



Universidade Federal de Goiás
Instituto de Matemática e Estatística
Programa de Mestrado Profissional em
Matemática em Rede Nacional



CRIPTOGRAFIA

Tulio Fernando da Mata

Goiânia

2015

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR AS TESES E DISSERTAÇÕES ELETRÔNICAS (TEDE) NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou *download*, a título de divulgação da produção científica brasileira, a partir desta data.

1. Identificação do material bibliográfico: **Dissertação** **Tese**

2. Identificação da Tese ou Dissertação

Autor (a):	Tulio Fernando da Mata		
E-mail:	Prof.mat.tulio@gmail.com		
Seu e-mail pode ser disponibilizado na página?	<input checked="" type="checkbox"/> Sim	<input type="checkbox"/> Não	
Vínculo empregatício do autor	Mestrando Bolsista e Professor De matemática		
Agência de fomento:	Coord. de Aperf. Pessoal de Nível Superior Sec. de Educação do Estado de Goiás	Sigla:	CAPES SEDUC
País:	Brasil	UF:	GO
		CNPJ:	
Título:	Criptografia		
Palavras-chave:	Criptografia, matemática, sigilo, codificação, decodificação.		
Título em outra língua:	Cryptographic		
Palavras-chave em outra língua:	Cryptography, mathematics, confidentiality, coding, decoding.		
Área de concentração:	Matemática do Ensino Básico		
Data defesa: (dd/mm/aaaa)	06/08/2015		
Programa de Pós-Graduação:	Mestrado em Matemática-PROFMAT		
Orientador (a):	Prof. Dra. Ivonildes Ribeiro Martins Dias		
E-mail:	ivonildes@ufg.br		
Co-orientador (a):*			
E-mail:			

*Necessita do CPF quando não constar no SisPG


3. Informações de acesso ao documento:

Concorda com a liberação total do documento SIM NÃO¹

Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF ou DOC da tese ou dissertação.

O sistema da Biblioteca Digital de Teses e Dissertações garante aos autores, que os arquivos contendo eletronicamente as teses e ou dissertações, antes de sua disponibilização, receberão procedimentos de segurança, criptografia (para não permitir cópia e extração de conteúdo, permitindo apenas impressão fraca) usando o padrão do Acrobat.

Assinatura do (a) autor (a)

Data: 27 / 08 / 2015 

¹ Neste caso o documento será embargado por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Os dados do documento não serão disponibilizados durante o período de embargo.

Tulio Fernando da Mata

CRIPTOGRAFIA

Trabalho de Conclusão de Curso apresentado ao Instituto de Matemática e Estatística da Universidade Federal de Goiás, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Área de Concentração: Matemática do Ensino Básico

Orientador: Prof. Dra. Ivonildes Ribeiro Martins Dias

Goiânia

2015

Ficha catalográfica elaborada automaticamente
com os dados fornecidos pelo(a) autor(a), sob orientação do Sibi/UFG.

da Mata, Tulio Fernando
Criptografia [manuscrito] / Tulio Fernando da Mata. - 2015.
LXI, 61 f.

Orientador: Prof. Dr. Ivonildes Ribeiro Martins Dias.
Dissertação (Mestrado) - Universidade Federal de Goiás, Instituto de
Matemática e Estatística (IME) , Programa de Pós-Graduação em
Matemática, Goiânia, 2015.

Bibliografia.

Inclui lista de figuras.

1. Conhecimento Prévio para Criptografia. 2. Criptografia, Usos,
Importância e Limites. 3. Criptografia. I. Ribeiro Martins Dias, Ivonildes ,
orient. II. Título.

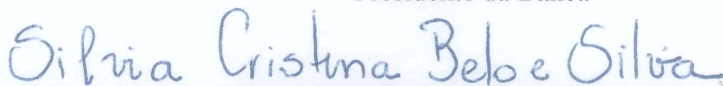
Tulio Fernando da Mata

Criptografia

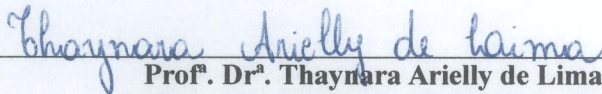
Trabalho de Conclusão de Curso defendido no Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT/UFG, do Instituto de Matemática e Estatística da Universidade Federal de Goiás, como requisito parcial para obtenção do título de Mestre em Matemática, área de concentração Matemática do Ensino Básico, aprovado no dia 06 de agosto de 2015, pela Banca Examinadora constituída pelos professores:



Prof. Dr. Ivonildes Ribeiro Martins Dias
Instituto de Matemática e Estatística-UFG
Presidente da Banca



Prof. Dr. Sílvia Cristina Belo e Silva
Membro externo/ PUC/GO



Prof. Dr. Thaynara Arielly de Lima
Instituto de Matemática e Estatística - UFG

Todos os direitos reservados. É proibida a reprodução total ou parcial deste trabalho sem a autorização da universidade, do autor e do orientador.

Tulio Fernando da Mata graduou-se em Licenciatura Plena em Matemática pela UEG, na cidade Goiás, na turma de 2003, durante o curso e até o ano de 2005 foi professor de física e química no regime de contrato temporário. Em outubro de 2005, passou no concurso para carteiro, indo trabalhar na cidade de Mozarlândia, onde também conseguiu um contrato de professor, trabalhando como carteiro durante o dia e professor durante a noite. No ano de 2006, passou no concurso para professor de matemática do Estado de Goiás, tendo sua convocação em abril de 2007, obrigando-o a deixar os serviço nos Correios, passando a ser exclusivo como professor de matemática. Em 2009, fez pós-graduação em Metodologia de Ensino e Pesquisa na Educação em Matemática e Física. Tentou o ingresso no **PROFMAT** em 2011, não conseguindo, conquistando a vaga apenas no ano de 2013.

Esse trabalho é dedicado a minha família, esposa, Pollyana Claudina, e filhos, Paulo Fernando e Eduarda, pessoas muito especiais em minha vida, que me fazem a cada momento querer me superar, que fazem ter esperança num futuro melhor. Minha família é a melhor parte de minha vida e o que mais amo neste mundo, um amor sem limite e é a eles que dedico não só este trabalho, mas a minha vida e todas as minhas vitórias.

Agradecimentos

Sobretudo e em primeiro lugar, quero agradecer ao meu bom Deus, Jeová, que me deu capacidade, inteligência, força e perseverança para concluir este curso.

Também quero deixar registrado o meu agradecimento a minha querida e amada esposa, Pollyana Claudina, que me apoiou, me encorajou e fez dos meus grandes problemas, pequenos obstáculos. Devo também um agradecimento especial aos meus filhos, Paulo Fernando e Eduarda, que compreenderam os meus objetivos, mesmo as vezes tento que sacrificar o lazer da família.

Agradeço ainda minha mãe, Maria Luiza e minha tia Valdeli (Zinha) que sempre acreditaram na minha capacidade e me deram força nas horas difíceis.

Agradeço aos amigos Gisele Luiza, Ana Cley, Maria Aparecida (Branca), Suelene, Agleydson, Valdeci, Suzana, Marcos Antônio (Markão) e muitos outros por me incentivarem, intuitivamente a ser melhor para poder acompanhá-los.

Agradeço também aos colegas, que são muitos, por me entenderem e me ajudarem todas vezes que precisei.

Deixo um abraço de agradecimento aos amigos de sala, em especial aos Hugleidson, Cleuber, Gean, Bruno e Samira pelas experiências trocadas, dúvidas tiradas e amizades construídas.

Devo um agradecimento carinhoso ao amigo João Luis, amigo muito especial que fiz no curso, mas por motivo particulares ele desistiu.

A minha orientadora, Prof. Dra. Ivonildes Ribeiro Martins Dias, devo a ela mais que um agradecimento, pois apesar de eu não ter sido tão pontual, ela foi.

Agradeço a todos que direta ou indiretamente me ajudaram ou mesmo torceram por mim.

E por fim, agradeço a **CAPES** pelo suporte financeiro, sem ele talvez não teria conseguido fazer o curso.

Resumo

O presente trabalho faz uma breve leitura sobre a situação de crise vivida pelo ensino de matemática na escola pública brasileira nos últimos anos, analisando algumas das razões e motivos dessa crise e tentando apontar caminhos para que esse ensino se torne melhor e mais eficiente e acima de tudo apresentando a matemática como uma ciência de fundamental importância para o mundo atual, apontando sua aplicabilidade em situações cotidianas que podem despertar o interesse dos alunos e se apresentam como desafios para suas capacidades de raciocinar e de aprender. Na perspectiva de mostrar a aplicabilidade e a importância da matemática apresenta-se a criptografia, elegendo-se como base de análise o método criptográfico RSA, um dos mais difundidos em todo o mundo, para apresentá-lo como uma ferramenta que usa algoritmos matemáticos para a codificação e/ou decodificação de dados, permitindo a proteção e o sigilo de informações confidenciais transmitidas via satélite em transações comerciais e bancárias. O trabalho apresenta a importância geral da criptografia no contexto do mundo globalizado e tecnológico da atualidade, assim como dentro da história, ressaltando, inclusive, sua contribuição decisiva para a vitória dos Aliados contra os alemães na 2.^a Guerra Mundial. Apresenta-se ainda a base matemática necessária para criptografia, ou seja, os conhecimentos prévios de matemática que são usados para criptografar mensagens e dados, bem como se apresenta exemplos de codificação e decodificação de mensagens simples. Por fim, faz-se uma abordagem geral sobre a criptografia, desde seu conceito e definições mais comuns, apontando os requisitos garantidos pelo seu uso e os principais tipos de algoritmos para cifragem e decifragem de códigos, também chamadas de chaves criptográficas.

Palavras-chave Criptografia, matemática, sigilo, codificação, decodificação.

Abstract

This paper makes a brief reading on the crisis experienced by the mathematics education in Brazilian public schools in recent years, analyzing some of the reasons and motives of this crisis and trying to point out ways that this teaching will become better, more efficient and above all presenting mathematics as a fundamental importance for today's world science, pointing their applicability in everyday situations that may arouse the interest of students and present themselves as challenges to their ability to think and learn. In order to show the applicability and the importance of mathematics shows the encryption, if elected as a basis for analysis the cryptographic method RSA, one of the most widespread throughout the world, to present it as a tool that uses mathematical algorithms to encoding and/or decoding of data, enabling the protection and confidentiality of sensitive information transmitted via satellite in commercial and banking transactions. The paper presents the general importance of cryptography in the context of a globalized and technological world of today, as well as within the story, noting even its decisive contribution to the Allied victory against the Germans in the 2nd World War. It presents also the mathematical basis for encryption, prior knowledge of mathematics that are used to encrypt messages and or data, and presents examples of encoding and decoding simple messages. Finally, a general approach on the encryption is done, since its concept and common definitions, pointing secured requirements for its use and the main types of algorithms for encryption and decryption codes, also called cryptographic keys.

Keywords

cryptography, mathematics, confidentiality, coding, decoding.

Lista de Figuras

1	Pedreiro trabalhando	3
2	Máquina de Criptografia	4
3	Alan Turing	5
1.1	Evolução dos Números	7
1.2	Pierre de Fermat	14
1.3	Marin Mersenne	15
1.4	Números indo-arábicos	16
2.1	Avanço Tecnológico	32

Sumário

Introdução	1
1 Conhecimento Prévio para Criptografia	7
1.1 Números Naturais	7
1.1.1 Destaque para o Axioma da Indução	8
1.2 Números Primos	9
1.2.1 Quantos Números Primos Existem?	10
1.2.2 Como Reconhecer um Número Primo	11
1.2.3 Os Números de Fermat	13
1.2.4 Os Números de Mersenne	14
1.3 Números Inteiros	16
1.3.1 Números Negativos: Origens	16
1.3.2 Os Inteiros	16
1.4 Mínimo Múltiplo Comum	17
1.5 Máximo Divisor Comum	18
1.6 Teorema Fundamental da Aritmética	20
1.6.1 Fatoração	20
1.7 Divisibilidade	21
1.7.1 O Algoritmo da Divisão	21
1.7.2 O Algoritmo de Euclides	21
1.7.3 Critérios de Divisibilidade	23
1.8 Números Perfeitos	26
1.9 Congruência	26
1.9.1 Teorema de Invertíveis	28
1.10 Pequeno Teorema de Fermat	29

2	Criptografia, Usos, Importância e Limites	30
2.1	Conceituando a Criptografia	30
2.2	A Criptografia e sua Importância	31
2.3	Requisitos Garantidos pela Criptografia	33
3	Criptografia	35
3.1	Criptografia RSA	35
3.2	Codificação	37
3.3	Decodificação	38
3.4	Por que Funciona?	41
3.5	RSA Realmente é Seguro?	42
3.6	Os Primos Perfeitos Para o RSA	43
	Considerações Finais	44
	Referências Bibliográficas	46

Introdução

O ensino de matemática na escola pública vem sendo discutido há vários anos e se constitui num grande desafio a ser superado pelos atores envolvidos nesse processo.

Muito se tem falado sobre os objetivos, as metodologias e diversos estudos e pesquisas têm sido feitas para encontrar a raiz ou as raízes do problema da baixa aprendizagem matemática dos alunos, mas os resultados de avaliações oficiais mostram que as ações empreendidas se mostram ineficientes e a matemática, como disciplina escolar, continua sendo o calcanhar de Aquiles da educação brasileira.

Muitas são as razões para o ensino da matemática e as justificativas para sua presença nos currículos escolares. A aprendizagem e as aquisições de competências matemáticas além de fornecer ao indivíduo uma linguagem para expressar seu pensamento, o dota de ferramentas com as quais ele pode gerar novos pensamentos e desenvolver raciocínios, conforme acentua NUNES, [11];

“A Matemática não é simplesmente uma disciplina, mas também uma forma de pensar. É por isso que a Matemática, assim como a alfabetização, é algo que deve ser tornado possível para todos”.
(1997, p. 95)

Em defesa do ensino e da aprendizagem desta ciência ou disciplina escolar, visto que no âmbito escolar ela assume um aspecto menos formal e as vezes perdendo o extremo rigor academicista, cabe ressaltar ainda que as formas de pensamento características da matemática podem expandir-se para outros raciocínios, impulsionando a capacidade global de aprendizado. Ao trabalhar matemática exercita-se a mente com uma série de ações que exigem muito raciocínio e atitudes intelectuais complexas, pois é comum fundamentar o pensamento em um conjunto de axiomas, na geração e validação de hipóteses, no desenvolvimento de algoritmos e procedimentos de resolução de problemas, estabelecendo conexões e fazendo estimativas. Essas ferramentas são aplicáveis a um

conjunto amplo de situações similares, pois permitem a análise de situações particulares e sua inserção nas estruturas mais amplas e globais e isso torna possível construir estruturas de pensamento que podem ser úteis e contribuir muito em situações não relacionadas a matemática experimentada na vida em sociedade.

Os PCN's - Parâmetros Curriculares Nacionais defendem a ideia de que a aprendizagem matemática contribui para a formação do cidadão quando aponta que um currículo de matemática deve:

“[...] procurar contribuir, de um lado, para a valorização da pluralidade sociocultural, impedindo o processo de submissão no confronto com outras culturas; do outro, criar condições para que o aluno transcenda um modo de vida restrito a um determinado espaço social e se torne ativo na transformação de seu ambiente.”(Brasil, 1998, p. 30)

Quer se goste dela ou não, a Matemática é uma ciência que está presente no cotidiano de todo cidadão. Essa presença pode ser de forma clara e explícita e em certas situações de forma sutil.

Verificar o preço de um produto no supermercado, conferir o troco em uma compra, verificar as horas no relógio quando necessário, quando achamos que um determinado endereço está longe ou perto, ao dizer que a bola chutada pelo jogador do time entrou no ângulo, estamos “lendo” a linguagem matemática, exercitando nossa capacidade de abstração e utilizando conhecimentos matemáticos construídos ao longo de vários séculos pela humanidade. Até mesmo para compreender certas notícias veiculadas nas páginas de um jornal ou de uma revista, é indispensável uma determinada dose de conhecimento matemático e um domínio mínimo das linguagens inerentes a essa ciência.

A matemática é cada vez mais presente em diversas situações e é cada vez mais empregada para descrever, modelar e resolver problemas nas mais diversas áreas da atividade humana.

Representações em forma de porcentagens, gráficos ou tabelas são usuais em diversas situações como na descrição e análise de vários assuntos relacionados a preços, pesquisas de opinião e de intenção de votos, situações de mercado financeiro, inflação, aumento de salários, taxas e impostos, etc.



Figura 1: Pedreiro trabalhando

São situações que usam elementos da matemáticos portanto, um médico que interpreta um eletrocardiograma, está fazendo a leitura de um gráfico que pode ser a representação de uma função; um mestre de obras ou mesmo um pedreiro que sem conhecimentos de área, volume, ângulos constantemente aplica tais saberes em seu trabalho (Figura 1), um menino ou um aposentado que vende picolés na rua e calcula quanto ganha pelas vendas do dia usando conhecimentos de porcentagem.

Esse e infinitos outros exemplos da realidade provam tanto a presença da matemática no cotidiano das pessoas quanto a importância desta ciência para a vida, a sociedade e o desenvolvimento do mundo.

Em face da grande importância da Matemática para o desenvolvimento intelectual, pessoal e para o exercício da cidadania, esta ciência tem ainda a importância de ter contribuído de forma decisiva para o desenvolvimento da humanidade, sendo um dos pilares do desenvolvimento científico e tecnológico que o mundo vem experimentando ao longo de sua história. Mesmo diante de tão notáveis contribuições e tão sobeja importância a matemática é alvo do desprezo da quase absoluta maioria dos alunos, o que gera angústia e frustração nos professores dessa disciplina, que não devem se deixar vencer pelos argumentos contrários e sem fundamentos que visam colocá-la como a grande vilã do ensino escolar.

Em meio a tantos desafios encontrados na árdua tarefa de ensinar matemática, um dos maiores enfrentados pelos professores é a necessidade de conscientizar os discentes sobre a importância dos conteúdos estudados em sala de aula, deixando claro para eles que tais conteúdos podem perfeitamente transpor esse limite, mostrando que os conteúdos ganham significado em diversos contextos e situações práticas e podem ser perfeitamente aplicáveis no cotidiano.

Superar situações nas quais os professores da área de ciências exatas, mais precisamente o professor de matemática, ouve corriqueiramente nas aulas indagações tais como: “Onde vou usar este conteúdo, professor?”, “Por que eu preciso aprender isto?”, “Essa matéria serve pra alguma coisa na minha vida?” é um dos pontos cruciais para se alavancar o ensino da matemática nas nossas escolas. Nesse sentido, dotar os con-

teúdos de significado, vinculando-os a realidade e mostrando sua aplicabilidade prática é, possivelmente, a maior barreira a ser superada no trabalho de se produzir melhores resultados no ensino/aprendizagem dessa ciência.

Diante dessa problemática, a presente pesquisa visa amenizar esse problema da desvinculação dos conteúdos curriculares de matemática da realidade prática vivenciada pelos alunos provando que as verdades matemáticas podem ser aplicadas ao mundo real dando-lhe fundamentação lógica e concreta.

Nesse particular é importante lembrar que os números surgiram naturalmente, e que o conhecimento matemático evoluiu pautado pelas necessidades da humanidade, dentro de cada contexto e período da história, levando as sociedades que a estudam e empregam seus conhecimentos para suprir suas necessidades e interesses a grandes conquistas, como por exemplo vencer uma guerra, através do uso da criptografia.



Figura 2: Máquina de Criptografia

Durante a segunda Guerra Mundial, os aliados perceberam que a Teoria da Lógica Matemática poderia ser usada para decifrar as mensagens dos alemães (Figura 2), apenas através de cálculos rápidos e precisos. Quem mais contribuiu para essa quebra de códigos foi o matemático inglês Alan Turing (Figura 3). Ele foi convocado pela Escola de Cifras e Códigos do Governo para decifrar as mensagens codificadas do inimigo alemão, este possuía um sofisticado e moderno sistema de codificação, chegando a acreditar que esse sistema era infalível. Turing precisava decifrar as mensagens em tempo hábil, por exemplo se a mensagem fosse para destruir um navio, a mensagem deveria ser decifrada antes que o navio fosse destruído, caso contrário, essa mensagem não seria mais útil. Além disso, os Aliados

tinham que disfarçar a ponto do inimigo alemão nem suspeitar que a mensagem havia sido decifrada.

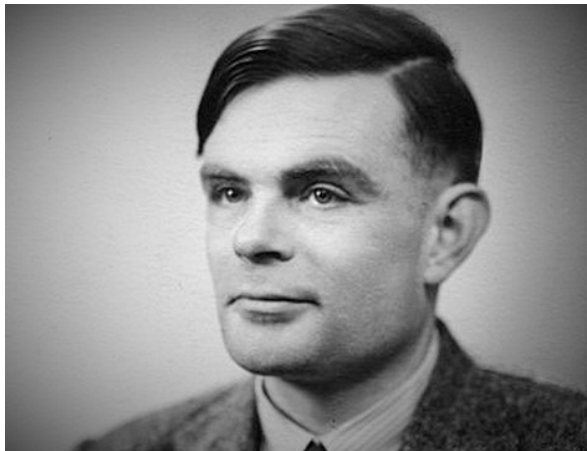


Figura 3: Alan Turing

Essa foi certamente uma das maiores e melhores armas de guerra dos Aliados usada fora do campo de batalha. Diante de tais realizações, não é nenhum absurdo dizer que a segunda Guerra Mundial também foi a “guerra dos matemáticos”.

A criptografia é uma batalha entre o criador do código e aquele que tenta decifrá-lo, além do destinatário. O desafio para o codificador é misturar a mensagem até um ponto em que ela seja, teoricamente, indecifrável, para um possível intermediador indesejado, sendo fácil

a decifração da mensagem para o destinatário. Para maiores informações consulte as referências [2] e [13]

Atualmente vivemos uma guerra de quebra de códigos muito intensa exemplificadas nas compras realizadas com cartões de crédito, através de sites na internet, etc. Muitos mal intencionados tentam decifrar os códigos, e assim obterem informações privilegiadas e confidenciais do cliente para posteriormente usá-las causando prejuízo financeiro e uma série de outros transtornos. Em contrapartida os bancos juntamente com as lojas virtuais tentam tornar suas codificações cada vez mais complexas, objetivando maior segurança, e para isso é crucial o uso da matemática.

Os matemáticos consideram importantíssimas matérias da teoria dos números tais como números primos, máximo divisor comum, mínimo múltiplo comum e fatoração, conceitos comuns porém fundamentais para sistema de criptografia tal como o RSA. Conseqüentemente, esta pesquisa se dirige aos estudantes com conhecimento básico sobre a fatoração de inteiros e primos, que tenha certa facilidade no cálculo com fórmulas elementares e que tenha interesse matemático suficiente para apreciar argumentos de demonstrações bastante básicas, despertando a curiosidade do aluno sabendo que curiosidade é capaz de levar o indivíduo muito além do que se pode imaginar.

O nosso trabalho foi dividido de um modo que no primeiro capítulo são feitas referências e demonstrações de tópicos fundamentais da matemática que são requisitos para a criptografia. Entre esses conhecimentos prévios de matemática necessários para a criptografia estão destacados números inteiros, números primos, mínimo múltiplo comum (MMC) e máximo divisor comum, fatoração, números inteiros, divisibilidade,

números perfeitos, congruência e o pequeno teorema de Fermat, mostrando sua adequação e aplicabilidade nas aulas de matemática no Ensino Médio.

O Capítulo 2 é dedicado à definição da criptografia, e ainda se ocupa em apresentar os requisitos de segurança garantidos pela criptografia e os principais tipos de chaves para cifragem e decifragem de códigos criptografados.

A definição e um breve histórico da criptografia são o tema do Capítulo 3, ressaltando sua contribuição para a vitória dos Aliados contra os alemães na Segunda Grande Guerra, destaca o método de criptografia RSA e apresenta exemplos de codificação e decodificação de mensagens por meio desse método.

Capítulo 1

Conhecimento Prévio para Criptografia

1.1 Números Naturais

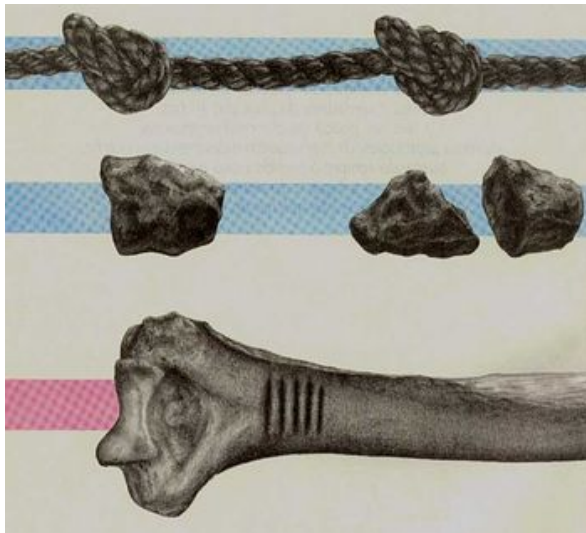



Figura 1.1: Evolução dos Números

A civilização humana lentamente foi dominando o modelo de contagem (um, dois, três,...) que são os números naturais. Conforme as necessidades do homem foram se tornando complexas (Figura 1.1), foi se aumentando as necessidades e reflexões sobre a evolução do sistema de contagem, posteriormente sobre a matemática.


Na teoria matemática, todas as vezes que há necessidade de definir algo, isso é feito com base em conceitos anteriores ou a partir de definições anteriores que sustentam, comprovam ou corroboram com o novo conceito que se quer demonstrar.

Havendo a necessidade de conceitos primitivos, ou seja, sem uma explicação definida,

introduz-se alguns axiomas, ou seja, certas proposições que se tomam como verdadeiras independente de qualquer demonstração. 

Pode-se dizer que hoje os números naturais (representados pelo símbolo \mathbb{N}) se caracterizam essencialmente pelo significado da palavra sucessor, ou seja que **secede**, que vem depois, segundo o dicionário contemporâneo da língua portuguesa. Afirmarmos que se $n, n' \in \mathbb{N}$, e se n' é sucessor de n , podemos com certeza afirmar que não existe outro número natural entre n e n' . ~~Porem essa característica não define matematicamente os números naturais,~~ foram formulado por Peano os seguintes axiomas:

- i)* Zero (representado pelo símbolo 0) é um número natural
- ii)* Todo número natural tem um único sucessor;
- iii)* Números naturais diferentes têm sucessores diferentes;
- vi)* Existe um único número natural, o zero, que não é sucessor de nenhum outro número;
- v)* Seja X um conjunto de números naturais (isto é, $X \subset \mathbb{N}$). Se $0 \in X$ e se, além disso, o sucessor de todo elemento de X ainda pertence a X , então $X = \mathbb{N}$.


Para esclarecimentos maiores consulte as referências [7] 

1.1.1 Destaque para o Axioma da Indução

O último dos axiomas de Peano, Axioma da Indução, é a base eficiente de demonstração de proposições referentes a números naturais, que estabelece o seguinte princípio; Princípio da indução: seja P_n uma propriedade relativa ao número natural n . Suponha que;

- i)* P_1 é válida;
- ii)* Para todo $n \in \mathbb{N}$, a validade de P_n implica a validade de $P_{n'}$, onde n' é o sucessor de n ;

Então P_n é verdadeira para qualquer que seja o número natural n .

O axioma da indução é uma forma de dizer que qualquer número natural n pode ser alcançado se partirmos de 1 e se continuarmos a repetir a operação tomar o sucessor de um número natural, segundo Hygino H. Domingues: 

Seja $L = \{x \in \mathbb{N} / x \geq a \text{ e } P_a \text{ é falsa}\}$. Basta provar então que $L = \emptyset$. Suponhamos que $L \neq \emptyset$ e seja m o menor elemento de L . Logo P_m é falsa e como, por hipótese, P_a é verdadeira, então $m > a$. Desta última relação segue que $m > 0$; portanto $m = 1 + u$, para algum $u \in \mathbb{N}$, e daí $u < m$.

Mas $m > a$ implica que $m \geq a + 1$. Assim $m = 1 + u \geq a + 1$, do que resulta $u \geq a$.

Em resumo: $m > u \geq a$. Mas isto obriga $P_{(u)}$ a ser verdadeira (se fosse falsa, u estaria em L , o que não é possível pois $u < m = \min L$). Então, devido a $P_{m+1} = P_m$ é verdadeira. Absurdo. (Fundamentos de Aritmética pg 23)

Exemplo 1.1.1. Usando o método de indução, mostremos a igualdade $3^{2n} + 7 = 8k$, para todo número natural n ;

Para $n = 1$ temos que;

$$3^{2n} + 7 = 3^{2 \cdot 1} + 7$$

$$3^{2n} + 7 = 3^2 + 7$$



$$3^{2n} + 7 = 9 + 7$$

$$3^{2n} + 7 = 16$$

$3^{2n} + 7 = 8 \cdot k_1$. Com $k_1 = 2$ logo a afirmação é verdadeira.

Suponhamos que para algum $p > 1$, $p \in \mathbb{N}$ a afirmação seja verdadeira, ou seja;

$$3^{2p} + 7 = 8k_p$$

Queremos provar a validade para $n = p + 1$ como

$$3^{2p} + 7 = 8k_p \text{ multiplicamos os dois lados da igualdade por 9 obtendo}$$

$$9 \cdot (3^{2p} + 7) = 9 \cdot 8k_p$$

$$9 \cdot 3^{2p} + 63 = 72k_p \text{ subtraindo 56 em ambos os lados da igualdade}$$

$$9 \cdot 3^{2p} + 63 - 56 = 72k_p - 56 \text{ fatorando } 9 = 3^2, \text{ no primeiro lado da igualdade temos}$$

$$3^2 \cdot 3^{2p} + 7 = 72k_p - 56 \text{ fatoramos } 72k_p - 56 = 8(9k_p - 7) \text{ assim}$$

$$3^{2p+2} + 7 = 8(9k_p - 7) \text{ fazendo } 9k_p - 7 = k_q, \text{ ou seja}$$

$$3^{2(p+1)} + 7 = 8k_q \text{ cqd.}$$

Logo, a afirmação é verdadeira para todo $n \in \mathbb{N}$.

Para maiores informações consulte a referência [3].

1.2 Números Primos



Se a e b são naturais, dizemos que a divide b , podendo escrever $a \mid b$, se existir um natural k_1 tal que $b = k_1 \cdot a$, podendo afirmar que a é divisor de b e que b é múltiplo de

a.

Definição 1.2.1. Um número inteiro $n(n > 1)$ possuindo somente dois divisores positivos n e 1 é chamado primo.

Segundo essa definição o número 1 não é um número primo, pois o mesmo não apresenta dois divisores distintos.

O número 2 é o único número primo par, já que todos os demais números pares possuem ao menos 3 divisores, dentre eles o número 1 , o próprio número e o número 2 .

Números naturais não nulos que possuem mais de dois divisores são chamados de números compostos.

Proposição 1. Se $p \mid a.b$, sendo p primo, então $p \mid a$ ou $p \mid b$.

Demonstração. Se $p \nmid b$, por definição $b = k_1.p$, sendo k_1 um número natural, supondo que $p \nmid a$ (a não é divisível por p), logo $a = k_2.p + d$ onde k_2 e d também são números naturais, podemos multiplicar ambos lados da igualdade por b ficando $a.b = k_2.p.b + d.b$, lembrando que $b = k_1.p$ e fazendo a substituição apenas no segundo lado da igualdade $a.b = k_2.p.k_1.p + d.k_1.p$, colocando p em evidência no segundo lado da igualdade $a.b = (k_2.p.k_1 + d.k_1).p$, e chamando $k_2.p.k_1 + d.k_1 = k_3$, logo $a.b = k_3.p$, o que implica $p \mid a.b$. \square

1.2.1 Quantos Números Primos Existem?

No livro IX, BOYER [p 79] nos diz que:

“O Livro IX, o último dos três sobre teoria dos números, contém vários resultados interessantes. Desses, o mais célebre é a Proposição: números primos são mais do que qualquer quantidade fixada de números primos. Isto é, Euclides dá aqui a prova elementar bem conhecida do fato de que há infinitos números primos. A prova é indireta, pois mostra-se que a hipótese de haver somente um número finito de primos leva a uma contradição”.

Segundo o teorema fundamental

Teorema 1.2.2. “Existem uma infinidade de números primos”.

O que é muito bem demonstrado por Euclides:

Demonstração. “Suponhamos que a sucessão $p_1=2, p_2=3, \dots, p_r$, dos r números primos seja finita. Façamos $P = p_1.p_2.\dots.p_r + 1$, e seja p um número primo que divide P . Esse número p não pode ser igual a qualquer um dos números p_1, p_2, \dots, p_r , porque então ele dividiria a diferença $P - p_1.p_2.\dots.p_r=1$, o que é impossível. Assim p não é um número primo que não pertence a sucessão p_1, p_2, \dots, p_r , e por consequência podendo afirmar que r não representa todos os números primos.” (Números Primos Velhos Mistérios e Novos Recordes, pg 1) \square

Exemplo 1.2.3. De acordo com a definição $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$ e $p_5 = 11$ e como $P = p_1.p_2.\dots.p_r + 1$ logo,

$$P = 2.3.5.7.11 + 1$$

$$P = 2310 + 1$$

$$P = 2311$$

portanto, P possui um primo p que no caso $p = 2311$, diferente dos apresentado na sequência $p_1.p_2.p_3.p_4.p_5$

Goldbach também fez uma demonstração bastante simples;

Demonstração do Teorema 1.2.2 segundo Goldbach. “Basta achar uma sucessão infinita $a_1 < a_2 < a_3 < \dots$ de números naturais, primos entre si, ou seja sem fator comum entre si. Se p_1 é fator primo de a_1, p_2 um fator primo de a_2, \dots, p_n fator primo de a_n, \dots , então $p_1, p_2, p_3, \dots, p_n, \dots$ são distintos.” (Números Primos Velhos Mistérios e Novos Recordes, pg 4) \square

1.2.2 Como Reconhecer um Número Primo

No artigo 329 das **Disquisitiones** Arithmeticae, Gauss escreveu:

“O problema de distinguir os números primos dos números compostos e de exprimir estes últimos à custa de seus fatores primos deve ser considerado como um dos mais importantes e dos mais úteis em aritmética. A própria dignidade da ciência requer que todos os meios possíveis sejam explorados para a resolução de um problema tão elegante e tão famoso”.(Números Primos Velhos Mistérios e Novos Recordes, pg 13)

O primeiro pensamento para verificar se um número n é primo é o da fatoração, mas existe outro procedimento aplicável a todo natural \mathbb{N} , que indicará, com um número

finito de cálculo, se n é primo ou composto. Sendo o número natural \mathbb{N} , basta tentar dividi-lo sucessivamente por $n = 2, 3, 5, 7, \dots, k$, sendo k o número natural igual ou inferior a n .

O Crivo de Eratóstenes

Como a multiplicação é operação mais fácil de executar do que a divisão, **Eratóstenes** no século III A.C., teve a ideia de organizar os cálculos sob a forma de crivo, que leva seu nome. O crivo serve para a determinar todos os números primos e também os fatores dos números compostos a um número N dado arbitrariamente.

Vamos ilustrar o processo tomando como exemplo $N = 131$

O processo é realizado da seguinte maneira:

- i)* escreva todos os números até 131;
- ii)* risca-se todos os múltiplos de 2, superior a 2
- iii)* em cada nova etapa, são riscados todos os múltiplos do menor inteiro p , ainda não riscados e que são maiores que p .
- iv)* basta chegar ao número p tal que p^2 já ultrapassa 131

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131									

Assim todos os múltiplos de 2, 3, 5, 7, 11, $13 < \sqrt{131}$ são expurgados. O número 53, por exemplo, é primo porque não foi expurgado. Então, os números primos inferiores ou iguais a 131 são 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131.

Para maiores informação veja as referências [10], [12] e [14]

1.2.3 Os Números de Fermat



Figura 1.2: Pierre de Fermat

O matemático francês Pierre de Fermat (1601-1665) (Figura 1.2) é famoso pela sua extensa contribuição em teoria dos números. Suas principais contribuições são o pequeno teorema de Fermat, o último teorema de Fermat (demonstrado por A. Wiles), números de Fermat, entre outros. Neste trabalho, exploraremos algumas propriedades elementares dos números de Fermat. Um número de Fermat é um número da forma

$$F_n = 2^{2^n} + 1.$$

Para $n = 0, 1, 2, 3, 4$ Fermat conjecturou que esses números eram todos primos, de fato, para $n = 0, 1, 2, 3, 4$ dão realmente números primos 3, 5, 17, 257, 65537. Entretanto Euler mostrou que;

Proposição 2. F_5 é divisível por 641.

Demonstração. ~~O argumento usado abaixo é devido a~~ Kraitchik. Note que

$$641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1;$$

$$2^4 = 641 - 5^4, (I) \text{ e}$$

$$5 \cdot 2^7 = 641 - 1 (II)$$

$$2^{2^5} = 2^{32} = 2^4 \cdot 2^{28} = (641 - 5^4) \cdot 2^{28} \text{ de (I)}$$

$$2^{2^5} = 641 \cdot 2^{28} - 5^4 \cdot 2^{28} \text{ (propriedade distributiva)}$$

$$2^{2^5} = 641 \cdot 2^{28} - 5^4 \cdot 2^{28} \equiv -5^4 \cdot 2^{28} \pmod{641} \text{ (primeira parcela é múltiplo de 641)}$$

$$2^{2^5} \equiv -5^4 \cdot 2^{28} \equiv 5^4 \cdot 2^{28} \equiv (5 \cdot 2^7)^4 \equiv (641 - 1)^4 \equiv 1 \pmod{641}, \text{ de (II) logo}$$

641 divide F_5 . □

Atualmente os únicos números primos de Fermat conhecidos, são aqueles apresentados pelo próprio Fermat.

1.2.4 Os Números de Mersenne



ficou muito colado o com o texto

Figura 1.3: Marin Mersenne

$M_7 = 127$ são primos, enquanto que o próximo número de Mersenne $M_{11} = 2047$ é composto, sendo $M_{11} = 23 \times 89$.

O crescimento destes números é da ordem exponencial 2, o que explica que, até o momento, apenas sejam conhecidos 48 e o maior possui mais de 17 milhões de dígitos: $2^{57.885.161} - 1$. No entanto, já em 1640, Mersenne tinha identificado como primos os acima apresentados e ainda aqueles com $q = 13, 17, 19, 31, 127$. Todos os primos de Mersenne que existem com $q \leq 127$ foram descobertos antes da era do computador.

Em 1951, Alan Turing fez a primeira tentativa (frustrada) para encontrar novos primos de Mersenne usando um computador. No início do ano seguinte, Robinson, Lucas e Lehmer, descobriram, usando um programa de computador, os primos M_{521} e M_{607} . Ainda no final do ano de 1952, conseguem descobrir os primos M_{1279} , M_{2203} e M_{2281} .

Para maiores esclarecimento consulte as referências [2], [10] e [14].

Marin Mersenne (1588-1648) (Figura 1.3) foi um monge com interesses matemáticos, que se correspondia com os maiores vultos da cena científica do seu tempo. Cerca de 1640, numa das suas missivas, descreve números da forma

$$M_q = 2^q - 1.$$

Na forma apresentada, q é um número primo, isto tem ligação com o seu estudo sobre **números perfeitos**, que é aquele número cuja a soma dos divisores é igual ao dobro do número. Desde então sabemos que alguns desses números, ditos de Mersenne, são primos, outros não. Por exemplo, $M_2 = 3$, $M_3 = 7$, $M_5 = 31$ e

1.3 Números Inteiros

1.3.1 Números Negativos: Origens

HINDU 300 a.C.	-	=	≡	♀	♂	♁	♂	♁	?	
HINDU 500 d.C.	7	7	3	8	4	(7	^	9	0
ÁRABE 900 d.C.	1	٢	٣	٤	٥	٦	٧	٨	٩	٠
ÁRABE (ESPAÑHA) 1000 d.C.	1	٢	٣	٤	٥	٦	٧	٨	٩	٠
ITALIANO 1400 d.C.	1	2	3	4	5	6	7	8	9	0
ATUAL	1	2	3	4	5	6	7	8	9	0

Figura 1.4: Números indo-arábicos

De acordo com Hygino [3] os algarismos que usamos hoje tiveram seu surgimento na Índia e sua difusão pelo mundo ocorreu principalmente pelos árabes justificando sua designação indo-arábicos. Com o passar do tempo a maneira de se grafar esses algarismos foi mudando, podendo afirmar que a maneira que escrevemos esses algarismos hoje tem pouca, ou nenhuma semelhança com a grafia original, como indica a figura 1.4

O sistema de numeração posicional decimal começou a ser padronizado pelo mundo na época medieval, e coube aos hindus a classificação do zero como um número que antes era somente o símbolo de ausência.

Também, não mais ou menos importante, os hindus introduziram os números negativos com o objetivo de indicar débitos. O primeiro hindu a usar os números negativos, de acordo com os registros, foi Brahmagupta(598-668), que dominava as quatro operações fundamentais com números negativos.

Os hindus não se preocuparam com a parte teórica dos números negativos, que foi verificada posteriormente na Índia, tendo sua aceitação por completa num processo longo e cheio de controvérsias.

1.3.2 Os Inteiros

A grosso modo, os números inteiros, nada mais são que a diferença entre dois números $a - b$, onde $b > a$, (nos dando a ideia que devo mais que tenho, ou seja a ideia de débitos) agregados com os próprios números naturais. Com naturalidade podemos determinar $0-1= 1-2= 2-3= \dots = -1$ (estou retirando mais do que tenho, estou ficando em débito). E de maneira análoga determinamos $-2, -3, -4, \dots$

E esses números juntos com os números naturais, que agora, por estética, são escritos da forma $1= +1, 2= +2, 3= +3, \dots$ formam o conjunto dos números inteiros, que são

denotados por \mathbb{Z} :

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

Podendo se tirar quaisquer dúvidas nas referências [3], [7], [12] e [14].



1.4 Mínimo Múltiplo Comum

Definição 1.4.1. Dizemos se um número inteiro a divide um número inteiro b , denotando por $a \mid b$, se $b = c.a$, para algum $c \in \mathbb{Z}$. Neste caso dizemos que a é divisor de b e que b é múltiplo de a .

Proposição 3. Se a, b e c são inteiros, $a \mid b$ e $b \mid c$, então $a \mid c$.

Demonstração. Como $a \mid b$, logo existe um inteiro k_1 tal que $b = k_1.a$, sendo também $b \mid c$, logo também existe um inteiro k_2 tal que $c = k_2.b$, e como $b = k_1.a$, logo $c = k_2.k_1.a$, que implica $a \mid c$. \square

Um número inteiro é um múltiplo comum de dois números inteiros dados se ele é simultaneamente múltiplo de ambos os números. Por exemplo, os números $a.b$ e 0 são sempre múltiplos comuns de a e b .

Em aritmética e em teoria dos números o mínimo múltiplo comum (MMC) de dois inteiros a e b é o menor inteiro positivo que é múltiplo comum de a e de b . Se não existir tal inteiro positivo, por exemplo, se $a = 0$ ou $b = 0$, então $\text{MMC}(a, b)$ é zero por definição.

Definição 1.4.2. Um número inteiro $m \geq 0$ é um mínimo múltiplo comum (MMC) dos números inteiros a e b , quando vale:

- i) m é um múltiplo comum de a e b , e
- ii) se c é um múltiplo comum de a e b , então c divide m (escreveremos $c \mid m$).

Para calcular o MMC de dois ou mais números podemos usar a regra da decomposição simultânea. Acompanhe o cálculo do MMC de 60, 40 e 24:

- 1º Escrevemos os números dados, separando-os por vírgulas, e colocando um traço ao lado do último número. À direita do traço, colocando o menor dos fatores primos dos números dados, seja ele comum ou não.

$$60, 40, 24 | 2$$

2° Sob cada número que for divisível pelo fator primo, colocamos o quociente da divisão (no exemplo sob 60 colocamos 30, sob 40 colocamos o 20 e sob 24 o 12)

Os números não divisível pelo fator primo devem ser repeditos.

$$\begin{array}{r|l} 60, 40, 24 & 2 \\ 30, 20, 12 & \end{array}$$

3° Prosseguimos com esse processo até chegar ao quociente 1 sob todos os números. O MMC é o produto dos fatores primos colocados à direita do traço:

$$\begin{array}{r|l} 60, 40, 24 & 2 \\ 30, 20, 12 & 2 \\ 15, 10, 6 & 2 \\ 15, 5, 3 & 3 \\ 5, 5, 1 & 5 \\ 1, 1, 1 & \end{array}$$

Assim o MMC $(60, 40, 24) = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 2^3 \cdot 3 \cdot 5 = 120$

1.5 Máximo Divisor Comum

Atualmente a definição de Máximo Divisor Comum (MDC) pode ser assim formalizada: Sejam a, b e c números inteiros não nulos, dizemos que c é um divisor comum

de a e b se: c divide a ($c \mid a$) e c divide b então ($c \mid b$).

Definição 1.5.1. Um número inteiro $d > 0$ é um máximo divisor comum (MDC) de dois inteiros a e b se possuir as seguintes propriedades:

i) d é um divisor comum de a e de b , e

ii) d é divisível por todo divisor comum de a e b .

Para calcular o MDC de dois ou mais números também podemos usar a regra da decomposição simultânea. Acompanhe a explicação do cálculo do MDC de 60, 40 e 24.

1º Escrevemos os números dados, separando-os por vírgulas, e colocando um traço ao lado do último número. À direita do traço, colocando o menor do fator primo comum dos números dados. Se não houver fator primo comum, os números são primos entre si e o MDC é igual a 1.

$$60, 40, 24 \mid 2$$

2º Sob cada número colocamos o quociente da divisão pelo fator primo comum. À direita do traço, colocamos o menor fator primo comum dos quocientes encontrados.

Método Prático para calcular o Máximo Divisor Comum

$$\begin{array}{r|l} 60, 40, 24 & 2 \\ 30, 20, 12 & 2 \end{array}$$

3º Dividimos cada quociente pelo fator primo comum e indicamos, sob cada número, o resultado encontrado. Prosseguimos assim até encontrar quocientes que não tenham fator comum, isto é, que sejam primos entre si.

$$\begin{array}{r|l} 60, 40, 24 & 2 \\ 30, 20, 12 & 2 \\ 15, 10, 6 & \end{array}$$

O MDC é o produto dos fatores primos comuns colocados à direita do traço.

$$\text{MDC} = 2 \cdot 2 = 2^2 = 4$$

1.6 Teorema Fundamental da Aritmética

Teorema 1.6.1. *Para todo número natural $a > 1$ existem números primos p_1, p_2, \dots, p_r ($r \geq 1$), de maneira que $a = p_1 \cdot p_2 \cdot \dots \cdot p_r$. Além disso, se também $a = q_1 \cdot q_2 \cdot \dots \cdot q_s$ ($s \geq 1$), onde os q_i são primos, então $r = s$ e cada p_i é igual a algum dos q_j .*

Demonstração. Vimos que o mínimo múltiplo comum (MMC) de dois inteiros a e b é o menor inteiro positivo que é múltiplo simultaneamente de a e de b . Se não existir tal inteiro positivo, por exemplo, se $a = 0$ ou $b = 0$, então $\text{MMC}(a, b)$ é zero por definição. Se $p_1 \cdot p_2 \cdot \dots \cdot p_r = q_1 \cdot q_2 \cdot \dots \cdot q_s$ conforme o enunciado, então p_1 divide o segundo membro e portanto divide um de seus fatores, pois tanto p_r quanto q_s são números primos, logo se algum p_r divide $q_1 \cdot q_2 \cdot \dots \cdot q_s$ então p_r divide um de seus fatores, pois se p_r é primo e $p_r \mid q_1 \cdot q_2 \cdot \dots \cdot q_s$ então $p_r \mid q_1$ ou $p_r \mid q_2$ ou ... ou $p_r \mid q_s$, digamos que esse fator é q_1 , sendo apenas 1 e q_1 os divisores de q_1 , pois todos q_s são primos, e sendo $p_1 > 1$, então $p_1 = q_1$. Repetindo esse argumentando o quanto for necessário chegaremos a unicidade. □

1.6.1 Fatoração

A decomposição de um número inteiro forma um produto entre duas ou mais potências de números primos. A fatoração consiste:

- Na decomposição $a = p_1 \cdot p_2 \cdot \dots \cdot p_r$, é evidente que nem todos os fatores são diferentes entre si, e a reunião de possíveis fatores iguais leva a expressão

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_s^{\alpha_s}$$

onde $1 \leq s \leq r$, $p_s \leq p_r$, sempre que $s \leq r$ e $\alpha_i \geq 1$, além disso $p_1 \leq p_2 \leq \dots \leq p_r$,

- Pode ser conveniente as vezes que, ao lidar com dois ou mais números maiores que 1, estejam eles escritos como potência dos mesmos primos. Isso é possível, obviamente, desde que utilizem expoentes nulos, como no exemplo;

$$120 = 2^3 \cdot 3 \cdot 5 \cdot 7^0 \text{ e } 350 = 2 \cdot 3^0 \cdot 5^2 \cdot 7.$$

1.7 Divisibilidade

1.7.1 O Algoritmo da Divisão

Teorema 1.7.1. *Dados dois inteiros a e b , $b > 0$, existe um único par de inteiros q e r tais que*

$$a = q.b + r, \text{ com } 0 \leq r < b \text{ (} r = 0 \Leftrightarrow b \mid a \text{)}$$

(q é chamado de quociente e r de resto da divisão de a por b).

Demonstração. Como $b > 0$, existe q satisfazendo:

$$q.b \leq a < (q + 1).b$$

o que implica $0 \leq a - q.b$ e $a - q.b < b$. Desta forma, se definirmos $r = a - q.b$ teremos, garantida, a existência de q e r . A fim de demonstrarmos a unicidade, vamos supor a existência de outro q_1 e r_1 verificando:

$$a = q_1.b + r_1 \text{ com } 0 \leq r_1 < b$$

Disto temos $(q.b + r) - (q_1.b + r_1) = 0 \Rightarrow b.(q - q_1) = r_1 - r$, o que implica $b \mid (r_1 - r)$. Mas como $r_1 < b$ e $r < b$, temos $|r_1 - r| < b$ e, portanto, como $b \mid (r_1 - r)$ devemos ter $r_1 - r = 0$ o que implica $r = r_1$. logo $q_1.b = q.b \Rightarrow q = q_1$, uma vez que $b \neq 0$. \square

Podendo se tirar quaisquer dúvidas nas referências [12][14]

1.7.2 O Algoritmo de Euclides

Teorema 1.7.2. *Sejam $r_0 = a$ e $r_1 = b$ inteiros não-negativos com $b \neq 0$. Se o algoritmo da divisão for aplicado sucessivamente para obter*

$$r_j = q_j.r_{j+1} + r_{j+2}, \quad 0 \leq r_{j+2} < r_{j+1}$$

para $j = 0, 1, 2, \dots, n - 1$ e $r_{n+1} = 0$ então $MDC(a, b) = r_n$, o último resto não nulo.

Demonstração. Inicialmente aplicaremos o teorema 1.7.1 para dividir $r_0 = a$ por $r_1 = b$ obtendo $r_0 = q_1.r_1 + r_2$, em seguida divideremos r_1 por r_2 obtendo $r_1 = q_2.r_2 + r_3$ e assim, sucessivamente, até a obtenção do resto $r_{n+1} = 0$. Como, a cada passo o resto

é sempre menor do que o anterior, e estamos lidando com números inteiros positivos, é claro que após um número finito de aplicações do *teorema 1.7.1*, teremos resto nulo. Temos, pois, a seguinte sequência de equações:

$$r_0 = q_1.r_1 + r_2 \quad 0 < r_2 < r_1$$

$$r_1 = q_2.r_2 + r_3 \quad 0 < r_3 < r_2$$

$$r_2 = q_3.r_3 + r_4 \quad 0 < r_4 < r_3$$

⋮

$$r_{n-2} = q_{n-1}.r_{n-1} + r_n \quad 0 < r_n < r_{n-1}$$

$$r_{n-1} = q_n.r_n + 0$$

A última destas equações nos diz que o máximo divisor comum de r_n e r_{n-1} é r_n . A penúltima, que o $\text{MDC}(r_{n-1}, r_{n-2})$ também é r_n e, prosseguindo desta maneira teremos

$$r_n = \text{MDC}(r_n, r_{n-1}) = \text{MDC}(r_{n-1}, r_{n-2}) = \dots = \text{MDC}(r_2, r_1) = \text{MDC}(r_1, r_0)$$


Portanto o máximo divisor comum de a e b é o último resto não-nulo da sequência de divisões. □

Para maiores esclarecimento consulte as referências [3] [12] [14]

Dados dois números inteiros quaisquer, é possível somá-los, subtraí-los e multiplicá-los e o resultado sempre será também um número inteiro, nem sempre isso é possível com a divisão de dois números inteiros, por exemplo: em \mathbb{Z} não é possível dividir 3 por 6, mas é possível dividir 6 por 3. Lembrando da *definição 1.4.1* que se um inteiro a divide um inteiro b , escrevendo $a \mid b$, quando existir $k_1 \in \mathbb{Z}$ tal que $b = k_1.a$. Neste caso, diremos também que a é um divisor ou um fator de b ou, ainda, que b é um múltiplo de a .

Suponha que $a \mid b$, onde $a \neq 0$, e seja $c \in \mathbb{Z}$ tal que $b = c.a$, sejam $a, b, c \in \mathbb{Z}$. Tem-se que;

Proposição 4. $1 \mid a$, $a \mid a$ e $a \mid 0$.

~~Proposição 5.~~ $0 \mid a \iff a = 0$. 

~~Proposição 6.~~ a divide b se, e somente se, $|a|$ divide $|b|$.

~~Proposição 7.~~ se $a \mid b$ e $b \mid c$, então $a \mid c$ (*Propriedade transitiva*).

Demonstração. i) Isso decorre das igualdades $a = a.1, a = 1.a$ e $0 = 0.a..$

ii) Suponha que $0 | a \Rightarrow a = c.0$, como $c.0 = 0$, então $a = 0$, o que é um absurdo, pois $a \neq 0$ conforme a definição.

iii) a divide b logo $b = f.a$ com $f \in \mathbb{Z}$, podemos considerar $b = (-f).(-a)$ logo $-a$ divide b , então $\pm a$ divide b ou ainda podemos multiplicando ambos termos da igualdade por (-1) ficando $-b = -(f.a)$, logo $-b = f.(-a)$ ou $-b = (-f).a$, então $\pm a$ divide $-b$ contudo $\pm a$ divide $\pm b$, podendo concluir que $|a|$ divide $|b|$.

iv) $a | b$ e $b | c$ implica que existem $f, g \in \mathbb{Z}$, tais que $b = f.a$ e $c = g.b$. Substituindo o valor de b da primeira equação na outra, obtem $c = g.b = g.(f.a) = (g.f).a$, o que nos mostra que $a | c$. Os itens (i) e (ii) da proposição acima nos dizem que todo número inteiro a é divisível por ± 1 e por $\pm a$.

□

1.7.3 Critérios de Divisibilidade

Veremos oito modelos de divisibilidade.

- 1) Divisibilidade por 2: Um número natural é divisível por 2 quando ele é par.

Demonstração. Todo número pode ser escrito da forma $2n$, para números pares, ou $2n + 1$, para números ímpares, $n \in \mathbb{Z}$, logo ;

$$2 | 2n \text{ para qualquer } n \in \mathbb{Z}$$



$$2 \nmid 2n + 1 \text{ para qualquer } n \in \mathbb{Z}$$

□

- 2) Divisibilidade por 3: Um número é divisível por 3 quando a soma dos valores absolutos dos seus algarismos for divisível por 3.

Demonstração. Seja um número qualquer $\alpha_x \dots \alpha_3 \alpha_2 \alpha_1$, de x algarismos, podendo ser representado como:

$$\alpha_x \dots \alpha_3 \alpha_2 \alpha_1 = \alpha_x.10 \dots 00 + \dots + \alpha_3.100 + \alpha_2.10 + \alpha_1$$

$$= \alpha_x.(99 \dots 99 + 1) + \dots + \alpha_3.(99 + 1) + \alpha_2.(9 + 1) + \alpha_1$$

$$= \alpha_x.99 \dots 99 + \alpha_x + \dots + \alpha_3.99 + \alpha_3 + \alpha_2.9 + \alpha_2 + \alpha_1$$

$$= (99 \dots 99 \alpha_x + \dots + 99 \alpha_3 + 9 \alpha_2) + \alpha_x + \dots + \alpha_3 + \alpha_2 + \alpha_1$$

$$= 3(33\dots33\alpha_x + \dots + 33\alpha_3 + 3\alpha_2) + \alpha_x + \dots + \alpha_3 + \alpha_2 + \alpha_1$$
 sendo $\rho = 33\dots33\alpha_x + \dots + 33\alpha_3 + 3\alpha_2$ e $\alpha_x + \dots + \alpha_3 + \alpha_2 + \alpha_1$

$$= 3\rho + \theta$$
 como a primeira parcela é múltiplo de 3 o número só vai ser múltiplo de três se θ também for, ou seja se $\alpha_x + \dots + \alpha_3 + \alpha_2 + \alpha_1$ for múltiplo de 3 o número geral é.

□

- 3) Divisibilidade por 4: Um número é divisível por 4 quando termina em 00 ou quando o número formado pelos dois últimos algarismos da direita for divisível por 4.

Demonstração. Seja um número qualquer $\beta_x\dots\beta_3\beta_2\beta_1$, um número de x algarismos, podendo ser representado como:

$$\begin{aligned}
 \beta_x\dots\beta_3\beta_2\beta_1 &= \beta_x \cdot 100\dots00 + \dots + \beta_3 \cdot 100 + \beta_2\beta_1 \\
 &= \beta_x \cdot 4 \cdot 2500\dots00 + \dots + \beta_3 \cdot 4 \cdot 25 + \beta_2\beta_1 \\
 &= 4 \cdot (\beta_x \cdot 2500\dots00 + \dots + \beta_3 \cdot 25) + \beta_2\beta_1
 \end{aligned}$$

como a primeira parcela é múltiplo de 4 o número só vai ser múltiplo de 4 se $\beta_2\beta_1$ também for, ou $\beta_2 = 0$ e $\beta_1 = 0$, assim ficará só a primeira parcela que é múltiplo de 4.

□

- 4) Divisibilidade por 5: Um número natural é divisível por 5 quando ele termina em 0 ou 5.

Demonstração. Seja o mesmo número da demonstração anterior $\beta_x\dots\beta_3\beta_2\beta_1$, um número de x algrismos, podendo ser representado como:

$$\begin{aligned}
 \beta_x\dots\beta_3\beta_2\beta_1 &= \beta_x \cdot 100\dots00 + \dots + \beta_3 \cdot 100 + \beta_2\beta_1 \\
 &= \beta_x \cdot 5 \cdot 200\dots00 + \dots + \beta_3 \cdot 5 \cdot 20 + \beta_2 \cdot 5 \cdot 2 + \beta_1 \\
 &= 5 \cdot (\beta_x \cdot 200\dots00 + \dots + \beta_3 \cdot 20 + \beta_2 \cdot 2) + \beta_1
 \end{aligned}$$

se $\rho = \beta_x \cdot 200\dots00 + \dots + \beta_3 \cdot 20 + \beta_2 \cdot 2$ logo;

$$= 5\rho + \beta_1$$
 como a primeira parcela é múltiplo de 5 o número só vai ser múltiplo de 5 se β_1 também for, ou se $\beta_1 = 0$, assim ficará só a primeira parcela que é múltiplo de 5.

□

- 5) Divisibilidade por 6: Um número é divisível por 6 quando é divisível por 2 e por 3.

Ou seja se o número for par e múltiplo de 3 o número é múltiplo de 6.

~~Demonstração. A mesma demonstração da divisibilidade de 3 e 2, ao mesmo tempo.~~

□

- 6) Divisibilidade por 8: Um número é divisível por 8 quando termina em 000, ou quando o número formado pelos três últimos algarismos da direita for divisível por 8.

Demonstração. Muito parecida com a demonstração da divisibilidade por 4, $\beta_x \dots \beta_4 \beta_3 \beta_2 \beta_1$, um número de x algarismos, podendo ser representado como:

$$\beta_x \dots \beta_4 \beta_3 \beta_2 \beta_1 = \beta_x \cdot 100 \dots 00 + \dots + \beta_3 \cdot 100 + \beta_2 \beta_1$$

$$= \beta_x \cdot 8 \cdot 12500 \dots 00 + \dots + \beta_4 \cdot 8 \cdot 125 + \beta_3 \beta_2 \beta_1$$

$= 8 \cdot (\beta_x \cdot 12500 \dots 00 + \dots + \beta_4 \cdot 125) + \beta_3 \beta_2 \beta_1$ como a primeira parcela é múltiplo de 8 o número só vai ser múltiplo de 8 se $\beta \gamma \theta$ também for, ou $\beta = 0$, $\gamma = 0$ e $\theta = 0$ assim ficará só a primeira parcela que é múltiplo de 8.

□

- 7) Divisibilidade por 9: Um número é divisível por 9 quando a soma dos valores absolutos dos seus algarismos for divisível por 9.

Demonstração. Seja um número qualquer $\alpha_x \dots \alpha_3 \alpha_2 \alpha_1$, de x algarismos, podendo ser representado como:

$$\alpha_x \dots \alpha_3 \alpha_2 \alpha_1 = \alpha_x \cdot 10 \dots 00 + \dots + \alpha_3 \cdot 100 + \alpha_2 \cdot 10 + \alpha_1$$

$$= \alpha_x \cdot (99 \dots 99 + 1) + \dots + \alpha_3 \cdot (99 + 1) + \alpha_2 \cdot (9 + 1) + \alpha_1$$

$$= \alpha_x \cdot 99 \dots 99 + \alpha_x + \dots + \alpha_3 \cdot 99 + \alpha_3 + \alpha_2 \cdot 9 + \alpha_2 + \alpha_1$$

$$= (99 \dots 99 \alpha_x + \dots + 99 \alpha_3 + 9 \alpha_2) + \alpha_x + \dots + \alpha_3 + \alpha_2 + \alpha_1$$

$$= 9(11 \dots 11 \alpha_x + \dots + 11 \alpha_3 + 1 \alpha_2) + \alpha_x + \dots + \alpha_3 + \alpha_2 + \alpha_1 \text{ sendo } \rho = 11 \dots 11 \alpha_x + \dots + 11 \alpha_3 + 1 \alpha_2 \text{ e } \alpha_x + \dots + \alpha_3 + \alpha_2 + \alpha_1$$


$= 9\rho + \theta$ como a primeira parcela é múltiplo de 9 o número só vai ser múltiplo de 9 se θ também for, ou seja se $\alpha + \beta + \gamma$ for múltiplo de 9 o número geral é.

□

8) Divisibilidade por 10: Um número natural é divisível por 10 quando ele termina em 0, ou seja um número é divisível por 10 se ele for divisível por 2 e 5.

Demonstração. É todo número divisível por 2, já demonstrado, e divisível por 5, também já demonstrado, ou seja para ser divisível por 5 e ser divisível por 2 ao mesmo tempo tem que ser um número terminado em 0. □


1.8 Números Perfeitos

Definição 1.8.1. Um número ~~se diz~~ perfeito se **é** igual a metade da soma de seus divisores 

Os números como 6 e 28, com a propriedade de serem iguais à metade da soma de seus divisores, tiveram o poder de fascinar os gregos antigos, que os chamaram de números perfeitos. Até a Idade Média, conheciam-se apenas os seguintes números perfeitos: 6, 28, 496, 8 128 e 33 550 336.

Atualmente, conhecem-se outros números perfeitos. Um fato curioso é que todos os números perfeitos conhecidos são pares. Não se sabe nada sobre a existência ou não de números perfeitos ímpares e sabe-se que todos os números perfeitos são da forma $2^{p-1} \cdot (2^p - 1)$, onde $(2^p - 1)$ é um primo de Mersenne o que nos leva a dizer que são conhecidos apenas 48 números perfeitos

1.9 Congruência

~~Trata-se da realização de uma aritmética com os restos da divisão euclidiana por um número fixado.~~  Seja m um número natural, diremos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais.

Quando os inteiros a e b são congruentes módulo m , escreve-se $a \equiv b \pmod{m}$.

Exemplo 1.9.1. Temos que $21 \equiv 13 \pmod{2}$, já que os restos da divisão de 21 e de 13 por 2 são iguais a 1.

Proposição 8. Se a, b, m e d são inteiros, $m > 0$, podemos afirmar;

i) $a \equiv a \pmod{m}$

ii) se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$

iii) se $a \equiv b \pmod{m}$ e $b \equiv d \pmod{m}$, então $a \equiv d \pmod{m}$

Demonstração. i) Como $m|0$, então $m|(a - a)$, o que resulta $a \equiv a \pmod{m}$

ii) Se $a \equiv b \pmod{m}$, então $a = b + k_1m$, para $k_1 \in \mathbb{Z}$. Logo $b = a - k_1m$, o que implica $b \equiv a \pmod{m}$.

iii) se $a \equiv b \pmod{m}$ e $b \equiv d \pmod{m}$, então existem $k_1, k_2 \in \mathbb{Z}$ tal que; $a = b + k_1m$ e $b = d + k_2m$, assim;

$$k_1m = a - b \text{ e } k_2m = b - d, \text{ somando as duas equações temos que}$$

$$(k_1 + k_2)m = a - d, \text{ o que implica em } a \equiv d \pmod{m}.$$

□

Proposição 9. Se, a, b, m e d são inteiros tais que $a \equiv b \pmod{m}$, podemos afirmar que

i) $a + d \equiv b + d \pmod{m}$

ii) $a - d \equiv b - d \pmod{m}$

iii) $ad \equiv b.d \pmod{m}$

Demonstração. i) e ii) Como $a \equiv b \pmod{m}$, logo

$$a = b + k_1m, \text{ então}$$

$$a - b = k_1m, \text{ podendo somar e subtrair a mesma parcela}$$

$$a - b - d + d = k_1m,$$

$$(a + d) - (b + d) = (a - b) - (b - d) = k_1m, \text{ o que implica em}$$

$$a + d \equiv b + d \pmod{m} \text{ e } a - d \equiv b - d \pmod{m}$$

iii) Como $a \equiv b \pmod{m}$, logo

$$a = b + k_1m, \text{ então}$$

$$a - b = k_1m, \text{ multiplicar por uma mesma parcela}$$

$$ad - bd = k_1dm, \text{ logo}$$

$$ad \equiv bd \pmod{m}.$$

□

Proposição 10. Se a, b, k e m são inteiros com $k > 0$ e $a \equiv b \pmod{m}$, então $a^k \equiv b^k \pmod{m}$.

Demonstração. Seja $a \equiv b \pmod{m}$, logo

$$a - b \equiv 0 \pmod{m} \text{ multiplicando por } d$$

$$(a - b).d \equiv 0.d \pmod{m}$$

$$(a - b).d \equiv 0 \pmod{m} \text{ supomos } d = a^{k-1} + a^{k-2}.b + a^{k-3}.b^2 + \dots + a^2.b^{k-3} + a.b^{k-2} + b^{k-1},$$

logo

$$(a - b).a^{k-1} + a^{k-2}.b + a^{k-3}.b^2 + \dots + a^2.b^{k-3} + a.b^{k-2} + b^{k-1} \equiv 0 \pmod{m}, \text{ como}$$


$$a^k - b^k = (a - b).a^{k-1} + a^{k-2}.b + a^{k-3}.b^2 + \dots + a^2.b^{k-3} + a.b^{k-2} + b^{k-1}, \text{ logo}$$

$$a^k - b^k \equiv 0 \pmod{m}, \text{ assim}$$

$$a^k \equiv b^k \pmod{m} \text{ C.Q.D}$$

□

Exemplo 1.9.2. Qual o resto da divisão de 367^{134} por 11?

 Calcular a potência 367^{134} , é inviável, pois o resultado é um número de muitos algarismos, então basta calcular;

$$367^{134} \equiv? \pmod{11} \text{ o que ainda está difícil}$$

$$367 \equiv 4 \pmod{11}, \text{ resto da divisão de } 367 \text{ por } 11$$

$$367^2 \equiv 4^2 \equiv 16 \equiv 5 \pmod{11}, \text{ elevamos os dois lados ao quadrado, e o resultado é o resto da divisão de } 16 \text{ por } 11$$

$$367^6 \equiv 5^3 \equiv 125 \equiv 4 \pmod{11}, \text{ elevamos os dois lados ao cubo, e o resultado é o resto da divisão de } 125 \text{ por } 11$$

$$367^{12} \equiv 4^2 \equiv 5 \pmod{11}, \text{ elevamos ao quadrado mais uma vez}$$

$$367^{36} \equiv 5^3 \equiv 4 \pmod{11}, \text{ novamente elevamos ao cubo}$$

$$367^{108} \equiv 4^3 \equiv 64 \equiv 9 \pmod{11} \text{ elevamos os dois lados ao cubo, e o resultado é o resto da divisão de } 64 \text{ por } 11$$

$$367^{108+12} \equiv 9.5 \equiv 45 \equiv 1 \pmod{11} \text{ multiplicamos } 9 \text{ vezes } 5, \text{ } 1 \text{ e o resultado e resto da divisão de } 45 \text{ por } 11$$

$$367^{120+12} \equiv 1.5 \equiv 5 \pmod{11}$$

$$367^{132+2} \equiv 5.5 \equiv 25 \equiv 3 \pmod{11}$$

Logo o resto da divisão de 367^{134} por 11 é 3.

Para maiores informações veja as referências [2], [10] e [4]

1.9.1 Teorema de Invertíveis

Proposição 11. Um número inteiro a é invertível módulo m quando existe b tal que $a.b \equiv 1 \pmod{m}$. Então, todos os números invertíveis módulo m são os coprimos com

m (ou seja, $\text{mdc}(a, m) = 1$).

Demonstração. Suponhamos $\text{mdc}(a, m) \neq 1, a < m$. Então, se

$$a \cdot b \equiv 1 \pmod{m}, \text{ logo}$$

$$a \cdot b = k \cdot m + 1, \text{ então}$$

$$a \cdot b - k \cdot m = 1$$

→ O que significa que uma combinação linear de a, m é igual a 1. Absurdo, pois a menor combinação linear que pode ocorrer entre dois números é seu mdc, que, neste caso, é diferente de 1. *De fato,*

Suponhamos que $a, b \in \mathbb{Z}$, com $a > b$ e seja $m = \text{mdc}(a, b)$, logo

$a = m \cdot k_1$ e $b = m \cdot k_2$, como $a > b$ logo $k_1 > k_2$, podendo afirmar que

$k_1 = k_2 + \alpha$ e $\alpha \in \mathbb{N}$, assim

$$a = m \cdot k_1$$

$$a = m \cdot (k_2 + \alpha)$$

$$a = m \cdot k_2 + m \cdot \alpha \text{ como } b = m \cdot k_2$$

$$a = b + m \cdot \alpha$$

$a - b = m \cdot \alpha$ sendo a diferença entre dois números igual a um múltiplo do $\text{mdc}(a, B)$, podendo se fazer uma combinação de a e b , ficando

$c \cdot a - d \cdot b = m \cdot \alpha$, com $c, d \in \{\mathbb{N} - 0\}$, sendo o menor resultado possível quando $\alpha = 1$.

□

1.10 Pequeno Teorema de Fermat

Se p é um número primo e se a é um número natural, então $a^p \equiv a \pmod{p}$. Em particular, se p não divide a , então $a^{p-1} \equiv 1 \pmod{p}$.

Demonstração. O resultado é verdadeiro para $a = 1$. Suponhamos seja verdadeiro para $a \geq 1$, então temos $(a + 1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}$, porque os coeficientes binomiais, $\binom{a}{k}$, $1 \leq k \leq p - 1$, são múltiplos de p .

□

Capítulo 2

Criptografia, Usos, Importância e Limites

2.1 Conceituando a Criptografia



Criptografia (do Grego *kryptós*, “escondido”, e *gráphein*, “escrita”) é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, com o intuito que seja conhecida apenas por seu destinatário, o que a torna difícil de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade. De fato, o estudo da criptografia cobre bem mais do que apenas cifragem e decifragem. É um ramo especializado da teoria da informação com muitas contribuições de outros campos da matemática e do conhecimento. A criptografia moderna é basicamente formada pelo estudo dos algoritmos criptográficos que podem ser implementados em computadores.

O primeiro uso conhecido da criptografia foi encontrado em hieróglifos irregulares esculpidos em monumentos do Antigo Império do Egito (há cerca de 4500 anos). Porém, não podem ser considerados como tentativas sérias de comunicações secretas, mas sim de ser mensagens misteriosas, intrigas ou mesmo diversão para os alfabetizados. Seguem outros exemplos de usos da criptografia. Algumas tabuletas de argila na Mesopotâmia, que um pouco mais tarde, foram utilizadas para proteger informações, por exemplo, receitas de valor comercial. Mais tarde ainda, estudiosos hebreus fizeram uso

de simples cifras de substituição monoalfabética começando talvez em torno de 500 a 600 a.C.

A criptografia pode ser entendida como uma técnica ou conjunto de técnicas que com o emprego de chave cifradora/decifradora possibilita tornar ininteligíveis textos claros e legíveis e, de forma inversa, tornar inteligíveis cifrados, com o objetivo de proteger uma informação contra qualquer acesso não autorizado.

Segundo definição do dicionário HOUAISS:

“Conjunto de princípios e técnicas empr. para cifrar a escrita, torná-la ininteligível para os que não tenham acesso às convenções combinadas; [...] em operações políticas, diplomáticas, militares, criminais etc., modificação codificada de um texto, de forma a impedir sua compreensão pelos que não conhecem seus caracteres ou convenções.(HOUAISS, 2007)”

Assim, ampliando a definição dada pelo dicionarista, é pertinente dizer que a criptografia pode ser definida como um conjunto de princípios ou de técnicas que podem ser utilizadas para codificar ou decodificar a escrita, seja ela uma mensagem, um texto, uma senha numérica ou alfanumérica, etc. com o objetivo de impedir sua compreensão, ou seja, torná-la ininteligível, para quem não possui conhecimento ou acesso às técnicas de cifragem ou decifragem.

Segundo o Instituto Nacional de Tecnologia da Informação (ITI), da Presidência da República, o processo de codificação ou ocultação é chamado de cifragem, enquanto que o processo inverso, no qual se obtém a informação original a partir do texto cifrado, chama-se decifragem.

Na ação de criptografar um texto é necessária a utilização de uma chave cifradora, ou chave criptográfica, que é um conjunto de bits que se constitui em uma espécie de senha, baseada em um determinado algoritmo, sendo que este algoritmo tenha a capacidade de codificar e de decodificar um texto ou um conjunto de informações.

Existem dois tipos ou categorias de chaves criptográficas: as chamadas chaves simétricas e chaves assimétricas.

2.2 A Criptografia e sua Importância



Figura 2.1: Avanço Tecnológico

Conforme Coutinho, em *Números Inteiros e Criptografia RSA*, o mundo moderno, fortemente marcado pela tecnologia e pelo uso da comunicação em massa por meio da internet, cada vez mais são criadas facilidades e comodidades com a pretensão e o objetivo de tornar mais ágil, prática e dinâmica a vida das pessoas. Todas essas tecnologias disponíveis por um lado tornam mais práticas certas tarefas do dia-a-dia, mas também nos levam ao desejo crescente de buscar soluções prontas, feitas sob medida para atender nossas necessidades.

Os bancos, ancorados em sistemas de comunicação via satélite, criaram os caixas eletrônicos e com eles o conceito de autoatendimento, que representou um grande avanço, pois ampliaram os locais de oferta dos serviços bancários aos clientes, reduzindo o tempo que os clientes precisavam gastar para realizar tais serviços e reduzindo custos com funcionários e toda a estrutura de funcionamento, que vai desde dispêndios com formulários impressos, aluguel e manutenção de imóveis próprios, etc. Além desse exemplo dos bancos, o uso da tecnologia se tornou uma característica marcante do mundo atual e os sistemas de informação ganha importância vital no cenário mundial nas últimas décadas.

Essa tecnologia, hoje indispensável para a vida das pessoas, para o funcionamento das instituições e para a manutenção da própria ordem mundial, porém tem uma espécie de “calcanhar de Aquiles”, pois junto com a as comodidades vieram alguns ônus, como a necessidade de proteção das informações que transitam através desses sistemas. Nesse particular, a criptografia ganhou elevada importância, pois desde a sua mais remota gênese ela teve o papel de proteger de terceiros, através de técnicas, algoritmos e códigos próprios, as mensagens trocadas entre um emissor e um receptor.

Hoje, desde o correio eletrônico (emissão e recepção de e-mails) à telefonia celular, do acesso seguro a servidores WEB ao uso da moeda eletrônica (cartões bancários e de crédito), a criptografia é parte vital para a segurança e confiabilidade dos sistemas de informação.

A criptografia é o elemento primordial para garantir a privacidade e a acurácia das

informações e, além disso, pode ajudar a imputar responsabilidade, promover a justiça, pois usada adequadamente protege a anonimidade e fornece provas de identidade de pessoas.


A criptografia previne fraudes em transações comerciais feitas através do chamado comércio eletrônico, garante a validade de transações financeiras, pode impedir vândalos, também chamados hackers, de alterarem páginas alheias na internet, assim como pode impedir competidores industriais de lerem seus documentos confidenciais, além de tudo isso a criptografia ainda tem grande importância por garantir a segurança de dados estratégicos de empresas, instituições e governos, garantindo inclusive segredos militares e informações diretamente ligadas à soberania nacional dos diversos países.

2.3 Requisitos Garantidos pela Criptografia



Atualmente as técnicas criptográficas são utilizadas para garantir a segurança dos sistemas de informações que tenham como requisitos sigilo, autenticação, integridade, não-repúdio e anonimato.


O sigilo é a proteção de dados contra divulgação não autorizada, impedindo que pessoas não autorizadas tenham acesso ou conhecimento desses dados ou informações.

Autenticação é um processo empregado na confirmação da identidade de uma pessoa ou entidade ou a fonte de uma mensagem. A autenticação tem como objetivo principal assegurar a veracidade e consistência de dados ou informações, bem como comprovar de forma segura e inequívoca a identidade e fidelidade da fonte e do usuário ou do emissor e do receptor.

 Integridade é a garantia que os dados recebidos são íntegros, ou seja, não sofreram quaisquer modificações e estão exatamente na forma como foram enviados por uma entidade autorizada.

Repudiar um fato ou uma ação é negar sua autoria para fugir da responsabilidade sobre ela. Os serviços de Não-repúdio usam os métodos de criptografia para impedir que um indivíduo ou uma entidade neguem a execução de uma ação particular relacionada aos dados fornecendo prova da origem.

 Possui a garantia de não ter a identidade revelada num sistema de comunicação, ou seja, não ter o nome revelado de acordo com a necessidade ou conveniência. 

 Chave é um algoritmo, uma espécie de código que se combina previamente para a cifragem e decifragem de uma mensagem para a qual se deseja um determinado nível

de sigilo.

Na ação de criptografar um texto é necessária a utilização de uma chave cifradora, ou chave criptográfica, um conjunto de bits que se constitui em uma espécie de senha, baseada em um determinado algoritmo, sendo que este algoritmo tenha a capacidade de codificar e de decodificar um texto ou um conjunto de informações.

Existem dois tipos ou categorias de chaves criptográficas: as chamadas chaves simétricas e chaves assimétricas.

A chamada chave simétrica é também denominada como chave secreta ou chave única. Sempre objetivando a garantia de confidencialidade dos dados, nessa modalidade, usa-se a mesma chave nos dois processos, o de codificação e o de decodificação.

A chave simétrica apresenta limites, pois se codificação e a decodificação forem feitas por mais de uma pessoa ou por equipamentos diferentes ela precisa ser previamente combinada entre as partes, o que para evitar o comprometimento da chave, deve ser feito através de um canal de comunicação seguro, o que fragiliza o sistema, tornando-o suscetível à falhas e reduzindo seu grau de segurança, uma vez que na transmissão dessa chave entre as partes ela pode ser acessada por terceiros. Além desse limite o uso de chaves simétricas tem outros pontos negativos, como, por exemplo, a necessidade de uma grande quantidade de chaves caso muitas pessoas ou entidades estejam envolvidas.

Criptografia de Chave Assimétrica também **conheida** como criptografia de chave pública, usa duas chaves distintas: uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo pelo dono. Uma vez que a informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la.

A escolha de qual chave deve-se usar para codificar depende do nível de proteção que se deseja, se confidencialidade ou autenticação, integridade ou não-repúdio. Existem diversos métodos criptográficos que usam chaves assimétricas, dentre os quais se destacam, RSA, DSA, ECC e Diffie-Hellman, sendo o RSA um dos mais difundidos e sobre o qual fez-se análise mais profunda no Capítulo 3 deste trabalho.

Capítulo 3

Criptografia

3.1 Criptografia RSA

De acordo com Coutinho [2], na década de 70, dois cientistas da computação que trabalhavam no Massachusetts Institute of Technology (M.I.T.), uma das melhores universidades americanas, Ronald Rivest e Adi Shamir, estavam empenhados em criar um método de criptografia de chave assimétrica eficiente. Eles foram ajudados pelo matemático Leonard Adleman, que validava as ideias dos dois pelo ponto de vista matemático. Em 1977 os três registraram a patente do método RSA.

O RSA foi construído sobre uma das áreas mais clássicas da matemática, a Teoria dos números. O método se baseia na dificuldade em fatorar um número em seus componentes primos.

Para usarmos o método RSA, primeiramente devemos converter uma mensagem, em que não há números, em uma sequência numérica.

Faremos a pré-codificação, convertendo as letras em números:

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

Para o espaço entre duas palavras será usado o número 99.

Por exemplo a frase “Amo minha família” ficaria assim convertida:

1022249922182317109915102218211810.

Tendo em mente que todas as letras teriam que ser representadas por um número de dois algarismos, visto que caso contrário, 12 poderia ser tanto a codificação de AB, quanto a codificação de L, que é a décima segunda letra do nosso alfabeto.

Agora precisamos de dois números primos quaisquer p e q , não podendo ser números pequenos, mas no exemplo apresentado escolheremos dois números primos pequenos, só para entendimento, os números primos são eles: 11 e 17, depois de escolhidos os dois primos determinaremos n , sendo;

$$n = p \cdot q,$$

$$\text{logo } n = 11 \cdot 17 = 187$$



Agora separamos a sequência acima em blocos, tomando os seguintes cuidados:

- i) Os blocos não pode ser maior que n ;
- ii) Os blocos não podem começarem com zero.

Com essas exigências temos que nossa mensagem fica assim pré-codificada

102 – 22 – 49 – 92 – 21 – 82 – 31 – 7 – 109 – 91 – 5 – 102 – 21 – 82 – 11 – 8 – 10.

Para maiores informações consulte as referências [2] e [4].

3.2 Codificação

Nessa etapa, destacamos a importância de “ n ”, e agora precisamos de um “ e ”, que seja ímpar, ou seja $\text{MDC}(e, \phi(n))=1$, onde $\phi(n) = (p-1).(q-1)$.

Lembrando que nosso exemplo $p = 11$ e $q = 17$, $\phi(n) = (11-1).(17-1) = 10.16 = 160$. O que nos dá uma imensa possibilidade de $e \in \{3, 7, 9, \dots\}$ e no nosso caso escolheremos um $e = 3$, que é o menor primo que não divide $\phi(n) = 160$.

Não nos esquecendo que a pré-codificação anterior dividiu a mensagem em blocos menores, que denominaremos de b e a codificação desse pequeno bloco de $C(b)$, agora é só codificar cada bloco um a um, denominando (n, e) como chave de codificação, sendo:

$C(b) = \text{resto da divisão de } b^e \text{ por } n$

Sendo o exemplo do bloco $b = 102$, que é o primeiro bloco da pré-codificação, ficará codificado como resto da divisão 102^3 por 187;

$$102^3 \equiv 170 \pmod{187};$$

Mas, como chegamos a esse resultado;

$102 \equiv 102 \pmod{187}$ pela definição $a \equiv a \pmod{m}$

$102 \equiv -85 \pmod{187}$, pois $102 = k_1.187 + (-85)$

$102^2 \equiv (-85)^2 \equiv 119 \pmod{187}$ elevando a 2 os dois lados da equivalência

$$102^3 \equiv 119.(-85) \equiv -17 \equiv 170 \pmod{187}$$

Logo o bloco $b = 102$ codificado é igual a 170, ou seja $C(102) = 170$.

Codificando o segundo bloco $b = 22$, que também é o resto da divisão de 22^3 por 187;

$$22^3 \equiv 176 \pmod{187}$$

Explicando como chegamos a esse resultado:

$22 \equiv 22 \pmod{187}$ (não convém expressar $22 \equiv -165 \pmod{187}$, pois -165 tem módulo maior que o módulo de 22)

$$22^3 \equiv 22^3 \equiv 176 \pmod{187}$$

Logo o bloco $b = 22$ codificado é igual a 176, ou seja $C(102) = 176$.

Agora codificando toda mensagem temos

$$\begin{aligned}
 C(102) &\equiv 102^3 \pmod{187} = 170; \\
 C(22) &\equiv 22^3 \pmod{187} = 176; \\
 C(49) &\equiv 49^3 \pmod{187} = 26; \\
 C(92) &\equiv 92^3 \pmod{187} = 20; \\
 C(21) &\equiv 21^3 \pmod{187} = 98; \\
 C(82) &\equiv 82^3 \pmod{187} = 92; \\
 C(31) &\equiv 31^3 \pmod{187} = 58; \\
 C(7) &\equiv 7^3 \pmod{187} = 156; \\
 C(109) &\equiv 109^3 \pmod{187} = 54; \\
 C(91) &\equiv 91^3 \pmod{187} = 148; \\
 C(5) &\equiv 5^3 \pmod{187} = 125; \\
 C(102) &\equiv 102^3 \pmod{187} = 170; \\
 C(21) &\equiv 21^3 \pmod{187} = 98; \\
 C(82) &\equiv 82^3 \pmod{187} = 92; \\
 C(11) &\equiv 11^3 \pmod{187} = 22; \\
 C(8) &\equiv 8^3 \pmod{187} = 138; \\
 C(10) &\equiv 10^3 \pmod{187} = 65;
 \end{aligned}$$

Ficando toda mensagem codificada assim na forma

170-176-26-20-98-92-58-156-54-148-125-170-98-92-22-138-65

Para maiores informação consulte as referências [2] e [4].

3.3 Decodificação

Para decodificar uma mensagem precisamos de conhecer dois números, n e o inverso de e em, $\phi(n)$, que denominaremos por d . Dividindo $\phi(187) = 160$ por $e = 3$, temos;

$160 \equiv 1 \pmod{3}$, pois

$$160 = 3 \cdot 53 + 1$$

$$1 = 160 + 3 \cdot (-53)$$

logo, o inverso de 3 módulo 160 é -53, como tem que ser um número inteiro positivo então;

$$d = 160 - 53 = 107, \text{ pois; } -53 \equiv 107 \pmod{160};$$

Chamaremos o par (n, d) de chave de decodificação. Seja a um bloco da mensagem codificada, então $D(a)$ será o resultado do processo de decodificação, onde

$$D(a) = \text{resto da divisão de } a^d \text{ por } n$$

Sendo o bloco codificado 170, que é o primeiro bloco da codificação, ficará descodificado como resto da divisão de 170^{107} por 187; ou seja

$$170^{107} \equiv 102 \pmod{187}$$

Explicando como chegamos a esse resultado:

$$\begin{aligned} 170 &\equiv 170 \pmod{187} \text{ pela definição } a \equiv a \pmod{m} \\ 170 &\equiv -17 \pmod{187} \text{ pois } 170 = k_1 \cdot 187 + (-17) \\ 170^2 &\equiv (-17)^2 \equiv 102 \pmod{187} \text{ elevando a 2 os dois lados da equivalência} \\ 170^4 &\equiv 102^2 \equiv 119 \pmod{187} \text{ elevando a 2 todas as equivalências} \\ 170^8 &\equiv 119^2 \equiv 136 \pmod{187} \\ 170^{16} &\equiv 136^2 \equiv 170 \equiv -17 \pmod{187} \\ 170^{32} &\equiv (-17)^2 \equiv 102 \pmod{187} \\ 170^{64} &\equiv 102^2 \equiv 119 \pmod{187} \\ 170^{64+32} &\equiv 119 \cdot 102 \equiv 170 \equiv -17 \pmod{187} \\ 170^{96+8} &\equiv (-17) \cdot 136 \equiv -68 \equiv 119 \pmod{187} \\ 170^{104+2} &\equiv 119 \cdot 102 \equiv 170 \equiv -17 \pmod{187} \\ 170^{106+1} &\equiv (-17) \cdot (-17) \equiv 102 \pmod{187} \end{aligned}$$

E no passo inverso da codificação, agora decodificamos toda mensagem;

Como queríamos demonstrar, codificamos o bloco b , e sua decodificação voltou ao mesmo bloco b que foi codificado para originar o bloco a no início. Logo, $D(a) = b$, e neste caso temos $a = 170$ que descodificado é igual a 102.

Mas, para termos certeza iremos descodificar mais um bloco.

Que é o segundo bloco da codificação, ficará descodificado como resto da divisão de 176^{107} por 187; ou seja

$$176^{107} \equiv 22 \pmod{187}$$

Novamente demonstraremos isso:

$$\begin{aligned} 176 &\equiv 176 \pmod{187} \text{ pela definição } a \equiv a \pmod{m} \\ 176 &\equiv -11 \pmod{187} \text{ pois } 176 = k_1 \cdot 187 + (-11) \\ 176^3 &\equiv (-11)^3 \equiv -22 \pmod{187} \text{ elevando a 3 os dois lados da equivalência} \\ 176^6 &\equiv (-22)^2 \equiv 110 \pmod{187} \text{ elevando a 2 todas as equivalências} \\ 176^{12} &\equiv 110^2 \equiv 132 \pmod{187} \end{aligned}$$

$$\begin{aligned}
176^{24} &\equiv 132^2 \equiv 33 \pmod{187} \\
176^{48} &\equiv 33^2 \equiv 154 \equiv -33 \pmod{187} \\
176^{96} &\equiv (-33)^2 \equiv 154 \equiv -33 \pmod{187} \\
176^{96+6} &\equiv (-33) \cdot 110 \equiv -77 \pmod{187} \\
176^{102+3} &\equiv (-77) \cdot (-22) \equiv 11 \pmod{187} \\
176^{105+1} &\equiv 11 \cdot (-11) \equiv -121 \pmod{187} \\
176^{106+1} &\equiv (-121) \cdot (-11) \equiv 22 \pmod{187}
\end{aligned}$$

E, mais uma vez pudemos a confirmar que decodificando o bloco $a = 176$, encontramos 22, que é exatamente b

Agora decodificaremos toda mensagem;

$$\begin{aligned}
D(170) &\equiv 170^{107} \pmod{187} = 102 \\
D(176) &\equiv 176^{107} \pmod{187} = 22 \\
D(26) &\equiv 26^{107} \pmod{187} = 49 \\
D(20) &\equiv 20^{107} \pmod{187} = 92 \\
D(98) &\equiv 98^{107} \pmod{187} = 21 \\
D(92) &\equiv 92^{107} \pmod{187} = 82 \\
D(58) &\equiv 58^{107} \pmod{187} = 31 \\
D(156) &\equiv 156^{107} \pmod{187} = 7 \\
D(54) &\equiv 54^{107} \pmod{187} = 109 \\
D(148) &\equiv 148^{107} \pmod{187} = 91 \\
D(125) &\equiv 125^{107} \pmod{187} = 5 \\
D(170) &\equiv 170^{107} \pmod{187} = 102 \\
D(98) &\equiv 98^{107} \pmod{187} = 21 \\
D(92) &\equiv 92^{107} \pmod{187} = 82 \\
D(22) &\equiv 22^{107} \pmod{187} = 11 \\
D(138) &\equiv 138^{107} \pmod{187} = 8 \\
D(65) &\equiv 65^{107} \pmod{187} = 10
\end{aligned}$$

Ficando a mensagem decodificada igual a pré-codificação;

$$102 - 22 - 49 - 92 - 21 - 82 - 31 - 7 - 109 - 91 - 5 - 102 - 21 - 82 - 11 - 8 - 10.$$

Para maiores informação consulte as referências [2] e [4].

3.4 Por que Funciona?

O sistema RSA tem parâmetros p e q , com $n = p \cdot q$, sendo os dados codificados em parâmetros n e e , chave de codificação, e decodificado em parâmetro n e d , chave de decodificação. Contudo queremos apenas provar que $D(C(b)) \equiv b \pmod{n}$, para isso vamos lembrar que;

i) para codificação temos;

$$C(b) = \text{resto da divisão de } b^e \text{ por } n,$$

$$b^e \equiv C(b) \pmod{n}$$



ii) para decodificação temos;

$$D(a) = \text{resto da divisão de } a^d \text{ por } n$$

$$a^d \equiv D(a) \pmod{n}$$

iii) e que ainda;

$$C(b) = a \text{ e } D(a) = b$$

Contudo;

$$a^d = C(b)^d \equiv (b^e)^d \equiv D(a) = b \pmod{n}$$

Como b é um número maior que 1 e menor que $(n - 1)$, a congruência acontece se a igualdade for verdadeira, por isso temos que escolher blocos b , da pré-codificação, menores que n .

$$D(C(b)) \equiv (b^e)^d \equiv b^{e \cdot d} \pmod{n}.$$

Como d é o inverso de e módulo $\phi(n)$, temos que $e \cdot d = 1 + K \cdot \phi(n)$, onde K pertence a \mathbb{Z} . Veja que, $e, d \in \mathbb{Z}$, onde $e, d > 2$ e $\phi(n) > 0$, portanto $k > 0$, nos possibilitando substituir $e \cdot d$ por $1 + K \cdot \phi(n)$, sendo assim;

$$D(C(b)) \equiv (b^e)^d \equiv b^{1+K \cdot \phi(n)} \equiv b \cdot b^{K \cdot \phi(n)} \pmod{n} \text{ como } \phi(n) = (p-1)(q-1)$$



$$D(C(b)) \equiv (b^e)^d \equiv b^{e \cdot d} \equiv b^{1+K \cdot \phi(n)} \equiv b \cdot b^{K \cdot \phi(n)} \equiv b \cdot b^{K \cdot (p-1)(q-1)} \equiv b \cdot b^k \cdot b^{p-1} \cdot b^{q-1} \pmod{n}$$

i) Supondo que p não divide b , então, pelo Pequeno Teorema de Fermat;

$$b^{p-1} \equiv 1 \pmod{p} \text{ logo;}$$

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

ii) Supondo que p divide b ;

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

$b^{ed} \equiv b \pmod{p}$ para qualquer b

E fazemos, o mesmo para q , por analogia.

Demostramos que $b^{ed} - b$ é divisível por p e por q , pelo Pequeno Teorema de Fermat, logo podemos afirmar que $b^{ed} - b$ é divisível por n , sendo $n = p.q$.

Portanto $b^{ed} \equiv b \pmod{n}$, ou seja $D(C(b))=b$

Para maiores informação consulte a referência [2].

3.5 RSA Realmente é Seguro?

Sendo o RSA um método de chave pública, de parâmetro p e q , sendo $n = p.q$, tem o par (n, e) acessível a qualquer usuário.

Logo, a chave de codificação é acessível a qualquer um, ou seja, um dos segredos é decodificar a mensagem, pois codificá-la qualquer um que tenha o conhecimento matemático necessário conseguirá fazer e decodificar a mensagem ficará mais difícil quanto mais difícil for calcular d , conhecendo apenas n e e .

Mas, teoricamente, só conseguiremos calcular d se soubermos $\phi(n)$, que é determinado por $\phi(n) = (p - 1).(q - 1)$. Poderíamos tentar fatorar n e assim determinarmos p e q , entretanto n é um número muito grande, o que torna difícil fatorá-lo.

Supostamente, se consiga calcular $\phi(n)$ a partir de (n, e) , sem fatorar n , então o que queremos agora é calcular p e q , não esquecendo que;

$$n = p.q \text{ e}$$

$$\phi(n) = (p - 1).(q - 1) \text{ aplicando propriedade distributiva}$$

$$\phi(n) = p.q - p - q + 1$$

$$\phi(n) = n - (p + q) + 1$$

$$(p + q) = n - \phi(n) + 1$$



O que seria fácil determinar pois conhecemos n e $\phi(n)$.

$$(p + q) = p.q - (p - 1).(q - 1) + 1 \text{ substituido } n = p.q \text{ e } \phi(n) = (p - 1).(q - 1)$$

$(p + q) = p.q - p.q + p + q - 1 + 1$, elevando ao quadrado e depois subtraindo $4n = 4p.q$ em ambos lados da igualdade

$$(p + q)^2 - 4n = (p^2 + q^2 + 2p.q) - 4p.q$$

$$(p + q)^2 - 4n = p^2 + q^2 - 2p.q$$

$$(p + q)^2 = (p - q)^2 + 4n$$

$$(p - q) = \sqrt{(p - q)^2 + 4n}.$$

Determinado $(p + q)$ e $(p - q)$, fica fácil calcularmos p e q , ou seja fatoramos n , o que não adianta para a decodificação, pois não teríamos meio de chegarmos a chave decodificadora (d, n)

Ainda podemos imaginar que conseguimos determinar d diretamente usando apenas n e e , como $\text{mdc}(e, d) = 1$, conseguimos nada a mais que um múltiplo de $\phi(n)$

Acredita-se que quebrar o RSA e, ou, fatorar n sejam equivalentes e teoricamente impossível, embora ninguém até agora tenha demonstrado. E até agora isso tem sido o suficiente para dizer que o sistema RSA é extremamente seguro.

Para maiores informação consulte a referência [2].

3.6 Os Primos Perfeitos Para o RSA

Uma questão muito importante, a ponto de tornar a segurança do RSA questionável, é a escolha dos números primos, p e q , pois a segurança do RSA não está nos cálculos para codificar ou decodificar, e sim na fatoração de n , ou seja temos que tornar essa fatoração quase que impossível, não podendo esquecer que na escolha dos primos p e q ;

- i)* não podem serem números pequenos, pois números pequenos facilitaria a fatoração de n ;
- ii)* logo, então tem que ser números grandes, tornando n um número maior ainda, pois $n = p \cdot q$;
- iii)* não basta escolher p e q grandes, mas também é importante que $|p - q|$ seja pequeno;
- iv)* verificar se $p - 1, q - 1, p + 1, q + 1$ não tem vários fatores primos pequenos;
- v)* p e q tem que ter a ordem aproximadamente entre 100 e 200 algarismos, para assim dificultar ainda mais o de fatoração;

Se prestarmos atenção a esses critérios, qualquer algoritmo de fatoração já conhecido se tornará inadequado para a fatoração de n .

Para maiores informação consulte as referências [2].

Considerações finais

A criptografia foi no passado e é nos dias atuais um elemento de grande importância para a proteção de mensagens, dados e informações transmitidas de um emissor para um receptor através de um meio que possa ser acessado por terceiros, permitindo assim a quebra do sigilo sobre o teor da mensagem, sobre as informações ou sobre os dados transmitidos.

~~A criptografia~~ se baseia fundamentalmente na codificação e decodificação de informações por meio de algoritmos matemáticos que usam conhecimentos fundamentais da matemática, como os conceitos de números naturais, números inteiros, números primos, fatoração, mínimo múltiplo comum (MMC), máximo divisor comum (MDC), critérios de divisibilidade etc., todos esses conceitos trabalhados no Ensino Fundamental e possíveis de serem retomados no Ensino Médio.

A cifragem e decifragem de mensagens podem ser amplamente trabalhadas em sala de aula, pois se trata de um tema atual, de grande importância, que possui aplicabilidade e refere a temas de grande interesse da juventude nessa fase escolar, quais sejam informática, internet, redes sociais, etc.

Como o ensino de matemática na escola pública brasileira vive um momento de profunda crise, sendo que esta ocupa o primeiro lugar entre as mais temidas e rejeitadas disciplinas do currículo escolar, sendo alvo de críticas e apresentando os piores resultados e os mais baixos índices de aprendizagem, o que aponta para a necessidade de se criar novas estratégias de ensino e mostrar a importância e aplicabilidade dos conhecimentos matemáticos em situações importantes da vida real das pessoas.

A aplicação da criptografia e o ensino da codificação e decodificação de mensagens em sala de aula podem representar um fator importante para a motivação dos alunos para a aprendizagem dos conceitos matemáticos empregados nos processos de cifragem e decifragem, bem como mostrar a matemática como algo significativo, prático, que pode ser aprendido e que possui aplicabilidade e significado real dentro do seu contexto

de vida e das suas áreas de interesse.

Referências Bibliográficas

- [1] CHEFEZ, A. & VILLELA, M.L., *Códigos Corretores de Erros*, Rio de Janeiro: IMPA, 2008.
- [2] COUTINHO, S.C., *Números Inteiros e Criptografia RSA*, Rio de Janeiro: IMPA, 2014.
- [3] DOMINGUES, H.H., *Fundamentos de Aritmética* Atual Editora.
- [4] HEFEZ, A., *MA 14- Aritmética- unidades 1-24* SBM.
- [5] IEZZI, G., *Fundamentos de Matemática Elementar* volumes 1-11, 8 ed. São Paulo: ATUAL EDITORA, 2013.
- [6] IFRAH, G., *Os Números a história de uma grande invenção* 6 ed. São Paulo: EDITORA GLOBO, 1994.
- [7] LIMA, E.L., *A matemática do ensino médio* volumes 1,2 e 3, 10 ed. Rio de Janeiro: IMPA, 2012.
- [8] LIMA, E.L., *Meu professor de Matemática e outras histórias* 6 ed. Rio de Janeiro: SBM, 2012;
- [9] MACHADO, A.S., *MATEMÁTICA TEMAS E METAS* volumes 1-6, 8 ed. São Paulo: ATUAL EDITORA, 1998
- [10] MARTINEZ, F.B., MOREIRA, C.G., SADANHA, N. & TENGAN, E., *Teoria dos números um passeio com primos e outros números familiares pelo mundo inteiro* 2 ed. Rio de Janeiro: IMPA, 2013
- [11] NUNES, TEREZINHA & BRYANT, PETER, *Crianças fazendo matemática* Porto Alegre: Artes Médicas, 1997.

- [12] SANTOS, J.P.O., *Introdução à Teoria dos Números*, 3 ed. Rio de Janeiro: IMPA, 2014.
- [13] SINGH, S., *O Último Teorema de Fermat* 13 ed. Rio de Janeiro: EDITORA RECORD, 2008.
- [14] RIBENBOIM, P., *Números Primos Velhos Mistérios e Novos Recordes*, 1 ed. Rio de Janeiro: IMPA, 2014.
- [15] TAO, T., *Como Resolver Problemas Matemáticos* Rio de Janeiro: SBM, 2013.
- [16] FIGURA: *Pedreiro trabalhando* <http://deciopedreiro.blogspot.com.br/2012/11/deciopedreiro.html>.
- [17] FIGURA: *Máquina de Criptografia* <http://segundaguerradocsdvd.blogspot.com.br/2014/07/codigo-enigma-legendado-dvd-r.html>.
- [18] FIGURA: *Alan Turing* <http://www.biography.com/people/alan-turing-9512017>.
- [19] FIGURA: *Evolução dos Números* <http://matematica.no.sapo.pt/nconcreto.htm>.
- [20] FIGURA: *Pierre de Fermat* <http://www.rugusavay.com/pierre-de-fermat-quotes>.
- [21] FIGURA: *Marin Mersenne* [https://pt.wikipedia.org/wiki/Marin Mersenne](https://pt.wikipedia.org/wiki/Marin_Mersenne).
- [22] FIGURA: *Números indo-arábicos* <http://numeros-g06.blogspot.com.br/p/o-sistema-de-numeracao-indo-arabico.html>.
- [23] FIGURA: *Avanço Tecnológico* <http://tecnologia.culturamix.com/noticias/alergia-a-tecnologia-uma-doenca-curiosa>.