UNIVERSIDADE FEDERAL DO TOCANTINS
CÂMPUS PROF. DR. SÉRGIO JACINTHO LEONOR
MESTRADO PROFISSIONAL EM MATEMÁTICA

VALÉRIA BATISTA DA SILVA

NÚMEROS PRIMOS E CRIPTOGRAFIA: DO CONCEITO AO SISTEMA RSA

ARRAIAS-TO
2019

VALÉRIA BATISTA DA SILVA

NÚMEROS PRIMOS E CRIPTOGRAFIA: DO CONCEITO AO SISTEMA RSA

Dissertação apresentada ao Programa de Pós-Graduação em Matemática como requisito parcial para à obtenção do grau de Mestre em Matemática.

Orientador: Prof[a]. Dr[a]. Alcione Marques Fernandes

ARRAIAS-TO
2019

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da Universidade Federal do Tocantins

S586n Silva, Valéria Batista da.

Números Primos e Criptografia: do Conceito ao Sistema RSA. / Valéria Batista da Silva. – Arraias, TO, 2019.

88 f.

Dissertação (Mestrado Profissional) - Universidade Federal do Tocantins – Câmpus Universitário de Arraias - Curso de Pós-Graduação (Mestrado) Profissional em Matemática, 2019.

Orientadora : Alcione Marques Fernandes

1. Números Primos. 2. Criptografia. 3. Criptografia RSA. 4. Educação Básica. I. Título

CDD 510

Elaborado pelo sistema de geração automática de ficha catalográfica da UFT com os dados fornecidos pelo(a) autor(a).

VALÉRIA BATISTA DA SILVA[1]

NÚMEROS PRIMOS E CRIPTOGRAFIA: DO CONCEITO AO SISTEMA RSA

Dissertação apresentada ao Programa de Pós-Graduação Mestrado Profissional em Matemática em Rede (ProfMat) da Universidade Federal do Tocantins (UFT), como requisito parcial para obtenção do título de Mestre em Matemática e aprovada em sua forma final pela Orientadora e pela Banca Examinadora.

Data de Aprovação: 13/12/2019

BANCA EXAMINADORA:

Dra. Alcione Marques Fernandes – UFT/Matemática
Orientadora

Dra. Eunice Cândida Pereira Rodrigues – CUR/UFMT
Examinadora

Élis Gardel da Costa Mesquita

Dr. Élis Gardel da Costa Mesquita – UFT/Matemática
Examinador

Arraias - TO
2019

1 O presente trabalho foi realizado com apoio da Pró-Reitoria de Pesquisa e Pós-Graduação (Propesq) da Universidade Federal do Tocantins (UFT).

Aos meus pais, irmãs e amigos.

Agradecimentos

A Deus, antes de tudo, por derramar bençãos todos os dias sobre minha vida, me dar sustento em dias difíceis e garantir que sou capaz de alcançar aquilo que Ele escolheu para mim.

A minha família, minha mãe Brasilene e meu pai Aldenor, por serem o motivo de buscar meus sonhos, me apoiar, entender e me tornar um ser humano melhor, sinto-me extremamente orgulhosa e privilegiada por Deus ter me abençoado com vocês. As minhas irmãs Valcene, Vanúbya e Cíntia pelo companheirismo e ajuda sempre que necessito, inclusive por ouvir minhas angústias.

Aos meus amigos, que me inspiram e apoiam a buscar por novos conhecimentos, estão comigo em várias situações e me ajudam a formar uma segunda família em Cristo. Aqueles que estão por perto e aos que precisam se distanciar mas que se fazem presentes no coração. Obrigada pelo companheirismo e amizade incondicional.

Aos professores do mestrado e do curso de Matemática da Universidade Federal do Tocantins campus Prof. Dr. Sérgio Jacintho Leonor. Aos meus colegas de mestrado, pela companhia e por tornarem alguns momentos mais leves.

A minha orientadora Alcione pela competência, profissionalismo e dedicação; por ter acreditado em minhas ideias para desenvolver esse trabalho, as contribuições valiosas e as conversas que me deixavam mais tranquila.

Aos membros da banca examinadora que gentilmente aceitaram participar e colaborar com esta dissertação.

A Universidade Federal do Tocantins, ao conceder a bolsa por meio do Programa de Tutoria de Pós-Graduação da PROGRAD e PROPESQ. Aos meus tutorandos, que permitiram uma parte desse trabalho ser possível, acolheram minhas ideias, compartilharam seus conhecimentos e reflexões.

Enfim, a cada pessoa que contribui para minha formação humana e profissional, que acreditam em mim e ajudam na realização dos meus sonhos.

Os primos são as pérolas que adornam a vastidão infinita do universo de números que os matemáticos exploraram ao longo dos séculos. Eles despertam a admiração dos matemáticos: 2, 3, 5, 7, 11, 13, 17, 19, 23... — números eternos que existem em uma espécie de mundo independente de nossa realidade física. São um presente da natureza para o matemático. (Marcus du Sautoy)

Resumo

Esta dissertação tem como objetivo apresentar os números primos e a criptografia para a Educação Básica por meio de atividades de ensino. Dessa forma, são exibidas uma experiência vivenciada na turma de tutoria do Programa de Pós-Graduação e propostas de atividades aos professores. No âmbito educacional, o trabalho tem a finalidade de favorecer a reflexão dos professores em relação a maneira de ensino dos números primos aliados a criptografia, ressaltando que esses são essenciais para a criação de chaves públicas no sistema criptográfico RSA. Para o desenvolvimento da pesquisa foi necessário realizar uma pesquisa bibliográfica para permitir uma exploração do conceito dos números e da criptografia; desenvolvemos também atividades de ensino como experiência de ensino e propomos atividades para evidenciar que a relação entre esses números e a criptografia é possível em sala de aula. Sendo assim, a pesquisa é caracterizada como exploratória, de cunho qualitativo. As atividades sugeridas pretendem instigar o professor de Matemática da Educação Básica a refletir sobre as novas formas de abordar os números primos, mostrar uma das principais aplicações do conteúdo ao cotidiano dos alunos para que assim possibilitem a seus alunos ver a Matemática além da sala de aula.

Palavras-chaves: Números Primos. Criptografia. Criptografia RSA. Educação Básica.

Abstract

This dissertation aims to present prime numbers and cryptography for Basic Education through teaching activities. Thus, an experience lived in the Graduate Program tutoring class and proposals for activities to teachers are displayed. In the educational field, the work aims to encourage teachers to reflect on how to teach prime numbers combined with cryptography, emphasizing that these are essential for the creation of public keys in the RSA cryptographic system. For the development of the research it was necessary to perform a bibliographic search to allow an exploration of the concept of numbers and cryptography; We also develop teaching activities as a teaching experience and propose activities to show that the relationship between these numbers and cryptography is possible in the classroom. Thus, the research is characterized as exploratory, qualitative in nature. The suggested activities are intended to prompt the Basic Education Mathematics teacher to reflect on the new ways of approaching prime numbers, to show one of the main applications of content to the students' daily life so that they allow their students to see mathematics beyond the classroom.

Key-words: Prime numbers. Encryption RSA encryption. Basic Education.

Sumário

1 INTRODUÇÃO 11

2 OS NÚMEROS 13
2.1 Breve contexto histórico do número 13
2.2 Simbologia dos números 19

3 OS NÚMEROS PRIMOS 23
3.1 Breve introdução histórica 23
3.2 Aritmética básica 24
3.3 Números primos 28
3.4 Métodos para encontrar números primos 31
3.4.1 Crivo de Eratóstenes 31
3.4.2 Fórmulas polinomiais 32
3.4.3 Fórmulas exponenciais 33
3.4.3.1 Primos de Mersenne 33
3.4.3.2 Primos de Fermat 34
3.5 Conjecturas 34

4 CRIPTOGRAFIA 36
4.1 Contextualização histórica 36
4.2 A criptografia RSA 46
4.3 Por que o sistema RSA funciona? 51
4.4 Por que o RSA é seguro? 52
4.5 Assinaturas digitais 53

5 NÚMEROS PRIMOS E CRIPTOGRAFIA NA SALA DE AULA 55
5.1 Uma experiência com números primos 55
5.2 Resultados da atividade 57
5.3 Atividades envolvendo a criptografia para sala de aula 64

6 CONSIDERAÇÕES FINAIS 80

REFERÊNCIAS 82

APÊNDICES 84
6.1 Questionário de sondagem de conhecimentos 84
6.2 Teste de aprendizagem 84

6.3 Atividade 1 . . . . . **85**
6.4 Atividade 2 . . . . . **85**
6.5 Atividade 3 . . . . . **87**

1 INTRODUÇÃO

Os números são fundamentais para a humanidade, tendo em vista que eles surgem nas mais variadas atividades do cotidiano das pessoas. Estudar as propriedades dos números inteiros positivos é o objetivo central da Teoria dos Números. Nos preocupamos neste trabalho em estudar os números primos e conceitos matemáticos importantes para a compreensão do método criptográfico chamado RSA, o qual se utiliza desses números para a criação de chaves.

Apresentamos um estudo sobre tais números e a criptografia com o intuito de motivar o professor da Educação Básica ao ensino desses, por meio de atividades que envolvam uma parte da Teoria dos Números e a ciência de escrever em códigos, como uma forma de estimular o ensino da Matemática sob abordagens diferentes do habitual. Os números primos são fundamentais para o sistema RSA, o mais conhecido método criptográfico de chave pública; é por meio deles que temos segurança ao enviar e-mails, fazer transações bancárias on-line, compras virtuais e isso é interessante para apresentar ao aluno a fim de evidenciar em quais aspectos os conteúdos matemáticos são perceptíveis além da sala de aula.

A pergunta motivadora do trabalho foi *de que forma os números primos e a criptografia podem ser levados para a Educação Básica?* Uma de nossas hipóteses é que a relação entre esses números e a criptografia constitui uma forma de mostrar aos alunos da Educação Básica que conceitos aparentemente abstratos, estão por trás de muitas situações do nosso cotidiano. Assim, nosso objetivo geral consiste em estudar maneiras de apresentar essa relação em sala de aula. Instigamo-nos a realizar tal tarefa estudando as propriedades dos números primos; a criptografia em vários aspectos e destacando o sistema RSA; analisando metodologias para o ensino dos números primos e os aspectos em que a criptografia pode ser explorada em sala de aula pelo professor.

Em relação aos objetivos, nossa pesquisa é caracterizada como exploratória, pois busca proporcionar visão geral sobre o assunto; além de ser também bibliográfica no sentido de proporcionar um levantamento de fatos relacionados a nosso objeto de estudo e quanto a análise de informações é caracterizada como qualitativa pois é reflexiva, a finalidade do trabalho não é apenas descrever situações e atividades mas maneiras de o professor se preocupar com um ensino de matemática mais significativo fazendo ligação com situações da vida dos alunos.

Esta dissertação está dividida em seis capítulos. Na introdução fazemos considerações iniciais a respeito do trabalho. No segundo capítulo, intitulado “Os Números”, exibimos um contexto histórico destacando algumas características da construção do con-

ceito de número, desde as primeiras descobertas em relação a quantidade, a criação dos algarismos até a forma com que os utilizamos atualmente. Abordamos ainda, as simbologias destes desde a antiguidade e a caracterização dos números de acordo com suas propriedades.

No terceiro capítulo, estudamos os números chamados primos pelos gregos, que foram caracterizados dessa forma por serem constituídos apenas pela unidade. Neste, apresentamos algumas de suas propriedades, o Teorema Fundamental da Aritmética que ajuda-nos a compreender o porquê de os números primos gerarem todos os outros multiplicativamente. Além de métodos para encontrar primos e conjecturas sobre esses; comentamos também que esses números podem ser muito grandes.

Tal fato é um dos motivos de estudarmos a criptografia, que será apresentada em nosso quarto capítulo. Neste, abordamos algumas características históricas dessa ciência e destacamos o sistema RSA que é o método criptográfico de chave pública mais conhecido e, que é responsável por nossa segurança no ambiente virtual. Esse destaque acontece, pois os números primos são essenciais para a criação das chaves.

No quinto capítulo, unimos os números primos e a criptografia com a proposta de levá-los para a Educação Básica; para isso apresentamos uma experiência de ensino desses números utilizando o material concreto Escala Cuisenaire com a finalidade de explorar o conceito de tais números e a decomposição de qualquer número em fatores primos por meio do recurso didático. Assim, pretendemos expor ao professor da Educação Básica uma forma de estudar o conceito desses números antes de relacioná-los com a criptografia RSA em sala de aula, mas já destacando o motivo de tal estudo para os alunos. Apresentamos também atividades que contemplam a criptografia em sala de aula explorando alguns conteúdos matemáticos do currículo escolar, com o objetivo de mostrar que a criptografia pode ser levada para a sala de aula sob diferentes enfoques. E, exibimos a atividade que exprime a relação dos números primos com a criptografia RSA, como uma possibilidade de exibir essa relação evidenciando que isso é possível em sala de aula, pois se utiliza de conceitos que os alunos conhecem.

O sexto capítulo é direcionado as considerações finais, neste apresentamos também possibilidades de pesquisas futuras sob essa perspectiva e que podem ser possíveis na Educação Básica.

2 OS NÚMEROS

Neste capítulo abordaremos as características dos números desde as primeiras concepções às definições que atualmente utilizamos em nosso dia a dia ou em sala de aula. Para tal recorreremos a alguns textos como o de Mendes (2003), Stewart (2014) e Ifrah (2005). Com o objetivo de abordar o significado do número e suas relações com a vida humana, e assim evidenciar aos professores de Matemática uma abordagem mais significativa sobre tal conceito matemático que se faz importante para a construção do conhecimento dos alunos.

2.1 Breve contexto histórico do número

Vivemos cercados pelos números, em nossos dias desde o momento em que acordamos ao adormecer percebemos-os no despertador, no celular, no relógio da cozinha, na esteira da academia, no carro, nas páginas dos livros que lemos, aprendemos a contar nossos dias, meses, anos e outras atividades. Assim como o tempo, é indispensável para o ser humano outra condição associada ao número, o dinheiro. Enfim, em todos os nossos afazeres há números. Mas como o conceito de número surgiu para o homem?

Segundo Mendes (2003), a maneira como os povos sem escrita concebiam e utilizavam o número mostra-nos as relações míticas entre o universo numérico e a explicação do mundo. Ifrah (2005) destaca a visão de alguns povos que relacionavam os números aos deuses, por exemplo, os magos da Babilônia aderiam em ordem decrescente (simbolizando a hierarquia) um número a cada um dos deuses do panteão, assim Anu, deus do céu (era associado ao número 60), Enlil, deus da terra (associado ao número 50), Ea, deus das águas (associado ao número 40) etc.

Para Eves (2004), o homem tinha senso numérico desde as épocas mais primitivas, não com grandes manifestações de contagem, mas com discernimento do que era menos ou mais, o ato de retirar ou acrescentar, a quantidade de pessoas que viviam na tribo, a quantidade de alimentos suficiente para alimentar a todos, e outros. Devido a isso e com a evolução humana em vários aspectos, não há como descartar que em algum momento surgiria processos de contagem mesmo sendo simples.

A história do número começou a ser delineada empiricamente, ou seja, por meio de necessidades práticas e utilidades corriqueiras dos povos. Por exemplo, aqueles que zelavam dos animais precisavam saber quantos deles saíram e se todos retornaram para o curral, os cuidadores dos mantimentos precisavam saber se a quantidade de alimento

era a mesma todos os dias assim como no caso das armas e homens depois de retornarem de suas expedições militares. Segundo Stewart (2014), o número surgiu há 10 mil anos atrás com os contadores. Estes controlavam quem tinha o quê e quanto, antes mesmo de a escrita ser inventada e ter atribuição de símbolos para os números. No lugar dos símbolos que conhecemos atualmente os contadores antigos utilizavam objetos pequenos feitos de argila e denominados *tokens* que em suas diversas formas representavam os itens da época. Por exemplo, esferas pequenas representavam volumes de grãos, em forma de cilindros representavam os animais e outros; os tokens mais antigos datam de 8000 a.C., e foram utilizados durante 5 mil anos. Com o passar do tempo, tiveram a ideia de representar os números por sinais gráficos, porém essas representações variavam e, depois de muitas transformações dos símbolos ocorreu a invenção dos algarismos.

Os contadores, sacerdotes, astrônomos-astrólogos e depois os matemáticos guiaram a invenção e a evolução dos sistemas de numeração segundo Ifrah (2005), ele destaca ainda que,

> É também uma história completamente anônima, apesar da importância das invenções. Feita por e para as coletividades, ela não concedeu certificados. [...] Frequentemente, conhecemos também os nomes daqueles que transmitiram, exploraram, comentaram algarismos e sistemas de numeração. Mas os dos próprios inventores estão certamente perdidos para sempre. Talvez porque as invenções remontem a uma antiguidade muito remota. Talvez, ainda, porque estas invenções geniais foram feitas por homens relativamente humildes, que não tinham direito a registro. Talvez, enfim, porque elas são o produto de práticas coletivas e, não poderiam ser atribuídas de modo preciso a ninguém. (IFRAH, 2005, p. 11)

E complementa que,

> Dois acontecimentos foram, na história da humanidade, tão revolucionários quanto o domínio do fogo, o desenvolvimento da agricutura ou o progresso do urbanismo e da tecnologia: *a invenção da escrita e a invenção do zero e dos algarismos denominados "arábicos"*. Do mesmo modo que os primeiros, elas modificaram completamente a existência do ser humano. (IFRAH, 2005, p. 130, grifo do autor)

A invenção da escrita aconteceu sobretudo para registrar a linguagem falada, respondendo as necessidades de representação visual e de memorização do pensamento e a invenção dos algarismos se deu como uma forma de possibilitar uma notação coerente para os números e ainda, oferecer a qualquer pessoa a oportunidade de efetuar cálculos sem utilizar as mãos ou uma tábua de contar. Porém, essa invenção não aconteceu do dia para a noite, foram muitas tentativas, regressões e revoluções para traçar a história que conhecemos hoje.

A atividade de controlar as quantidades pelos contadores ficou conhecida como *correspondência um a um*, que consiste em atribuir comparação unidade a unidade em duas coleções e assim saber se as coleções possuem a mesma quantidade ou não de objetos. Em um exemplo simples, podemos verificar a quantidade de poltronas e passageiros em um ônibus, que com uma observação rápida analisamos se a quantidade de poltronas corresponde aos passageiros e qual dos dois conjuntos possui mais elementos; desse modo, se há tantos passageiros quanto o número de poltronas dizemos que há uma correspondência um a um, ou ainda, "[...] há uma equiparação (ou ainda uma *correspondência biunívoca*, ou também, em termos de matemática moderna, uma *bijeção*) [...]" (IFRAH, 2005, p. 26, grifo do autor).

Outra forma de correspondência biunívoca teve origem em épocas remotas quando os povos usavam os dedos das mãos para expressar quantidades, "para uma contagem de carneiros, por exemplo, podia-se dobrar um dedo para cada animal" (EVES, 2004, p. 26). Desse modo, a escrita dos símbolos primitivos que representavam os números 1, 2, 3 e 4 eram riscos verticais ou horizontais correspondendo aos dedos levantados ou estendidos. Assim, podemos entender o porquê da utilização da palavra *dígito* (isto é, dedo) para os algarismos de 1 a 9. Ainda segundo Eves (2004),

> [...] Por exemplo, usando a mão esquerda, representava-se o 1 dobrando-se parcialmente para baixo o dedo mínimo; o 2 dobrando-se parcialmente para baixo os dedos médio e anular; o 3 dobrando-se parcialmente para baixo os dedos mínimo, anular e médio; o 4 dobrando-se para baixo os dedos médio e anular; o 5 dobrando-se para baixo o dedo médio; o 6 dobrando-se para baixo o dedo anular; o 7 dobrando-se completamente para baixo o dedo mínimo; o 8 dobrando-se completamente para baixo os dedos mínimo e anular; e o 9 dobrando-se completamente para baixo os dedos mínimo, anular e médio. (EVES, 2004, p. 29)

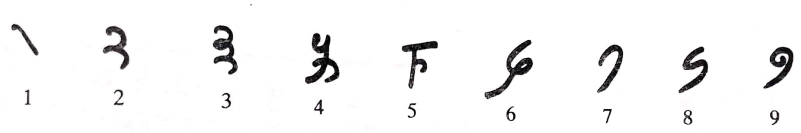
Os dedos das duas mãos podem representar coleções que contém até dez elementos e utilizando também os dedos dos pés, as coleções poderiam ter até vinte elementos, para Boyer (2010), dessa forma as comunidades primitivas podiam fazer as comparações que necessitavam usando os dedos. Ainda segundo o autor, quando os dedos eram insuficientes para representar determinados elementos, o homem usava pedras agrupadas de cinco em cinco, pois observavam quantidades com as mãos e pés humanos como parâmetros.

No processo de construção dos números, as pedras tiveram um papel importante, já que eram utilizadas como uma forma de registro dos algarismos. Uma pedrinha era tomada para representar a unidade, uma um pouco maior representava a dezena, outra maior do que esta representava a centena, e assim por diante. Porém, nem sempre haviam pedras com o mesmo formato para fazer as correspondências, principalmente quando tinha-se a necessidade de representar números grandes, pois as formas e tamanhos das pedras são irregulares. Desse modo, este sistema necessitava de adaptações. Pode-se perceber que

as pedras, apesar de úteis, não eram suficientes para representar quantidades já que os agrupamentos não podiam ser mantidos de forma definitiva, pois a chuva, animais e outros poderiam facilmente desagrupá-las. Assim, o homem pré-histórico às vezes fazia registros em bastão ou ossos com marcas equivalentes às quantidades que queriam registrar.

Para Ifrah (2005), nossa numeração moderna tem origem por volta do século V da era cristã, no norte da Índia. Antes de chegar ao que conhecemos hoje os povos da Índia usaram por longo tempo uma numeração muito rudimentar, esta compreendia uma das características do nosso sistema moderno: seus nove primeiros algarismos eram distintos e não lembravam visivelmente os números correspondentes, por exemplo, o 9 não era composto por nove barras ou pontos, mas era escrito de uma forma mais convencional, como podemos ver na figura a seguir. Notemos também que eles são muito parecidos com os nove algarismos usados atualmente.

Figura 1 - Numeração hindu



Fonte: (IFRAH, 2005, p. 265)

Para escrever números maiores, esse sistema também tinha algarismos particulares que denotavam as dezenas, centenas e cada unidade de milhar. Vejamos como era a escrita do número 7.629:

Figura 2 - Representação do número 7.629

Fonte: (IFRAH, 2005, p. 266)

Essa numeração foi muito limitada, como várias outras. As operações aritméticas mesmo sendo uma simples adição não era possível já que o maior número do sistema era 99.999. Para fugir das dificuldades, os hindus nomearam os números, já que segundo Ifrah (2005),

> Como não podiam representar os números grandes por algarismos, eles tiveram desde muito cedo a idéia de exprimi-los, como se diria hoje, "por extenso". Sem o saber, eles tomavam o caminho que levaria um dia à descoberta do princípio de posição e do zero, pois este sistema já trazia na origem estas duas descobertas fundamentais. Apesar de oral, esta numeração foi de excelente qualidade. (IFRAH, 2005, p. 267)

Assim, os números recebiam os nomes:

eka	*dvi*	*tri*	*catur*	*pañca*	*sat*	*sapta*	*asta*	*nava*
1	2	3	4	5	6	7	8	9

As nomeações consistiam em inicialmente dar nomes a cada um dos nove primeiros algarismos. Utilizando a base 10, em seguida eram atribuídos nomes particulares às dezenas e cada uma de suas potências, além de nomes compostos a todos os outros números. Enquanto pronunciamos os números com as potências em ordem decrescente, os hindus pronunciavam em ordem crescente, logo o número 3.709 (três mil setecentos e nove) para eles era expressado como:

nava sapta sata ca trisahasra
(nove sete centos e três mil)

Para Ifrah (2005), o sistema de numeração hindu sofreu uma grande mudança no século V de nossa era, com a finalidade de abreviar, os matemáticos e astrônomos da época suprimiram qualquer menção à indicadores da base e das potências (dasa = dez; sata = cem; sahasra = mil etc) e preservaram apenas a sucessão dos nomes das unidades correspondentes, respeitando a ordem de sua sequência regular e se conformando com a leitura de acordo com a ordem das potências crescente de 10. A partir disso, os números como 7.629 passaram a ser expressos como:

"NOVE. DOIS. SEIS. SETE"
(= 9 + 2 x 10 + 6 x 100 + 7 x 1.000)

Com tal mudança, os sábios hindus tinham elaborado uma numeração oral de posição. Ao dizer "UM. UM", por exemplo, neste sistema atribuía-se valor a uma unidade simples ao primeiro UM e uma dezena ao segundo. Já para exprimir o número 301, por exemplo, não havia a mesma facilidade pois não havia até o momento um algarismo que representasse a dezena que faltava. Foi a partir dessa necessidade que substituíram a falta pela palavra *śũnya* que significa vazio. E assim o número 301 tinha a representação:

eka *śũ*nya tri
("UM. VAZIO. TRÊS")

Desse modo não havia mais equívoco, depois dos babilônicos e seguramente ao mesmo tempo que os maias, os hindus acabavam de inventar o zero. Consequentemente, tudo o que era necessário para se estabelecer a numeração moderna se encontrava a disposição dos sábios da Índia. Porém, apenas oralmente. O que é justificado por Mendes (2003) ao defender que a compreensão do número está ligada ao desenvolvimento linguístico, pois

antes de conceituar o número, o ser humano desenvolve expressões numéricas por meio da fala. Assim,

> [...] a representação visual do número está assentada em dois referenciais: a palavra que expressa a quantidade e o símbolo que a representa. Podemos concluir daí que o nome do número (a palavra) é essencial para qualquer conceituação do número. (MENDES, 2003, p.10)

No início do século VI d. C, por meio de calculadores do norte da Índia os nove primeiros algarismos que já eram representados no ábaco, receberam valores variáveis de acordo com a posição em que estavam nas representações numéricas. O zero foi simbolizado por um ponto ou, por razões desconhecidas, por um círculo pequeno, assim acabava de nascer o zero que utilizamos em nosso sistema de numeração.

A escrita das unidades nas diferentes ordens decimais não seria feita recorrendo às potências de 10; os números não iniciavam mais pelas unidades simples mas da direita para a esquerda de acordo com as potências decrescentes de 10 a partir do número associado a unidade mais elevada. Por exemplo, o número 9.100 seria escrito como:

Figura 3 - Representação do número 9.100

Fonte: (IFRAH, 2005, p. 285)

Segundo Ifrah (2005),

> Ao liberar definitivamente seus algarismos significativos das colunas do ábaco de areia e ao inventar um signo zero, os sábios da Índia conduziram a uma série de importantes progressos. Especialistas nesta arte, elas simplificaram consideravelmente suas regras, aperfeiçoando-as continuamente, antes de lançar o que viria a constituir, alguns séculos mais tarde, as próprias bases de nosso cálculo atual. (IFRAH, 2005, p. 286)

Os números apresentam uma história relacionada a diversas atividades humanas. Para Mendes (2003), antes mesmo dos primeiros registros dos números por meio dos símbolos que hoje conhecemos, eram representados pelos dedos das mãos e tais representações variavam de acordo com os povos se tornando uma atividade relacionada a evolução do homem, uma "invenção inteiramente humana" (IFRAH, 2005, p. 322). É importante ressaltar que além de os algarismos serem considerados a única linguagem universal, a invenção da nossa numeração de posição possibilitou consequências admiráveis para a humanidade por facilitar o desenvolvimento da ciência e da matemática.

2.2 Simbologia dos números

Os aritméticos gregos tiveram a ideia de escrever números por meio de letras alfabéticas, e assim fizeram surgir versos e composições literárias em dois gêneros, o dístico (grupo de dois versos) e o epigrama (verso curto). Assim, surgiu também a possibilidade de atribuir um número a conjuntos de palavras; segundo Ifrah (2005), mais tarde os árabes desenvolveram a arte de escrever em composição de cronogramas (mesmo estilo dos gregos); o *ramz* dos poetas, historiadores, biógrafos da África e da Espanha e o *tarikh* dos turcos e persas. Tais regras consistiam em agrupar em uma frase o conjunto das letras cuja soma dos valores fornecessem a data de um acontecimento histórico. Os poetas da época aproveitaram para usar a imaginação e forjar frases significativas tendo como valor numérico a data de lembranças as quais queriam que fossem lembradas e assim, se desenvolveu a *numerologia*, levando seus adeptos a todos os tipos de especulações e interpretações mágicas.

De acordo com Ifrah (2005), há uma lenda, sobre um príncipe da Idade Média em que seu nome era equivalente ao número 284, ele procurava uma noiva cujo nome correspondesse ao número 220 pois acreditava que teria felicidade conjugal garantida "pela virtude dos números", já que esses eram denominados *números amigos*. A propriedade por trás dos números amigos é que a soma (denotaremos $s(n)$, $n \in \mathbb{N}$) dos divisores próprios (são todos os divisores inteiros positivos de um número n exceto o próprio n) de um é igual ao outro, assim, $s(220) = 1+2+4+5+10+11+20+22+44+55+110 = 284$ e $s(284) = 1+2+4+71+142 = 220$.

Outros exemplos que se referem aos números e crenças é o 17, que desde a antiguidade romana é considerado de mau augúrio; conta-se que Napoleão Bonaparte adiou para o dia 18 seu golpe de Estado previsto para uma sexta-feira 17 e também que não há quarto, andar em hotéis e nem assentos em aviões italianos com o número 17, segundo Ifrah (2005). Ele também aponta que assim como o 17, o número 13 é sinônimo de azar até os dias atuais em algumas tradições européias, .

Além das crenças que acabamos de comentar, há também outros tipos de significados atribuídos aos números. Segundo Ifrah (2005) o número um é associado à obra da criação; em acordo com ele Mendes (2003) também faz referência ao número um como aquele que representava a força criadora de tudo, era o deus dos números e do Sol, o centro das energias vitais. Já o número dois era considerado para Ifrah (2005) o que corresponde à dualidade do feminino e do masculino, à simetria do corpo humano e à oposição. E, segundo Mendes (2003), o dois era o símbolo da justiça, assim como designava o princípio feminino. O número três era o símbolo da unidade e da dualidade, pois $1 + 2 = 3$, formando a trindade divina - pai, filho e espírito santo. Geometricamente é representado pelo triângulo equilátero. Para os povos da antiguidade, o número 3 estava relacionado

aos três reinos universais - céu, terra e inferno ou aos três reinos da natureza - animal, vegetal e mineral.

O número quatro é relacionado ao quadrado, à cruz significando a solidez, o tangível, o sensível, a plenitude, a universalização e a totalidade. O número refere-se também às operações básicas da aritmética, aos quadrantes do círculo trigonométrico, aos naipes do baralho, aos pontos cardeais, as fases da lua, as estações do ano, os quatro elementos (água, terra, ar, fogo) e as fases da vida (infância, juventude, maturidade e velhice). O cinco era representado pelos pitagóricos como o símbolo do casamento, pois é formado pela união do número que representa a feminilidade e a masculinidade ($2 + 3 = 5$). Outro detalhe que evidencia ainda o símbolo da união é que este é a soma do primeiro número par com o primeiro ímpar. É considerado também como o número da harmonia, do equilíbrio e dos cinco sentidos.

O número seis era tido como o signo da perfeição e é representado através de seis triângulos equiláteros que compõem o hexágono regular inscrito na circunferência. O número seis corresponde a soma e ao produto dos três primeiros números ($1 + 2 + 3 = 6$ e $1 \cdot 2 \cdot 3 = 6$) e além disso pode ser representado ainda como $6^2 = 1^3 + 2^3 + 3^3$. É também relacionado a religião pois, de acordo com a Bíblia, foi o total de dias para a criação, foi no sexto dia que o homem foi criado e, no sexto dia da semana aconteceu a morte de Cristo. O número sete totaliza os dias da criação, é também a quantidade de cores do arco-íris assim como as maravilhas do mundo antigo. Para a religião, assim como era expresso no Novo Testamento, o número 7 representa as sete palavras que Jesus disse na cruz, os sete pecados capitais e as dores de Nossa Senhora. Além de que temos que são sete os dias da semana, os dias de cada fase da lua e os anões da Branca de Neve.

O número 8 era considerado para os sábios antigos, o número que representava o equilíbrio e a igualdade entre as pessoas e quando utilizado em posição horizontal representava o infinito. O número 9 era considerado como o número do começo e fim, atribuindo-o a Cristo (alfa e ômega), para os sábios antigos representava a matéria no sentido de ela ser variável, mas não destruída. O número 10 para os mágicos antigos representava a perfeição devido ser o resultado de $1 + 2 + 3 + 4$. Geometricamente, o ponto é representado pelo número 1, a reta pelo número 2 (já que ligando dois pontos quaisquer temos um segmento de reta), o plano pelo número 3 (já que três pontos não colineares determinam um plano) e o 4 representa o espaço (pelo sistema tridimensional de coordenadas). Assim para eles a soma de todos esses números constituía o universo e era representado pelo número 10. Para outras pessoas o número 10 significava, também, a união fraternal simbolizada pelo aperto das mãos (com os 10 dedos).

Atribui-se aos pitagóricos os primeiros passos do desenvolvimento da teoria dos números e do misticismo numérico, já que eles classificavam os números de acordo com crenças místicas. Devido a isso, segundo Eves (2004), Jâmblico, filósofo neoplatônico que

viveu por volta de 320 d. C, atribuiu a Pitágoras a descoberta dos números amigáveis. Os Pitagóricos consideravam os números tão importantes que basearam sua filosofia e modo de viver neles.

Segundo Boyer (2010), para os pitagóricos o número um é o gerador dos números e o número da razão; o dois além de ser o primeiro par, ou feminino é o número da opinião; o três é o primeiro número masculino verdadeiro e o número da harmonia; o quatro é o número da justiça; o cinco, o número do casamento (união dos dois primeiros verdadeiros feminino e masculino); o seis é o número da criação; para eles, cada número tinha uma atribuição especial, porém o mais sagrado era o dez pois representava o número do universo. "É um tributo à abstração da matemática pitagórica que a veneração ao número dez evidentemente não era ditada pela anatomia da mão ou pé humanos" (BOYER, 2010, p. 36).

Para Mendes (2003), a primeira divisão que fizeram dos números eram em pares e ímpares, sendo que um número par era aquele em que a divisão por dois seria possível sem restar mônada (unidade para os gregos, neste caso, a divisão não deve deixar restos, ou seja, a divisão deve ser exata) entre elas. Já o número ímpar deixa mônada na divisão em duas partes iguais. Alguns historiadores analisam as concepções pitagóricas sobre os números ímpares, sob três aspectos: os *primeiros e não-compostos* como 3, 5, 7, 11, 13, ... , pois nenhum outro o divide a não ser a unidade. Estes números não são compostos de outros números, mas gerados pela unidade. Os *segundos e compostos* que são os ímpares que são compostos de outros números como por exemplo, o 9, 15, 21, 25, 27, ... Notemos que o nove tem uma terça parte que é o 3; o quinze tem uma terça parte que é o 5 e uma quinta parte que é 3. E o terceiro aspecto, o mais complexo, classifica os ímpares como *segundos (classificados acima) e compostos, mas com referência a outro número*, são divisíveis, mas não possuem divisores em comum, por exemplo, os números 9 e 25 aos quais tem-se que o 3 divide 9, mas não divide 25.

Segundo Mendes (2003), os números pares também foram divididos e caracterizados como *perfeitos, deficientes, superabundantes ou superfeitos*. Os números *perfeitos* são aqueles que são iguais à soma de seus divisores próprios, vejamos que $s(6) = 1+2+3 = 6$. Os chamados *deficientes* são aqueles que são maiores do que a soma de seus divisores próprios, ou ainda, $s(n) < n$. Por exemplo, o número 8, já que $s(8) = 1+2+4 = 7 < 8$. São exemplos de números *superabundantes* os números 12 e 24. Ainda segundo o autor, para os antigos gregos os números que tinham suas partes em excesso eram chamados de superfeitos, já os deficientes eram comparados aos cíclopes, que só tinham um olho e os perfeitos eram considerados como aqueles que tinham limite médio, ou ainda, tinham limite entre o excesso e a deficiência. Assim, "os números perfeitos são, como as virtudes, poucos, ao passo que as outras duas classes são como os vícios: numerosos, desordenados e indefinidos" (MENDES, 2003, p. 37).

Durante o capítulo percebemos como os números foram conceituados de acordo com aspectos relacionados ao cotidiano dos povos desde a antiguidade; vimos como os gregos classificavam os números segundo determinadas características próximas daquilo que viviam, já que para eles os números eram o centro de tudo. Assim, destacando os ímpares chamados primeiros ou não-compostos que também são conhecidos como *números primos*, podemos acreditar erroneamente que tal nome é devido a uma relação de parentesco, porém, para Coutinho (2003) o significado do nome destes números não é ligada a esse aspecto. Segundo o autor, os romanos apenas observaram a tradução literal da palavra grega primeiro que é *primus* e daí em diante conhecemos esses números como números primos.

3 OS NÚMEROS PRIMOS

No Capítulo anterior, vimos o processo de desenvolvimento dos números, além de terem sido caracterizados de acordo com algumas características místicas ou relacionadas a determinadas propriedades. Neste, estudaremos os chamados números primos e suas propriedades, os primos de Mersenne e os primos de Fermat, assim como conjecturas relacionadas a esses números que se tornaram ao longo do tempo objeto de estudo e curiosidade de muitos matemáticos. Destacaremos ainda conceitos da Teoria dos Números necessários para a aplicação da criptografia RSA, ou seja, organizaremos a base matemática que tanto professores quanto alunos precisarão para compreender o conteúdo e atividades propostas no capítulo 5.

3.1 Breve introdução histórica

Os números primos apresentam uma longa história; desde os estudos gregos antigos aos dias atuais é tema de interesse e investigação por vários matemáticos. Segundo Eves (2004), os principais resultados sobre eles na Antiguidade foram a prova da infinitude dos primos e o crivo de Eratóstenes. Na concepção pitagórica, a ideia de números primos apresentava-se a partir da conceituação de números ímpares. Mendes (2003) apresenta três concepções pitagóricas sobre tais números, em uma delas os números 3, 5, 7, ..., eram chamados de não-compostos pois nenhum número os divide além da unidade; e não são compostos de outros números, mas gerados unicamente pela unidade - estes são chamados de números primos.

Já em Stewart (2014) esses números são apresentados por meio da decomposição em fatores menores, por exemplo, o número $10 = 2 \cdot 5$ e $12 = 3 \cdot 4$; alguns números, porém, não se decompõem dessa forma, como 2, 3, 5, 7, 11 e outros. Chamando assim os números em que a decomposição é possível de *números compostos* e de primos aqueles que não são obtidos dessa forma. O autor destaca ainda que "eles formam os blocos construtivos básicos para todos os números, no sentido de que números maiores são criados multiplicando números menores." (STEWART, 2014, p. 121)

Ainda segundo Stewart (2014), Euclides destacou os números primos no Livro VII de *Os Elementos*, com a afirmativa e prova de que qualquer número composto é medido por algum primo - isto é, pode ser escrito utilizando números primos. Euclides mostrou que dado um número inteiro qualquer, este pode ser decomposto em fatores primos e essa fatoração é única, exceto pela ordem dos fatores; e, no livro IX afirma e demonstra a infinitude dos números primos.

3.2 Aritmética básica

Antes de estudarmos propriedades referentes aos números primos, é necessário abordar alguns conceitos que serão necessários para alguns resultados. Para isso utilizaremos essencialmente Domingues (2009) e Hefez (2014).

Dizemos que um número inteiro a *divide* um número inteiro b se $b = a \cdot c$, para algum $c \in \mathbb{Z}$ e que a é *divisor* de b e que b é *múltiplo* de a, ou ainda que b é *divisível* por a. Escreveremos $a|b$ quando a divide b e $a \nmid b$ se a não divide b. Sejam os números 3, 14 e 15, temos que, $3|15$ pois $15 = 3 \cdot 5$, temos também que 3 é divisor de 15 e 15 é múltiplo de 3. E, $3 \nmid 14$ pois não existe $c \in \mathbb{N}$ tal que $14 = c \cdot 3$ é satisfeita.

Dados a e b ambos diferentes de zero e pertencentes ao conjunto dos inteiros, cada um pode ser associado ao conjunto de divisores $D(a)$ e $D(b)$ de a e b, respectivamente. Temos que a intersecção destes conjuntos nunca é vazia, pois pelo menos o número 1 pertence aos dois conjuntos, então pode-se determinar um maior inteiro na intersecção. Este é chamado de *máximo divisor comum (mdc)*. Pode ser utilizada, também, a seguinte definição.

Definição 3.2.1. *Dado um inteiro $d \geq 0$ e d é um máximo divisor comum de a e b, se possuir as seguintes propriedades:*
i) d é um divisor comum de a e b;
ii) d é divisível por todo divisor comum de a e b.

Podemos verificar a partir da definição de máximo divisor comum apresentada por Domingues (2009), que ele é único. A notação utilizada para o máximo divisor comum entre a e b que utilizaremos será $mdc(a,b)$. Como o mdc não depende da ordem em que a e b são tomados, temos que $mdc(a,b) = mdc(b,a)$.

Exemplo 3.2.1. *Temos que mdc(12, 28) = 4, pois $D(12) = \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm12\}$ e $D(28) = \{\pm1, \pm2, \pm4, \pm7, \pm14, \pm28\}$.*

Uma forma eficiente de encontrarmos o mdc entre dois números é por meio do *algoritmo de Euclides* que se baseia na divisão euclidiana.

Teorema 3.2.1. *(Divisão Euclidiana) Sejam a e b dois números inteiros com $b \neq 0$. Existem dois únicos números inteiros q e r tais que $a = bq + r$, com $0 \leq r < |b|$.*

Para demonstração desse fato, veja Hefez (2014). Na divisão euclidiana, temos que a é chamado de divisor, b é o dividendo, q é o quociente e r é o resto.

Exemplo 3.2.2. *Dados $a = 2019$ e $b = 5$ temos que existe $q = 403$ e $r = 4$ tal que $2019 = 5 \cdot 403 + 4$ sendo $4 < 5$.*

O Algoritmo de Euclides pode ser descrito como:

1. $a = bq_1 + r_1$, com $0 < r_1 < b$;
2. $b = r_1q_2 + r_2$, com $0 < r_2 < r_1$;
3. $r_1 = r_2q_3 + r_3$, com $0 < r_3 < r_2$;
   $\vdots$
4. $r_{n-2} = r_{n-1}q_n + r_n$, com $0 < r_n < r_{n-1}$;
5. $r_{n-1} = r_nq_{n+1}$.

Basicamente, o que acontece no algoritmo é o que está demonstrado no diagrama seguinte:

	q_1	
a	b	
r_1		

Ao continuar a divisão de acordo com o que descrevemos acima, obtemos $b = r_1q_2 + r_2$, que no diagrama é representado como:

	q_1	q_2	
a	b	r_1	
r_1	r_2		

Prosseguindo, enquanto for possível, teremos:

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

Exemplo 3.2.3. *Determinar o mdc entre 2019 e 30:*

	67	3	3
2019	30	9	3
9	3		

Observe que o algoritmo nos fornece:

$$3 = 30 - 3 \cdot 9$$
$$9 = 2019 - 67 \cdot 30$$

Assim,

$$3 = 30 - 3 \cdot 9 = 30 - 3 \cdot (2019 - 67 \cdot 30) = 30 - 3 \cdot 2019 + 201 \cdot 30 = 202 \cdot 30 - 3 \cdot 2019.$$

Logo, temos que $mdc(2019, 30) = 3 = 202 \cdot 30 + (-3) \cdot 2019$

Utilizando o algoritmo de Euclides como apresentado acima, percebemos que ele também nos fornece um meio de escrever o mdc de dois números como soma de múltiplos dos números em questão. Quando o algoritmo for usado para expressar $mdc(a,b)$ como $ma+nb$, com $m,n \in \mathbb{Z}$ chamaremos-o de *Algoritmo de Euclides Estendido.*

Dois números inteiros a e b são ditos *primos entre si*, ou *coprimos*, se $mdc(a,b) = 1$; ou seja, se o único divisor comum positivo de ambos é 1. Temos ainda que

Proposição 3.2.1. *Dois números inteiros a e b são primos entre si se, e somente se, existem números inteiros m e n tais que $ma+nb=1$.*

Teorema 3.2.2. *(Lema de Gauss) Sejam a, b e c números inteiros. Se $a|bc$ e $mdc(a,b) = 1$, então $a|c$.*

A demonstração dos dois últimos resultados pode ser encontrada em Hefez (2014).

Dados dois números inteiros a e b, dizemos que c é um *múltiplo comum* de a e b se c é múltiplo simultaneamente de ambos os números. Define-se *mínimo múltiplo comum (mmc)* entre a e b como o menor múltiplo comum entre a e b, ou ainda,

Definição 3.2.2. *Diremos que um número inteiro $m \geq 0$ é um mínimo múltiplo comum (mmc) dos números inteiros a e b, se possuir as seguintes propriedades:*
i) m é um múltiplo comum de a e b, e
ii) se c é um múltiplo comum de a e b, então $m|c$

A notação utilizada para mínimo múltiplo comum entre a e b é $mmc(a,b)$. O mínimo múltiplo comum entre a e b é único.

Exemplo 3.2.4. *Veja que 32 é um múltiplo comum de 4 e 8, mas não é o mmc dos números. O número 8 é mmc entre 4 e 8.*

Diremos que dois números inteiros a e b são *congruentes* módulo m, com $m \in \mathbb{N}$, se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escrevemos $a \equiv b \mod m$. Por exemplo, $22 \equiv 25 \mod 3$, já que os restos da divisão de 22 e 25 por 3 são iguais a 1. Se $a \equiv b \mod m$ não for verdadeira, diremos que *a não é congruente* a b módulo m ou que são *incongruentes* módulo m e escreveremos $a \not\equiv b \mod m$.

Proposição 3.2.2. *Suponha que a, b, $m \in \mathbb{Z}$, com $m > 1$. Tem-se que $a \equiv b \ mod \ m$ se, e somente se, $m|b-a$.*

Proposição 3.2.3. *Sejam $m, n \in \mathbb{N}$. Para todos $a, b, c, d \in \mathbb{Z}$ com $m > 1$, tem-se que:*
i) $a \equiv a \ mod \ m$;
ii) se $a \equiv b \ mod \ m$, então $b \equiv a \ mod \ m$;
iii) se $a \equiv b \ mod \ m$ e $b \equiv c \ mod \ m$, então $a \equiv c \ mod \ m$;
iv) se $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$, então $a + c \equiv b + d \ mod \ m$;
v) se $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$, então $ac \equiv bd \ mod \ m$;
vi) se $a \equiv b \ mod \ m$, então $a^n \equiv b^n \ mod \ m$.

As duas últimas proposições e suas respectivas demonstrações podem ser encontradas em Hefez (2014), assim como a definição a seguir.

Definição 3.2.3. *Um sistema reduzido de resíduos módulo m é um conjunto de números inteiros $r_1, ..., r_s$ tais que*
i) $mdc(r_i, m) = 1$, para todo i = 1, ..., s;
ii) $r_i \not\equiv r_j \ mod \ m$, se $i \neq j$;
iii) Para cada $n \in \mathbb{Z}$ tal que $mdc(n, m) = 1$, existe i tal que $n \equiv r_i \ mod \ m$.

Será designado por $\varphi(m)$ o número de elementos de um sistema reduzido de resíduos módulo $m > 1$, que corresponde à quantidade de números naturais entre 0 e $m-1$ que são primos com m. A *função φ de Euler*, também conhecida como *função totiente de Euler* é definida como a quantidade de inteiros positivos menores ou iguais a m que são relativamente primos a n. Notemos que $\varphi(1) = 1$ e se m é primo, então $\varphi(m) = m - 1$, como podemos verificar em Hefez (2014). Esta função é de grande utilidade em Teoria dos Números e especialmente na criptografia.

Exemplo 3.2.5. *Para determinar $\varphi(10)$, poderíamos calcular o mdc entre 10 e todos os naturais menores do que 10 e contarmos aqueles em que o resultado do mdc é igual a 1. Porém, podemos economizar tempo observando que:*
i) como 10 é par então todo número natural par a é tal que $mdc(a, 10) \neq 1$; já que, nesse caso, $mdc(a, 10) \geq 2$;
ii) como 10 é um múltiplo de 5, então todo número natural b múltiplo de 5 é tal que $mdc(b, 10) \neq 1$; já que, nesse caso, $mdc(b, 10) \geq 5$.

Dessa forma, não precisamos calcular o mdc entre 10 e os números naturais menores do que 10 que são pares ou múltiplos de 5. Assim, mdc(10, 1) = 1; mdc(10, 3) = 1; mdc(10, 7) = 1; mdc(10, 9) = 1. Portanto, concluímos que $\varphi(10) = 4$.

Exemplo 3.2.6. *Para determinar $\varphi(23)$ basta fazermos $\varphi(23) = (23 - 1) = 22$.*

Teorema 3.2.3. *(Teorema de Euler) Sejam $m, a \in \mathbb{Z}$ com $m > 1$ e mdc(a, m) = 1. Então, $a^{\varphi(m)} \equiv 1$ mod m.*

A demonstração deste fato pode ser encontrada em Hefez (2014). Para aplicar o Teorema de Euler, é necessário saber calcular $\varphi(m)$. O cálculo será realizado por meio da proposição a seguir. Tal resultado será muito útil para o método criptográfico RSA que será estudado no capítulo 4.

Proposição 3.2.4. *Sejam $m, m' \in \mathbb{N}$ tais que $mdc(m, m') = 1$. Então $\varphi(mm') = \varphi(m)\varphi(m')$.*

Demonstração: O resultado é trivial se $m = 1$ ou $m' = 1$. Portanto, vamos supor que $m > 1$ e $m' > 1$. Considere a seguinte tabela formada pelos números naturais de 1 a $m \cdot m'$:

$$\begin{array}{ccccccc} 1 & 2 & ... & \mathrm{k} & ... & m' \\ m'+1 & m'+2 & ... & m'+k & ... & 2m' \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ (m-1)m'+1 & (m-1)m'+2 & ... & (m-1)m'+k & ... & m \cdot m' \end{array}$$

Como se tem que $mdc(t, m \cdot m') = 1$ se, e somente se, $mdc(t, m') = mdc(t, m) = 1$, para calcular $\varphi(m \cdot m')$, devemos determinar os inteiros na tabela acima que são simultaneamente primos com m e m'.

Se o primeiro elemento de uma coluna não for primo com m', então todos os elementos da coluna não são primos com m'. Portanto, os elementos primos com m' estão necessariamente nas colunas restantes que são em número $\varphi(m')$, cujos elementos são primos com m', como é fácil verificar. Vejamos agora quais são os elementos primos com m em cada uma dessas colunas.

Como $mdc(m, m') = 1$, a sequência $k, m'+k, ..., (m-1)m'+k$ forma um *sistema completo de resíduos módulo* m e, portanto, $\varphi(m)$ desses elementos são primos com m. Logo, o número de elementos simultaneamente primos com m' e m é $\varphi(m) \cdot \varphi(m')$. □

Exemplo 3.2.7. *Para determinar $\varphi(230) = \varphi(10 \cdot 23) = \varphi(10) \cdot \varphi(23) = 4 \cdot 22 = 88$.*

3.3 Números primos

Um número natural maior do que 1 que só possui como divisores positivos 1 e ele próprio é chamado de *número primo*. Os números primos são 2, 3, 5, 7, 11, 13, ... Todo número maior do que 1 que não for primo é chamado número composto, logo 4, 6, 8, 9, 10 são os primeiros números compostos.

Para Hefez (2014), em relação a estrutura multiplicativa dos naturais, os números primos são os mais simples e ao mesmo tempo suficientes para gerar todos os números naturais, ou ainda, todos os inteiros não nulos, pelo *Teorema Fundamental da Aritmética* também chamado de *Teorema da Fatoração Única*, que veremos mais adiante; por meio dele entendemos que "os números primos são tijolos de construção a partir dos quais os outros inteiros são formados multiplicativamente" (EVES, 2004, p. 622).

Segundo Coutinho (2003), para provar que a fatoração de um número em primos é escrita de maneira única, ou seja, é possível escrever qualquer número inteiro maior do que 1 usando os números primos, é necessário estudar a *propriedade fundamental dos números primos*, mas antes de vê-la precisamos do lema seguinte.

Lema 3.3.1. *Sejam a, b e c inteiros positivos e suponhamos que a e b são primos entre si.*
(i) Se b divide o produto ac então b divide c.
(ii) Se a e b dividem c então o produto ab divide c.

Demonstração:
i) Temos por hipótese, inicialmente, que a e b são primos entre si; isto é, mdc(a, b) = 1. Pelo algoritmo de Euclides estendido, existem inteiros α e β tais que

$$\alpha \cdot a + \beta \cdot b = 1.$$

Multiplicando esta equação por c, obtemos

$$\alpha \cdot a \cdot c + \beta \cdot b \cdot c = c. \tag{3.1}$$

Nesta equação temos que a segunda parcela é evidentemente divisível por b e a primeira também é, pois pela hipótese de i), b divide o produto ac. Assim o lado esquerdo de 3.1 é divisível por b. Portanto, c é divisível por b, como queríamos demonstrar.

i) Se a divide c, podemos escrever $c = at$, para algum $t \in \mathbb{Z}$. Mas b também divide c. Como a e b são primos entre si, segue da afirmação i) que b tem que dividir t. Assim teremos que $t = bk$, para algum $k \in \mathbb{Z}$. Portanto,

$$c = at = a(bk) = (ab)k$$

é divisível por ab, que é a afirmação ii). □

Agora podemos enunciar a propriedade fundamental dos números primos, segundo Coutinho (2003), ela aparece como a proposição 30 do livro VII dos Elementos de Euclides e também é chamada de *Lema de Euclides*.

Proposição 3.3.1. *(Propriedade Fundamental dos primos) Seja p um número primo e a e b inteiros positivos. Se p divide o produto ab então p divide a ou p divide b.*

Demonstração: Suponhamos que p não divide a, neste caso usamos o fato de que p é primo, e assim, como p não divide a então eles são primos entre si. Isto acontece pois qualquer divisor comum a p e a divide p; mas os únicos divisores positivos de p são 1 e p. Portanto, se p não divide a, então $mdc(a,p) = 1$. Desse modo, podemos aplicar o lema 3.3.1: como p e a são primos entre si e como p divide ab temos que p divide b. □

O Teorema Fundamental da Aritmética foi enunciado pela primeira vez por Gauss em seu livro *Disquisitiones arithmeticae*, fato que não garante que matemáticos gregos tivessem usado-o implicitamente desde a Grécia Antiga, segundo Coutinho (2003).

Teorema 3.3.1. *(Teorema Fundamental da Aritmética) Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Demonstração: Usaremos a segunda forma do Princípio de Indução (veja em Hefez (2014)). Se $n = 2$, o resultado é obviamente verificado.

Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar. Suponhamos, então, que n seja composto. Logo, existem números naturais n_1 e n_2 tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, ..., p_r$ e $q_1, ..., q_s$ tais que $n_1 = p_1 \cdots p_r$ e $n_2 = q_1 \cdots q_s$. Portanto, $n = p_1 \cdots p_r q_1 \cdots q_s$.

Vamos, agora, provar a unicidade da escrita. Suponha que tenhamos $n = p_1 \cdots p_r = q_1 \cdots q_s$, onde os p_i e os q_j são números primos. Como $p_1 | q_1 \cdots q_s$, temos que $p_1 = q_1$ para algum j, que, após reordenamento de $q_1, ..., q_s$, podemos supor que seja q_1. Portanto, $p_2 \cdots p_r = q_2 \cdots q_s$.

Como $p_2 \cdots p_r < n$, a hipótese de indução acarreta que $r = s$ e p_i e q_j são iguais aos pares. □

Teorema 3.3.2. *Existem infinitos números primos*

Uma demonstração deste fato pode ser encontrada em Hefez (2014). No livro IX, proposição 20, Euclides demonstra a infinitude dos números primos, segundo Eves (2004), tal demonstração é considerada pelos matemáticos como um modelo de elegância matemática. Essencialmente, como é apresentado em Boyer (2010), Euclides provou que supondo um número finito de primos, denotando-os por $a, b, ..., k$, fazendo $A = a \cdot b \cdots k$ e $N = A + 1$, temos que N não pode ser primo, já que isso contraria a hipótese de A ser o produto de todos os primos. Logo, N é composto e deve ser medido por algum número p. Mas p não pode ser nenhum dos fatores primos de A, senão seria um fator de 1. Então p deve ser um primo diferente de todos os fatores de A; portanto, a hipótese de A ser o produto de todos os primos é um absurdo.

Teorema 3.3.3. *(Pequeno Teorema de Fermat) Seja p um número primo, tem-se que p divide o número $a^p - a$, para todo número inteiro a.*

Em notação de congruências, temos

Teorema 3.3.4. *Sejam $a \in \mathbb{Z}$ e p um número primo tem-se que $a^p \equiv a \ mod \ p$.*

Deste teorema, temos o seguinte corolário:

Corolário 3.3.1. *Se p é um número primo e se a é um número natural não divisível por p, então p divide $a^{p-1} - 1$.*

Em notação de congruências, temos

Corolário 3.3.2. *Sejam $a \in \mathbb{Z}$ e p um número primo tais que $mdc(a,p) = 1$. Tem-se que $a^{p-1} \equiv 1 \ mod \ p$.*

As demonstrações do teorema e corolário são encontradas em Hefez (2014).

3.4 Métodos para encontrar números primos

Nesta seção estudaremos o *Crivo de Eratóstenes* já que este é um dos métodos mais antigos para determinar primos e duas fórmulas, as *polinomiais* e *exponenciais* que fornecem valores primos dentre várias existentes.

3.4.1 Crivo de Eratóstenes

O matemático grego Eratóstenes, que nasceu por volta de 284 a. C., criou um *crivo* (peneira) para determinar primos e por isso o método é chamado de *Crivo de Eratóstenes*. Segundo Coutinho (2003), o crivo foi introduzido pela primeira vez por Nicômaco em sua *Aritmética* e enunciado como: *O método para obtê-los [os números primos] é chamado por Eratóstenes de uma peneira, porque tomamos os números ímpares misturados de maneira indiscriminada e, por este método, como se fosse pelo uso de um instrumento ou peneira, separamos os primos ou indecomponíveis dos secundários ou compostos.* Logo, por meio do crivo agindo como uma peneira, obtemos apenas números primos em um determinado conjunto de números.

Vejamos como o crivo funciona. Inicialmente, sabemos que o crivo determina todos os números primos até um certo inteiro positivo n escolhido. O método consiste em listar todos o números ímpares de 3 até o n, o número 2 não é tomado já que ele é o único primo par. Como o primeiro número de nossa lista é o 3, riscamos os demais números da lista de 3 em 3, ou seja, estamos riscando todos os múltiplos de 3 maiores do que ele

próprio. Logo depois procuramos o menor elemento da lista, maior que 3, que não tenha sido riscado; que é o 5 e riscamos os demais números da lista de 5 em 5, ou ainda, todos os seus múltiplos. Assim, o mesmo procedimento se repete até chegar ao número n.

Tomando $n = 45$, a lista de números ímpares é

3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45

Após a primeira passagem do crivo (3 em 3) temos

3 5 7 ~~9~~ 11 13 ~~15~~ 17 19 ~~21~~ 23 25 ~~27~~ 29 31 ~~33~~ 35 37 ~~39~~ 41 43 ~~45~~

Após a segunda passagem do crivo (5 em 5) ficamos com

3 5 7 ~~9~~ 11 13 ~~15~~ 17 19 ~~21~~ 23 ~~25~~ ~~27~~ 29 31 ~~33~~ ~~35~~ 37 ~~39~~ 41 43 ~~45~~

Ao final da terceira passagem (7 em 7) a lista continua a mesma e assim por diante. Portanto, os números primos menores que 45 são

$$2 \quad 3 \quad 5 \quad 7 \quad 11 \quad 13 \quad 17 \quad 19 \quad 23 \quad 29 \quad 31 \quad 37 \quad 41 \quad 43.$$

Para não repetir o processo de passar riscando números até chegar em n observamos que se m é um inteiro da lista, então $m \leq n$. Se m for composto, então terá um fator menor ou igual a $\sqrt{m}$. Mas $\sqrt{m} \leq \sqrt{n}$, isto é, qualquer número composto da lista tem um fator menor ou igual a $\sqrt{n}$. Assim, não precisamos riscar números de r em r quando $r > \sqrt{n}$. No exemplo acima temos então que $6 < \sqrt{45} < 7$, logo, é suficiente riscar de 3 em 3 e de 5 em 5, apenas.

Para Coutinho (2003), o Crivo de Eratóstenes é um bom recurso para determinar primos, mas tem suas limitações, como por exemplo, quando se trata de encontrar primos muito grandes já que não é possível utilizar o algoritmo se o número n for grande o suficiente para gerar dificuldades ao se fazer a lista de todos os seus antecessores ímpares.

3.4.2 Fórmulas polinomiais

A fórmula polinomial é um dos tipos mais simples para encontrar primos. Nos referimos a um polinômio $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, cujos coeficientes $a_n, a_{n-1}, ..., a_1, a_0$ são números inteiros e satisfazem a condição $f(m)$ é primo, para todo inteiro positivo m.

Vejamos o que acontece se tomarmos como exemplo o polinômio $f(x) = x^2 + 1$:

Inicialmente, podemos perceber que quando x é ímpar, $f(x)$ é par. Desse modo, a não ser que x seja igual a 1, o valor de $f(x)$ é sempre composto (e múltiplo de 2). Em

x	$f(x)$
1	2
2	5
3	10
4	17
5	26
6	37
7	50
8	65
9	82
10	101

outras palavras, quando $x > 1$ temos que $f(x)$ será primo se x for par. Mas nos atentemos a $f(8) = 65$ que é composto, então esse polinômio não nos dá uma fórmula para primos.

Podemos tentar outros polinômios a fim de, por meio deles encontrar números primos, porém, segundo Coutinho (2003), esses polinômios devem ter muitas variáveis cujos valores positivos são sempre primos e possuem grau muito alto, o que os tornam fórmulas complicadas.

3.4.3 Fórmulas exponenciais

Há duas fórmulas exponenciais importantes, ambas foram muito estudadas pelos matemáticos do século XVII, principalmente por Fermat. Essas fórmulas são $M(n) = 2^n - 1$ e $F(n) = 2^{2^n} + 1$, sendo n inteiro e não-negativo. Os números $M(n)$ e $F(n)$ são conhecidos como *números de Mersenne* e *números de Fermat*, respectivamente.

3.4.3.1 Primos de Mersenne

Marin Mersenne (1588-1648) foi frade e matemático, teve contato por correspondências com vários matemáticos de sua época, editou trabalhos de matemáticos gregos e escreveu sobre vários assuntos, mas é notadamente conhecido pelos denominados *primos de Mersenne*, que apresentou-os em seu trabalho *Cogitata physico-mathematica* de 1644, nesse também escreveu sobre a relação entre os primos de Mersenne e os números perfeitos, segundo Eves (2004).

Um número é dito primo de Mersenne se tem a forma $M(n) = 2^n - 1$, com n primo, assim os primeiros números $M(n)$ são primos quando $n = 2, 3, 5, 7, 13, 17$. A recíproca da afirmação não é verdadeira, já que se n for primo isto não significa que $M(n)$ seja primo. Já que $M(11) = 2047 = 23 \cdot 89$ é um número composto.

Atualmente há cinquenta e um números primos de Mersenne, o último descoberto corresponde a $2^{82.589.933} - 1$ e tem 24.862.048 dígitos, a descoberta se deve ao grupo Great Internet Mersenne Prime Search (GIMPS) (Veja mais em: https://www.mersenne.org/).

3.4.3.2 Primos de Fermat

Apesar de os dados sobre Fermat serem incertos, para Eves (2004) o registro de seu nascimento é aparentemente confiável, nele diz que Fermat nasceu em Beaumont de Lomagne, perto de Toulouse em 17 de agosto de 1601. Sabe-se que ele morreu em Castres ou Toulosuse em 12 de janeiro de 1665.

Segundo Coutinho (2003), em uma carta a um matemático amador, Fermat expôs os números da forma $f(n) = 2^{2^n} + 1$ para os valores de n entre 0 e 6. Esses números são 3, 5, 17, 257, 65537, 4294967297 e 18446744073709551617. Posteriormente conjecturou que todos os números dessa forma são primos para todo inteiro não-negativo n. Mas Euler provou que a conjectura estava errada para $n = 5$, mostrando que $f(5)$ é um número composto. Para Eves (2004), $f(n)$ é composto para $5 \leq n \leq 16$ e para pelo menos mais outros quarenta e sete valores, talvez o maior deles seja $n = 1945$.

A fórmula que gera os números de Fermat é duplamente exponencial, isto é, nela temos a exponencial de uma exponencial, isso faz com que estes números sejam mais difíceis de serem calculados.

3.5 Conjecturas

Ao se estudar determinado assunto são construídas proposições, quando estas não podem ser demonstradas são chamadas de *conjecturas*. Ao longo dos anos se formaram várias conjecturas relacionadas ao números primos e muitas delas ainda estão em aberto, aqui apresentaremos a *conjectura de Goldbach* e a *conjectura dos primos gêmeos*.

A conjectura feita por Christian Goldbach (1690 - 1764) é um dos problemas da Teoria dos Números mais antigos que ainda está em aberto. Formalmente o enunciado é: *todo número par maior ou igual a 4 é a soma de dois primos*. Datada de 1742 em uma carta enviada por Goldbach a Leonhard Euler, a conjectura foi apresentada. Vejamos sua validade para os primeiros números pares:

$4 = 2 + 2;$
$6 = 3 + 3;$
$8 = 5 + 3;$
$10 = 3 + 7 = 5 + 5;$
$12 = 5 + 7;$
$14 = 7 + 7;$
$16 = 13 + 3;$
$18 = 13 + 5;$
$20 = 13 + 7;$
$\vdots$

Outra conjectura em aberto se trata dos chamados *primos gêmeos*, que são primos da forma p e $p+2$, por exemplo 3 e 5. Para Moreira e Martínez (2010), dois números primos p e q são chamados primos gêmeos se $|p - q| = 2$, o autor destaca ainda que foi conjecturado mas não demonstrado se existem infinitos pares de primos gêmeos. Para

Pantoja (2012), são poucos os avanços dados na busca da solução desse problema e aponta que os primeiros pares de primos com essa característica e menores do que 250 são (3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43),(59, 61), (71, 73), (101, 103), (107, 109), (137, 139), (149, 151),(179, 181), (191, 193), (197, 199), (227, 229), (239, 241).

Ainda segundo o autor, "[...] a maioria dos primos gêmeos muito grandes descobertos são da forma $k \cdot 2^n \pm 1$ pois existem eficientes testes de primalidade para números quando k não é muito grande, como o teorema de Proth" (PANTOJA, 2012, p. 2). Um exemplo de primos gêmeos dessa forma forma é apresentado por Moreira e Martínez (2010) e se trata dos números $65516468355 \cdot 2^{333333} \pm 1$, que têm 100355 dígitos cada, segundo os autores.

Em Eves (2004), são apresentadas perguntas sobre os números primos que ainda não foram respondidas, estas são: *há uma infinidade de primos da forma* n^2+1? *Sempre há um primo entre* n^2 *e* $(n+1)^2$? *É um n qualquer, de um certo ponto em diante, ou um quadrado ou a soma de um primo e um quadrado*? *Há uma infinidade de números primos de Fermat (primos da forma* $2^{2^n}+1$*)*?

Ao estudarmos os números primos percebemos o quanto podem ser grandes, destacamos tal fato ao comentar sobre os primos de Mersenne, Fermat e os primos gêmeos. Essa característica será muito útil ao estudarmos criptografia, já que números primos grandes são fundamentais para o método RSA, que veremos adiante.

4 CRIPTOGRAFIA

Uma das aplicações imediatas dos números primos no cotidiano das pessoas é a criptografia RSA, ela se encarrega de preservar dados em segredo e se faz mais necessária a cada dia. A privacidade é prezada pelas pessoas como uma forma de manter suas informações importantes sob sigilo; a segurança de dados secretos está se tornando indispensável tendo em vista a crescente eficiência e velocidade de transmissão de informações advindas do desenvolvimento tecnológico. Vale lembrar que,

> [...] Hoje em dia nossas chamadas telefônicas saltam entre satélites e nossos *e-mails* passam por vários computadores. Ambas as formas de comunicação podem ser interceptadas facilmente, ameaçando nossa privacidade. (SINGH, 2005, p. 12, grifo do autor)

Desse modo, necessitamos da codificação como um meio de nos certificar que além da privacidade, transações bancárias e compras on-line serão feitas de forma segura; é nesse sentido que, "a criptologia faz parte da história humana porque sempre houve fórmulas secretas e informações confidenciais que não deveriam cair no domínio público ou na mão de inimigos" (MORENO; PEREIRA; CHIARAMONTE, 2005, p. 22), assim, a criptografia se tornou essencial para a vida do homem.

Com estes argumentos apresentamos brevemente a importância da criptografia; estudaremos neste capítulo uma contextualização história desta sem nos prender a tantos detalhes como é de fato sua extensa e rica história, em seguida abordaremos a criptografia RSA que é o método criptográfico ao qual nos dedicamos neste trabalho. Para tal utilizamos os textos de Singh (2005) e Coutinho (2003).

4.1 Contextualização histórica

A palavra criptografia deriva da união das palavras gregas *kriptos*, que significa "secreto" ou "oculto" e *graphia* que quer dizer "escrita" logo, significa "escrita secreta". Para Singh (2005) a criptografia não pretende ocultar a existência de uma mensagem mas esconder seu significado, processo a qual é denominado *encriptação*. Para que o significado da mensagem não seja compreensível, o texto é alterado de acordo com uma regra em que apenas o transmissor e receptor conhecem.

Para Singh (2005, p. 23) a criptografia pode ser dividida em dois ramos chamados de *transposição* e *substituição*. A transposição consiste em apenas rearranjar as letras da mensagem, criando assim anagramas. Tal processo não é seguro quando a palavra é pequena, já quando a palavra possui um número maior de letras, rapidamente a quantidade

de arranjos cresce significativamente, fazendo com que se torne muito difícil retornar à mensagem original, salvo o caso em que o processo de mistura seja conhecido. O autor destaca ainda que,

> Uma transposição ao acaso das letras oferece um nível muito alto de segurança, porque não será possível que o interceptador inimigo consiga recompor até mesmo uma frase curta. Mas há uma desvantagem. A transposição efetivamente gera um anagrama incrivelmente difícil e, se as letras forem misturadas ao acaso, sem rima ou fundamento, a decodificação do anagrama se tornará impossível, tanto para o destinatário quanto para o interceptador inimigo. Para que a transposição seja eficaz, o rearranjo das letras deve seguir um sistema direto, previamente acertado pelo remetente e o destinatário, mas que permaneça secreto para o inimigo. (SINGH, 2005, p. 23-24)

Já a substituição, como é fácil induzir, consiste em substituir cada letra por uma diferente, processo que complementa a transposição. Nesta, cada letra mantém sua identidade mas muda a posição e no processo de substituição, as letras mudam de identidade preservando a posição. Para Singh (2005), *cifra* é qualquer forma de substituição criptográfica em que cada letra é substituída por outra letra ou um símbolo.

A cifra de substituição mais conhecida e a mais simples é a *Cifra de César*. O imperador romano Júlio César utilizava a escrita secreta com tanta frequência que foi possível escrever um tratado sobre cifras, mas não resistiu ao tempo e não tivemos acesso a ele, segundo Singh (2005). As mensagens enviadas por César baseava-se na substituição de cada letra da mensagem por outra três casas a frente no alfabeto. Por exemplo,

Texto claro: CRIPTOGRAFIA
Texto cifrado: FULSWRJUDILD

A substituição obedece a seguinte correspondência:

Alfabeto: A B C D E F G H I J KL M N O P Q R S T U V W X Y Z
Cifra: D E F G H I J KL M N O P Q R S T U V W X Y Z A B C

Pode ser atribuído, também, um valor numérico a cada letra, desse modo temos,

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Segundo Stallings (2015, p. 26), "se for conhecido que determinado texto cifrado é uma cifra de César, então uma criptoanálise pela força bruta será facilmente realizada.

Basta experimentar todas as 25 chaves possíveis". Desse modo, esse tipo de encriptação não é considerada segura.

As *cifras de substituição monoalfabéticas* são cifras de substituição na qual o alfabeto cifrado pode ser composto por símbolos bem como letras ou símbolos. Além de utilizarem essas cifras, os árabes também foram capazes de quebrá-las; segundo Singh (2005) eles inventaram a *criptoanálise*, o que permite decifrar uma mensagem sem conhecer a chave. Os criptoanalistas árabes descobriram uma forma de encontrar o significado original de uma mensagem codificada por meio do método de contagem de frequência das letras do alfabeto.

Além de outros fatores, a invenção da criptoanálise dependia do desenvolvimento dos estudos religiosos, para Singh (2005), os teólogos queriam saber a cronologia das revelações de Maomé contidas no Corão, e faziam a contagem da frequência das palavras contidas em cada revelação. Com o tempo, eles começaram a analisar também a frequência de cada letra e assim descobriram que algumas aparecem mais do que outras, isto levaria ao primeiro avanço da criptoanálise.

Embora não se saiba com certeza quem observou primeiro a contagem por frequência, Singh (2005) afirma que a técnica foi atribuída ao cientista do século IX Abu Yusef Ya'qub ibn Is-haq ibn as-Sabbah ibn omran ibn Ismail al-Kindi, conhecido como "o filósofo dos árabes", e denominada *análise de frequência*; esta dispensa a verificação de várias chaves e revela o texto original analisando a frequência das letras que aparecem na mensagem cifrada, quando se conhece bem o idioma utilizado.

Entre os anos de 800 a 1200 os árabes conseguiram significativas conquistas, enquanto al-Kindi escrevia sobre a invenção da criptoanálise os europeus ainda tentavam lidar com elementos básicos da criptografia, apenas nos mosteiros europeus é que se explorava mais a escrita secreta para descobrir os significados ocultos na Bíblia. O primeiro livro sobre criptografia escrito pelos europeus foi escrito no século XIII pelo monge franciscano Roger Bacon intitulado *Epistle on the Secret Works of Art and the Nullity of Magic*.

Por volta do século XV a criptografia na Europa crescia mais rapidamente devido ao renascimento das artes, ciência e educação durante a Renascença. Percebia-se avanços, também na diplomacia através de mensagens enviadas pelos chefes de estado aos embaixadores com informações secretas de como seria implementada sua política externa. Assim, para Singh (2005),

> Ao mesmo tempo em que a criptografia estava se tornando uma ferramenta rotineira da diplomacia, a ciência de criptoanálise começava a aparecer no Ocidente. Os diplomatas tinham acabado de se familiarizar com as habilidades necessárias para se manterem comunicações, seguras e já existiam indivíduos tentando destruir esta segurança. É bem pos-

> sível que a criptoanálise tenha sido descoberta independentemente na Europa, mas pode também ter vindo do mundo árabe. As descobertas islâmicas na ciência e na matemática tiveram uma forte influência no renascimento da ciência européia, e a criptoanálise pode ter figurado entre os conhecimentos importados. (SINGH, 2005, p. 44)

Com o tempo, a cifra de substituição monoalfabética foi enfraquecendo sua segurança e para impedir que mensagens interceptadas fossem descobertas, foram inventados os *nulos* que consistiam em símbolos ou letras que não tinham seu significado em letras verdadeiras, mas correspondiam ao número 0, que não representava nada. De acordo com Singh (2005), a utilização dos nulos era eficiente pois gerava confusão para o interceptador ao tentar decifrar uma mensagem pela análise de frequência, já o receptor sabendo da utilização dos nulos apenas os ignorava. Outra alternativa destacada pelo autor e utilizada pelos criptógrafos para garantir a segurança de suas mensagens consistia em escrevê-las com a grafia errada antes de codificá-las, isso fazia com que os interceptadores se confundissem e o receptor poderia entender a mensagem lendo-a com a grafia errada desde que não fosse incompreensível.

Ainda com o objetivo de reforçar a segurança da cifra de substituição monoalfabética, houve a inserção de palavras-código para criptografar mensagens. Para Singh (2005), o termo *código* é usado para descrever métodos secretos de comunicação, o autor defende ainda que tecnicamente o código é utilizado para a substituição de palavras ou frases enquanto as cifras substituem letras. Desse modo, para o autor, *cifrar* significa misturar uma mensagem usando uma cifra e, quando é utilizado o código o termo relativo é *codificar*. Da mesma forma, tem-se *decifrar* quando uma mensagem cifrada é revelada e *decodificar* quando se trata de uma mensagem codificada. Há ainda as expressões como *encriptar* e *decriptar* que são relativas a codificação e decodificação de códigos e cifras; esses são termos mais gerais que podem ser utilizados sem prejuízo ao sentido dos textos.

Aparentemente a utilização de códigos oferecem mais segurança do que as cifras, já que nas palavras é mais difícil aplicar a análise de frequência e para as cifras há um total de 26 letras disponíveis para testar a chave, enquanto que os códigos podem ser associados a centenas ou milhares de palavras-código. Porém, segundo Singh (2005), podemos perceber duas desvantagens dos códigos em relação as cifras, já que deveria ser criada uma palavra-código para cada uma das milhares possíveis em um texto, isso resultaria na escrita de um livro de códigos que poderia ser transformado em um grande transtorno ao tentar levá-lo de um lugar para outro. A segunda desvantagem é que, no caso de este livro estar em posse de inimigos, toda a comunicação codificada seria descoberta e as consequências seriam as piores, além do fato de que, no momento em que o código fosse descoberto, teriam que criar um novo livro de códigos totalmente diferente para ser novamente distribuído aos interessados.

Com o progresso da criptoanálise primeiro pelos estudos dos árabes e em seguida pelos europeus acabou com a segurança da cifra de substituição monoalfabética. Com a possibilidade de ser descoberta a mensagem caso esta fosse interceptada, os criptógrafos sentiam a necessidade de criar uma cifra mais forte em que os criptoanalistas não pudessem desvendar. Assim, em 1640, segundo Singh (2005), Leon Battista Alberti escreveu um ensaio que poderia ser uma nova cifra, esta baseava-se em não utilizar apenas um único alfabeto para substituição, mas dois ou mais alfabetos que seriam usados alternativamente com a finalidade de confundir os criptoanalistas.

Porém, ainda segundo o autor, tal descoberta não foi levada adiante por seu idealizador, assim Johannes Trithemius e Giovanni Porta aperfeiçoaram a ideia. Anos mais tarde o diplomata francês Blaise de Vigenère tomou conhecimento dos trabalhos de Alberti, Trithemius e Porta consolidando uma nova cifra que ficou conhecida como *cifra de Vigenère*. Esta não usa apenas um alfabeto mas 26 alfabetos distintos cifrados para criar uma mensagem cifrada. A cifra de Vigenère utiliza a ideia da cifra de César, o primeiro alfabeto é cifrado deslocando uma letra em relação ao alfabeto original, o segundo deslocando duas e assim sucessivamente, como é mostrado na tabela 1.

Para decifrar uma mensagem, o destinatário precisa saber que linha foi utilizada para a cifragem de cada letra, lembrando que se for usada apenas uma linha a cifragem é a mesma feita na cifra de César. Assim é necessário estabelecer um sistema para intercalar as linhas e cifrar uma determinada mensagem, assim obtém-se a chave de codificação que pode ser uma palavra-chave. Vejamos um exemplo de cifragem utilizando a cifra de Vigenère, a frase a ser cifrada será DISSERTAÇÃO PROFMAT e vamos usar como palavra-chave NUMERO.

Para cifrar a primeira letra D, identificamos a primeira letra da palavra-chave que é N, esta define uma linha na tabela de Vigenère que é a linha 13. Logo, utilizaremos esta linha para substituir a letra D, para isto olhamos qual coluna encabeçada pela letra D cruza com a fileira iniciada por N, o que revela a letra **Q**. Para cifrar a segunda letra I o processo é repetido, porém agora olhamos a segunda letra da palavra-chave que é U que define a linha 20, então a letra I na linha é representada pela letra **C**. Quando todas as letras da palavra-chave já tiverem sido usadas volta-se para a primeira.

Portanto, o processo de cifragem é dado por:

Palavra-chave: N U M E R O N U M E R O N U M E R O
Texto original: D I S S E R T A C A O P R O F M A T
Texto cifrado: Q C E W V F G U O E F D E I R Q R H

Segundo Singh (2005) além de ser protegido da análise de frequência essa cifra possui um número enorme de chaves. O remetente e o destinatário podem escolher qualquer palavra,

Tabela 1 - Tabela de Vigenère

Alfabeto correto	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Fonte: Singh (2005, p. 66)

combinação de letras ou até mesmo criar palavras novas como chave. Seria muito difícil um criptoanalista decodificar a mensagem já que o número de opções de chave é grande.

Devido a sua segurança a cifra de Vigenère foi amplamente adotada. Tal estilo de cifra é conhecida como *polialfabética*, pois se utiliza de vários alfabetos cifrados por mensagem; esse foi o motivo de ser tão utilizada, mas também pelo desuso já que o nível maior de complexidade em sua aplicação desestimulou a maioria das pessoas, segundo Singh (2005). Assim os criptógrafos buscavam um tipo de cifra em que não houvesse a dificuldade encontrada na polialfabética e mais difícil de quebrar do que a monoalfabética. Uma das candidatas era a *cifra de substituição homofônica*, que por sua vez, consiste em substituir cada letra por "uma variedade de substitutivos, seu número potencial sendo proporcional à frequência da letra" (SINGH, 2005, p. 70-71). Em resumo, o objetivo dessa cifra é garantir que o texto cifrado possua a mesma frequência de símbolos e, como a chance de aparecer um símbolo mais frequente do que outro é menor, o texto cifrado desafiará os criptoanalistas ao tentarem utilizar a análise por frequência para decifrar uma mensagem. Apesar de a cifra homofônica poder ser quebrada, para Singh (2005), ela

é mais segura do que a cifra monoalfabética, além de que,

> Uma cifra homofônica pode parecer semelhante a uma cifra polialfabética no sentido de que cada letra do alfabeto original pode ser cifrada de modos diferentes, mas não existe uma diferença crucial; na verdade, a cifra homofônica não passa de uma cifra monoalfabética. [...] Em outras palavras, uma letra no texto original pode ser representada por vários símbolos, mas cada símbolo pode representar apenas uma letra. (SINGH, 2005, p. 72)

Charles Babbage (1791-1871), conhecido por ter desenvolvido o precursor dos computadores, foi um britânico que conseguiu quebrar a cifra de Vigenère, feito que produziu o maior avanço na área desde que os árabes decifraram a cifra monoalfabética por meio da contagem de frequência. Provavelmente a quebra da cifra ocorreu no ano de 1854, mas não foi imediatamente publicada. Apenas no século XX quando estudiosos examinavam as anotações de Babbage é que veio a se tornar pública. Entretanto, segundo Singh (2005), desde 1863, a técnica tem sido vinculada como uma descoberta independentemente de Friedrich Wilhelm Kasiski que a publicou no *Die Geheimschriften und die Dechiffrir-kunst* (A escrita secreta e a arte de decifrá-la) e ficou conhecida como o Teste de Kasiski sem menção à contribuição de Babbage.

Para Singh (2005), na metade do século XIX por mais que os criptógrafos tenham tentado a criação de novas cifras, não se obteve resultados extraordinários e a criptografia profissional se afundou em confusão. Conforme as pessoas se acostumavam com as cifras, houve uma grande variedade em manifestar as habilidades criptográficas. Os apaixonados que não podiam expressar seu sentimento publicamente, por exemplo, começaram a trocar mensagens cifradas por meio de jornais na coluna dedicada aos leitores que eram chamadas de “colunas de óbitos”; os criptoanalistas curiosos com as mensagens comprometedoras observavam e tentavam decifrá-las. Babbage também se interessou pelas mensagens e juntamente com seus amigos Sir Charles Wheatstone e o barão Lyon Playfair foram responsáveis pela criação de uma hábil cifra que ficou conhecida como *cifra de Playfair*, que consiste em substituir cada par de letras no texto original por outro par de letras. Alguns outros tipos de cifras foram criadas utilizando os jornais nesta época.

No fim do século XIX, segundo Singh (2005), a criptografia continuava em situação de confusão. Em 1894, o físico italiano Guglielmo Marconi inventou o rádio. O telégrafo já existia, mas necessitava de um fio para transportar a mensagem, já o rádio poderia transmitir informação através de até 2,5 quilômetros de distância sem o uso de fio. Porém no uso do rádio havia tanto facilidade de comunicação quanto de interceptação e isto ficou evidente com o início da Primeira Guerra Mundial. Ainda segundo o autor, os comandantes militares precisavam de uma cifragem segura, mas entre 1914 e 1928 não houve nenhuma cifra que se destacasse. Mas,

> Uma das cifras de guerra mais famosas foi a cifra ADFGVX, introduzida no dia 5 de março de 1918, um pouco antes da grande ofensiva alemã que começou a 21 de março. Como em qualquer ataque, o avanço alemão se beneficiaria do elemento surpresa e um comitê de criptógrafos selecionara a cifra ADFGVX entre as várias candidatas, acreditando que ela ofereceria a maior segurança. De fato eles estavam confiantes de que fosse imbatível. A força da cifra estava em sua natureza complexa, sendo uma mistura de substituição e transposição. (SINGH, 2005, p. 121)

Porém essa também fora quebrada, como um exemplo típico da criptografia durante a época, assim,

> [...] Nos anos posteriores à Primeira Guerra Mundial, com todos os seus fracassos criptográficos, continuou a busca por um sistema prático que pudesse ser usado no conflito seguinte. Felizmente, para os criptógrafos, não demorou muito para que se fizesse uma descoberta, algo que reestabeleceria a comunicação secreta no campo de batalha. De modo a reforçar suas cifras, os criptógrafos foram forçados a abandonar a abordagem do papel e do lápis e explorar a tecnologia mais avançada para mandar mensagens. (SINGH, 2005, p. 143)

Desse modo, em 1918, Arthur Scherbius e Richard Ritter fundaram a empresa Scherbius & Ritter, de engenharia mas que trabalhava com tudo. Os amigos tinham o propósito de substituir o sistema inadequado de criptografia usado na Primeira Guerra Mundial e que utilizasse a tecnologia do século XX. Assim Scherbius desenvolveu uma versão elétrica do instrumento conhecido como cifra de Alberti criado anteriormente, a criação foi chamada de Enigma e mais tarde se tornaria o sistema mais temível de cifragem já utilizado.

A forma básica da Enigma consiste em três elementos conectados por fios que são, um teclado para a entrada do texto original, uma unidade misturadora que transforma a letra digitada na letra da mensagem cifrada e um mostrador que são várias lâmpadas que indicam as letras do texto cifrado. O processo de cifragem de uma mensagem acontece segundo Singh (2005), com

> O misturador, um espesso disco de borracha cheio de fios, é a parte mais importante da máquina. Partindo do teclado, os fios entram no misturador em seis pontos diferentes e fazem um série de voltas e torções dentro do misturador antes de emergirem de outros seis pontos no lado oposto. A fiação interna do misturador determina como as letras serão cifradas (SINGH, 2005, p. 146-147).

E na decifragem,

> O destinatário precisa ter outra máquina Enigma e uma cópia do livro de códigos contendo o ajuste inicial dos misturadores para aquele dia específico. Ele ajusta a máquina de acordo com o livro e datilografa o

> texto cifrado, letra por letra, enquanto o painel de lâmpadas vai indicando o texto original. Em outras palavras, o remetente datilografou o texto original para gerar o texto cifrado, e agora o receptor da mensagem datilografa o texto cifrado para obter o texto original - cifragem e decifragem são processos opostos como imagens num espelho. E a facilidade da decifragem é uma consequência da existência do refletor (SINGH, 2005, p. 152).

É fácil prever que inimigos não podem ter acesso ao livro de códigos da Enigma. Caso uma máquina seja capturada será necessário saber os ajustes para a cifragem que constam no livro e sem ele não será possível decifrar qualquer mensagem.

Scherbius acreditava que a Enigma era invencível e que seu poder criptográfico despertaria grande interesse, porém seu alto custo desanimou os possíveis compradores. Os militares alemães também não se entusiasmaram pois não acreditavam nos danos causados por suas cifras inseguras durante a guerra. Segundo Singh (2005), devido a dois documentos ingleses os alemães voltaram a atenção à Enigma e quase uma década depois perceberam a fragilidade de suas comunicações. Após investigações os alemães concluíram que a máquina Enigma seria a solução durante a guerra e posteriormente Scherbius iniciou a produção das máquinas, estas eram diferentes dos modelos comerciais. Tal invenção permitiu aos alemães o melhor sistema de comunicações sigilosas do mundo.

Com a tentativa de decifrar a Enigma foram empregados matemáticos como decifradores de códigos. A “Sala 40” sempre fora o lugar utilizado pelos ingleses para tal atividade, porém com o recrutamento dos matemáticos estes foram levados para Bletchley Park em Buckinghamshire onde ficava a Escola de Cifras e Códigos do Governo, esta organização viria a se tornar o lugar da Sala 40 na quebra de códigos. Os cientistas e matemáticos de Bletchley começaram a estudar a Enigma e rapidamente estavam dominando as técnicas polonesas na tentativa de decifrar a máquina.

Para Singh (2005), as decifragens de Bletchley se tornavam cada vez mais importantes. Um dos matemáticos mais importantes e que contribuiu de forma considerável para a criptoanálise e as descobertas da época foi Alan Turing, ele identificou e explorou a maior fraqueza da máquina Enigma. Foi por meio das contribuições de Turing que se tornou possível quebrar a cifra da Enigma, mesmo em circunstâncias difíceis utilizando as chamadas bombas de Turing. Ele se tornou conhecido entre os criptoanalistas da época e foi reconhecido como um decifrador de códigos com um dom extraordinário. Depois de decifrar a Enigma, as conquistas de Bletchley Park por meio de Turing continuavam em segredo, os britânicos tinham o intuito de continuar decifrando códigos e hesitavam em divulgar suas competências.

Ainda segundo Singh (2005), durante a Segunda Guerra Mundial, os britânicos seguiam quebrando códigos, nisto eles se destacavam mais do que os alemães, pois os homens e mulheres que trabalhavam em Bletchley Park acompanhavam as ideias dos po-

loneses com a construção de máquinas que pudessem quebrar códigos. Além das bombas de Turing, usadas para quebrar a cifra da máquina Enigma os britânicos também inventaram o *Colossus*, um aparelho decifrador para atacar uma cifra ainda mais poderosa, a cifra alemã Lorenz. Foi esse aparelho que se tornou o grande destaque criptográfico no século XX e se tornou o precursor do computador.

Logo após o fim da guerra, Colossus e tudo o que havia em Bletchey Park foi destruído e todos os que trabalhavam ali impedidos de falar o que fizeram durante o período, de acordo com Singh (2005). Porém os criptoanalistas continuavam a trabalhar e desenvolver tecnologias como o computador para quebrar cifras. Uma das diferenças mais significativas entre as máquinas de cifragem e os computadores é que estes utilizam números no lugar de letras do alfabeto, eles usam números binários (sequências de zero e um que são conhecidos como *digítos binários* ou *bits*, abreviação do inglês *binary digits*).

Whitfield Diffie nasceu em 1944 e se destaca entre os criptógrafos como o mais entusiasmado de sua geração. Segundo Singh (2005),

> Diffie imaginou dois estranhos se encontrando via Internet e se perguntou como eles poderiam trocar uma mensagem cifrada. Ele também considerou o cenário de uma pessoa querendo comprar um produto na Internet. Como esta pessoa poderia mandar um *e-mail* contendo informações cifradas sobre seu cartão de crédito, de modo que apenas o vendedor da da Internet pudesse decifrá-la? Em ambos os casos parecia que as duas partes precisariam trocar uma chave, mas como poderiam trocar chaves em segurança? [...] Diffie temia que a necessidade de distribuir chaves impediria o público de ter acesso à privacidade digital e ele tornou-se obcecado com a idéia de encontrar uma solução para o problema. (SINGH, 2005, p. 279) (grifo do autor)

Ainda segundo o autor, em 1974, Diffie soube de Martin Hellman que também se interessava pelo problema da distribuição de chaves depois de uma palestra. Depois de algum tempo estavam estudando juntos. O problema da distribuição de chaves consiste em se preocupar com a segurança da troca de mensagens secretas por meio de uma chave, "[...] resumindo, antes que duas pessoas possam partilhar um segredo (a mensagem cifrada), elas devem antes partilhar outro segredo (a chave)" (SINGH, 2005, p. 281).

Diffie e Hellman estavam inspirados em procurar uma solução para o problema da distribuição das chaves. Para Singh (2005), a pesquisa dos dois se concentrava no exame de várias funções matemáticas, não eram funções de mão dupla mas de mão única já que estas são mais difíceis de serem solucionadas; uma vez que as de mão duplas são fáceis fazê-las e desfazê-las. Um exemplo de função de mão única no cotidiano é misturar água, açúcar e o pó de café; é fácil fazer a mistura mas impossível revertê-la. Na matemática, um exemplo de função de mão única é a aritmética modular, também chamada de *aritmética do relógio*.

De acordo com Singh (2005), depois de passarem dois anos estudando a aritmética modular e as funções de mão única, os estudos de Hellman começou a ter os primeiros resultados, ele mostrou a Diffie e Merkle que concordaram. Assim, em 1976 demonstraram publicamente na Conferência Nacional de Computação e no ano seguinte fizeram a requisição da patente. Apesar de esta ser uma das maiores descobertas da criptografia, ainda necessitava de mais estudos para que se resolvesse por completo o problema da distribuição de chaves.

Enquanto Hellman continuava com estudos relacionados a seu método de troca de chaves, Diffie trabalhava em uma ideia completamente diferente, ele criou um novo tipo de cifra, a chamada *chave assimétrica*. Todas as chaves anteriormente mencionadas são do tipo *simétricas*, ou ainda, aquelas em que o processo de decifragem é o oposto da cifragem. No sistema de chave assimétrica, a chave de cifragem e decifragem são distintas. Assim, o emissor de uma mensagem pode criar seu próprio par de chaves, a de cifragem e a de decifragem; esta é chamada de *chave particular* e a outra chamada de *chave pública*. Segundo Singh (2005),

> [...] A idéia de Diffie funcionaria na teoria, mas não na prática. Não obstante, no final de 1976, a equipe de Diffie, Hellman e Merkle tinha revolucionado o mundo da criptografia. Eles tinham convencido o resto do mundo de que havia uma solução para o problema de distribuição de chaves e tinham criado a troca de chaves Diffie-Hellman-Merkle - um sistema imperfeito, mas que funcionava. Eles também tinham proposto o conceito das cifra assimétrica - um sistema perfeito mas que ainda não funcionava.(SINGH, 2005, p. 297)

Eles continuaram os estudos, mas sem encontrar a função de mão única que garantisse que a cifra assimétrica funcionasse.

4.2 A criptografia RSA

Anos depois, três pesquisadores do oitavo andar do Laboratório de Ciência e Computação do Massachussets Institute of Technology (MIT) se uniram para estudar o trabalho de Diffie e Hellman. Os estudantes eram Rivest, que persuadiu Adleman a trabalhar com ele na ideia e Adi Shamir que se uniu aos outros dois mais tarde.

Segundo Singh (2005), os três passaram a Páscoa na casa de um estudante, em 1977, e consumiram muito vinho antes de voltarem para casa. Rivest que perdera o sono ao retornar, deitou-se em um sofá e estava lendo um livro de Matemática; ele começou a pensar sobre o problema das cifras assimétricas e a função de mão única que poderia solucionar o problema e conseguiu uma ideia que fora formalizada e mostrada aos outros dois. Ao formalizar um artigo sobre sua descoberta, Rivest assinou-o colocando os autores em ordem alfabética (já que os outros dois haviam colaborado com ele por cerca de um

ano): Adleman, Rivest e Shamir. Porém ao ler o trabalho, Adleman sugeriu que seu nome ficasse por último por pensar que este era o trabalho menos interessante que já havia participado. Entretanto, o sistema chamado RSA (Rivest, Shamir, Adleman) se tornou a cifra mais importante da criptografia moderna.

Para Singh (2005) a função de mão única baseada no tipo de funções modulares está no coração da cifra assimétrica de Rivest. Um detalhe particular dela é o número n, ele torna a função de mão única reversível em certas condições o que a torna ideal para o uso desse tipo de cifra. Essencialmente, o método se baseia em multiplicar dois números primos distintos que gerará uma chave, esta chave somente será decodificada se quem investiga conhece os dois fatores; a importância de ser números primos é que eles garantem a unicidade da fatoração. E mais ainda, quando estes dois fatores são primos muito grandes, a tarefa de decodificar a chave se torna muito difícil, pois ainda não há um método fácil, rápido e eficaz que permite descobrir os valores dos fatores da chave.

De acordo com Singh (2005),

> O único problema para a segurança da criptografia de chave pública RSA é que, em alguma época no futuro, alguém possa encontrar um modo rápido de fatorar N. É concebível que daqui a uma década, ou mesmo amanhã, alguém possa descobrir um método para a fatoração rápida e aí a RSA se tornará inútil. Contudo, por dois mil anos os matemáticos têm tentado e fracassado em encontrar um atalho, e por enquanto, a fatoração continua sendo um cálculo muito trabalhoso. A maioria dos matemáticos acredita que a fatoração é uma tarefa inerentemente difícil e que existe alguma lei matemática que proíbe a existência de qualquer atalho. Vamos presumir que eles estejam certos: deste modo, a RSA estará segura durante o futuro previsível. (SINGH, 2005, p. 303)

O desenvolvimento da criptografia de chave pública pelos três estudantes permitiu que recebessem a fama e notoriedade pelo crédito da descoberta, porém, segundo Singh (2005), de acordo com o governo britânico a criptografia de chave pública fora inventada no Quartel-General de Comunicações do Governo (GCHQ) em Cheltenham por pessoas que ainda ficaram em Bletchley Park depois da Segunda Guerra Mundial. Mais especificamente, a descoberta foi feita por Clifford Coks que soube da teoria de James Ellis sobre o assunto e começou a trabalhar na ideia da função de mão única que garantiria a segurança da criptografia de chave pública que até o momento ninguém conseguira encontrar. A partir de 1973 ele conseguiu pensar na mesma formulação feita por Rivest, Hellman e Adleman, mas não podia apreciar o real significado de sua conquista, pois tais descobertas poderiam ajudar os generais em suas batalhas e comunicações militares logo, tanto Ellis como Coks foram impedidos de contar a qualquer pessoa fora do GCHQ sobre seus trabalhos.

Segundo Coutinho (2003), a primeira etapa do método é a **pré-codificação** que consiste em converter a mensagem desejada em uma sequência de números. No caso em

que ilustraremos tomaremos nossa mensagem sem números grandes, para simplificar a descrição das etapas.

Para a conversão das letras em números como desejamos utilizaremos o quadro seguinte:

Δ	A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

O espaço entre duas palavras será substituído pelo número 99, quando fizermos a conversão. A frase que utilizaremos como exemplo será TEORIA DOS NÚMEROS, feita a conversão para números segundo o quadro acima temos:

$$291424271810991324289923302214272428.$$

Os parâmetros do sistema RSA são dois números primos que denotaremos por p e q, faremos $n = pq$. A última parte do processo de pré-codificação consiste em dividir o número obtido em blocos menores que n. Assim, fazendo $p = 11$ e $q = 17$ temos $n = 11 \cdot 17 = 187$ e os blocos do número acima podem ser:

$$2 - 91 - 42 - 42 - 7 - 18 - 10 - 99 - 132 - 42 - 89 - 92 - 3 - 30 - 22 - 142 - 72 - 42 - 8.$$

Esses blocos poderiam ser escritos de outras formas, porém é preciso ter cuidado com aqueles que começam com o número 0, pois é mais fácil surgir problemas no momento da decodificação. Assim é finalizada a etapa de pré-codificação.

A segunda etapa é chamada de **codificação**, segundo Coutinho (2003). Nesta etapa precisaremos de n, assim como um número e que seja inversível módulo $\varphi(n)$, ou ainda, mdc$(e,\ \varphi(n)) = 1$. Como temos p e q definidos é fácil calcular $\varphi(n)$, pois $\varphi(n) = (p-1)(q-1)$. O par (n, e) será chamado de chave de codificação. Cada bloco que obtemos na etapa da pré-codificação será codificado separadamente e a mensagem codificada será a sequencia dos blocos codificados.

Em nosso caso temos $\varphi(n) = \varphi(187) = (11-1)(17-1) = 160$. Nosso número e será o menor primo que não divide 160, logo $e = 3$, assim temos a chave de codificação $(n, e) = (187, 3)$. A codificação de um bloco b será dada por

$$\text{C(b)} = \text{resto da divisão de } b^e \text{ por } n, \text{ sendo } b \text{ um bloco da mensagem.}$$

Em termos de aritmética modular temos,

$$C(b) \equiv b^e \bmod n, \text{ com } 0 < C(b) < n.$$

Codificando cada bloco obtemos:

Como $2^3 = 8$ e $8 \equiv 8 \bmod 187$, logo, $\mathbf{C(2) = 8}$.

Como $91^3 = 91^2 \cdot 91$, $91 \equiv 91 \bmod 187$ e $91^2 \equiv 53 \bmod 187$ então, $91^3 \equiv 91 \cdot 53 \equiv 148 \bmod 187$. Logo, $\mathbf{C(91) = 148}$.

Como $42^3 = 42^2 \cdot 42$, $42 \equiv 42 \bmod 187$ e $42^2 \equiv 81 \bmod 187$ então, $42^3 \equiv 81 \cdot 42 \equiv 36 \bmod 187$. Logo, $\mathbf{C(42) = 36}$.

Como $7^3 = 343$ e $343 \equiv 156 \bmod 187$, logo, $\mathbf{C(7) = 156}$.

Como $18^3 = 18^2 \cdot 18$, $18 \equiv 18 \bmod 187$ e $18^2 \equiv 137 \bmod 187$ então, $18^3 \equiv 137 \cdot 18 \equiv 35 \bmod 187$. Logo, $\mathbf{C(18) = 35}$.

Como $10^3 = 1000$ e $1000 \equiv 65 \bmod 187$, logo, $\mathbf{C(10) = 65}$.

Como $99^3 = 99^2 \cdot 99$, $99 \equiv 99 \bmod 187$ e $99^2 \equiv 77 \bmod 187$ então, $99^3 \equiv 77 \cdot 99 \equiv 143 \bmod 187$. Logo, $\mathbf{C(99) = 143}$.

Como $132^3 = 132^2 \cdot 132$, $132 \equiv (-55) \bmod 187$, $132^2 \equiv 33 \bmod 187$ então, $132^3 \equiv 33 \cdot (-55) \equiv -132 \equiv 55 \bmod 187$. Logo, $\mathbf{C(132) = 55}$.

Como $89^3 = 89^2 \cdot 89$, $89 \equiv 89 \bmod 187$ e $89^2 \equiv 67 \bmod 187$ então, $89^3 \equiv 67 \cdot 89 \equiv 166 \bmod 187$. Logo, $\mathbf{C(89) = 166}$.

Como $92^3 = 92^2 \cdot 92$, $92 \equiv 92 \bmod 187$ e $92^2 \equiv 49 \bmod 187$ então, $92^3 \equiv 49 \cdot 92 \equiv 20 \bmod 187$. Logo, $\mathbf{C(92) = 20}$.

Como $3^3 = 27$ e $27 \equiv 27 \bmod 187$, logo, $\mathbf{C(3) = 27}$.

Como $30^3 = 30^2 \cdot 30$, $30 \equiv 30 \bmod 187$ e $30^2 \equiv 152 \bmod 187$ então, $30^3 \equiv 152 \cdot 30 \equiv 72 \bmod 187$. Logo, $\mathbf{C(30) = 72}$.

Como $22^3 = 22^2 \cdot 22$, $22 \equiv 22 \bmod 187$ e $22^2 \equiv 110 \bmod 187$ então, $22^3 \equiv 110 \cdot 22 \equiv 176 \bmod 187$. Logo, $\mathbf{C(92) = 20}$.

Como $142^3 = 142^2 \cdot 142$, $142 \equiv 142 \bmod 187$ e $142^2 \equiv 155 \bmod 187$ então, $142^3 \equiv 155 \cdot 142 \equiv 131 \bmod 187$. Logo, $\mathbf{C(142) = 131}$.

Como $72^3 = 72^2 \cdot 72$, $72 \equiv 72 \bmod 187$ e $72^2 \equiv 135 \bmod 187$ então, $72^3 \equiv 135 \cdot 72 \equiv 183 \bmod 187$. Logo, $\mathbf{C(72) = 183}$.

Como $8^3 = 512$ e $512 \equiv 138 \bmod 187$, logo, $\mathbf{C(8) = 138}$.

Assim, a sequência dos blocos codificados é:

8 - 148 - 36 - 36 - 156 - 35 - 65 - 143 - 55 - 36 - 166 - 20 - 27 - 72 - 176 - 131 - 183 - 36 - 138.

Agora, veremos como **decodificar** a mensagem que acabamos de codificar de acordo com Coutinho (2003), este processo consiste em encontrar o bloco da mensagem original por meio de uma determinada regra aplicada ao bloco codificado. Trataremos de um bloco específico, pois o processo é análogo para os outros. Para isso precisamos do número n e o inverso de e em $\varphi(n) = d$. Desse modo, teremos a chave de decodificação (n, d). Seja a um bloco da mensagem codificada, então D(a) será o resultado da decodificação realizada, assim

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

Ou ainda,

$$D(a) \equiv a^d \bmod n, \text{ com } 0 < D(a) < n.$$

Precisamos conhecer d para decodificar, porém, só sabemos como calculá-lo utilizando o algoritmo de Euclides estendido a e e $\varphi(n)$. Em nosso caso temos que $n = 187$, $e = 3$ e $\varphi(n) = 160$. Aplicando o algoritmo para encontrar d, temos que

$$160 = 3 \cdot 53 + 1, \text{ donde } 1 = 160 + (-53) \cdot 3.$$

Logo o inverso de 3 módulo 160 é -53. Como vamos usar d como expoente de potências, precisamos que d seja positivo. Portanto, $d = 160 - 53 = 107$ que é o menor inteiro positivo congruente a -53 módulo 160.

Para decodificar o bloco 8 da nossa mensagem codificada, calculamos a forma reduzida de 8^{107} módulo 187. Assim, como $107 = 3 \cdot 5 \cdot 7 + 2$ temos que

$$8^3 = 512 \equiv 138 \bmod 187.$$

Pelo item vi) da proposição 3.2.3,

$$\begin{aligned}
(8^3)^5 &\equiv 138^5 \bmod 187 \\
&\equiv 138^2 \cdot 138^2 \cdot 138 \bmod 187 \\
&\equiv 19044 \cdot 19044 \cdot 138 \bmod 187 \\
&\equiv 157 \cdot 157 \cdot 138 \bmod 187 \\
&\equiv 3401562 \bmod 187 \\
&\equiv 32 \bmod 187.
\end{aligned}$$

Assim $8^{15} = (8^3)^5 \equiv 32 \bmod 187$. Ainda temos que,

$$\begin{aligned}(8^{15})^7 &\equiv 32^7 \bmod 187\\ &\equiv 32^3 \cdot 32^3 \cdot 32 \bmod 187\\ &\equiv 32768 \cdot 32768 \cdot 32 \bmod 187\\ &\equiv 43 \cdot 43 \cdot 32 \bmod 187\\ &\equiv 59168 \bmod 187\\ &\equiv 76 \bmod 187.\end{aligned}$$

E, $8^{105} = (8^{15})^7 \equiv 76 \bmod 187$. Portanto,

$$\begin{aligned}8^{107} = 8^{105} \cdot 8^2 &\equiv 76 \cdot 64 \bmod 187\\ &\equiv 4864 \bmod 187\\ &\equiv 2 \bmod 187.\end{aligned}$$

Notemos que o resto é igual a 2 e tal número corresponde exatamente ao primeiro bloco da mensagem original. Desse modo conseguimos voltar para o texto em que pretendíamos codificar e decodificar inicialmente. O processo é análogo para os demais blocos, porém quanto maior o número relativo ao bloco mais complexos serão os cálculos.

4.3 Por que o sistema RSA funciona?

Adotando as notações que utilizamos anteriormente temos um sistema RSA de parâmetros p e q; $n = pq$; dados de codificação com o par (n, e) e dados de decodificação com o par (n, d). Mostraremos porque o sistema funciona, segundo Coutinho (2003). Para tal tarefa precisamos verificar que se b é um inteiro e $1 \leq b \leq n-1$, e denotando o bloco decodificado por DC(b) = b, provaremos que $DC(b) \equiv b \bmod n$, isto é suficiente já que tanto DC(b) quanto b estão no intervalo 1 e $n-1$, logo só podem ser congruentes módulo n se forem iguais. É por esse motivo que no processo de codificação os blocos devem ser menores do que n e precisamos mantê-los separados mesmo depois da codificação.

Por definição, temos que

$$D(C(b)) \equiv (b^e)^d \equiv b^{ed} \ mod \ n \tag{4.1}$$

Como d é o inverso de e módulo $\varphi(n)$, logo $ed = 1 + k\varphi(n)$ para algum k. Observemos que e e d são inteiros maiores que 2 e $\varphi(n) > 0$, então $k > 0$. Substituindo em 4.1 temos

$$b^{ed} \equiv b^{1+k\varphi(n)} \equiv b(b^{\varphi(n)})^k \ mod \ n. \tag{4.2}$$

Usando o Teorema de Euler temos $b^{\varphi(n)} \equiv 1 \bmod n$, daí resta-nos apenas que $b^{ed} \equiv b \bmod n$. Porém, para usarmos o Euler e concluir que $b^{\varphi(n)} \equiv 1 \bmod n$ apenas seria possível se soubéssemos que $\text{mdc}(b,n) = 1$, mas isso nem sempre é possível já que é difícil controlar os números dos blocos da mensagem. Assim, a solução é tentar provar a congruência sem usar o Teorema de Euler.

Temos que $n = pq$, com p e q primos distintos; calcularemos b^{ed} módulo p e módulo q. Como o cálculo é análogo para ambos, faremos apenas um caso.

De $ed = 1 + k\varphi(n) = 1 + k(p-1)(q-1)$, e de 4.2 temos

$$b^{ed} \equiv b^{1+k(p-1)(q-1)} \equiv b \cdot (b^{p-1})^{(q-1)k} \bmod p.$$

Queremos usar o Teorema de Fermat, mas precisamos supor que p não divide b, no caso disso ser verdade teremos $b^{p-1} \equiv 1 \bmod p$ por Fermat e assim obtemos, $b^{ed} \equiv b \bmod p$, porém ainda estamos com o mesmo problema.

O fato de p ser primo permite que vejamos o caso em que p divide b. Neste caso teremos $b \equiv 0 \bmod p$ e a congruência é verificada. Assim $b^{ed} \equiv b \bmod p$ vale para qualquer valor de b. Note que não podemos usar um argumento semelhante para n e encerrarmos a discussão, pois mdc(n, b) $\neq 1$ não significa necessariamente que $b \equiv 0 \bmod n$ já que n é composto.

Daí, temos que $b^{ed} \equiv 0 \bmod p$ vale para qualquer b. Analogamente temos que $b^{ed} \equiv b \bmod q$. Em outras palavras $b^{ed} - b$ é divisível por p e q. Como p e q são primos distintos temos que mdc(p, q) $= 1$, donde pq divide $b^{ed} - b$ pelo lema 3.3.1.

Como $n = pq$ concluímos que $b^{ed} \equiv b \bmod n$ para qualquer inteiro b como queríamos demonstrar.

4.4 Por que o RSA é seguro?

Lembremo-nos de que o sistema RSA é um sistema de chave pública, consideramos anteriormente os primos p e q como os parâmetros do sistema e $n = pq$. A chave de codificação é a chave pública logo, o par (n, e) é acessível para qualquer usuário e a chave de decodificação é a chave privada, logo o par (n, d) é de uso restrito. O sistema somente será seguro se for difícil calcular d quando apenas n e e são conhecidos.

Para Coutinho (2003) só podemos quebrar códigos se conseguirmos fatorar n, mas quando esse n é grande, fatorá-lo é uma tarefa difícil já que não conhecemos algoritmos de fatoração rápidos que tornem a atividade fácil. Outro fator relevante na discussão sobre a segurança do RSA consiste na escolha dos primos que são os parâmetros do método, pois se são pequenos o sistema é fácil de ser quebrado e além disso, não basta apenas que os

primos sejam grandes, já que |p - q| é pequeno então, fica fácil fatorar $n = pq$. Por esse motivo se faz importante pensar em quais primos são "ideais" para garantir a segurança do método.

Nesse sentido, Terada (1988) destaca que o ponto importante do sistema RSA é o fato de ainda não existir um algoritmo que permita a decomposição de números em fatores primos de forma rápida, ressalta ainda que por meio do algoritmo Schroeppel e usando um computador capaz de efetuar uma multiplicação em um microssegundo (10^{-6} seg) o tempo para "quebrar" o RSA, quanto ao número de algarismos de n, é dado pela tabela 2:

Tabela 2 - "Quebra" do RSA por meio do algoritmo Schroeppel

Nº de algarismos de n	Tempo necessário para "quebrar" o RSA
50	3,9 horas
75	104 dias
100	74 anos
200	3,8 x 10^7 séculos
300	4,9 x 10^{13} séculos
500	4,2 x 10^{23} séculos

Fonte: Terada (1988)

Assim,

> [...] O que podemos dizer se usarmos o equipamento moderno? Dados os grandes avanços em poder computacional, números de cem algarismos devem ser evitados. Já em 2005, chaves de 200 dígitos eram consideradas quebráveis por especialistas usando grandes supercomputadores. Os avanços em fatoração chegaram a duas frentes: computadores melhores e algoritmos melhores. (ROSSEAU; SAINT-AUBIN, 2015, p. 237)

Desde a implementação do sistema RSA, muitos estudos tem sido desenvolvidos e necessariamente sobre métodos de fatoração, segundo Rosseau e Saint-Aubin (2015), mas sem muito sucesso, já que o sistema permanece não quebrado. Para os autores, não é possível saber ainda se quebrar o RSA é equivalente a descobrir a fatoração ou se existem alternativas mais baratas, porém o que se sabe é que todos os esforços até o momento em quebrá-lo usando técnicas que não envolvam a fatoração de n não tiveram sucesso.

4.5 Assinaturas digitais

Para Coutinho (2003), em sistemas de chave pública como o RSA há a facilidade em enviar mensagens assinadas. As assinaturas digitais não apenas garantem que a mensagem seja transmitida de forma segura, como também garante que não será adulterada no processo, já que qualquer alteração da mensagem desvincula a assinatura do documento.

O método consiste em, por exemplo, ter as funções C_e e D_e de codificação e decodificação da empresa, respectivamente, e C_b e D_b as funções de um banco.

Seja a um bloco da mensagem que a empresa quer enviar ao banco. De acordo com a seção 4.2 a empresa deveria codificar a como $C_b(a)$ e enviá-lo por linha telefônica. Para enviar a mensagem assinada, ao invés de $C_b(a)$ enviamos $C_b(D_e(a))$. Isto é, primeiro aplicamos a função decodificação da empresa a a e só depois codificamos o bloco usando a função codificação do banco.

Tendo recebido o bloco $C_b(D_e(a))$ o banco aplica sua função de decodificação para obter $D_e(a)$, e a este último bloco aplica a função codificação da empresa para obter a, que é o bloco original. Observemos que C_e é público, por isso é conhecido do banco.

5 NÚMEROS PRIMOS E CRIPTOGRAFIA NA SALA DE AULA

Após estudarmos as propriedades relativas aos números primos e alguns momentos históricos sobre a Criptografia, direcionaremos nosso estudo para a utilização dos principais conceitos apresentados para sala de aula da Educação Básica. Destacamos os números primos, pois estes são fundamentais para o método RSA que se tornou o mais importante algoritmo para a criptografia de chave pública. Com este capítulo queremos evidenciar que é possível levar tanto os números primos como a criptografia para a sala de aula de forma atrativa.

Dividiremos o capítulo em duas partes; a primeira trata-se de uma experiência com os números primos que consiste em uma sequência de atividades para o ensino desses números utilizando um material concreto para explorar os principais conceitos do conteúdo. O objetivo de exibirmos as atividades já executadas, é que essas podem ser levadas para a sala de aula como uma forma de ensinar os alunos os números primos para depois apresentar a atividade sobre criptografia RSA. Na segunda parte, apresentamos atividades de criptografia para a sala de aula, explorando alguns tipos de cifras relacionando-as a conteúdos estudados na Educação Básica e por fim, destacaremos a criptografia RSA e como são utilizados os números primos no processo de codificação e decodificação deste método.

Logo, o público-alvo ao qual desejamos atingir são os professores da Educação Básica que desejam ensinar os números primos de uma maneira mais atrativa relacionando-os a um conceito essencial para a vida em sociedade que é a criptografia RSA.

5.1 Uma experiência com números primos

A atividade com números primos foi desenvolvida em uma turma de tutoria para os alunos do curso de Licenciatura em Matemática da Universidade Federal do Tocantins (UFT), Campus Prof. Dr. Sérgio Jacintho Leonor/Arraias-TO, com 7 alunos que desenvolveram todas as atividades propostas. A tutoria é um programa das Pró-reitorias de Graduação (PROGRAD) e de Pesquisa, Pós-Graduação e Inovação (PROPESQ), ofertada como uma revisão de conceitos básicos de Matemática Geral com o intuito de apoiar os estudantes de graduação para melhor aproveitamento das disciplinas durante o curso.

A partir da proposta de atividade investigativa apresentada pelos professores da disciplina Tópicos em Educação do PROFMAT em Arraias-TO, surgiu a possibilidade de trabalhar os conceitos de números primos com os alunos participantes da tutoria, já

que o objetivo geral da atividade consistia em propor novos caminhos para o processo de ensino e aprendizagem de conteúdos da Matemática. Fomos orientados a selecionar um conteúdo matemático e executar uma atividade de diagnóstico de dificuldades ou lacunas apresentadas pelos alunos no processo de ensino-aprendizagem, a partir disso trabalhar com novas propostas metodológicas e analisar os resultados da intervenção.

Com o objetivo de investigar quais conceitos, que envolvem números primos, os alunos da graduação conhecem e quais apresentam dificuldades, utilizamos questionários e como uma forma de estimular a aprendizagem de conceitos ou reforçar conhecimentos sobre o assunto optamos pelo material manipulável Escala Cuisenaire para, além de despertar a curiosidade sobre o material, perceber os conceitos de aritmética que podem ser estudados por meio dele.

Esta atividade buscou evidenciar os conceitos necessários para se estudar os números primos, assim como demonstrar sua importância por meio de recursos visuais e experimentais como vídeos, discussões, Escala Cuisenaire e atividades escritas; além de explorar e demonstrar que tais números se manifestam em várias atividades humanas, buscamos aliar o estudo ao fato de que primos muito grandes podem despertar o interesse por novos estudos para contribuir com o desenvolvimento das ciências e de determinadas áreas que garantem a segurança dados por meio da criptografia.

No primeiro encontro ocorreu a aplicação de um questionário de sondagem de conhecimentos (ver Apêndice 6.1), composto por oito questões, para avaliar quais conceitos os alunos sabiam e que são necessários para o estudo dos números primos, como resto de uma divisão, divisores, múltiplos e decomposição de números naturais em fatores primos. Neste questionário também havia questionamentos para sondar se os alunos conheciam a importância do estudo dos números primos e se conheciam números primos maiores do que 11.

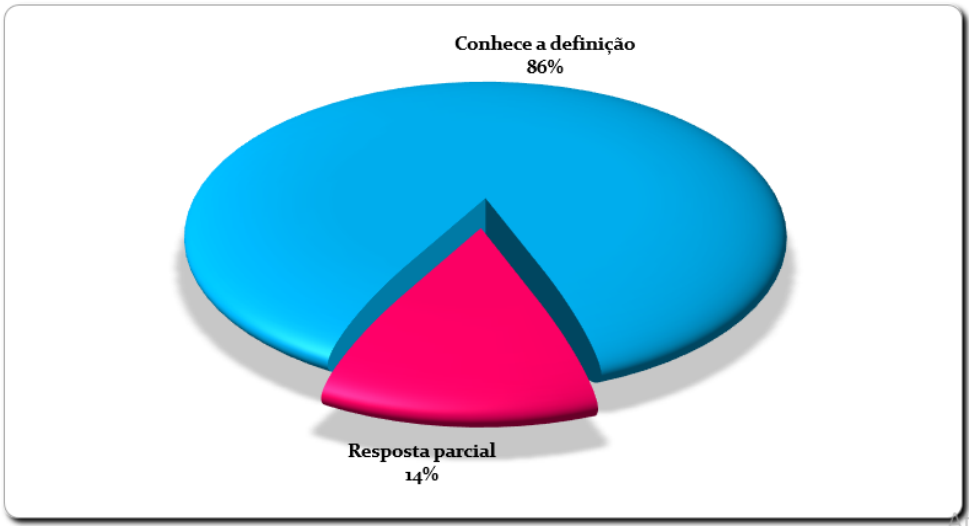
No segundo encontro, aconteceu o desenvolvimento de atividades sobre números primos. Inicialmente, os alunos foram convidados a assistir o vídeo “Como funciona a criptografia” (disponível no YouTube em <https://www.youtube.com/watch?reload=9&v=glGrlf5mWcY>), este define de forma fácil e compreensível o que são números primos e suas utilidades para as pessoas, enfatizando a criptografia para a segurança da vida em sociedade. Depois de uma conversa para socializar o vídeo, as atividades de aprendizagem foram iniciadas com o “Crivo de Eratóstenes Móvel” (ver Apêndice 6.3), que é utilizado para verificar a existência de números primos em determinado intervalo de números. Em seguida, os alunos foram estimulados a conhecer a Escala Cuisenaire, para que a partir do material manipulativo, visualizassem a definição de números primos por meio das barras, explorassem os conceitos de múltiplos e divisores e, visualizassem como pode ser feita a decomposição de números em fatores primos. Por fim, para revisar todos os conceitos explorados durante o encontro, participaram de uma gincana de revisão.

5.2 Resultados da atividade

Para sondagem dos conhecimentos, foi aplicado o questionário de sondagem para perceber o quanto os alunos conheciam sobre os números primos. Neste, continham perguntas sobre o que caracteriza os números primos, identificação de números primos em uma lista de números, múltiplos e divisores de números naturais, resto da divisão de números naturais e a decomposição de números em fatores primos; com a pretensão de analisar quais desses conceitos os alunos mais sentiam dificuldades para então desenvolver a atividade de intervenção.

No primeiro questionamento, o objetivo era saber se os alunos conheciam a definição de números primos. Vejamos no gráfico 1, que a maior parte dos alunos conhecem a definição; as respostas classificadas como parcial são aquelas em que o aluno respondeu que os primos são aqueles que dividem apenas ele mesmo, esquecendo o fato que ele também divide o número 1.

Gráfico 1 - Percentual das respostas quanto a definição de números primos



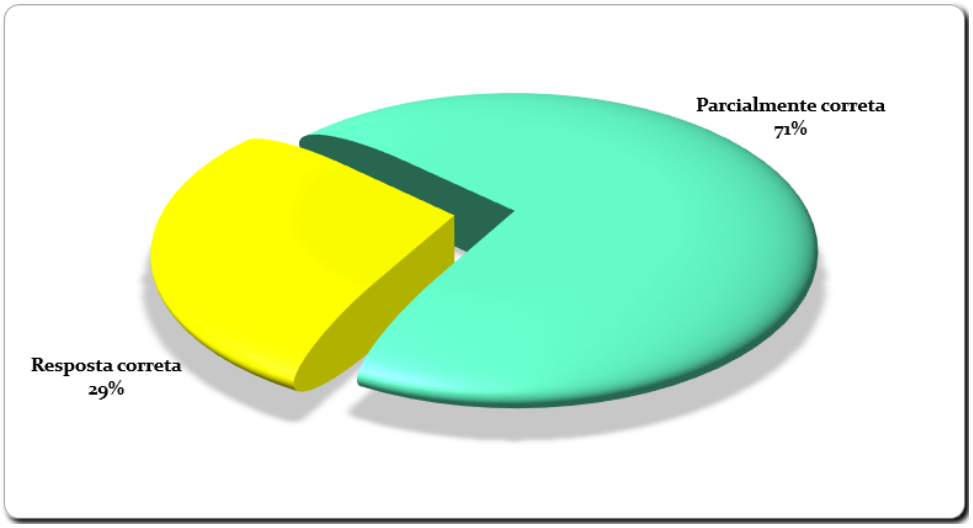
Fonte: elaborado pela autora

Questionados se sabiam para que servem ou em que situações são utilizados os números primos (Questão 2) nota-se que, salvo as exceções que disseram que eles serviam para decompor/fatorar outros números, a maioria dos alunos não sabem, deixaram em branco ou responderam não. A finalidade de tal questionamento, era explorar se conheciam a utilização de tais números no contexto social, demonstrando que os conhecem apenas sob o enfoque da sala de aula.

Na questão 3, havia uma lista com alguns números que pertencem ao intervalo 1 a 100, com números primos e compostos para que os alunos identificassem quais deles eram primos. A lista apresentava vinte e sete números dos quais treze eram primos; destes, nove eram primos maiores do que 19. Nota-se que os alunos reconheceram corretamente

todos os números primos menores do que 19, mas a maioria dos alunos apresentaram dificuldades em reconhecer primos maiores do que estes. O gráfico 2 traz o percentual de acertos na questão.

Gráfico 2 - Percentual de respostas da questão 3



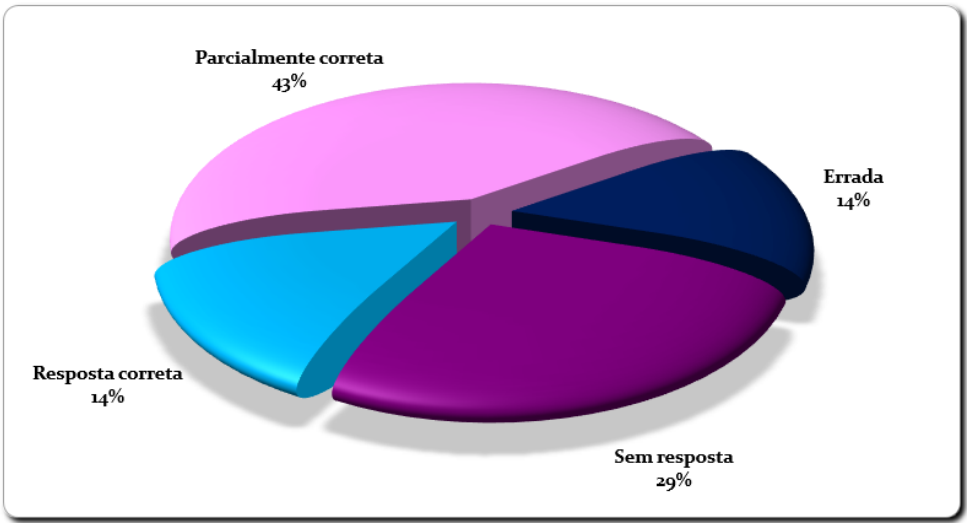
Fonte: elaborado pela autora

Nas questões 4 e 5, foi explorado o conceito de múltiplos, percebe-se uma uniformidade quanto ao nível de acertos, a maioria dos alunos sabiam o conceito de um número ser múltiplo de outro (Questão 4), assim como identificaram corretamente os múltiplos de um determinado número (Questão 5). Os erros detectados nessas questões consistiam no fato de confundirem o conceito de múltiplo e divisor. Assim como nessas, a questão 6 também apresentou um bom índice de aproveitamento, esta abordava o conceito de divisor, nota-se pequenos erros, por distração e não por falta de conhecimento; o que também ocorreu na questão 7, onde foi examinado o que os alunos sabiam sobre restos da divisão de números naturais.

Na questão 8, foi proposta a decomposição de um número em fatores primos. Nota-se que houve uma mesma quantidade de respostas corretas e erradas. Um percentual maior do que certo ou errado foi de a questão ser deixada sem resposta, o que nos leva a pensar que os alunos não sabiam responder. As respostas chamadas de parcialmente correta, foram aquelas em que foi percebido, falta de detalhes ou o procedimento com inversão de números na decomposição, fica perceptível pela percentagem do gráfico 3, a dificuldade dos alunos em decompor números em fatores primos.

A partir dos resultados obtidos com a aplicação do questionário de sondagem, foram desenvolvidas atividades com esses alunos para revisar o conteúdo com a finalidade de romper as dificuldades apresentadas. A primeira atividade proposta foi o Crivo de Eratóstenes Móvel, esta recebeu este nome pelo fato de o material utilizado não ter uma

Gráfico 3 - Percentual de respostas da questão 8



Fonte: elaborado pela autora

tabela em um papel - como geralmente é feito - mas, com fichas numeradas de 1 a 100 para serem dispostas em forma de tabela, pelos alunos de modo que pudessem ser retiradas ou colocadas de acordo com o que fosse solicitado.A montagem da tabela é mostrada na imagem a seguir.

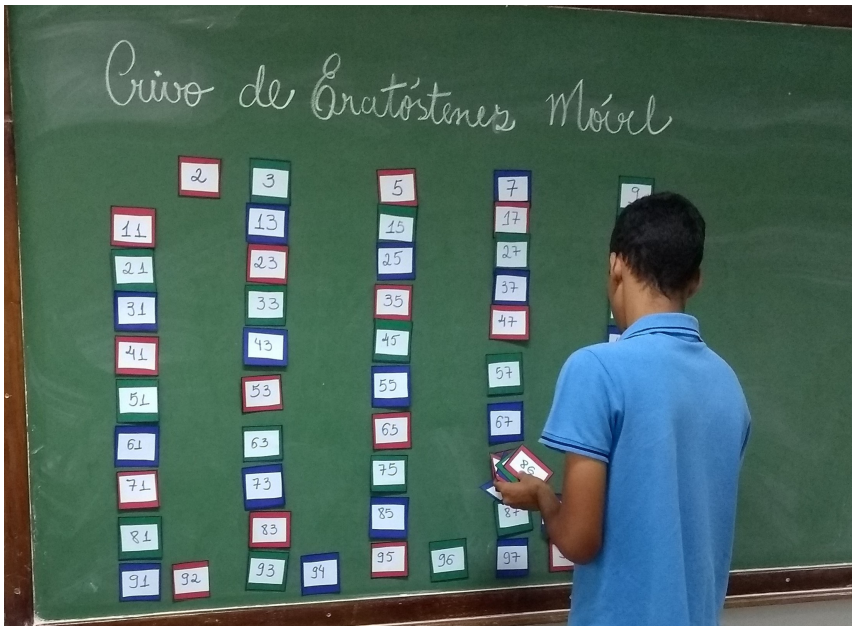
Imagem 1 - Montagem da tabela para o Crivo de Eratóstenes Móvel pelos alunos

Fonte: acervo pessoal

A atividade consiste em deixar o número 1 em destaque para despertar a curiosidade dos alunos e explicar o porquê de ele não ser considerado um número primo. Um aluno foi convidado a ir até tabela e sabendo que o número 2 é um primo (como foi percebido pela aplicação do questionário), retirar todos os múltiplos de 2 da tabela, como

podemos ver na imagem a seguir. Em seguida, repetiu-se o mesmo procedimento para os primos 3, 5 e 7. Para saber até que primo retirar, foi mostrado aos alunos que basta calcular a raiz quadrada do último número do intervalo, caso seja primo este será definido como critério de parada, caso não seja, basta analisar o menor primo antes dele.

Imagem 2 - Retirada dos múltiplos de 2 da tabela



Fonte: acervo pessoal

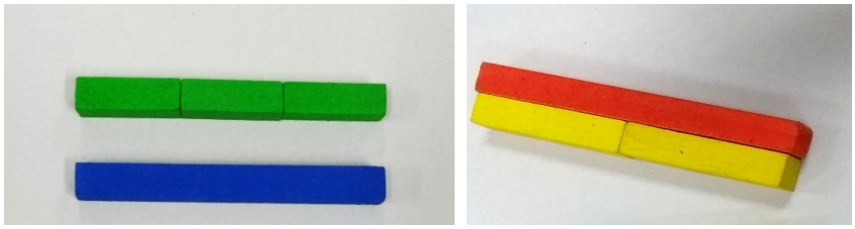
Com o desenvolvimento da atividade, foi possível perceber mais uma vez a facilidade que os alunos tinham com o conceito de múltiplos de números e para a retirada de todos, uns ajudavam os outros quando esqueciam algum número. Com a finalização da atividade, eles foram levados a pensar sobre questões relacionadas aos números primos como, por exemplo, qual o menor primo; se existe um maior primo; se existe algum primo par; quantos e quais são, por meio de uma roda de conversa rápida onde se manifestaram livremente, sem aparente constrangimento.

Em seguida, de acordo com a Atividade 2 (ver Apêndice 6.4), apresentamos a Escala Cuisenaire aos alunos falando brevemente sua história, qual a finalidade de sua invenção, e quais os conteúdos podem ser estudados por meio dela. Inicialmente, sugerimos que os alunos manuseassem livremente para se adaptarem ao material. A atividade foi dividida em três momentos, além deste introdutório.

No primeiro momento, os alunos foram orientados a tomar uma barrinha de cada cor e buscar outra barra de forma que pudesse reproduzir o comprimento da barra escolhida utilizando quantas outras fossem necessárias, com a exceção de não tomar a barrinha branca para fazer o procedimento. Na figura 4 vejamos duas das produções dos alunos; na figura à esquerda o aluno escolheu a barra azul que pode ser representada também pela

união de três barras verdes e na figura à direita, o aluno representou a barra laranja com duas barras amarelas.

Figura 4 - Representações de uma barra pela utilização de outras barras



Fonte: acervo pessoal

A discussão inicial foi pautada pela escolha das cores, depois de montarem as representações, mostramos a eles o porquê do conceito de múltiplos e divisores por meio do que fizeram, exemplificando com os números aos quais as barrinhas correspondem. Neste momento, os alunos demonstraram o interesse em relacionar o conceito estudado com as representações fazendo novas montagens e comentavam utilizando as cores e os números. Percebemos que o desenvolvimento da atividade foi útil no sentido de permitir que visualizassem aquilo que já sabiam, pelos comentários.

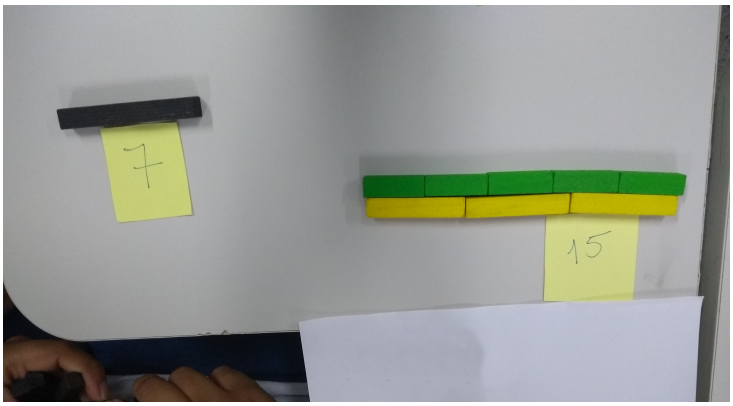
Depois do diálogo, foram entregues fichas com alguns números para que os alunos fizessem as possibilidades de escrever os números com as barrinhas, deixando-os livres para mostrar todas as possibilidades e assim notar os múltiplos e divisores do número. Vejamos na figura 5, como um aluno fez as representações para o número 12 e o número 4. Assim que os alunos faziam as representações, escreviam também os múltiplos e os divisores dos números comparando com o que haviam feito usando as barras.

Figura 5 - Representação dos números 12 e 4 utilizando as Barras Cuisenaire

Fonte: acervo pessoal

No segundo momento, pedimos aos alunos que identificassem quais dos números que haviam recebido e que a representação não era possível a não ser que fosse utilizada a barrinha branca, ao mostrarem, perguntamos o motivo disso acontecer, e a partir do que já haviam feito e pelo conceito de primo que já sabiam, identificaram que isso somente acontecia com números primos. O que demonstra que além do conceito aprendido em sala de aula, puderam reafirmar por meio da utilização do material manipulável. Vejamos uma representação na figura 6.

Figura 6 - Visualização de um número primo e um composto por meio das barras



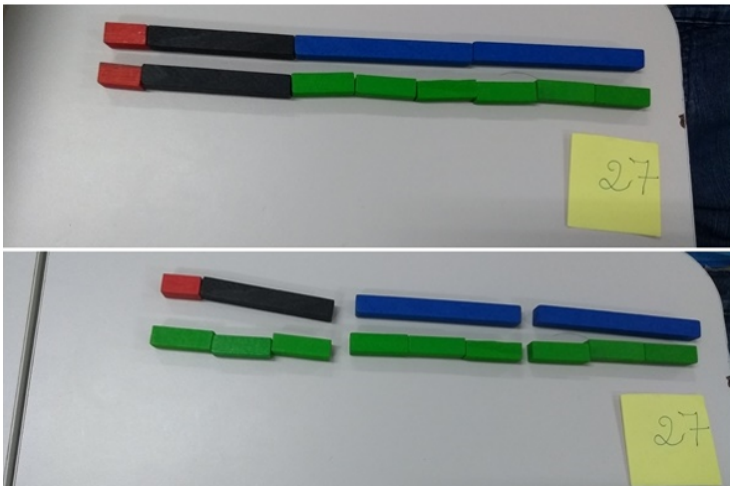
Fonte: acervo pessoal

No terceiro momento, estimulamos os alunos a entender o processo de decomposição de números em fatores primos. Vejamos na figura 7, a decomposição produzida por um aluno, ele escreveu o número 27 inicialmente, como 9 (barra azul) + 9 (barra azul) + 7 (barra preta) + 2 (barra vermelha). Em seguida, escreveu-o substituindo as barras azuis utilizando 6 barrinhas verde-claro mantendo ainda as barras preta e vermelha. Em uma nova representação, sabendo que uma barra vermelha + uma barra preta equivale a barra azul, representou-a usando três barras verde-claro. Assim, ele reescreveu o número 27 usando apenas o primo 3.

A etapa de escrever $9 = 7 + 2$ não seria necessária desde que o aluno usasse as três barras azuis; porém, é interessante analisar que ao solicitar que representassem os números com barrinhas que representavam primos, ele pensou nos primos 7 e 2, mas substituiu depois por barras equivalentes, assim é perceptível o processo de descobrimento da decomposição, onde os alunos, devem pensar em quais primos deve dividir o número para conseguir o resultado correto. Acontecendo isto, é importante destacar aos alunos que a decomposição em fatores primos é feita por meio do produto.

Após eles perceberem como é feita a decomposição de números em fatores primos por meio da escala, solicitamos que fizessem a decomposição de alguns números na lousa agora sabendo como é o processo correto, já que havíamos analisado por meio do questionário de sondagem que a maioria dos alunos apresentavam dificuldades em relação ao

Figura 7 - Representação da decomposição do número 27



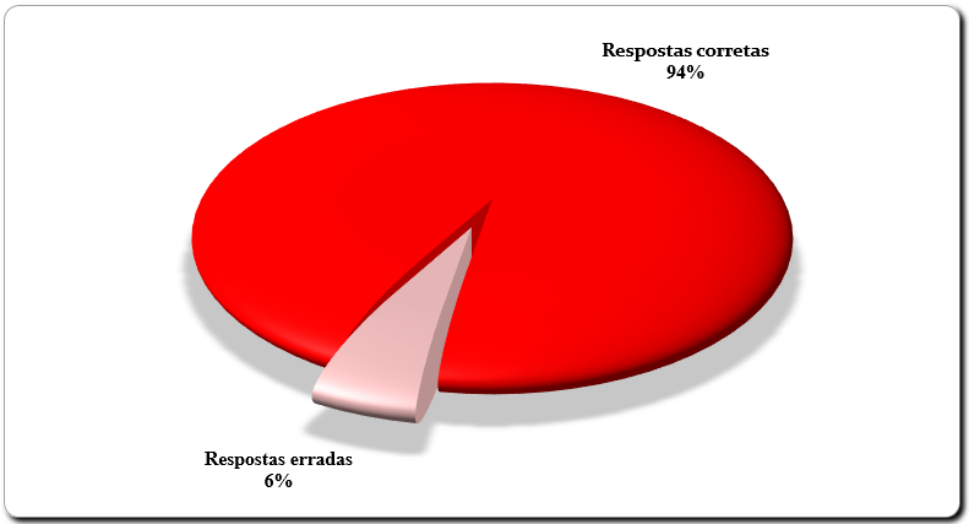
Fonte: acervo pessoal

procedimento correto ou não sabiam como fazer. Eles realizaram as decomposições e, ao ir à lousa quando percebia alguma dúvida solicitava ajuda aos colegas, antes que fizesse alguma intervenção para que assim, compartilhassem conhecimento.

Como uma forma de organizar o conhecimento após as atividades, propusemos uma gincana simples com o intuito de revisar todo o conteúdo estudado. Os alunos foram orientados a pegarem uma ficha em uma caixa a qual continha vários números e, com o número em mãos, anotava-os em uma folha. Em uma outra caixa havia afirmativas como: é um número primo, é um número composto, possui o primo 3 em sua decomposição etc. Assim que era sorteado um número e este atendia ao que estava na ficha sorteada por eles, o aluno pontuava. Nas fichas em que havia a afirmativa de um primo em sua decomposição, pedíamos a eles que fizessem a decomposição dos números para ter certeza; assim como as fichas em que indicava o múltiplo ou divisor de um determinado número, que visualizassem por meio da escala, já que durante todo o encontro, o material estava disponível. Inicialmente, havíamos pensado em três rodadas, mas como se sentiram à vontade com o desenvolvimento da atividade, os alunos pediram que fossem realizadas mais algumas rodadas.

A questão 8, do questionário de sondagem em que os alunos mais apresentaram dificuldades era em relação a decomposição de números em fatores primos, além da apresentação pela Escala Cuisenaire apliquei um teste para saber o nível de aprendizagem a partir das últimas atividades propostas. O gráfico 4 ilustra a percentagem de acertos dos alunos, ele demonstra que a aprendizagem foi reforçada, evidenciando o baixo índice de erros das questões. Percebe-se que as atividades contribuíram positivamente com a aprendizagem dos alunos participantes.

Gráfico 4 - Percentual de acertos e erros nas questões do teste de aprendizagem



Fonte: elaborado pela autora

5.3 Atividades envolvendo a criptografia para sala de aula

Nesta seção apresentaremos atividades que podem ser levadas para a sala de aula com destaque à criptografia; antes de propormos a atividade relativa a criptografia RSA, exploraremos outras formas de codificação de mensagens com o intuito de apresentar algumas maneiras de levar o assunto para a sala de aula, destacando conteúdos matemáticos estudados sob outro enfoque normalmente. Desse modo, propomos uma maneira alternativa de os professores ensinarem tais conteúdos, assim como uma forma de apresentar atividades que despertem a curiosidade dos alunos em relação à Matemática.

Atividade nº 01

Objetivo Geral: Evidenciar o processo de codificação utilizado por César.

Objetivos Específicos:

- Reforçar a aprendizagem sobre divisão;
- Destacar o resto de uma divisão.

Púbico-Alvo: Alunos a partir do sexto ano.

Pré-Requisitos: Os alunos devem saber calcular divisões.

Materiais: Lápis, borracha, ficha de atividades.

Dicas ao professor: É importante que o professor acompanhe todas os momentos da atividade verificando se os alunos apresentam dificuldades no processo de divisão e para considerar o resto a fim de evitar que não obtenham o resultado esperado por distrações.

Descrição da atividade: Codificar a mensagem NÚMEROS INTEIROS usando a cifra de César.

A atividade consiste em mostrar o processo de encriptação de uma mensagem por meio da cifra de César, porém aqui não utilizamos como chave a substituição das letras pela terceira seguinte, utilizaremos um número maior já que o processo é análogo.

1º Momento: Associar cada letra da mensagem a um número, de acordo com o quadro:

Quadro 1 - Correspondência

Δ	A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

O espaço entre duas palavras será indicado pelo símbolo Δ e associado ao número 0. Logo,

N	U	M	E	R	O	S	Δ	I	N	T	E	I	R	O	S
14	21	13	5	18	15	19	0	9	14	20	5	9	18	15	19

Seja a a chave do código, tomemos $a = 15$. O próximo passo consiste em somar a chave a cada um dos blocos acima. Logo, obteremos:

29 - 36 - 28 - 20 - 33 - 30 - 34 - 15 - 24 - 29 - 35 - 20 - 24 - 33 - 30 - 34.

Quando o valor obtido for maior que 27, deve-se considerar o resto da divisão do número por 27, assim a nova sequência será:

$$2-9-1-20-6-3-7-15-24-2-8-20-24-6-3-7. \tag{5.1}$$

De acordo com o quadro 1 teremos a nova sequência de letras:

B I A T F C G O X B H T X F C G.

Que é a mensagem codificada.

2º Momento: Para decodificar a mensagem usando a chave a, basta codificá-la novamente usando a regra $27 - a$ a qual chamaremos de b. Em nosso caso, $b = 27 - 15 = 12$. Somando b na sequência 5.1 obtemos:

14 - 21 - 13 - 32 - 18 - 15 - 19 - 27 - 36 - 14 - 20 - 32 - 36 - 18 - 15 - 19.

Nos números maiores que 27 consideramos o resto da divisão, então a sequência será:

14 - 21- 13 - 5 - 18 - 15 - 19 - 0 - 9 - 14 - 20 - 5 - 9 - 18 - 15 - 19.

Que pelo quadro 1 corresponde exatamente a NÚMEROS INTEIROS, que é a mensagem original.

Atividade extra:

- Codifique a palavra ARITMÉTICA, utilizando a chave $a = 2019$.
- Qual chave deve ser utilizada para decodificar a mensagem?

Atividade adaptada do exemplo apresentado por Silva (2003).

Atividade nº 02

Esta atividade envolve o conceito de matrizes que não foi abordado no corpo do texto pois, não era nosso foco. Utilizamos os conceitos a seguir para sugerir ao professor da Educação Básica uma forma de levar a criptografia para a aula por meio de conteúdos presentes no currículo e assim, propor uma abordagem diferente do que se costuma apresentar aos alunos.

Objetivo Geral: Estudar o processo de codificação e decodificação usando a Cifra de César com uma chave escrita em matriz.

Objetivos Específicos:

- Evidenciar o processo de codificação feito por Júlio César;
- Estudar conceitos sobre matrizes: produto de matrizes e matriz inversa.

Púbico-Alvo: Alunos da 2ª série do Ensino Médio.

Pré-Requisitos: Os alunos devem saber fazer divisões, calcular o produto de matrizes e a matriz inversa.

Dicas ao professor: Esta atividade foi pensada para reforçar o conhecimento sobre matrizes aliada ao conhecimento de um dos mais antigos sistemas de criptografia de mensagens (Cifra de César), portanto, deve ser levada para a sala de aula como uma forma de mostrar que os conceitos matemáticos podem ser utilizados de diversas formas. Para que esta seja desenvolvida a fim de obter bons resultados, os conceitos matemáticos relativos a matrizes devem ter sido explorados anteriormente a fim de não causar desinteresse pela atividade de codificar e decodificar utilizando os métodos que serão propostos.

Descrição da atividade: Codificar a mensagem BOM TRABALHO utilizando a chave $\begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix}$.

1º Momento: Associar as letras da mensagem aos números do quadro 1, assim,

B	O	M	Δ	T	R	A	B	A	L	H	O
2	15	13	0	20	18	1	2	1	12	8	15

Então a sequência de números correspondente a mensagem é

215130201812112815.

Dividir a sequência em blocos com dois elementos:

21 - 51 - 30 - 20 - 18 - 12 - 11 - 28 - 15

Considerar cada um dos blocos como uma matriz 2 x 1:

$$\begin{pmatrix}2\\1\end{pmatrix} \quad \begin{pmatrix}5\\1\end{pmatrix} \quad \begin{pmatrix}3\\0\end{pmatrix} \quad \begin{pmatrix}2\\0\end{pmatrix} \quad \begin{pmatrix}1\\8\end{pmatrix} \quad \begin{pmatrix}1\\2\end{pmatrix} \quad \begin{pmatrix}1\\1\end{pmatrix} \quad \begin{pmatrix}2\\8\end{pmatrix} \quad \begin{pmatrix}1\\5\end{pmatrix}$$

Multiplicar cada uma dessas matrizes pela chave $\begin{pmatrix}1 & 2\\3 & 7\end{pmatrix}$:

$$\begin{pmatrix}1 & 2\\3 & 7\end{pmatrix} \cdot \begin{pmatrix}2\\1\end{pmatrix} = \begin{pmatrix}1\cdot 2+2\cdot 1\\3\cdot 2+7\cdot 1\end{pmatrix} = \begin{pmatrix}4\\13\end{pmatrix}$$

$$\begin{pmatrix}1 & 2\\3 & 7\end{pmatrix} \cdot \begin{pmatrix}5\\1\end{pmatrix} = \begin{pmatrix}1\cdot 5+2\cdot 1\\3\cdot 5+7\cdot 1\end{pmatrix} = \begin{pmatrix}7\\22\end{pmatrix}$$

$$\begin{pmatrix}1 & 2\\3 & 7\end{pmatrix} \cdot \begin{pmatrix}3\\0\end{pmatrix} = \begin{pmatrix}1\cdot 3+2\cdot 0\\3\cdot 3+7\cdot 0\end{pmatrix} = \begin{pmatrix}3\\9\end{pmatrix}$$

$$\begin{pmatrix}1 & 2\\3 & 7\end{pmatrix} \cdot \begin{pmatrix}2\\0\end{pmatrix} = \begin{pmatrix}1\cdot 2+2\cdot 0\\3\cdot 2+7\cdot 0\end{pmatrix} = \begin{pmatrix}2\\6\end{pmatrix}$$

$$\begin{pmatrix}1 & 2\\3 & 7\end{pmatrix} \cdot \begin{pmatrix}1\\8\end{pmatrix} = \begin{pmatrix}1\cdot 1+2\cdot 8\\3\cdot 1+7\cdot 8\end{pmatrix} = \begin{pmatrix}17\\59\end{pmatrix}$$

$$\begin{pmatrix}1 & 2\\3 & 7\end{pmatrix} \cdot \begin{pmatrix}1\\2\end{pmatrix} = \begin{pmatrix}1\cdot 1+2\cdot 2\\3\cdot 1+7\cdot 2\end{pmatrix} = \begin{pmatrix}5\\17\end{pmatrix}$$

$$\begin{pmatrix}1 & 2\\3 & 7\end{pmatrix} \cdot \begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}1\cdot 1+2\cdot 1\\3\cdot 1+7\cdot 1\end{pmatrix} = \begin{pmatrix}3\\10\end{pmatrix}$$

$$\begin{pmatrix}1 & 2\\3 & 7\end{pmatrix} \cdot \begin{pmatrix}2\\8\end{pmatrix} = \begin{pmatrix}1\cdot 2+2\cdot 8\\3\cdot 2+7\cdot 8\end{pmatrix} = \begin{pmatrix}18\\62\end{pmatrix}$$

$$\begin{pmatrix}1 & 2\\3 & 7\end{pmatrix} \cdot \begin{pmatrix}1\\5\end{pmatrix} = \begin{pmatrix}1\cdot 1+2\cdot 5\\3\cdot 1+7\cdot 5\end{pmatrix} = \begin{pmatrix}11\\38\end{pmatrix}$$

Assim, obtemos os blocos:

413 - 722 - 39 - 26 - 1759 - 517 - 310 - 1862 - 1138

Como no quadro 1 associamos as letras aos números de 0 a 26, então a sequência acima deve ser escrita como números menores que 27. Para isso, quando o número for maior que 27, deve-se considerar o resto da divisão do número por 27, então os novos blocos serão:

8 - 20 - 12 - 26 - 4 - 4 - 13 - 26 - 4

Logo, a mensagem codificada será H T L Z D D M Z D.

2º Momento: Para decodificar a mensagem, precisamos determinar a chave de decodificação que é a matriz inversa de $\begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix}$. A matriz inversa é obtida quando o produto de duas matrizes resulta numa matriz identidade de mesma ordem.

Tomando $A = \begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix}$, sua matriz inversa é representada por A^{-1}. Para obtê-la basta fazer $A \cdot A^{-1} = I$, então

$$\begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \implies \begin{pmatrix} 1 \cdot a + 2 \cdot c & 1 \cdot b + 2 \cdot d \\ 3 \cdot a + 7 \cdot c & 3 \cdot b + 7 \cdot d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Assim, obtemos as seguintes equações

i) $a + 2c = 1$ ii) $3a + 7c = 0$ iii) $b + 2d = 0$ iv) $3b + 7d = 1$

Em i) obtemos $a = 1 - 2c$ que substituiremos em ii) e em iii) obtemos $b = -2d$ que substituiremos em iv). Logo,

ii) $3a + 7c = 0 \iff 3(1 - 2c) + 7c = 0 \iff 3 - 6c + 7c = 0 \iff c = -3$, assim,
$a = 1 - 2c = 1 - 2 \cdot (-3) = 1 + 6 = 7$.

iv) $3b + 7d = 1 \iff 3(-2d) + 7d = 1 \iff -6d + 7d = 1 \iff d = 1$, assim, $b = -2 \cdot 1 = -2$.

Portanto, $A^{-1} = \begin{pmatrix} 7 & -2 \\ -3 & 1 \end{pmatrix}$.

Logo, a decodificação da mensagem será feita multiplicando A^{-1} por cada um dos blocos codificados. Assim,

$$\begin{pmatrix} 7 & -2 \\ -3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 13 \end{pmatrix} = \begin{pmatrix} 7 \cdot 4 - 2 \cdot 13 \\ -3 \cdot 4 + 1 \cdot 13 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 7 & -2 \\ -3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 22 \end{pmatrix} = \begin{pmatrix} 7 \cdot 7 - 2 \cdot 22 \\ -3 \cdot 7 + 1 \cdot 22 \end{pmatrix} = \begin{pmatrix} 5 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 7 & -2 \\ -3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 9 \end{pmatrix} = \begin{pmatrix} 7 \cdot 3 - 2 \cdot 9 \\ -3 \cdot 3 + 1 \cdot 9 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 7 & -2 \\ -3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 6 \end{pmatrix} = \begin{pmatrix} 7 \cdot 2 - 2 \cdot 6 \\ -3 \cdot 2 + 1 \cdot 6 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 7 & -2 \\ -3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 17 \\ 59 \end{pmatrix} = \begin{pmatrix} 7 \cdot 17 - 2 \cdot 59 \\ -3 \cdot 17 + 1 \cdot 59 \end{pmatrix} = \begin{pmatrix} 1 \\ 8 \end{pmatrix}$$

$$\begin{pmatrix} 7 & -2 \\ -3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 5 \\ 17 \end{pmatrix} = \begin{pmatrix} 7 \cdot 5 - 2 \cdot 17 \\ -3 \cdot 5 + 1 \cdot 17 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

$$\begin{pmatrix} 7 & -2 \\ -3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 10 \end{pmatrix} = \begin{pmatrix} 7 \cdot 3 - 2 \cdot 10 \\ -3 \cdot 3 + 1 \cdot 10 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 7 & -2 \\ -3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 18 \\ 62 \end{pmatrix} = \begin{pmatrix} 7 \cdot 18 - 2 \cdot 62 \\ -3 \cdot 18 + 1 \cdot 62 \end{pmatrix} = \begin{pmatrix} 2 \\ 8 \end{pmatrix}$$

$$\begin{pmatrix} 7 & -2 \\ -3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 11 \\ 38 \end{pmatrix} = \begin{pmatrix} 7 \cdot 11 - 2 \cdot 38 \\ -3 \cdot 11 + 1 \cdot 38 \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \end{pmatrix}$$

Que correspondem aos números 21 - 51 - 30 - 20 - 18 - 12 - 11 - 28 - 15 e a sequência referente a mensagem que desejávamos codificar e decodificar inicialmente.

Atividade extra: Decodificar a mensagem NTUIMQDEOR usando a chave $M = \begin{pmatrix} 7 & 25 \\ 24 & 1 \end{pmatrix}$.

Atividade adaptada do exercício 4.33 apresentado por Silva (2003).

Atividade nº 03

Objetivo Geral: Mostrar o processo de codificação e decodificação de uma mensagem usando matrizes em um processo análogo ao da Cifra de César.

Objetivos Específicos:

- Revisar conceitos de matrizes: produto de matrizes, matriz inversa;
- Revisar plano cartesiano.

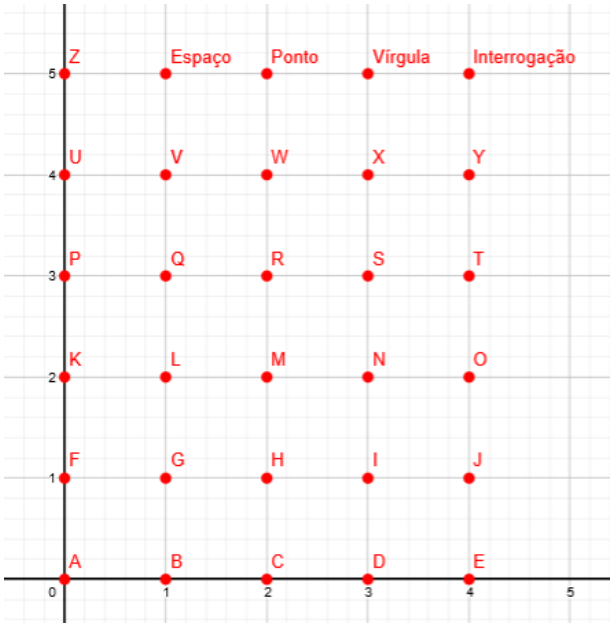
Público-Alvo: Alunos da segunda série do Ensino Médio.

Pré-Requisitos: Noções básicas sobre matrizes e plano cartesiano.

Dicas ao professor: Nesta atividade utilizamos a origem associada a letra A, mas esta pode ser associada a qualquer par ordenado do plano cartesiano; assim como deixamos as letras em forma de tabela, mas isso também fica a critério do professor ao instruir os aluno, a associação dos pares às letras pode ser feita aleatoriamente.

Descrição da atividade: Codificar a palavra TUTORIA utilizando a chave $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$.

Cada letra do alfabeto será associada a um par ordenado do plano cartesiano. Assim,



1º Momento: Segundo a associação feita acima temos os pares ordenados:

(4, 3) - (0, 4) - (4, 3) - (4, 2) - (2, 3) - (4, 1) - (0, 0)

$$\begin{pmatrix}4\\3\end{pmatrix} \quad \begin{pmatrix}0\\4\end{pmatrix} \quad \begin{pmatrix}4\\3\end{pmatrix} \quad \begin{pmatrix}4\\2\end{pmatrix} \quad \begin{pmatrix}2\\3\end{pmatrix} \quad \begin{pmatrix}4\\1\end{pmatrix} \quad \begin{pmatrix}0\\0\end{pmatrix}$$

Considerar cada um dos pares ordenados como uma matriz 2 x 1:

Multiplicando a chave de codificação por cada uma dessas matrizes, obtemos os seguintes blocos codificados:

$$\begin{pmatrix}1 & 1\\1 & 2\end{pmatrix}\cdot\begin{pmatrix}4\\3\end{pmatrix} = \begin{pmatrix}1\cdot 4+1\cdot 3\\1\cdot 4+2\cdot 3\end{pmatrix} = \begin{pmatrix}7\\10\end{pmatrix}$$

$$\begin{pmatrix}1 & 1\\1 & 2\end{pmatrix}\cdot\begin{pmatrix}0\\4\end{pmatrix} = \begin{pmatrix}1\cdot 0+1\cdot 4\\1\cdot 0+2\cdot 4\end{pmatrix} = \begin{pmatrix}4\\8\end{pmatrix}$$

$$\begin{pmatrix}1 & 1\\1 & 2\end{pmatrix}\cdot\begin{pmatrix}4\\3\end{pmatrix} = \begin{pmatrix}1\cdot 4+1\cdot 3\\1\cdot 4+2\cdot 3\end{pmatrix} = \begin{pmatrix}7\\10\end{pmatrix}$$

$$\begin{pmatrix}1 & 1\\1 & 2\end{pmatrix}\cdot\begin{pmatrix}4\\2\end{pmatrix} = \begin{pmatrix}1\cdot 4+1\cdot 2\\1\cdot 4+2\cdot 2\end{pmatrix} = \begin{pmatrix}6\\8\end{pmatrix}$$

$$\begin{pmatrix}1 & 1\\1 & 2\end{pmatrix}\cdot\begin{pmatrix}2\\3\end{pmatrix} = \begin{pmatrix}1\cdot 2+1\cdot 3\\1\cdot 2+2\cdot 3\end{pmatrix} = \begin{pmatrix}5\\8\end{pmatrix}$$

$$\begin{pmatrix}1 & 1\\1 & 2\end{pmatrix}\cdot\begin{pmatrix}4\\1\end{pmatrix} = \begin{pmatrix}1\cdot 4+1\cdot 1\\1\cdot 4+2\cdot 1\end{pmatrix} = \begin{pmatrix}5\\6\end{pmatrix}$$

$$\begin{pmatrix}1 & 1\\1 & 2\end{pmatrix}\cdot\begin{pmatrix}0\\0\end{pmatrix} = \begin{pmatrix}1\cdot 0+1\cdot 0\\1\cdot 0+2\cdot 0\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}$$

Estes blocos também podem ser escrito como os pares ordenados:

(7, 10) - (4, 8) - (7, 10) - (6, 8) - (5, 8) - (5, 6) - (0, 0).

2º Momento: Para decodificar a palavra, temos que determinar a matriz inversa da chave de codificação. Assim, tomando $A = \begin{pmatrix}1 & 1\\1 & 2\end{pmatrix}$, basta fazer

$$\begin{pmatrix}1 & 1\\1 & 2\end{pmatrix}\cdot\begin{pmatrix}a & b\\c & d\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} \Longrightarrow \begin{pmatrix}1\cdot a+1\cdot c & 1\cdot b+1\cdot d\\1\cdot a+2\cdot c & 1\cdot b+2\cdot d\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$$

Assim, obtemos as seguintes equações

i) $a+c=1$ ii) $a+2c=0$ iii) $b+d=0$ iv) $b+2d=1$

Em i) obtemos $a=1-c$ que substituiremos em ii) e em iii) obtemos $b=-d$ que substituiremos em iv). Logo,

ii) $a+2c=0 \Longleftrightarrow 1-c+2c=0 \Longleftrightarrow 1+c=0 \Longleftrightarrow c=-1$, assim, $a=1-c=1-(-1)=2$.

iv) $b+2d=1 \iff -d+2d=1 \iff d=1$, assim, $b=-d=-1$.

Portanto, $A^{-1}=\begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}$.

Logo, a decodificação da mensagem será feita multiplicando A^{-1} por cada um dos blocos codificados, como fizemos na atividade anterior.

Atividade adaptada do exemplo apresentado em <https://canal.cecierj.edu.br/012016/df07d34ee40255cee46c8f6bf63f5f29.pdf>

Atividade nº 04

Objetivo Geral: Estudar o processo de cifragem por transposição.

Objetivos Específicos:

- Estudar permutações;

Público-Alvo: Alunos da 1ª série do Ensino Médio

Dicas ao professor: A atividade pode ser desenvolvida como forma de entretenimento para os alunos, nesta utilizamos apenas uma chave, mas a medida que se tomam chaves diferentes os alunos podem visualizar a variedade de palavras diferentes sendo formadas, isto é, as permutações dos números associados as colunas permitem originar tantas palavras quanto forem possíveis.

Descrição da atividade: Um texto será escrito em forma de retângulo, linha por linha e para ser lido, deve-se tomar as colunas deste que serão rotuladas a números, desses números dependerão o processo de codificação da mensagem.

1º Momento: Escrever o texto INTRODUÇÃO À CRIPTOGRAFIA PROFMAT.

1	**2**	**3**	**4**	**5**	**6**
I	N	T	R	O	D
U	C	A	O	A	C
R	I	P	T	O	G
R	A	F	I	A	P
R	O	F	M	A	T

Quando a chave de codificação for 162435 o texto cifrado será IURRRDCGPTNCIAOROTIMTAPFFOAOAA. Para tornar uma cifra de transposição mais segura é possível codificar novamente, criando assim uma nova mensagem mais distante da original. Assim, se a mensagem que acabamos de codificar for novamente codificada fazendo o mesmo processo e utilizando a mesma chave, teremos

1	**2**	**3**	**4**	**5**	**6**
I	U	R	R	R	D
C	G	P	T	N	C
I	A	O	R	O	T
I	M	T	A	P	F
F	O	A	O	A	A

e a palavra codificada será ICIIFDCTFAUGAMORTRAORPOTARNOPA.

Atividade nº 05

Objetivo Geral: Mostrar o processo de cifragem de uma cifra polialfabética.

Objetivos Específicos:

- Compreender o processo de cifragem de uma cifra com mais de um símbolo associado;
- Revisar conceitos matemáticos;

Público-Alvo: Livre

Dicas ao professor: Na atividade a seguir exploramos números primos, pares e ímpares para montarmos a tabela, essa forma de montagem fica como sugestão. O professor pode utilizar qualquer regra que acredita ser conveniente para montar a tabela, inclusive considerar números aleatoriamente. Consideramos uma tabela com três colunas, o professor pode escolher uma tabela com mais colunas, se preferir.

Para a codificação de palavras com caracteres especiais (acento ou ç) pode-se inserir números correspondentes a esses para garantir que a decodificação seja mais difícil. No caso da proposta a seguir, ignoraremos os caracteres especiais assim como os espaços. Mas o professor pode sugerir aos alunos que façam novas correspondências e assim explorar múltiplos, divisores (e outros conceitos) de determinados números como uma forma de revisão, por exemplo.

Descrição da atividade: A cifra de César é um exemplo de cifra monoalfabética, aqui exploraremos a cifra polialfabética com o intuito de esclarecer dúvidas sobre como esta se caracteriza. Já fizemos durante o texto um exemplo da cifra de Vigenère que tem as mesmas características, aqui exploraremos um exemplo numérico. Os dois exemplos podem ser levados para a sala de aula.

Organizar uma tabela associando cada letra do alfabeto a três números (ou símbolos) distintos. Nesta atividade, na primeira coluna as letras serão correspondidas aos números primos menores que 100. Como uma letra ficará sem correspondência, esta será correspondida a 00. Na segunda coluna, as letras serão correspondidas aos números pares de dois dígitos, iniciando em ordem contrária à ordem da primeira coluna. Assim, como a letra A foi associada ao número 2 (já que é o único número par primo) então o segundo número par será associado a letra Z e assim seguem-se os outros. Devem ser listados todos os pares de dois dígitos mesmo que para isso ocupe a terceira coluna. Nos últimos espaços da tabela, insere-se os números ímpares que ainda não estão listados na tabela em ordem crescente.

Para cifrar uma mensagem, o valor (ou símbolo) associado a letra repete-se somente se aparecer mais de três vezes, cada vez que a letra aparecer será considerado um número associado diferente.

A	2	54	56
B	3	52	58
C	5	50	60
D	7	48	62
E	11	46	64
F	13	44	66
G	17	42	68
H	19	40	70
I	23	38	72
J	29	36	74
K	31	34	76
L	37	32	78
M	41	30	80

N	43	28	82
O	47	26	84
P	53	24	86
Q	59	22	88
R	61	20	90
S	67	18	92
T	71	16	94
U	73	14	96
V	79	12	98
W	83	10	1
X	89	8	9
Y	97	6	15
Z	00	4	21

A cifragem da palavra MATEMÁTICA seguindo a tabela acima em blocos é 41 - 2 - 71 - 11 - 30 - 54 - 16 - 23 - 5 - 56 e em sequência temos 412711130541623556.

Para cifrarmos a mensagem TESTE DE PRIMALIDADE, inicialmente observamos que a vogal E aparece quatro vezes, assim na quarta vez que ela aparecer, substituiremos por seu primeiro valor associado. Assim, seguindo a tabela acima a cifragem da mensagem em blocos é 71 - 11 - 67 - 16 - 46 - 7 - 64 - 53 - 61 - 23 - 41 - 2 - 37 - 38 - 48 - 54 - 62 - 11 logo, a sequência será 71116716467645361234123738485462 11.

Atividade extra:

i) Qual a cifragem da mensagem MÚLTIPLOS E DIVISORES?

ii) Qual a cifragem da mensagem OS NÚMEROS GOVERNAM O MUNDO. O MUNDO É CADA VEZ MAIS DOMINADO PELA MATEMÁTICA?

Atividade nº 06 - Criptografia RSA

Objetivo Geral: Mostrar como acontece o processo de codificação e decodificação de uma mensagem pelo método RSA, destacando os conceitos matemáticos importantes em cada etapa.

Objetivos Específicos

- Fortalecer aprendizado sobre divisões, mdc;
- Explorar a potenciação;
- Mostrar uma aplicação que envolve números primos.

Público-Alvo: Alunos a partir do 6º ano.

Pré-Requisitos: Os alunos deverão saber fazer divisões de números grandes e calcular potências.

Dicas ao professor: Ao conduzir a atividade proposta o professor deve acompanhar os alunos sempre que necessário a fim de intervir ao surgir dúvidas, de modo que estas não influenciem negativamente nos resultados da atividade proposta. Sugere-se o uso da calculadora quando os alunos apresentarem muitas dificuldades com as operações a serem feitas, já que em determinados momentos, a divisão e o cálculo das potências pode não ser trivial.

Descrição da atividade: Codificar e decodificar a palavra CÓDIGO.

A atividade consiste em mostrar passo a passo o que acontece, por meio de um exemplo, o que foi feito na seção 4.2. Porém, utiliza-se cálculos mais simples, adequando o processo ao que seria feito em uma sala de aula da Educação Básica; assim não será evidenciado, por exemplo, as congruências mas o processo de divisão e a utilização dos restos de tais divisões. Serão utilizados primos pequenos com o objetivo de facilitar as operações, quando são utilizados primos grandes o processo é análogo.

1º Momento (Codificação): Considere os números primos $p = 3$ e $q = 7$, logo $n = pq = 3 \cdot 7 = 21$. Precisamos determinar $\varphi(n)$, então $\varphi(n) = (3-1)(7-1) = 12$ e e, que é o menor primo que não divide $\varphi(n)$, logo $e = 5$, já que mdc(12, 5) = 1.

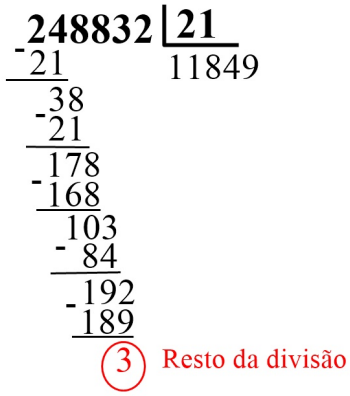
Utilize a tabela a seguir para fazer a conversão das letras da palavra para números:

Que será a sequência: 122413181624. Agora, separe-a em blocos, de modo que cada bloco seja menor que n: 12 - 2 - 4 - 13 - 18 - 16 - 2 - 4.

Seja b um bloco, para codificá-lo considere o resto da divisão de b^e por n. Ou ainda, no bloco 12 temos que $12^5 = 248.832$, dividindo-o por 21:

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



Sendo C(b) o bloco codificado, temos C(12) = 3. Fazendo o mesmo processo para os outros blocos obtemos:

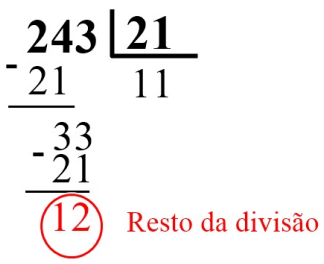
C(2) = 11; C(4) = 16; C(13) = 13; C(18) = 9; C(16) = 4; C(2) = 11 e C(4) = 16.

A sequência de blocos codificados é 3 - 11 - 16 - 13 - 9 - 4 - 11 - 16. Logo, a mensagem codificada será: 3111613941116.

2º Momento (Decodificação): Para decodificar a mensagem que acabamos de codificar também é utilizado o resto da divisão. Porém precisamos determinar d que é fácil já que conhecemos $\varphi(n) = 12$ e $e = 5$.

Em nosso caso, o número d é tal que este multiplicado por e deixa resto 1 na divisão por $\varphi(n) = 12$. Ou ainda, basta pensar no número em que mdc(12, d) = 1, que é o menor primo que não divide 12. Logo, $d = 5$.

Seja um bloco a da sequência de blocos codificados, a decodificação deste bloco será o resto da divisão de a^d por n. Assim, no bloco 3 temos que $3^5 = 243$, dividindo-o por 21 temos:



Sendo D(a) o bloco decodificado, note que neste caso o resto da divisão é exata-

mente o valor do primeiro bloco da mensagem original,ou ainda, D(3) = 12. De modo análogo obtemos os blocos:

D(11) = 2; D(16) = 4; D(13) = 13; D(9) = 18; D(4) = 16; D(11) = 2 e D(16) = 4.

A sequência de blocos decodificados é 12 - 2 - 4 - 13 - 18 - 16 - 2 - 4. E a mensagem decodificada (numericamente) 122413181624. Considerando os pares de números obtemos a correspondência (em letras) pela tabela inicial a palavra CODIGO, a qual queríamos de fato obter.

Atividade extra: Codificar e decodificar a palavra CALCULADORA, com os mesmos parâmetros da proposta anterior.

6 CONSIDERAÇÕES FINAIS

Os números primos são objeto de estudo dos matemáticos há muito tempo e tais estudos já permitiram a construção de muitos resultados interessantes para a Matemática, porém ainda há várias proposições que os envolvem sem prova. Assim como esses números, a Criptografia desperta o interesse das pessoas ao longo do tempo, pois por meio de codificações foi possível ao ser humano manter informações sigilosas e prezar por sua privacidade, porém, não sabemos até que momento os métodos conhecidos atualmente conseguirão manter nossas informações seguras. Desse modo, buscamos delinear que tanto os números primos como a criptografia podem ser levados para a sala de aula como uma forma de despertar o interesse nos alunos pela busca de uma nova forma de compreender a Matemática.

A possibilidade de levar os números primos para a sala de aula utilizando metodologias diferenciadas permite que este conteúdo não seja estudado apenas seguindo sua definição. Apresentamos uma experiência em que tais números podem ser estudados por meio de um recurso didático fácil de ser encontrado ou confeccionado, que é a Escala Cuisenaire, para que o professor reflita sobre as diversas formas de ensinar determinados conteúdos por meio de situações mais dinâmicas, em que os alunos podem fazer verificações e assim estimular um maior envolvimento com a disciplina.

Outra situação que gostaríamos de deixar como ponto de reflexão aos professores de Matemática da Educação Básica é a oportunidade de vincular os conteúdos estudados com aspectos do cotidiano; percebemos durante a pesquisa que os alunos não sabem para que os números primos são úteis além da decomposição em fatores primos, ou seja, conhecem apenas uma situação voltada para a sala de aula. A exposição sobre a criptografia permite a eles pensar em situações que dependeram dessa para guardar uma informação em segredo, por exemplo por meio de uma senha.

A criptografia por meio de atividades em sala de aula se mostra como entretenimento para os alunos; o professor não precisa destacar o conteúdo que será estudado imediatamente, pode começar propondo uma situação e a medida que eles se envolverem perceberão os conceitos matemáticos por trás de cada assunto. A questão de ocultar uma mensagem e depois obtê-la, chama a atenção dos alunos e isso pode ser feito de várias maneiras com conceitos e conteúdos que já aprenderam.

A criptografia pode ser destacada também por meio do estudo da segurança em nossos e-mails e também no whatsapp, podem ser desenvolvidos estudos que reforcem isto em sala de aula e assim apresentar aos alunos uma forma de um método criptográfico que dependemos cotidianamente. A transmissão de informações atualmente ocorre muito

rápido e podemos ser surpreendidos com a divulgação de algo sigiloso, para isso se faz necessário investigar métodos que nos garantam tranquilidade em nossas comunicações.

Referências

BOYER, C. B. **História da Matemática**. 3. ed. São Paulo: Blucher, 2010. Citado 3 vezes nas páginas 15, 21 e 30.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA**. 2. ed. Rio de Janeiro: IMPA, 2003. (Série de Computação e Matemática). Citado 14 vezes nas páginas 22, 29, 30, 31, 32, 33, 34, 36, 47, 48, 50, 51, 52 e 53.

DOMINGUES, H. H. **Fundamentos de Aritmética**. Florianópolis: Ed. da UFSC, 2009. Citado 1 vezes nas páginas 24.

EVES, H. **Introdução à história da matemática**. Campinas, SP: Editora da UNICAMP, 2004. Citado 9 vezes nas páginas 13, 15, 20, 23, 29, 30, 33, 34 e 35.

HEFEZ, A. **Aritmética**. 1. ed. Rio de Janeiro: SBM, 2014. (Coleção PROFMAT). Citado 7 vezes nas páginas 24, 26, 27, 28, 29, 30 e 31.

IFRAH, G. **Os números: a história de uma grande invenção**. 11. ed. São Paulo: Globo, 2005. Citado 7 vezes nas páginas 13, 14, 15, 16, 17, 18 e 19.

MENDES, I. A. **Antropologia dos Números: Significado Social, Histórico e Cultural**. Sociedade Brasileira de História da Matemática. (preprint). Coleção História da Matemática para Professores, Rio Claro - SP, 2003. Citado 6 vezes nas páginas 13, 17, 18, 19, 21 e 23.

MOREIRA, C. G.; MARTíNEZ, F. E. B. Primos gêmeos, primos de sophie germain e o teorema de brun. **Matemática Universitária**, n. 48/49, p. 93–101, 2010. Disponível em: <https://rmu.sbm.org.br/wp-content/uploads/sites/27/2018/03/n48_n49_Artigo06.pdf>. Acesso em: 31 jul. 2019. Citado 2 vezes nas páginas 34 e 35.

MORENO, E. D.; PEREIRA, F. D.; CHIARAMONTE, R. **Criptografia em Software e Hardware**. São Paulo: Novatec, 2005. 21-42 p. Disponível em: <http://www.martinsfontespaulista.com.br/anexos/produtos/capitulos/143116.pdf>. Acesso em: 22 jun. 2019. Citado 1 vezes nas páginas 36.

PANTOJA, P. Primos gêmeos e outras conjecturas. **Revista Escolar de la Olimpíada Iberoamericana de Matemática**, n. 45, p. 1–11, 2012. Citado 1 vezes nas páginas 35.

ROSSEAU, C.; SAINT-AUBIN, Y. **Matemática e Atualidade Volume 1**. 1. ed. Rio de Janeiro: SBM, 2015. (Coleção PROFMAT). Citado 1 vezes nas páginas 53.

SILVA, V. V. d. **Números: Construções e Propriedades**. Goiânia: Editora UFG, 2003. Citado 2 vezes nas páginas 66 e 70.

SINGH, S. **O livro dos códigos**. 5. ed. Rio de Janeiro: Record, 2005. Citado 12 vezes nas páginas 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46 e 47.

STALLINGS, W. **Criptografia e segurança de redes: princípios e práticas**. 6. ed. São Paulo: Pearson, 2015. Disponível em: <https://www.docdroid.net/BebtXZO/criptografia-e-seguranca-de-redes-6a-ed-2014.pdf>. Acesso em: 01 out. 2019. Citado 1 vezes nas páginas 37.

STEWART, I. **Em Busca do Infinito: Uma Hitória da Matemática dos Primeiros Números à Teoria do Caos**. 1. ed. [S.l.]: Editora Zahar, 2014. Citado 3 vezes nas páginas 13, 14 e 23.

TERADA, R. Criptografia e a importância de suas aplicações. **Revista do Professor de Matemática (RPM)**, São Paulo, n. 12, 1988. Disponível em: <http://rpm.org.br/cdrpm/12/1.htm>. Acesso em: 21 jul. 2019. Citado 1 vezes nas páginas 53.

APÊNDICES

6.1 Questionário de sondagem de conhecimentos

1. O que você entende por números primos?

2.Você sabe para que servem ou em quais situações são utilizados?

3. Dados os números abaixo quais são números primos?

2, 6, 7, 11, 12, 13, 15, 21, 23, 31, 47, 50, 53, 54, 55, 61, 67, 68, 69, 70, 79, 81, 85, 89, 92, 97, 99

4. Assinale V para as assertivas verdadeiras e F para as falsas, dada a multiplicação 24 = 3 x 8.
( ) 24 é um múltiplo de 3
( ) 24 é divisível por 8
( ) 3 não é um divisor de 24.

5. Quais são múltiplos de 4 dos números a seguir: 2, 3, 5, 9, 12, 27, 42, 56, 57, 60, 68.

6. Liste o conjunto de divisores do número 12.

7. Qual é o resto da divisão dos números 34, 52, 79 por 2?

8. Decomponha o número 144 em fatores primos.

6.2 Teste de aprendizagem

Faça a decomposição em fatores primos dos seguintes números:

a) 24 =

b) 42 =

c) 68 =

d) 75 =

e) 98 =

f) 200 =

g) 201 =

h) 501 =

6.3 Atividade 1

Atividade 1: Crivo de Eratóstenes Móvel

Objetivo da atividade: Reconhecer números primos em um determinado conjunto de números

Materiais: Números em papel cartão, fita adesiva

Descrição da atividade:

Os números de 1 a 100, escritos em papel cartão, devem ser dispostos em um mural em forma de tabela e sequencialmente. O papel cartão com o número 1 deve ser diferente dos demais de forma que os alunos percebam.

Os alunos serão orientados a:

- Um deles, ir ao mural, destacar o número 2 e em seguida remover todos os múltiplos de 2 dentre os números disponíveis. Conferir com os demais colegas se está faltando retirar algum número que não foi retirado ainda.

- Outro aluno, deve ir ao mural, destacar o número 3 e em seguida remover todos os múltiplos de 3 dentre os números disponíveis. Conferir se foram retirados todos.

Fazer o mesmo procedimento para os números 5 e 7.

Após a retirada de todos os múltiplos dos números, os alunos irão perceber que restaram os números 2,3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 e 97, estes são todos os números primos entre 1 e 100.

6.4 Atividade 2

Atividade 2: Os primos por trás da Escala Cuisenaire

Objetivo da atividade: Identificar números primos por meio do material Escala de Cuisenaire, destacar os conceitos de múltiplos e divisores, além de revisar o conceito de decomposição de números em fatores primos.

Materiais: Escala Cuisenaire, folhas para registro

Descrição da atividade:

- Perguntar aos alunos o que podem observar quanto aos tamanhos das barrinhas. Os alunos devem notar que, tomando como unidade a menor barrinha (que é um cubinho) para cada número n de 1 a 10 há uma barrinha cuja medida é exatamente n unidades (não esperamos que os alunos expressem desta forma, apenas que observem o fato e o relatem com suas palavras). Se eles não observarem este fato por conta própria, pedir que

alinhem barrinhas brancas ao lado de cada uma das barrinhas coloridas, de forma que possam realizar a observação desta relação.

- Definir a menor barrinha como unidade.

- Explicar aos alunos que todas as comparações agora serão feitas a partir dessa barrinha (branca).

- Uma cor por vez, os alunos devem tomar uma barrinha da cor da vez e buscar alguma outra cor de tal modo que possamos reproduzir o comprimento da barrinha da vez utilizando alguma quantidade de barrinhas desta outra cor. Por exemplo, a barrinha verde-escura que representa o número 6. Podemos substituí-la por três barrinhas vermelhas que representam o número 2, ou por duas barrinhas verde claros que representam o número 3. Recomendar que eles tentem realizar este exercício sem utilizar as barrinhas brancas e só as utilizem quando não houver outra opção.

- Sugerir por meio de fichas sorteadas números em que os alunos deverão fazer esse processo.

- Introduzir os termos múltiplos e divisores utilizando como exemplos os produtos registrados na ficha de acompanhamento. Nesta etapa recomenda-se que estas conceituações sejam feitas através de exemplos: $6 = 2 \cdot 3$, então 6 é múltiplo de 2 (e também de 3), pois pode ser obtido pela multiplicação de 2 por 3. Igualmente, 12 é múltiplo de 4 e de 3 porque pode ser representado pela multiplicação destes dois números. Para conceituar divisores usamos o mesmo método: 2 é divisor de 6, pois 6 pode ser dividido por 2 (sem sobrar resto). Também 3 é divisor de 6. Para 12, temos que 4 é divisor de 12 porque 12 pode ser dividido por 4 (com resto zero). Neste momento ainda não exploraremos mais profundamente os conceitos de múltiplos e divisores.

IDENTIFICANDO NÚMEROS PRIMOS

- Pedir aos alunos que verifiquem para quais dos comprimentos de 1 a 20 eles não conseguiram realizar o passo anterior sem utilizar as barrinhas que representam uma unidade. Por exemplo, para a barrinha amarela que representa o número cinco não há nenhuma outra cor (que não seja a branca ou a própria amarela) que, justapondo apenas barrinhas desta cor, nos dê o mesmo comprimento. Também para o número 13, obtido pela justaposição da barrinha laranja com a verde-claro, a única maneira de obter seu comprimento utilizando uma única cor de barrinha é utilizando as barrinhas brancas que representam a unidade.

- Explicar que estes números são chamados de números primos e explicar que um número recebe este nome sempre que é maior que 1 e só possui como divisores 1 e ele mesmo.

EXISTÊNCIA DA DECOMPOSIÇÃO DOS NATURAIS EM FATORES PRIMOS

- Obter qualquer dos números que não são primos, utilizando apenas números primos e

operações de multiplicação. Assim, por exemplo, partindo de $24 = 4 \cdot 6$, o aluno deve ser instruído a buscar na própria lista de números, uma forma de substituir o 6 por um produto de números primos. Encontrará $6 = 2 \cdot 3$, e substituindo na multiplicação, ficará com $24 = 2 \cdot 2 \cdot 2 \cdot 3$.

- Uma vez realizado o exercício proposto, o professor/mediador deve explicar aos alunos que essa forma de escrever um número que não é primo como produto de números primos chama-se decomposição do número em fatores primos (lembrar que cada termo em uma multiplicação é chamado de fator) e que, assim como ele obteve a decomposição em fatores primos de cada um dos números de 1 a 20, essa decomposição também pode ser obtida para qualquer outro número natural maior que 20.

Atividade adaptada de: <http://www.matematicacomvida.uff.br/index.php/modulosin\strucionais/2-modulosinstrucionais/18-fatoracao-e-primos-com-escala-cuisenaire.html>.

Acesso em 21 mai. 2019.

6.5 Atividade 3

Atividade 3: Gincana

Objetivos da atividade: Revisar todo o conteúdo trabalhado durante o encontro.

Material: ficha com números, fichas com afirmativas

Descrição da atividade:

Os alunos serão orientados a pegarem uma ficha, inicialmente, com o número em mãos a tutora pegará uma ficha com uma dica sobre o número, se o número em que o aluno estiver obedecer a aquilo que é falado, o aluno pontuará.

A tutora deverá orientá-los a escrever o número em um papel e sempre que necessário realizar as operações ou consultar a Escala Cuisenaire.

As afirmativas serão do tipo:
- número múltiplo de 2;
- número primo entre 1 e 10;
- divisor de 42, etc.;
- tem o primo 7 em sua decomposição.

Na segunda rodada, os alunos deverão pegar dois algarismos que formarão o número para a rodada.

Na terceira rodada, os alunos pegarão 3 algarismos.

Ao final da terceira rodada, o aluno que obteve maior pontuação vence a competição.