisão por 3?
   (b) Verifique que $2^{2k} \equiv 1 \bmod 3$ e que $2^{2k+1} \equiv 2 \bmod 3$ para todo k inteiro não negativo.
6. Se n é ímpar, qual o resto de n^2 por 8?
7. Se n é ímpar, qual o resto de $9n^2 + 3$ por 8?
8. Determine o resto na divisão por 8 do número $1^2 + 3^2 + 5^2 + 7^2 + \ldots 99^2$.
9. Determine o inverso de 11 nos seguintes módulos: 3, 5, 7 e 9.
10. Calcule o resto de 4^{100} por 5.

A.2 Teorema Fundamental da Aritmética e o Pequeno Teorema de Fermat

1. Encontre os restos da divisão de 2^{24} por

   (a) 5.

   (b) 7.

   (c)11.

   (d) 17.

2. Determine o resto de 2^{24} na divisão por 15.

Dica: Perceba que 15 = 3 · 5 e aplique o Teorema de Fermat para cada um desses primos.

3. Encontre o resto da divisão de $300^{3000} - 1$ por 1001.

4. Prove que $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ é um inteiro para todo inteiro n.

5. Verifique se o número 329 é primo.

6. Decomponha os números em fatores primos:

   (a) 180

   (b) 220

   (c) 4225

   (d) 5040

7. Indique o número cuja fatoração é:

   (a) 2 · 3 · 3 · 5

   (b) 2 · 2 · 3 · 7

   (c) 2 · 3 · 5 · 11

   (d) 5 · 5 · 11 · 13

ANEXO B – Respostas e soluções

B.1 Aritmética dos Restos e Divisibilidade

1.

(a) $x = 2$.

(b) $x = 8$.

(c) $x = 12$.

2. Como $100 \equiv 2 \bmod 7$, segue que $100 \cdot 103 \cdot 104 \equiv 2 \cdot 5 \cdot 6 \bmod 7 \equiv 60 \bmod 7 \equiv 4 \bmod 7$. Portanto, o resto é 4.

3. Como $100 \equiv 1 \bmod 9$, segue que $100^2 \cdot 102 \equiv 1^2 \cdot 3 \bmod 9 \equiv 3 \bmod 9$. Portanto, o resto é 3.

4.

(a) Como 101 deixa resto 1 na divisão por 4, segue que $101 \cdot 102 \cdot 103 + 1$ deixa o mesmo resto que $1 \cdot 2 \cdot 3 + 1 = 7$, ou seja, deixa resto 3 na divisão por 4.

(b) Como 73 deixa resto 1 na divisão por 4, segue que $73 \cdot 74 \cdot 75 + 2$ deixa o mesmo resto que $1 \cdot 2 \cdot 3 + 2 = 8$, ou seja, deixa resto 0 na divisão por 4.

5.

(a) Seguindo a tabela anterior, potências de 2 com expoente par sempre deixam resto 1 na divisão por 3. Portanto, caso o padrão seja mantido, 2^{2016} deve deixar resto 1 na divisão por 3.

(b) Como $2^2 \equiv 1 \bmod 3$, elevando ambos os lados da congruência a potência k, temos $2^{2k} = (2^2)^k \equiv 1^k = 1 \bmod 3$. Além disso, multiplicando a última congruência por 2, obtemos: $2 \cdot 2^{2k} \equiv 2 \cdot 1 \bmod 3$, daí, $2^{2k+1} \equiv 2 \bmod 3$.

6. Se n é ímpar, podemos escrever $n = 2k + 1$. Portanto, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$. Como $k(k+1)$ é o produto de dois números consecutivos, segue que $k(k+1)$ é par. Logo, $4k(k + 1)$ é múltiplo de 8 e n^2 deixa resto 1.

7. Sabemos que se n é ímpar, então n^2 deixa resto 1 por 8. Portanto, $9n^2 + 3$ deixa o mesmo resto que $9 \cdot 1 + 3 = 12 = 8 \cdot 1 + 4$ na divisão por 8. Consequentemente, o resto procurado é 4.

8. Como o quadrado de um inteiro ímpar deixa resto 1 na divisão por 8 e a soma dada possui 50 termos, o resto procurado é igual ao resto de $50 \cdot 1 = 6 \cdot 8 + 2$ por 8. Portanto, a resposta é 2.

9. Pelo Algoritmo de Euclides Estendido, como mdc (11, 3) = 1, podemos encontrar a combinação linear $11 \cdot 2 + 3 \cdot (-7) = 1$. Daí, $11 \cdot 2 \equiv 1 \bmod 3$. Procedendo de forma análoga, podemos encontrar $11 \cdot 1 \equiv 1 \bmod 5$, $11 \cdot 2 \equiv 1 \bmod 7$, $11 \cdot 5 \equiv 1 \bmod 9$.

10. Como $4 \equiv -1 \bmod 5$, temos $4^{100} \equiv (-1)^{100} = 1 \bmod 5$.

B.2 Teorema Fundamental da Aritmética e o Pequeno Teorema de Fermat

1. Como 2 é relativamente primo com todos os divisores mencionados, podemos usar o Pequeno Teorema de Fermat em todos os itens, obtendo:

   (a) $2^{(5-1)} \equiv 1 \bmod 5$, daí, $(2^4)^6 \equiv 1^6 \bmod 5$, logo, $2^{24} \equiv 1 \bmod 5$. Portanto, o resto é 1.

   (b) $2^{(7-1)} \equiv 1 \bmod 7$, daí, $(2^6)^4 \equiv 1^4 \bmod 7$, logo, $2^{24} \equiv 1 \bmod 7$. Portanto, o resto é 1.

   (c) $2^{(11-1)} \equiv 1 \bmod 11$, daí, $(2^{10})^2 \equiv 1^2 \bmod 11$, assim, $2^{20} \equiv 1 \bmod 11$, daí, $2^{20} \cdot 2^4 \equiv 1 \cdot 16 \bmod 11$, logo, $2^{24} \equiv 5 \bmod 11$. Portanto, o resto é 5.

   (d) $2^{(17-1)} \equiv 1 \bmod 17$, daí, $(2^{16}) \cdot 2^4 \cdot 2^4 \equiv 1 \cdot (-1) \cdot (-1) \bmod 17$, logo, $2^{24} \equiv 1 \bmod 17$. Portanto, o resto é 1.

2. Como $2^{(3-1)} \equiv 1 \bmod 3$ e $2^{(5-1)} \equiv 1 \bmod 5$, segue que $2^{24} = (2^2)^{12} \equiv 1^{12} \equiv 1 \bmod$

3. E, ainda, $2^{24} = (2^4)^6 \equiv 1^6 \equiv 1 \bmod 5$. Portanto, $2^{24} - 1$ e múltiplo de 3 e 5. Como mdc(3, 5) = 1, segue que $15 \mid (2^{24} - 1)$ e o resto é 1.

4. Primeiramente note que $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15} = \frac{3n^5 + 5n^3 + 7n}{15}$. Como mdc(3, 5) = 1, basta mostrarmos que o numerador é múltiplo de 3 e 5. Pelo teorema de Fermat $3n^5 + 5n^3 + 7n \equiv 5n^3 + 7n \equiv 5n + 7n \equiv 12n \equiv 0 \bmod 3$. E, ainda, $3n^5 + 5n^3 + 7n \equiv 3n^5 + 7n \equiv 3n + 7n \equiv 10n \equiv 0 \bmod 5$.

5. Não é primo, $7 \cdot 47$.

6.

   (a) $2^2 \cdot 3^2 \cdot 5$.

   (b) $2^2 \cdot 5 \cdot 11$.

   (c) $5^2 \cdot 13^2$.

   (d) $2^4 \cdot 3^2 \cdot 5 \cdot 7$.

7.

   (a) 90.

(b) 84.

(c) 330.

(d) 3575.