UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA
Mestrado Profissional em Matemática em Rede Nacional

Eliton Mendes Pedrosa Simes

Criptografia RSA para o Ensino Médio

RECIFE
2023

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA
Mestrado Profissional em Matemática em Rede Nacional

Eliton Mendes Pedrosa Simes

Criptografia RSA para o Ensino Médio

Dissertação de mestrado apresentada ao Departamento de Matemática da Universidade Federal Rural de Pernambuco como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Antônio José Ferreira Gomes Júnior

RECIFE
2023

Dados Internacionais de Catalogação na Publicação
Universidade Federal Rural de Pernambuco
Sistema Integrado de Bibliotecas
Gerada automaticamente, mediante os dados fornecidos pelo(a) autor(a)

S589c Simes, Eliton Mendes Pedrosa
Criptografia RSA para o Ensino Médio / Eliton Mendes Pedrosa Simes. - 2023.
94 f. : il.

Orientador: Antonio Jose Ferreira Gomes Junior.
Inclui referências.

Dissertação (Mestrado) - Universidade Federal Rural de Pernambuco, Programa de Mestrado Profissional em Matemática (PROFMAT), Recife, 2023.

1. Criptografia . 2. RSA. 3. Ensino Médio. I. Junior, Antonio Jose Ferreira Gomes, orient. II. Título

CDD 510

ELITON MENDES PEDROSA SIMES

"CRIPTOGRAFIA RSA PARA O ENSINO MÉDIO"

Trabalho apresentado ao Programa de Mestrado Profissional em Matemática – PROFMAT do Departamento de Matemática da UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO, como requisito parcial para obtenção do grau de Mestre em Matemática.

Aprovado em 30/08/2023

BANCA EXAMINADORA

_____

P**rof. Dr. Antonio José Ferreira Gomes Junior** (Orientador) – UFRPE

_____

Prof. Dr. Ricardo Burity Croccia Macedo - UFPB

_____

Prof. Dr. Rodrigo José Gondim Neves – PROFMAT/UFRPE

A mim, por todo o esforço!

Agradecimentos

Quero agradecer ao meu orientador por toda a ajuda prestada; a CAPES sob a presidência de Mercedes Bustamante, pelo incentivo à educação através das bolsas de iniciação científica; a minha mãe Sônia, por ter sempre se dedicado a mim e à minha irmã; aos meus filhos Matheus e Cecília, pelos livros presenteados que subsidiaram a escrita e por me mostrarem que é preciso ter coragem para mudar; ao amigo e colega de turma Antônio, por ter me auxiliado nas configurações do Látex; aos parceiros João Paulo, Fábio, Mayco e Ricardo, pela rotina semanal que somaram horas de estudo; e, em especial, aos meus alunos da Escola de Aplicação do Recife, por terem aceitado participar do trabalho.

"A matemática, senhora que ensina o homem a ser simples e modesto, é a base de todas as ciências e de todas as artes."

(Malba Tahan)

Resumo

Este trabalho leva ao conhecimento dos estudantes da educação básica, particularmente os do Ensino Médio, a importância da criptografia RSA como um instrumento relevante na comunicação e na transmissão de dados sem a quebra de sua integridade e de sua originalidade. Fazendo o uso da aritmética dos restos, sem a obrigatoriedade de falarmos em congruência modular, o trabalho mostrará como criptografar uma mensagem fazendo, primeiramente, uma pré-codificação associando cada caractere da mensagem original a um número estabelecido em uma tabela sequenciada de números naturais para posterior codificação, sendo o resultado final a sequência de números a ser transmitida. O trabalho também se propõe a mostrar como será feita a decodificação, bem como, estabelecer os parâmetros necessários para tornar possível a criptografia e mostrará o porquê do método funcionar e ter sua segurança garantida pelo simples fato de que a fatoração de números grandes é lenta e de difícil procedimento, uma vez que, os números primos escolhidos no processo possuem muitos dígitos. Além de levar o conhecimento dessa poderosa ferramenta de uso comum no mundo, nós propomos atividades para uso em sala de aula, simulando uma situação real de codificação e decodificação utilizando chaves públicas geradas na própria sala de aula.

Palavras-chave: Criptografia. RSA.

Abstract

This project brings to the knowledge of basic education students, particularly high school students, the importance of RSA encryption as a relevant instrument in the communication and transmission of data without compromising its integrity and originality. Making use of the arithmetic of the remainders, without the obligation to talk about congruence modulo m, the work will show how to encrypt a message by doing, first, a pre-coding associating each character of the original message to a number established in a sequenced table of natural numbers to subsequent encoding, the final result being the sequence of numbers to be transmitted. The work also proposes to show how the decoding will be done, as well as to establish the parameters necessary to make encryption possible and will show why the method works and has its security guaranteed by the simple fact that the factoring of large numbers is slow and difficult procedure, since the prime numbers chosen in the process have many digits. In addition to taking the knowledge of this powerful tool in common use in the world, we propose activities for use in the classroom, simulating a real situation of encoding and decoding using public keys generated in the classroom itself. This project proposes a small computer program, which already exists, capable of performing encryption and decryption using the generated keys, in activities with students in the classroom, with the intention of showing them how computers carry out the method and, thus, get even closer to a real situation.

Keywords: RSA. Encryption.

Lista de ilustrações

Lista de tabelas

Sumário

Introdução

A palavra criptografia deriva do grego ***kriptos*** (oculto) e ***graphein*** (escrever) e, o ato de criptografar sempre esteve presente em nossa História. Conforme Simon Singh, em sua obra *O livro dos códigos*(SINGH, 2001), "durante milhares de anos, rainhas e generais dependeram de comunicações eficientes de modo a governar seus países e comandar seus exércitos". A ideia de propor, em sigilo, mensagens relevantes foi um fator preponderante no avanço da ciência, uma vez que, houve uma busca histórica na melhoria das comunicações sigilosas. Com o desenvolvimento da tecnologia e a implementação de ferramentas tecnológicas no cotidiano das pessoas, principalmente, no decorrer da evolução da internet, o ato de enviar e receber mensagens, dados e informações, com o sigilo na transmissão sempre foi uma busca constante. Advindas das guerras, as mensagens criptografadas eram peças fundamentais nas estratégias e tomadas de decisão. Durante a Segunda Guerra Mundial, vários esforços foram despendidos por ambos os lados para interceptar e desvendar as informações coletadas mobilizando inúmeros profissionais da área como matemáticos e outros cientistas. Não era tarefa fácil, mas grandes cientistas mostraram que, até então, nenhum método de criptografia tinha sido tão eficaz que não pudesse ser quebrado. Com contribuições do matemático Alan Turing[1] na busca por decodificar mensagens que levassem os Aliados a vitória, essa busca fez criar métodos, pós-guerra, que não foram tão efetivos e caíram ao longo do tempo, deixando lacunas e, talvez, evitando o avanço da tecnologia de transmissão de dados mesmo que de maneira indireta, deixando espaço para que a ciência buscasse um mecanismo efetivo e definitivo para preencher esses intervalos. A busca por transmitir e receber mensagem com a intenção de manter em segredo as estratégias de uma guerra não foi exclusividade das guerras contemporâneas, mas uma vertente de todo o embate entre oposição de ideias ao longo da história. Dentre os métodos criados, efetivamente, o mais conhecido é o RSA. Como diz Coutinho(COUTINHO, 2014), até a edição do seu livro: "Há vários outros códigos de chave pública, mas o RSA é, atualmente, o mais usado em aplicações comerciais. Este é o método utilizado, por exemplo, no *Nestscape*, o mais popular dos *softwares* de navegação da *Internet*".

Com as iniciais dos seus inventores Ronald Linn Rivest, Adi Shamir e Leonard Max Adleman, o sistema de criptografia RSA tem eficiência garantida pela aritmética dos restos fazendo uso de números primos, mas não quaisquer primos, e sim imensos primos dificultando a fatoração, fortalecendo o método e tornando, praticamente, impossível a

[1] **Alan Methison Turing (1912-1954)** foi um matemático inglês, cientista da computação, lógico, criptoanalista, biólogo teórico e filósofo, influente no desenvolvimento da ciência da computação teórica, proporcionando uma formalização dos conceitos de algoritmo e computação com a máquina de Turing, que pode ser considerada um modelo de computador de uso geral.

quebra do sigilo das mensagens, de modo a garantir a integridade e originalidade dos dados. Em sua obra *Números Inteiros e Criptografia RSA*(COUTINHO, 2014), Coutinho fala de números primos de 60 ou mais algarismos. O algoritmo foi descrito em 1978, mas método equivalente foi criado pelo criptólogo britânico, Clifford Christopher Cocks, em 1973, mas ele não foi revelado até 1997. Evidentemente, na atualidade, o método de criptografia utilizando as Curvas Elípticas é uma realidade e, a partir do momento em que os computadores quânticos se popularizarem, com sua velocidade de processamento, o RSA se tornará obsoleto. Contudo, em nosso trabalho, trataremos a Criptografia RSA como, entre os métodos, o mais seguro e também é o primeiro método a possibilitar uma criptografia com chaves públicas com assinatura digital. Um usuário do sistema RSA cria uma chave pública com dois números primos muito grandes e publica juntamente com um valor auxiliar. Com os números primos em segredo, de posse da chave pública qualquer pessoa pode encriptar uma mensagem utilizando o método já publicado e, evidentemente, sendo a chave pública imensamente grande, apenas o alguém de posse dos números primos pode decodificar a mensagem de forma viável.

O sistema de criptografia RSA é de chave assimétrica e pública e o algoritmo utiliza um tema bem comum da Aritmética, a congruência modular. O tema não é abordado comumente na educação básica, especificamente, no Ensino Médio. Podemos dizer que raras as vezes um estudante da educação básica trate esse tema com real valor. Talvez, para um conjunto finito de estudantes, a congruência seja estudada para as provas olímpicas. O não estudo do assunto impossibilita o aprofundamento do algoritmo de criptografia e os estudantes passam por todo o Ensino Médio sem ouvir falar em criptografia, pelo menos, não o RSA. Isso é um fato, pois congruência não é tema do currículo escolar de Pernambuco[2].

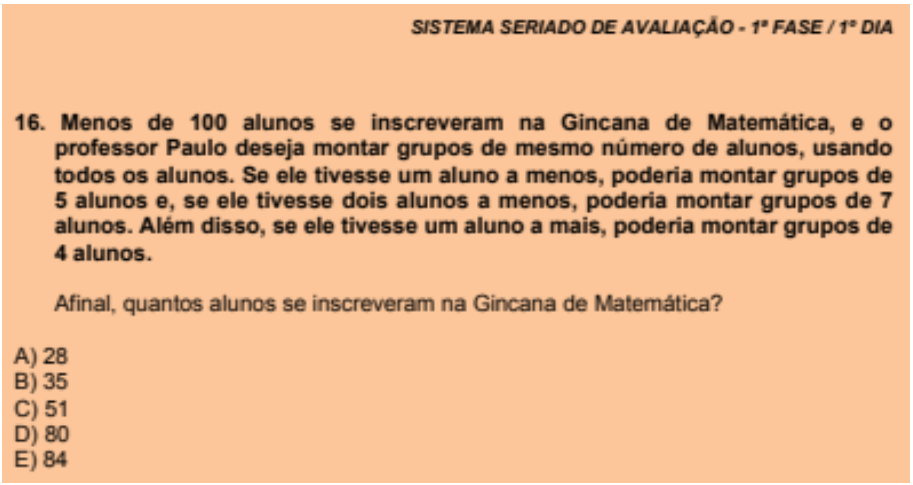
> *"Pensando dessa forma, entende-se que o currículo não é meramente uma prescrição, mas, acima de tudo, um campo de lutas e tensões que traduz a escola e a sociedade que se pretende construir (SILVA, 2002). Compreendido como fruto de uma construção coletiva e democrática, ele não visa aqui apenas definir os conhecimentos a serem aprendidos e ensinados, mas permitir práticas educativas críticas, reflexivas e contextualizadas, que estejam pautadas na dialogicidade como ato primordial na busca do conhecimento daqueles que fazem o processo educativo no seu dia a dia (FREIRE, 1987)."*(PERNAMBUCO, 2021)

Dessa forma, a dissertação propõe apresentar ao professor o algoritmo de criptografia sem a necessidade de o estudante estudar as congruências modulares. É um desafio proposto e o trabalho tenta dialogar com o Novo Ensino Médio, apresentando práticas educativas que visam estimular e a desafiar o estudante, na busca de uma educação de qualidade e que incremente no seu projeto de vida mais um sentido ao estudo da matemática, em especial a Aritmética.

Tentando justificar a escolha do tema, ao trabalhar com estudantes do ensino médio,

[2] Ver o currículo de Pernambuco no sítio www.educacao.pe.gov.br/portal

eu como estudante de mestrado e professor de matemática acredito que, o profissional da área de educação precisa estar constantemente atualizado nas informações que estão na mídia e em todo o contexto social. Na verdade, o professor, independente de qual segmento ele esteja atuando se Ensino Médio, Ensino Infantil, Ensino Fundamental ou Ensino Superior, precisa se informar das notícias atuais na área que leciona. Podemos ampliar e dizer que o professor precisa, para o bem do seu intelecto e dos seus estudantes, bem como para a melhoria de suas práticas, ler também sobre as outras áreas fora do seu campo de estudo. Acredito que isso o torne mais fluente em vários assuntos e apto a debater em vários campos sem perder seu poder de argumentação. E, em uma dessas etapas de estudo e leitura, o professor tende a analisar e resolver provas de várias avaliações de larga escala como Enem, Prova Brasil, SAEPE (Sistema de Avaliação da Educação de Pernambuco), SAEB (Sistema de Avaliação da Educação do Brasil) e, especialmente, o SSA (Sistema Seriado de Avaliação) da UPE (Universidade de Pernambuco), destinado aos alunos do ensino médio que almejam o ingresso na universidade. Em uma dessas análises de provas, comumente feita todo final de ano, logo após sua aplicação, deparei-me com a seguinte questão:



SISTEMA SERIADO DE AVALIAÇÃO - 1ª FASE / 1º DIA

16. Menos de 100 alunos se inscreveram na Gincana de Matemática, e o professor Paulo deseja montar grupos de mesmo número de alunos, usando todos os alunos. Se ele tivesse um aluno a menos, poderia montar grupos de 5 alunos e, se ele tivesse dois alunos a menos, poderia montar grupos de 7 alunos. Além disso, se ele tivesse um aluno a mais, poderia montar grupos de 4 alunos.

Afinal, quantos alunos se inscreveram na Gincana de Matemática?

A) 28
B) 35
C) 51
D) 80
E) 84

Figura 1 – Retirada do site processodeingresso.upe.pe.gov.br

É evidente que, o estudante, tomaria cada alternativa e verificaria se o número em questão deixaria tais restos mencionados. Por exemplo, se o número de alunos, dito no problema, tivesse um a menos ele formaria grupos de cinco estudantes, ou seja, ao dividir o número de alunos por cinco essa divisão deixa resto 1. Em seguida, se tivéssemos dois alunos a menos teríamos grupos de 7, ou seja, ao dividir o número de estudantes por sete, esta deixa resto 2. E, se ele tivesse um aluno a mais poderia formar grupos de quatro alunos, ou seja, ao dividir por quatro, esta divisão deixa resto 3. O aluno esperto, interpretando o enunciado, bastaria procurar a alternativa que deixa resto 1, 2 e 3 ao dividir por 5, 7 e 4, respectivamente, chegando na resposta 51. Uma outra possibilidade que demandaria um raciocínio mais engenhoso é pensar que o número n é na forma $5k + 1$, ou $7k + 2$ ou

ainda $4k + 3$ para algum $k \in \mathbb{N}$. Sendo assim, sabendo que $n < 100$, temos as seguintes possibilidades:
$5k + 1 = \{1, 6, 11, 16, 21, 26, 31, 36, 41, 46, \mathbf{51}, 56, \ldots, 96\}$.
$7k + 2 = \{2, 9, 16, 23, 30, 37, 44, \mathbf{51}, 58, \ldots, 91\}$.
$4k + 3 = \{3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, \mathbf{51}, 55, \ldots, 99\}$.

Fazendo uma simples varredura, o estudante encontra como intersecção a resposta do problema, **51**. Dentre todas as possibilidades de resoluções dispostas ao aluno, de certo, a mais elegante remete a um sistema de congruências e esse assunto não é abordado no Currículo de Pernambuco[3]. Exceto, apenas, em turmas olímpicas objetivamente. Por outro lado, essa constatação remeteu-me ao pensamento de levar o tema para a sala de aula de uma forma que não demandasse muito tempo e, também, que não fosse tão de encontro ao Currículo de Pernambuco. Então, surgiu-me a ideia de abordar, junto aos meus estudantes, algum trabalho concreto, manipulável, que o aluno compreendesse a importância na prática e, dessa forma, abrisse caminho para ampliar o aprendizado em aritmética sem a necessidade de partirmos direto ao ponto, imediatamente ao tema abordado no problema já mencionado, e dando ao estudante ferramentas e curiosidade para que, de maneira autônoma se por ventura, dele ampliar sua perspectiva sobre a matemática e seus campos de atuação. E, em diálogo com meu orientador, surgiu a ideia de abordar a criptografia, um tema que é vivido por todos nós no dia a dia e que se sabe tão pouco, e de como a matemática atua fazendo a segurança de dados. A seguir, veremos uma disputa entre os codificadores e decifradores de códigos e de como essa disputa acelerou o avanço tecnológico e, sobretudo, no desenvolvimento dos computadores modernos.

[3] Ver Currículo de Pernambuco no sítio www.educacao.pe.gov.br/portal

1 Um Pouco de História

Ao longo da história sempre houve a necessidade de enviar mensagens secretas de um ponto a outro e, é claro, sem que terceiros obtivessem o propósito comunicativo. De acordo com Framilson José Ferreira Carneiro(CARNEIRO, 2017), em seu livro "Criptografia e Teoria dos Números", essa arte de esconder mensagens, a criptografia, é mais antiga do que a própria escrita sendo encontrada no sistema de escrita egípcios, Hieroglífica, que tinha um propósito de esconder o real significado do texto. Podemos ampliar para outros povos como os gregos, hebreus, persas e árabes a utilização da criptografia para ocultar informações confidenciais em caso de receptação pelas mãos inimigas. A criptografia tem por finalidade não omitir a existência de uma mensagem, mas sim esconder seu real significado e, para tal, ela utiliza técnicas que, de maneira geral, consistem em processos lógicos para misturar ou cifrar os símbolos da mensagem podendo ser letras e/ou algarismos. Faremos uma pequena abordagem em alguns métodos de criptografia que temos conhecimento.

1.1 Cifra da Transposição

Permutar as letras de uma mensagem, de certa forma, traz alguma segurança ao ser interceptada porque o inimigo interceptador não conseguirá reorganizá-la. Contudo, a dificuldade também se dará para o destinatário. Então, a troca dos símbolos de posição precisa ser previamente acordada entre o remetente e o destinatário para evitar problemas futuros. O método de criptografia conhecido como "Cerca de Ferrovi" é uma técnica simples e eficiente de codificação de mensagens. A ideia básica do método é representar as letras da mensagem por meio de traços horizontais e verticais, que são desenhados em um "trilho" imaginário, formado por linhas horizontais. Essas linhas são chamadas de "trilhos" e podem ter qualquer comprimento, a depender da extensão da mensagem a ser codificada. Para entender melhor como o método funciona, vamos supor que queremos codificar a palavra "CRIPTOGRAFIA". Primeiramente, devemos escolher um número de trilhos que será utilizado na codificação (por exemplo, 4 trilhos). Em seguida, escrevemos a palavra na vertical, distribuindo suas letras pelos trilhos, como mostra a figura abaixo:

Figura 2 – Distribuição das letras pelos trilhos

Note que as letras da palavra são escritas em ordem, da esquerda para a direita e de cima para baixo, como se estivéssemos escrevendo uma matriz. Depois de distribuir as letras pelos trilhos, basta "ler" a mensagem da esquerda para a direita, percorrendo os trilhos na mesma ordem em que foram escritos. No exemplo acima, a mensagem codificada seria: "CRPOAITOGRFIAIPAF". Note que a ordem das letras foi alterada, mas ainda é possível recuperar a mensagem original, desde que saibamos o número de trilhos utilizado na codificação e a forma como as letras foram distribuídas pelos trilhos. O método de criptografia "Cerca de Ferrovia" pode ser facilmente implementado em um programa de computador ou mesmo utilizando papel e lápis. Além disso, é possível criar variações da técnica, como a utilização de diferentes tipos de traços (por exemplo, traços diagonais) ou a adição de caracteres aleatórios entre as letras da mensagem. Talvez, pelo fato desse método ser simples, ele seja bastante vulnerável.

Existe um método mais seguro de transpor os caracteres de uma mensagem. Nesse caso, necessitaremos de uma chave, na qual cada letra dessa chave, estará numerada em sequência conforme a ordem do alfabeto em uma tabela retangular. Em seguida, a mensagem é organizada letra por letra embaixo das letras da chave e, posteriormente, a mensagem encriptada sairá da sequência de letras que está abaixo das letras da palavra chave. Vejamos um exemplo.
A mensagem é **"EU AMO A MATEMÁTICA"**. A chave será **FERMAT**. Organizemos a chave e a mensagem na tabela abaixo.

Tabela 1 – Cifra da Transposição

ORDEM	3	2	5	4	1	6
CHAVE	F	E	R	M	A	T
	E	U	A	M	O	A
MENSAGEM	M	A	T	E	M	A
	T	I	C	A		

Fonte: Feita pelo autor

A sequência cifrada é "OMUAIEMTMEAATCAA".

Para decifrar a mensagem, o receptor deve fazer o processo contrário. Como a mensagem foi escrita em linhas e codificadas em colunas, o receptor em posse da chave, deve escrever em colunas e codificar em linhas.

1.2 Cifra das Substituições

Uma das cifras mais antigas e simples que se tem conhecimento é a "Cifra de César" em homenagem ao imperador romano Júlio César. Nesta, para comunicar seus planos de batalha, César substituía cada letra alfabética da mensagem pela letra que está a três

posições adiante no alfabeto. Por exemplo, a letra “A” é substituída pela letra “D”, a “B” pela letra “E” e assim até a última letra da mensagem. Então, se a mensagem original é **“EU AMO A MATEMÁTICA”** codificada pela cifra de César, a mensagem fica **"HW DPQ D PDWHPDLFKD"**.

Observando a mensagem codificada e, realmente, não parece ter sentido, despenderíamos pouco tempo para quebrar esse código se soubéssemos que foi usada a Cifra de César, porque existem apenas 25 valores possíveis para a chave.

Aprimorando o método de César, encontramos a Cifra de Substituição Monoalfabética, na qual cada um dos caracteres da mensagem é trocado por um outro de uma tabela já pré-estabelecida ou conforme uma chave, que pode ser um número que indica o número de posições que deve-se avançar no alfabeto para obter o texto cifrado. Os árabes eram conhecedores da cifra de substituição monoalfabética, no entanto, a eles não é atribuído nenhuma relevância no contexto da criptografia, na qual, além de utilizar as cifras, os estudiosos árabes eram capazes de quebrar as cifras. A eles é atribuído a invenção da criptoanálise, a ciência da dedução da mensagem original a partir da mensagem cifrada sem o conhecimento da chave utilizada no processo. Enquanto o criptógrafo procura e busca novos métodos de criptografia, cabe ao criptoanalista a bravura de encontrar fraquezas no método, com o propósito de decifrar as mensagens secretas. Simon Sing(SINGH, 2001), em sua obra “O livro dos códigos”, p.32, afirma: “A criptoanálise só pôde ser inventada depois que a civilização atingiu um nível suficientemente sofisticado de estudo, em várias disciplinas, incluindo matemática, estatística e linguística”.

As cifras monoalfabéticas tem certa facilidade de serem quebradas. Isto se deve pelo fato de a frequência média com que cada letra é utilizada em um idioma é mais ou menos constante. Na nossa língua portuguesa, por exemplo, temos:

- As vogais são mais frequentes do que as consoantes;
- A vogal com maior frequência é o A;
- As consoantes S e M são mais frequentes do que as outras.

Dessa forma, com apenas a análise das frequências de cada símbolo presente na mensagem/texto, pode-se descobrir a letra correspondente aos símbolos mais frequentes.

Durante muito tempo esse método, cifra de substituição monoalfabética, foi utilizado e mantinha bem guardada todas as mensagens enviadas. Com o passar dos tempos, com o desenvolvimento da análise de frequência, o método foi enfraquecendo e, qualquer mensagem envida pelo método estava fadada a ser quebrada. Cabiam, então, aos criptógrafos, em oposição aos criptoanalistas, encontrarem métodos novos de cifras resistentes a quebra.

1.3 Cifra de Substituição Polialfabética

Este método criptográfico foi reconhecido no final do século XVI, mas teve sua origem em Florença, pelo século XV, através do italiano Leon Battista Alverti, arquiteto e construtor da Fonte de Trevi em Roma. Um arquiteto que teve reconhecimento em diversas áreas, mas teve maior notoriedade na sua área ao escrever o primeiro livro sobre arquitetura, que serviu como a base da transição entre o estilo gótico e o renascentista.

Alberti, na criptografia, sugeriu, em 1460, a utilização de dois ou mais alfabetos e, alternadamente, utilizá-los durante a cifragem evitando, assim, a decriptação por frequência. É historicamente reconhecido como a primeira proposta de substituição polialfabética. Mas suas ideias não seguiram adiante e, dessa forma, com o método incompleto, ele não obteve o reconhecimento. Para que o método chegasse a sua completude teve que passar pelas mãos de vários intelectuais da época para um aperfeiçoamento sendo, o primeiro, o abade alemão Johannes Trithemius, depois foi o cientista italiano Giovanni Porta e, por último, o diplomata francês Blaise de Vigenère. Blaise tomou conhecimento das ideias dos cientistas e concatenou tornando o sistema seguro e eficiente e, por isso, o método de cifragem ficou conhecido como Cifra de Vigenère.

No ano de 1586, Blaise de Vigenère publica seu tratado sobre a escrita secreta, "Traicté des chiffres", e ele descreve todo o processo de criptografia. O método utiliza 26 alfabetos distribuídos em uma matriz conhecida como tabela de Vigenère, da forma como está na figura abaixo.

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

Figura 3 – Tabela de Vigenère

Para enviar uma mensagem pelo método devemos escrever sobre as letras da mensagem original, repetidamente, as letras da palavra chave até completar toda a mensagem. Na tabela, a letra da mensagem cifrada será onde se intercepta a letra da palavra-chave (linha da tabela) com a letra da mensagem original (coluna da tabela) e, sendo assim, segue-se até concluir a mensagem completa. Vejamos um exemplo:

A mensagem original é **"EU AMO A MATEMÁTICA"** e utilizaremos como palavra-chave **"PROFMAT"**. Teremos, então

Tabela 2 – Cifra de Substituição Polialfabética

Palavra-chave	PR	OFM	A	TPROFMATPR
Mensagem Original	EU	AMO	A	MATEMATICA
Mensagem Cifrada	TL	ORA	A	FPKSRMTBRR

Fonte: Feita pelo autor

A mensagem cifrada é **"TL ORA A FPKSRMTBRR".**

Para a decodificação por esse método, procede-se de maneira semelhante ao que acabamos de fazer. Escreve-se as letras da palavra-chave sobre cada letra da cifra até esgotar todas as letras da mensagem cifrada e depois, na tabela, deve-se correr na linha correspondente da letra da palavra-chave até encontrar a letra da cifra e subir, na mesma coluna da letra da cifra encontrada, até a letra que será a da mensagem original. O método de Vigenère é imune a quebra por frequência pois as letras com maior frequência na mensagem cifrada nem sempre correspondem a mesma letra na mensagem original. No nosso exemplo, a letra de maior frequência é o R e, na mensagem original, ela não corresponde a mesma letra. Além disso, a chave pode ser qualquer palavra do dicionário ou novas palavras criadas aumentando o leque de possibilidades e, dessa forma, um criptoanalista não conseguiria decodificar.

Não há como negar as significativas contribuições do arquiteto Leonel Alberti para a criptografia. Uma delas foi a criação da primeira máquina criptográfica que é o disco de cifra mostrado na figura abaixo.

Figura 4 – Disco de Cifra de Leonel Alberti

O disco de cifra foi construído da seguinte forma: Alberti construiu dois discos de cobre com diâmetros diferentes e escreveu o alfabeto ao longo de sua borda, em cada disco, e sobrepôs o disco menor no maior fixos por uma agulha no centro que servia como eixo

de rotação. O alfabeto do disco maior era tomado como sendo o da mensagem original, enquanto o do disco menor representava o alfabeto cifrado.

1.4 A Criptografia e as Máquinas

Com a criação do código Morse, após 1830, por Samuel Morse, a comunicação deu um salto. O código Morse foi a primeira representação binária (formada por ponto e traço) do alfabeto e teve grande aplicação com uso até hoje. O telégrafo, responsável por transmitir o código, exerceu grande importância na comunicação. Contudo, a proteção dessa comunicação era um dilema pois o operador do telégrafo precisava ler a mensagem para encaminhá-la e isso gerava um problema de sigilo. Então, a solução encontrada era codificar a mensagem antes de entregá-la ao operador. O código Morse passa a ter uma estabilidade e os criptógrafos perdem o interesse em quebrar a cifra de Vigenère. Eis que surge Babbage.

Charles Babbage nasceu em 1791 e foi o personagem mais intrigante da história da criptografia. Filho de Benjamin Babbage, um banqueiro rico de Londres que negou ao filho o acesso a sua fortuna por ter se casado contra seu consentimento. Charles Babbage não se abalou pois tinha dinheiro suficiente para se manter e, sem trabalhar, se dedicou a ciência com toda a sua atenção a problemas que o despertavam interesse e, entre eles, estava a cifra de Vigenère.

Em paralelo a Babbage, trabalhando em suas técnicas de quebrar códigos, estava um oficial da reserva do exército prussiano, Friedrich Wilhelm Kasiski, que publicou um livro sobre tais técnicas no ano de 1863 intitulado “Die Geheimschriften und die Dechiffrer-Kunst” (A Escrita Secreta e a Arte de Decifrá-la) e nele continham as técnicas para a quebra da cifra de Vigenère, ficando conhecido como o teste de Kasiski. Tal publicação lhe rendeu os créditos pela quebra da cifra de Vigenère e não se sabe ao certo o porquê de Babbage não ter chegado a divulgar seu trabalho sobre a quebra da cifra de Vigenère, uma vez que, foram encontrados manuscritos sobre o tema logo após sua morte. A teoria por trás é de que, a descoberta da quebra da cifra de Vigenére por Babbage, se deu após o início da guerra da Criméia, e, segundo relatos, a descoberta deu uma certa vantagem aos britânicos sobre os Russos, sendo bem possível que, Babbage foi obrigado, pelo serviço de espionagem britânico a manter todo o seu trabalho em sigilo. Sendo isso verdade, esse fato faz sentido, uma vez que, posteriormente na história, os britânicos mantiveram o sigilo, sob a justificativa da segurança nacional, sobre as descobertas feitas por Alan Turing no período da segunda guerra mundial.

Com as descobertas de Charles Babbage e Friedrich Kasiski, a cifra de Vigenère não era mais segura. Com a quebra da cifra, o sigilo e a integridade das mensagens não podiam mais serem garantidos pelos criptógrafos e, assim, todo o controle da disputa entre

aqueles que criam os métodos de criptografia e aqueles que quebram os métodos ficou nas mãos dos criptoanalistas. Os criptógrafos tentaram criar novas cifras, mas nada de novo surgiu durante a segunda metade do século XIX a não ser o interesse do público em geral pelas cifras. Na virada do século, o físico italiano Guglielmo Marconi realizou um feito poderoso para as telecomunicações aumentando a necessidade de uma codificação mais segura. Marconi inventou um equipamento que era capaz de emitir e receber pulsos elétricos a uma distância de até 2,5 km sem a necessidade de fio e, com isso, as mensagens podiam ser entregues e recebidas. Era um modo diferente de comunicação da época e foi dado o nome de rádio. Essa descoberta conquistou os militares que, mesmo com certa desconfiança, de um modo geral, possibilitou aos generais o contato contínuo com suas tropas nos quarteis. No entanto, essa facilidade proporcionada pelo rádio tinha sua fraqueza, pois as mensagens poderiam chegar onde não deveriam e, claramente, havia a necessidade de uma codificação confiável perante terceiros, caso as mensagens fossem interceptadas. A dupla característica do rádio, facilidade na comunicação e de interceptação, teve sua grande prova durante a Primeira Guerra Mundial. Existia a preocupação das nações em utilizar o rádio, mas não sabiam como garantir a segurança das mensagens. Diante disso, houve intensa busca por um método de criptografia seguro, mas não obtiveram êxito no período de 1914 a 1918. Todas as cifras criadas foram quebradas uma a uma. Apesar da fragilidade no envio de mensagens, o rádio estava sendo muito utilizado e o volume de mensagens era enorme durante a Primeira Guerra Mundial com seu devido risco de as mensagens serem interceptadas.

Devido ao fracasso da criptografia em criar um novo método, a busca por um sistema que pudesse ser usado em conflitos seguintes continuou nos anos seguintes a Primeira Guerra Mundial e, com muita insistência, a demora não foi grande para que os criptógrafos reestabelecessem a comunicação secreta no campo de batalha. Eles deixaram o lápis e o papel de lado e enveredaram na exploração da tecnologia da época para reforçar as cifras e, foi assim que, o alemão Arthur Scherbius, tendo estudado engenharia elétrica em Hanover e Munique, desenvolveu uma máquina criptográfica que em sua essência era uma versão elétrica do disco de Cifra de Alberti. Esta máquina foi nomeada de Enigma e se tornou o mais complicado sistema de cifragem da história e teve uso efetivo, pelos militares alemães, a partir de 1926 sendo o sistema de criptografia mais seguro do mundo até então.

De acordo com Framilson J.F. Carneiro(CARNEIRO, 2017), a máquina Enigma, ao contrário do que os alemães imaginavam, foi a derradeira da queda de Hitler. Durante o período da segunda guerra mundial, os britânicos estavam empenhados em decifrar as mensagens nazistas e montaram um grupo de trabalho formado por matemáticos que trabalhavam, em sigilo, para a quebra das mensagens e neste grupo tinha um ilustre matemático chamado de Alan Turing que foi fundamental na história.

Figura 5 – Máquina de Criptografia Alemã Enigma

Alan Turing, filho de Julius Turing, nasceu em 23 de junho de 1912 em Londres. Seu pai era funcionário do governo britânico e trabalha em Chatrapur, cidade do sul da Índia, julgava importante o filho nascer em Londres e junto com sua esposa, Ethel, fora para a Grã-Bretanha para o nascimento de Alan. Seus pais voltaram para a Índia e Alan foi criado no Reino Unido por babás e amigos da família. Em 1926, já com 14 anos de idade, teve sua vida escolar iniciada e, desde cedo, demonstrou interesse pela ciência realizando suas primeiras experiências em companhia do amigo Christopher Morcon, amizade esta que durou quatro anos pois, em 1930, seu amigo morre de tuberculose. Arrasado com sua perda, Turing resolve dedicar-se por completo a matemática para não dar espaço à tristeza e, no ano seguinte, foi admitido no King's College em Cambridge que era considerada o lugar da elite intelectual da época, levando uma vida normal como professor e misturando a matemática pura com suas atividades práticas. Em 1937, ele publica seu trabalho científico intitulado "On Computable Numbers" (Os números Computáveis), e nele ele descreve uma máquina imaginária que efetuaria cálculos matemáticos. Ele idealizava uma máquina para cada operação. Eram conhecidas como as Máquinas de Turing. Posteriormente, ele tornou a ideia um tanto radical e descreveu o que seria a máquina universal de Turing que era a idealização de uma máquina que faria todas as operações. Esta máquina serviu de base para os primeiros computadores uns dez anos depois. Em 1939, ele interrompe sua carreira acadêmica por causa do convite feito pela Escola de Cifras e Códigos do Governo da Inglaterra para se tornar um criptoanalista. Sediada na mansão Bletchley Park e com objetivo principal de conseguir quebrar as chaves da máquina alemã Enigma.

Uma réplica da Enigma já estava em posse dos britânicos, graças a traição de um alemão que tinha acesso a máquina. Mas ter a máquina não era suficiente para garantir a decodificação das mensagens e sim saber como ajustar a máquina pois a chave era mantida em segredo pelos alemães. Essa busca continuou incansavelmente até que Turing teve a brilhante ideia em seguir as ideias do matemático polonês Marian Rejewski que já havia quebrado o código da Enigma em uma versão mais simples da máquina e, juntamente com

os esforços dos demais pesquisadores, conseguiram decifrar as complicações adicionadas da Enigma. Essa descoberta alterou os rumos da guerra antecipando seu fim em 3 anos, terminando em 1945 onde tinha previsão de terminar em 1948. Alan Turing não obteve os méritos que lhe eram devidos. Homossexual assumido, nesse ponto o governo britânico era implacável e, no início dos anos 50, Alan foi humilhado em público, o governo o impôs um tratamento à base de hormônios, foi proibido de trabalhar em pesquisas de desenvolvimento do computador e, em 7 de junho de 1954, deprimido, cometeu suicídio aos 41 anos de idade. Essa versão de morte(G1, 2013), posteriormente, foi desmentida por biógrafos e estudiosos que concluíram que sua morte se deu devido a intoxicação pelos remédios que tomava para cumprir sua pena.

No ano de 2013, quase 60 anos mais tarde, a rainha Elizabeth II concedeu o perdão póstumo a Alan Turing pelo "crime" da homossexualidade. Segundo o site Aventuras da História, ao longo dos seus 70 anos de reinado, a rainha concedeu o perdão real em três ocasiões apenas: dois prisioneiros, no País de Gales, que salvou um funcionário penitenciário de um ataque de Javali e ao Matemático Alan Turing, o inventor do primeiro computador e decifrador dos códigos nazistas. O perdão foi solicitado pelo ministro da justiça, Chris Grayling, que afirmou:

> *"Turing merece ser lembrado e reconhecido pela sua fantástica contribuição aos esforços de guerra e por seu legado à ciência. Um perdão da Rainha é um tributo apropriado a esse homem excepcional."*(HISTóRIA, 2022)

1.5 A Criptografia Pós Segunda Guerra Mundial

Durante a segunda guerra mundial, o grupo de pesquisadores britânicos levou a melhor frente aos elaboradores de códigos alemães nazistas e, com o desenvolvimento de máquinas de quebra de códigos pelos pesquisadores da Bletchley Park e, dentre essas, está a máquina Colossus, considerada o ancestral do computador. Os criptoanalistas continuaram a empregar a tecnologia no computador aproveitando a velocidade e flexibilidade em pesquisar as possíveis chaves. Por outro lado, os criptógrafos começaram a explorar o poder do computador e começaram a criar cifras cada vez mais complexas. Nesse contexto, o computador desempenhou um papel fundamental nessa batalha entre codificadores e decodificadores no período pós-guerra. Até então, cifrar uma mensagem remetia ao processo semelhante do passado onde as velhas técnicas de transposição e da substituição e isso era um problema. Além disso, ter um computador era uma limitação pois somente os militares possuíam.

Melhorando seu desempenho e se tornando cada vez mais poderosos e, evidentemente custando menos, os computadores, na década de 60, tornaram-se mais populares e as empresas passaram a adquirir e mantê-los para fazer a cifragem de transações importantes como transferências de valores e, dessa forma, a codificação entre as comunicações se

difundiram. Outra preocupação era uma padronização pois as empresas usavam dois processos criptográficos: um para comunicações internas e outro para as comunicações externas.

O fato que torna um método criptográfico seguro é a quantidade de chaves que ele consegue gerar. Um criptoanalista, primeiro, se propõe a verificar todas as chaves possíveis. Quanto maior for o número de possibilidades de chave, mais tempo será necessário para encontrar a certa. E, um dos problemas de um método de criptografia, é a distribuição com segurança dessas chaves, coisa que os governos e os militares têm capacidade de enfrentar. Tentando solucionar esse problema da distribuição das chaves, surge um dos criptógrafos mais entusiasmado de sua geração, Whitfield Diffie. Nascido em 1944 e louco por matemática desde criança, graduou-se nesta ciência aos 21 anos de idade, no Instituto de Tecnologia de Massachussets (MIT). Trabalhou em empresas ligadas a segurança de computadores chegando a se tornar um especialista nesta área.

Convidado para ministrar uma palestra no laboratório Thomas J. Watson, da IBM, sobre as várias tentativas em solucionar o problema da distribuição de chaves, Diffie fica sabendo que existe um outro pesquisador que se interessa por esse problema, o professor de Stanford Martin Hellman, nascido em 1945. Sabendo do interesse de Martin, Diffie ligou prontamente para ele e os dois passam a trabalhar juntos, na tentativa de resolver o problema da distribuição de chaves e concentraram suas pesquisas na análise de várias funções matemáticas. Posteriormente, junta-se a eles Ralph Merkle, nascido em 1952, que tinha abandonado um grupo de pesquisa sob a justificativa de seu chefe não se importar para solucionar o problema de distribuição de chaves. Contudo, todo o mérito do trabalho de pesquisa, foi dado a Diffie e Hellman. Eles não estavam interessados em funções de mão dupla, ou seja, de métodos de cifragem com uso da mesma chave conhecido como método de cifra simétrica, devido a facilidade de fazê-las e desfazê-las, mas sim, de uma função de mão única porque seria fácil de fazer e seria muito difícil de desfazer e, sendo assim, Diffie e Hellman propuseram, teoricamente, o método de cifra assimétrica.

Até o momento, todos os métodos de criptografia descritos neste trabalho são de chave simétrica. Dizemos que um método de cifragem é de chave simétrica quando a chave que é usada para codificar é a mesma chave para decodificar. Nesse caso, não é interessante para um bom sistema de criptografia pois há o problema de como distribuir essa chave com a devida segurança. Eis o grande desafio dos pesquisadores: a busca por um método de cifragem de chave assimétrica, ou seja, a chave de encriptação é diferente da chave de decriptação. A criptografia Assimétrica, também conhecida como criptografia de chave pública, usa um par de chave, a chave pública e, diferente da primeira, a chave privada: os dados criptografados com a chave pública só podem ser descriptografados com a chave privada. Foram desafios que surgiram ao longo da história da criptografia abraçados por grandes cientistas e, digamos assim, grandes desafios exigem grandes responsabilidades

e dedicação, e foi assim que surgiu o atual e mais eficiente método de criptografia já inventado, o RSA. Diffie e Hellman conseguiram convencer a todos que existia uma solução para o problema da distribuição de chaves, e esta solução estava na criptografia assimétrica. Eles continuaram suas pesquisas, mas não conseguiram fazer a tal descoberta. Esse desafio foi vencido por um grupo de pesquisadores do Instituto de Tecnologia de Massachussets, o MIT. E foram eles, Ron Rivest, Adi Shamir, ambos cientistas da computação e Leonard Adleman, matemático.

Figura 6 – Ronald L. Rivest, Adi Shamir, Leonard Adleman.

Adleman, Rivest e Shamir já estavam trabalhando juntos há um ano e, cabia ao matemático Adleman, a responsabilidade de verificar as ideias e detectar as falhas para evitar que houvesse a perda de tempo em pistas falsas. E assim ele fez, detectando falha por falha até que, em abril de 1977, Rivest ao chegar tarde em sua casa, sem sono, foi ler um livro de matemática e começou a pensar na possibilidade de encontrar uma função de mão única para criar uma cifra assimétrica. Durante toda a madrugada, ele desenvolveu um trabalho científico que ficou pronto pela manhã. Estava resolvido o problema da criptografia assimétrica. Ele concluiu o trabalho citando os autores em ordem alfabética: Adleman, Rivest e Shamir (ARS). No dia seguinte, o trabalho foi entregue a Adleman, como de costume, para que ele fizesse a revisão e a verificação de possíveis falhas, mas nada de errado foi encontrado. A única crítica foi que Adleman queria que Rivest retirasse seu nome do trabalho sob a alegação de que os créditos do trabalho não eram seus, mas Rivest se recusou e, em comum acordo, deixaram para decidir posteriormente. Adleman passou a noite analisando o trabalho e, no dia seguinte, sugeriu que fosse feita uma modificação colocando seu nome como terceiro autor, e assim, o sistema de criptografia de chave assimétrica recebeu a sigla RSA (Rivest, Shamir, Adleman), tornando-se o sistema de criptografia de chave pública de maior influência no mundo moderno.

2 Teoremas Importantes

2.1 Divisibilidade

Divisibilidade é uma propriedade matemática que indica se um número pode ser dividido completamente por outro, sem deixar resto. Se um número é divisível por outro, dizemos que é um múltiplo do outro. A notação "b|a" indica divisibilidade. Se b|a é verdadeira, então "b" divide "a". Neste caso, "b" é divisor de "a" e, por sua vez, "a" é um múltiplo de "b". Por exemplo, 3|6 é verdadeiro, pois 3 é divisor de 6 e 6 é um múltiplo de 3.

Definição: Sejam a e $b \in \mathbb{N}$, se b divide a $(b|a)$, então existe $q \in \mathbb{N}$ tal que $a = bq$. A exemplo, 3|6, então $6 = 3 \times 2$. A negativa dessa afirmação é representada por $b \nmid a$, significando que não existe nenhum número natural q tal que $a = bq$. Por exemplo, $3 \nmid 4$. Suponha que $b|a$ e seja $q \in \mathbb{N}$ tal que $a = bq$. O natural q é chamado de quociente da divisão de a por b. Em seguida, estabeleceremos algumas propriedades da divisibilidade.

Propriedade 2.2.1. Sejam a, b e $c \in \mathbb{N}$. Tem-se que

i) $1|c$, $a|a$, $a|0$ e $0|0$.

ii)Se $c|b$ e $b|a$, então $c|a$.

Demonstração: Em i) decorre do fato de $c = c \cdot 1$, $a = a \cdot 1$ e $0 = a \cdot 0$. Já em ii), se $c|b$ e $b|a$, então existem $m, n \in \mathbb{N}$, tais quais $b = c.m$ e $a = b.n$. Agora, substituindo o valor de b da primeira equação na segunda, temos $a = c.m.n = c.(m.n)$, o que nos mostra que $c|a$.

Propriedade 2.2.2. Se a, b, c, $d \in \mathbb{N}$, com $a \neq 0$ e $c \neq 0$, então se $a|b$ e $c|d$ implica em dizer que $a.c|b.d$.

Demonstração: Se $a|b$ e $c|d$, então existem m e n naturais, tais quais $b = ma$ e $d = nc$. Portanto, $b \cdot d = (m \cdot a) \cdot (nc) = (a \cdot c) \cdot (m \cdot n)$, logo $a.c|b.d$.

Propriedade 2.2.3. Sejam a, b, $c \in \mathbb{N}$, com $a \neq 0$ e $b > c$, tais quais $a|(b + c)$ ou $a|(b-c)$. Então $a|b \Leftrightarrow a|c$.

Demonstração: Como $a|(b + c)$, então existe $m \in \mathbb{N}$ tal que $b + c = am$. Se $a|b$, existe $n \in \mathbb{N}$ tal que $b = an$. Substituindo a segunda igualdade na primeira, temos $an + c = am$ e, como $c \in \mathbb{N}$, tem-se $am > an$ e, consequentemente, $m > n$. Portanto, da última igualdade, segue que $c = am$ - $an = a(m$ - $n)$, o que implica em $a|c$. Analogamente, se $a|c \Rightarrow a|b$. Por outro lado, se $a|b$ e $a|c$, existem $m, n \in \mathbb{N}$, tais quais $b = am$ e $c = an$. Somando ambos os lados da igualdade, temos $b + c = am + an = a(m + n)$, o que implica em $a|(b + c)$. Para $a|(b-c)$ a demonstração é análoga.

Propriedade 2.2.4. Se a, b, $c \in \mathbb{N}$, com $a \neq 0$, e x, $y \in \mathbb{N}$ são tais quais $a|b$ e $a|c$, então $a|(xb + yc)$ e, se $xb > yc$, então $a|(xb - yc)$.
Demonstração: Como a/b e a/c, existem m e n naturais tais quais b = ma e c = na. Então, xb + yc = x(ma) + y(na) = a(xm + yn), o que nos mostra que a/(xb + yc). Para a/(xb – yc) a demonstração é análoga.

Propriedade 2.2.5. Dados a, $b \in \mathbb{N}^*$, temos que $a|b \Rightarrow a \leq b$.
Demonstração: Se a|b então existe c ∈ N tal que b = ac. Como c é natural, então c ≥ 1, que por sua vez, multiplicando ambos os lados por a, temos ac ≥ a, e como b = ac, decorre em b = ac ≥ a como queríamos mostrar.*

Propriedade 2.2.6. Sejam a, b, $n \in \mathbb{N}$, com $a > b > 0$. Temos que $(a - b)|(a^n - b^n)$.
Demonstração: Usaremos indução sobre n.
Para n = 0 a afirmação é verdadeira, pois a – b divide $a^0 - b^0 = 0$. Suponhamos que (a – b)|($a^n - b^n$). Vamos provar que a afirmação é válida para n + 1. Usaremos a técnica de somar e subtrair o mesmo termo. Escrevamos, $a^{n+1} - b^{n+1} = a.a^n - b.b^n = a.a^n - b.a^n + b.a^n - b.b^n = (a - b).a^n + b.(a^n - b^n)$. Como (a – b)|(a – b) e, pela hipótese (a – b)|($a^n - b^n$), então, pela propriedade 2.2.4, decorre que (a – b)|($a^{n+1} - b^{n+1}$).

Propriedade 2.2.7. Sejam a, b, $n \in \mathbb{N}$, com $a+b \neq 0$. Temos que $a+b$ divide $a^{2n+1}+b^{2n+1}$.
Demonstração: Usaremos indução sobre n e a mesma técnica de somar e subtrair o mesmo termo.
Obviamente, a afirmação é válida para n = 0, pois a + b divide $a^{2.0+1} + b^{2.0+1} = a + b$. Suponha que a + b divida $a^{2n+1} + b^{2n+1}$ e vamos provar que a afirmação vale para n + 1. Temos $a^{2(n+1)+1} + b^{2(n+1)+1} = a^{2n+1+2} + b^{2n+1+2} = a^2.a^{2n+1} + b^2.b^{2n+1} = a^2.a^{2n+1} - b^2.a^{2n+1} + b^2.a^{2n+1} + b^2.b^{2n+1} = (a^2 - b^2).a^{2n+1} + b^2.(a^{2n+1} + b^{2n+1})$. Como (a + b)|($a^2 - b^2$), pois $a^2 - b^2 = (a + b)(a - b)$ e, pela hipótese de indução, (a + b)|($a^{2n+1} + b^{2n+1}$), decorre que (a + b)|($a^{2(n+1)+1} + b^{2(n+1)+1}$).

Propriedade 2.2.8. Sejam a, b, $n \in \mathbb{N}$, com $a > b > 0$. Temos que $a + b$ divide $a^{2n} - b^{2n}$.
Demonstração: Mais uma vez, usaremos indução em n.
A afirmação é verdadeira para n = 0, pois a + b divide $a^{2.0} - b^{2.0} = 1 - 1 = 0$. Suponha que (a + b)|($a^{2n} - b^{2n}$) para algum n natural. Queremos provar que é verdade para n + 1. Escrevamos $a^{2(n+1)} - b^{2(n+1)} = a^{2n+2} - b^{2n+2} = a^2.a^{2n} - b^2.b^{2n} = a^2.a^{2n} - b^2.a^{2n} + b^2.a^{2n} - b^2.b^{2n} = (a^2 - b^2).a^{2n} + b^2.(a^{2n} - b^{2n})$. Como (a + b)|($a^2 - b^2$) e, pela hipótese de indução (a + b)|($a^{2n} - b^{2n}$), decorre que, pela propriedade 2.2.4, (a + b)|($a^{2(n+1)} - b^{2(n+1)}$).

2.2 Algoritmo de Divisão

Um algoritmo é uma sequência finita e bem definida de passos e instruções que, quando executadas, têm como objetivo resolver um problema ou realizar uma tarefa específica. Em outras palavras, é uma receita para resolver um problema ou realizar uma tarefa. Os algoritmos são a base da programação de computadores, pois eles fornecem as instruções que os computadores seguem para realizar tarefas. Algoritmos também são amplamente utilizados em outras áreas, como ciências da computação, engenharia e negócios. Os algoritmos têm características específicas, como entrada, saída e precisão, que os tornam úteis para resolver problemas e realizar tarefas. Além disso, eles devem ser claramente definidos e precisos, para que possam ser entendidos e seguidos de maneira consistente.

O algoritmo da divisão é um método para calcular o quociente e o resto de uma divisão entre dois números. Ele consiste em subtrair sucessivamente o divisor do dividendo, contando quantas vezes o divisor pode ser subtraído até que o dividendo se torne menor que o divisor. O número de vezes que o divisor foi subtraído é o quociente da divisão. Suponha que desejamos dividir o número a por b, $b \neq 0$, e admita que seja possível subtrair b um número q máximo de vezes de tal forma que $0 \leq a$ - $bq < b$. Esta diferença, a - $bq = r$, é chamada de resto e q é o quociente. Dessa última igualdade, concluímos que $a = bq + r$. Por exemplo, queremos dividir 1000 por 12. Podemos subtrair 12 de 1000 um número máximo de 83 vezes, pois $0 \leq 1000$ - $12 \times 83 = 4 < 12$. Nesse exemplo, temos quociente igual a 83 e resto igual a 4, sendo possível escrever $1000 = 12.83 + 4$. De acordo com S. C. Coutinho(COUTINHO, 2014) e A. Hefez(HEFEZ, 2011), podemos escrever o algoritmo de divisão assim:

Algoritmo de divisão
Entrada: inteiros positivos a e b. Saída: inteiros não negativos q e r tais quais $a = bq + r$ e $0 \leq r < b$.
Etapa 1: Comece fazendo $q = 0$ e $r = a$.
Etapa 2: Se $r < b$ escreva o quociente é q e o resto é r e pare; senão vá para a Etapa 3.
Etapa 3: Se $r \geq b$ subtraia b de r, incremente q de 1 unidade e volte à Etapa 2.

Como podemos interpretar essas etapas?

A entrada é fornecida por dois inteiros positivos a e b, enquanto a saída é composta por dois inteiros não negativos q e r, tal que $a = bq + r$ e $0 \leq r < b$. O algoritmo consiste de três etapas:
Etapa 1: Comece fazendo $q = 0$ e $r = a$.

Isso significa que inicialmente o quociente é definido como 0 e o resto é definido como o valor de a.

Etapa 2: Se $r < b$ escreva o quociente é q e o resto é r e pare; senão vá para a Etapa 3.

Se o resto for menor do que b, então a divisão inteira está completa e o quociente e o resto são escritos como q e r, respectivamente. Caso contrário, o algoritmo continua para a próxima etapa.

Etapa 3: Se $r \geq b$ subtraia b de r, incremente q de 1 unidade e volte à Etapa 2.

Se o resto for maior ou igual a b, então b é subtraído do resto, o quociente é incrementado em 1 unidade e o algoritmo volta para a Etapa 2 para continuar a divisão inteira. A cada ciclo de etapas damos o nome de laço. Vejamos um exemplo.
Vamos dividir 19 por 5 seguindo os passos do algoritmo:

Na entrada temos $a = 19$ e $b = 5$ e na saída teremos q e r. Na etapa 1, o quociente começa com $q = 0$ e o resto $r = 19$. Seguindo para a etapa 2, é verificado se $r = 19 < 5 = b$, como não é, segue para a etapa 3. Nesta, é feito o teste se $r = 19 \geq 5 = b$ e, como é, então será subtraído $b = 5$ de $r = 19$, ficando $r = 19$ - $5 = 14$ e será incrementado uma unidade em $q = 0 + 1$. Neste momento, foi concluído o primeiro laço e voltaremos para a etapa 2 para que o novo resto $r = 14$ seja testado. Na etapa 2, é verificado se $r = 14 < 5 = b$ e, como não é, segue para a etapa 3. Nesta, verifica-se que $r = 14 \geq 5 = b$, então será subtraído $b = 5$ de $r = 14$, ficando $r = 14$ - $5 = 9$ e será incrementado uma unidade em $q = 1 + 1 = 2$. Neste momento, fecha-se o segundo laço e voltaremos para a etapa 2 para que o novo resto $r = 9$ seja testado. Na etapa 2, novamente, é verificado se $r = 9 < 5 = b$ e, como não é, segue para a etapa 3. Nesta, verifica-se que $r = 9 \geq 5 = b$, então será subtraído $b = 5$ de $r = 9$, ficando $r = 9$ - $5 = 4$ e será incrementado uma unidade em $q = 2 + 1 = 3$. Neste momento, encerra-se o terceiro laço e voltaremos para a etapa 2 para que o novo resto $r = 4$ seja testado. Na etapa 2, verifica-se que $r = 4 < 5 = b$ e, dessa vez como ele é, o algoritmo escreverá "O quociente é 3 e o resto é 4" e ele para de testar.

O que garante que esse laço terá fim?
Ora, uma sequência de laços nos fornece a seguinte sequência de valores:

Valor inicial	1º laço	2º laço	3º laço	...
a	a - b	a - $2b$	a - $3b$	...

Estamos diante de uma sequência decrescente de inteiros. Sabemos que, entre a e 0, existe uma quantidade finita de inteiros, então essa sequência é finita e, eventualmente, chegará a um valor menor que b. Logo, o algoritmo sempre para.

Podemos perceber que o resultado fornecido pelo algoritmo está dentro das especificações de saída (é perceptível no exemplo dado). Perceba que q e r são obtidos pelo

algoritmo, onde $r = a$ - bq e $r < b$ e, conforme a finalização de cada laço, vamos obtendo restos cada vez menores. Podemos nos perguntar: *Não corre o risco de* $r < 0$*?* A resposta é não! No algoritmo, o processo para no laço de número q. Então, o laço anterior é de número (q - 1) e, nesse caso, o resto é a - $b(q$ - 1) que ainda é maior ou igual a b pois haverá mais um laço para chegar no laço de número q. Sendo assim, a - $b(q$ - 1) $\geq b$ e, no último laço, subtraindo b de ambos os lados da desigualdade a - $b(q$ - 1) - $b \geq b$ - b chegamos a a - $bq \geq 0$, mostrando que o resto $r = a$ - $bq \geq 0$.

Além disso, em $a = bq + r$, os valores de q e r são únicos. Mas o que significa dizer que q e r são únicos? Suponha que dados os números inteiros positivos a e b a duas pessoas, a intenção seja obter q e r da forma que elas quiserem satisfazendo a relação $a = bq + r$ com $0 \leq r < b$. A unicidade do quociente e do resto significa dizer que estas pessoas encontrarão os mesmos valores. Digamos que uma delas tenha encontrado q e r, $0 \leq r < b$ e a outra q' e r', $0 \leq r' < b$. Por enquanto, sabemos apenas que $a = bq + r$ e que $a = bq' + r'$ e o objetivo é mostrar que $q = q'$ e $r = r'$. Sem perda de generalidade, seja $r \geq r'$, e das duas equações obtemos $r = a - bq$ e $r' = a - bq'$. Subtraindo uma da outra, obtemos $r - r' = (a - bq) - (a - bq') = b(q' - q)$. Por outro lado, tanto r como r' são menores do que b e como estamos supondo $r \geq r'$, então $r - r' \geq 0$ e, por sua vez, $0 \leq r - r' < b$. Dessa forma, como $r - r' = b(q' - q)$, concluímos que $0 \leq b(q' - q) < b$. Desta última desigualdade, suponha que q' - $q \geq 1$, e multiplicando ambos os lados da desigualdade por b temos $b(q'$ - $q) \geq b$ e isso é um absurdo pois sabemos que $b(q' - q) < b$. Logo, $0 \leq q'$ - $q < 1$, então q' - $q = 0 \Rightarrow q' = q$. Disto segue, de imediato, que $r - r' = b(q'$ $- q) = b(q' - q') = b \cdot 0 = 0$ e, sendo assim, $r - r' = 0 \Rightarrow r = r'$ e a unicidade fica verificada.

2.3 Máximo Divisor Comum (MDC)

Sejam a e b números naturais diferentes de zero. Definimos o máximo divisor comum (mdc) entre a e b o número d, tal que d satisfaz as seguintes condições:

1) d é um divisor comum de a e b;

2) d é divisível por todo divisor comum de a e b, ou seja, se c é um divisor comum de a e b, então $c|d$.

Então, se d é o mdc de a e b, e c é um divisor comum desses números, tem-se $c|d$ pois d é o maior divisor comum de a e b. Logo $d = c \cdot k$, com k natural e $k \geq 1$ e, multiplicando ambos os lados da última desigualdade por c, temos $d = c \cdot k \geq c$. Isto nos mostra que o máximo divisor comum de dois números é efetivamente o maior dentre todos os seus divisores comuns. Além disso, se d e d' são dois mdc's de um mesmo par de números a e b, então $d \leq d'$ e $d' \leq d$ nos levando a concluir que $d = d'$. Dessa forma, o mdc de dois números é único. Denotamos o mdc de a e b como sendo (a, b). Se a e b são números naturais, tem-se que $(1, a) = 1$, $(0, a) = a$, $(a, a) = a$ e $(a, a \cdot n) = a$. Ainda mais, se

$$a|b \Leftrightarrow (a,b) = a$$

De fato, se $a|b$, então $b = a \cdot k$ com $k \geq 1$ e o $(a, a \cdot k) = a$. Reciprocamente, se $(a,b) = a$, segue-se que $a|b$. Vejamos como Euclides prova a existência do mdc de dois números.

(Lema de Euclides). Sejam a, b, $n \in \mathbb{N}$ com $a < na < b$. Se existe $(a, b - na)$, então (a,b) existe e $(a,b) = (b, b - na)$.
Demonstração: Seja $d = (a, b - na)$. Como $d|a$ e $d|(b - na)$, segue que, pela propriedade 2.2.4, $d|na$ e $d|(b - na + na) = b$. Logo, d é um divisor comum de a e b. Agora, conforme a condição 2)*, imagine que c seja um divisor comum de a e b. Logo, $c|a \Rightarrow c|na$ e, como $c|b$, pela propriedade 2.2.4, $c|(b - na)$ e, portanto, $c|d$. Tudo isso nos prova que $d = (a,b)$.*

(Algoritmo de Euclides). O algoritmo de Euclides é um método iterativo para o cálculo do máximo divisor comum (MDC) de dois números e, também, é conhecido como o método das divisões sucessivas. Nas escolas, entre os alunos, é conhecido como o método do jogo da velha.
Dados dois naturais a e b, tal que $1 < b < a$ e $b \nmid a$, aplicaremos sucessivamente o algoritmo da divisão para obter a sequência de igualdades:

$$\begin{array}{ll}
a = bq_1 + r_1 & \text{onde } 0 \leq r_1 < b \\
b = r_1q_2 + r_2 & \text{onde } 0 \leq r_2 < r_1 \\
r_1 = r_2q_3 + r_3 & \text{onde } 0 \leq r_3 < r_2 \\
r_2 = r_3q_4 + r_4 & \text{onde } 0 \leq r_4 < r_3 \\
... & ... \\
r_{n-2} = r_{n-1}q_n + r_n & \text{onde } 0 \leq r_n < r_{n-1} \\
r_{n-1} = r_nq_{n+1} &
\end{array}$$

Este procedimento não terá interações indefinidamente, se assim fosse, teríamos uma sequência infinita de números naturais $a > r_1 > r_2 > r_3 > ...$ pois, como a e os $r_{i's}$ são elementos de um subconjunto não vazio dos naturais, então ele terá um elemento mínimo. Dessa forma, para algum n, teremos $r_n|r_{n-1}$. Temos, então, o $mdc(a,b) = r_n$, sendo r_n o último resto não nulo no processo de divisão anterior. De fato, pois sejam a e b números naturais e (a,b) o mdc desses números. Então,

$(a,b) = (bq_1 + r_1, b)$ e pelo Lema de Euclides, teremos

$(a,b) = (bq_1 + r_1$ - $bq_1, b)$

$(a,b) = (r_1, b)$ e por sua vez $b = r_1q_2 + r_2$

$(a,b) = (r_1, r_1q_2 + r_2)$

$(a, b) = (r_1, r_1q_2 + r_2 \text{ - } r_1q_2)$

$(a, b) = (r_1, r_2)$

$(a, b) = (r_2q_3 + r_3, r_2)$

$(a, b) = (r_2, r_2q_3 + r_3 \text{ - } r_2q_3)$

$(a, b) = (r_2, r_3)$

...

$(a, b) = (r_{n-2},\ r_{n-1})$ e como $r_{n-2} = r_{n-1}q_n + r_n$

$(a, b) = (r_{n-1}q_n + r_n, r_{n-1})$

$(a, b) = (r_{n-1}, r_{n-1}q_n + r_n - r_{n-1}q_n)$

$(a, b) = (r_{n-1},\ r_n) = r_n$

O algoritmo acima pode ser escrito, na prática, da forma a seguir. Eis o motivo, pelo qual, os alunos conhecerem o método como jogo da velha por fazer uma intertextualidade com o famoso passa-tempo. Para iniciar, façamos a divisão $a = bq_1 + r_1$ escrevendo conforme o esquema:

	q_1	
a	b	
r_1		

Continuaremos fazendo a divisão $b = r_1q_2 + r_2$ ainda no esquema.

	q_1	q_2	
a	b	r_1	
r_1	r_2		

Vamos prosseguindo, enquanto possível, até a obtenção de um r_n divisível por r_{n-1}.

	q_1	q_2	q_3	...	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	...	r_{n-2}	r_{n-1}	$r_n = (a, b)$
r_1	r_2	r_3	r_4	...	r_n	0	

Vejamos o exemplo: Calculemos o mdc de 657 e 306.

	2	6	1	4
657	306	45	36	9
45	36	9	0	

Observando, no exemplo acima, o algoritmo de Euclides nos fornece os restos:
$9 = 45 - 1 \cdot 36$
$36 = 306 - 6 \cdot 45$
$45 = 657 - 2 \cdot 306$

Substituindo esses restos, temos:
$9 = 45 - 1 \cdot (306 - 6 \cdot 45) = 7 \cdot 45 - 306 = 7 \cdot (657 - 2 \cdot 306) - 306 = 7 \cdot 657 - 15 \cdot 306$

Temos, então, que
$(657, 306) = 9 = 7 \cdot 657 - 15 \cdot 306$

Perceba que conseguimos, por meio do Algoritmo de Euclides, escrever de trás para frente, o $(657, 306) = 9$ como um múltiplo de 657 menos um múltiplo de 306. O Algoritmo de Euclides nos fornece um meio prático de escrever o mdc de dois números por meio de uma diferença entre dois múltiplos desses números.

2.4 O Teorema de Bèzout

Etienne Bèzout (1730-1783) foi um matemático francês que fez contribuições significativas em diversas áreas da matemática, incluindo álgebra, geometria e teoria dos números. Ele é mais conhecido por seus trabalhos na teoria dos números, em particular pelo Teorema de Bèzout, que estabelece uma relação entre os múltiplos e o máximo divisor comum de dois números inteiros. Bèzout também contribuiu para o estudo das equações polinomiais e a teoria das curvas algébricas. Ele foi eleito para a Academia Francesa de Ciências em 1768 e serviu como professor na Escola Real Militar em Paris.

O Teorema de Bèzout, também conhecido como identidade de Bèzout, afirma que para quaisquer dois números inteiros a e b, existem inteiros x e y tais quais $ax + by = (a, b)$, onde (a, b) é o máximo divisor comum de a e b. Em outras palavras, o teorema de Bèzout garante que é sempre possível expressar o máximo divisor comum de dois números inteiros como uma combinação linear deles, utilizando coeficientes inteiros.

Teorema de Bèzout: Sejam a, $b \in \mathbb{Z}^*$, existem $x, y \in \mathbb{Z}$, tais quais, $ax + by = (a, b)$, onde (a, b) é o mdc de a e b.
Demonstração: Seja o conjunto $X = \{ax + by / x, y \in \mathbb{Z}\}$ *e o subconjunto* $S = X \cap \mathbb{N}^* \subseteq \mathbb{N}$. *S é não vazio, pois, tomando* $x = a$ *e* $y = b$, *temos* $ax + by = a \cdot a + b \cdot b = a^2 + b^2 \geq 2$. *Sendo S um subconjunto dos naturais, sabemos que existe um elemento mínimo e, digamos, que seja* $d \geq 1$. *Se* $d \in S$, *então* $d = ax_0 + by_0$. *Se* $d = (a, b)$, *então d satisfaz as duas condições abaixo:*

1) $d|a$ *e* $d|b$;

2) *Se* $c|a$ *e* $c|d \Rightarrow c|d$.

Em 1), *suponha por absurdo, que* $d|a$ *e* $d|b$ *é falso, isto é,* $d \nmid a$ *ou* $d \nmid b$. *Sem perda de generalidade, suponha que* $d \nmid a$. *Então,* $a = dq + r$, *onde* $1 \leq r < d$, *e, por conseguinte,*

$r = a$ - dq. Perceba que $r \in S$, pois r pode ser escrito na forma $r = ax + by$. De fato, substituindo $d = ax_0 + by_0$, temos $r = a$ - $dq = a$ - $q(ax_0 + by_0) = a(1$ - $x_0q) + b(-y_0q)$. Mas $r < d$ é absurdo, uma vez que, d é o menor elemento de S. Logo, $d|a$ e $d|b$.

Em 2), se $c|a$ e $c|b$, então c divide qualquer combinação linear de a e b, ou seja, $c|(ax_0 + by_0) = d$. Dessa forma, $c|d$.■

2.5 Os Números Primos

Os números primos desempenham um papel fundamental na matemática. Advindos de uma definição simples, tais números, em seu nome, trazem uma derivação do latim *Primus* que significa primeiro, geram todos os outros números do nosso sistema de numeração através da operação de multiplicação, mas não podem ser gerados por nenhum outro. Um número natural maior do que 1 é primo quando possui, apenas, dois divisores. A saber, 1 e ele mesmo. Sendo assim, 7 é primo porque só possui o 1 e ele próprio como divisores, mas o 14 não pois, além de ter o 1 e ele mesmo como divisores ainda possui o 7. A esses números não primos chamamos de compostos. O número 1, por obviedade, não é primo nem composto. O 2 é único número primo par, uma vez que, todo número par é na forma $2n$, $n \in \mathbb{N}$, e, além de ter 1 e ele mesmo como divisores também possui, no mínimo, o 2 como divisor. Podemos estender esse conceito e tomar dois ou mais números, não necessariamente primos, e dizer que são primos entre si ou co-primos quando o único divisor comum é o número 1. A exemplo, os pares 18 e 25 ou a tríade 18, 25 e 29. Podemos indagar:

"Os números primos são finitos ou infinitos?"

A seguir, apresentamos a demonstração da infinitude dos números primos conhecida como prova por contradição ou redução ao absurdo. Segundo (SINGH, 2016), esta é a forma como Euclides abordou o assunto em uma linguagem atual:

Supondo que o número de primos seja finito e que todos esses primos tenham sido reunidos em uma lista: $p_1, p_2, p_3, \cdots, p_n$, podemos explorar as consequências dessa declaração multiplicando todos os primos dessa lista e incrementando 1, o que cria um novo número: $N = p_1 \times p_2 \times p_3 \times \cdots \times p_n + 1$. Esse novo número N pode ser ou não ser um primo, mas, de qualquer forma, contradiz a afirmação inicial, pois, se N é primo, então não se encontra na lista original. Por consequência, a afirmação de que temos uma lista completa é falsa; se N não é primo, então deve ter divisores primos. Esses divisores devem ser novos primos, pois os primos contidos na lista original produzirão o resto 1 se dividir N. Portanto, mais uma vez, a afirmação de que temos uma lista completa é falsa.

Sendo assim, de fato, a lista de primos é infinita!

Se temos p e q primos e a um número natural, podemos analisar dois fatos:
I) Se $p \mid q$ (p divide q), como q é primo, então decorre que $p = 1$ ou $p = q$. Como p também é primo, então segue que $p = q$.
II) Se $p \nmid a$ (p não divide a), então $(p, a) = 1$. De fato, pois se $(p, a) = d$, então d divide a e divide p. Como p é primo então só resta $d = 1$.

Ainda sobre, considere a, b e p naturais não nulos, com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$. Para tal, basta provar que, se $p \mid ab$ e $p \nmid a$, então $p \mid b$. Mas, se $p \mid ab$, então $ab = pc$ e, dessa forma, se $p \nmid a$ então $(a, p) = 1$ e existem m e n, naturais, tais quais $an - pm = 1$. Multiplicando, ambos os lados, por b ficaremos com $abn - bpm = b$. Agora, basta substituir nesta última identidade ab por pc e ficaremos com $pcn - bpm = b$ que, evidenciando p, temos $p(cn - bm) = b$, na qual $p \mid b$.

Os números primos estão envolvidos diretamente no Teorema Fundamental da Aritmética e enunciá-lo será importante no decorrer do nosso trabalho.

(Teorema Fundamental da Aritmética) Todo número natural maior do que 1 ou é primo ou se escreve de forma única, a não ser pela ordem, como um produto de primos.

Demonstração: Usaremos indução. Se $n = 2$, o resultado fica verificado. Suponha que o resultado seja válido para todo natural menor do que n e temos que provar que vale para n. Se n é primo, nada temos a demonstrar. Vamos supor que n é composto, então existem n_1 e n_2 tais quais $n = n_1 \cdot n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, existem primos $p_1, p_2, \ldots, p_s$ e $q_1, q_2, \ldots, q_r$ tais quais $n_1 = p_1 \cdot p_2 \cdot \cdots \cdot p_s$ e $n_2 = q_1 \cdot q_2 \cdot \cdots \cdot q_r$. Sendo assim, $n = p_1 \cdot p_2 \cdot \cdots \cdot p_s \cdot q_1 \cdot q_2 \cdot \cdots \cdot q_r$. Sabemos que essa forma é única então, para provar sua unicidade, suponha que $n = p_1 \cdot p_2 \cdot \cdots \cdot p_s = q_1 \cdot q_2 \cdot \cdots \cdot q_r$. Podemos imaginar que $p_1 \mid q_1 \cdot q_2 \cdot \cdots \cdot q_r$, mas como os $q_{i's}$ são primos, então, $p_1 = q_i$, para algum i podemos supor que seja $p_1 = q_1$ (propriedade forte dos números primos). Consecutivamente, reorganizando e, portanto, $p_2 \cdot \cdots \cdot p_s = q_2 \cdot \cdots \cdot q_r$. Como $p_2 \cdot \cdots \cdot p_s < n$, a hipótese de indução nos leva a $s = r$ e os p_j e q_i são iguais aos pares. ■

3 Teoremas para o RSA

3.1 Obtenção de Restos

Obter restos de divisões, em até certo ponto, é uma tarefa fácil. Utilizando o algoritmo de Euclides e com o conhecimento de operações elementares, como a de multiplicação, qualquer pessoa pode chegar ao resto de uma divisão. Veja os exemplos:

85	35	127	35
(15)	2	(22)	3

Pelo algoritmo de Euclides sabemos que $85 = 2.35 + 15$ e $127 = 3.35 + 22$ pois, de modo geral, $D = q.d + r$, onde D é o dividendo, d é o divisor, q é o quociente e r é o resto sendo este $0 \leq r < d$. Se $r = 0$, temos uma divisão exata que equivale a dizer que o dividendo (D) é um múltiplo do divisor (d), ou seja, $D = q.d$. Vamos enunciar alguns teoremas que facilitarão o processo, mas também utilizaremos a calculadora para mostrar que é possível qualquer pessoa criptografar bastando, apenas, conhecer o método de criptografia RSA e a obtenção de restos. Nos exemplos anteriores obtemos restos 15 e 22 nas divisões de 85 e 127 por 35, respectivamente. Qual seria o resto da divisão da soma $85 + 127 = 212$ por 35?

212	35
(2)	6

Uma vez sabendo dos restos da divisão de 85 e 127 por 35 fica mais fácil chegar ao resto da divisão da soma $85 + 127 = 212$. Perceba que,

$212 = 85 + 127$

$212 = (2.35 + 15) + (3.35 + 22)$

$212 = (2.35 + 3.35) + (15 + 22)$

$212 = (2 + 3).35 + 37 = 5.35 + 37$

Observe que a soma é formada por um múltiplo de 35 (5.35) mais a soma dos restos 37 $(15 + 22)$ e que este deixa resto 2 ao ser dividido por 35. Ou seja, uma vez sabido dos restos das divisões das duas parcelas por 35, o resto da soma $85 + 127$ por 35 é igual ao resto da divisão da soma desses restos por 35. O teorema a seguir generaliza a situação e pode ser estendido para quantas parcelas tivermos.

Teorema 1. Seja a, b e n, números naturais. Se r_a e r_b são os restos das divisões de a por n e de b por n, respectivamente, então o resto da divisão de $a + b$ por n é igual

ao resto da divisão de $r_a + r_b$ por n.
Demonstração: Seja $a = n.q_a + r_a$ *e* $b = n.q_b + r_b$, *com* $0 \leq r_a, r_b \leq n$, *logo* $a + b = n.q_a + r_a + n.q_b + r_b = n.(q_a + q_b) + r_a + r_b$ (1)
E seja r *o resto da divisão de* $r_a + r_b$ *por* n. *Então, podemos escrever esta soma como sendo* $r_a + r_b = n.q + r$, $0 \leq r \leq n$, *e substituindo esta soma em* (1), *temos:*
$a + b = n.(q_a + q_b) + r_a + r_b = n.(q_a + q_b) + n.q + r$
$a + b = n(q_a + q_b + q) + r$. ■

Considere que r_i, com $i \in \mathbb{N}$ e $i \geq 1$ e, ainda $0 \leq r_i \leq n$, sejam os restos das divisões de a_i por n. Seja $a_i = n.q_i + r_i$ e, fazendo a soma de todos esses $a_{i's}$, temos:

$$a_1 + a_2 + a_3 + \cdots + a_k = n.q_1 + r_1 + n.q_2 + r_2 + n.q_3 + r_3 + \cdots + n.q_k + r_k \Leftrightarrow$$
$$a_1 + a_2 + a_3 + \cdots + a_k = n.(q_1 + q_2 + q_3 + \cdots + q_k) + (r_1 + r_2 + r_3 + \cdots + r_k)\ (1).$$

Seja r o resto da divisão de $r_1 + r_2 + r_3 + \cdots + r_k$ por n. Então, podemos escrever esta soma como sendo $r_1 + r_2 + r_3 + \cdots + r_k = n.q + r$, $0 \leq r \leq n$, e substituindo esta soma em (1), temos:

$$a_1 + a_2 + a_3 + \cdots + a_k = n.(q_1 + q_2 + q_3 + \cdots + q_k) + n.q + r \Leftrightarrow$$
$$a_1 + a_2 + a_3 + \cdots + a_k = n.(q_1 + q_2 + q_3 + \cdots + q_k + q) + r.$$

Dessa forma, o Teorema 1 é válido para k parcelas.

Vejamos, agora, um exemplo que será bem frequente no método de criptografia RSA, o resto da divisão de produtos entre números.
Sabendo que o resto da divisão de 1023 por 20 é 3, pois $1023 = 20.q + 3$ e o resto da divisão de 247 por 20 é 7, pois $247 = 20.t + 7$, qual o resto da divisão $1023 \times 247 = 252681$ por 20?

Fazendo $1023 \times 247 = (20.q + 3).(20.t + 7)$ e desenvolvendo a distributividade, temos:
$1023 \times 247 = 20q.20t + 20q.7 + 3.20t + 3.7$
$1023 \times 247 = 20(20qt + 7q + 3t) + 21$

Perceba que, ao multiplicar 1023 por 247 temos, como resultado, um múltiplo de 20 mais o produto dos restos (21). É possível reescrever essa identidade:
$1023 \times 247 = 20(20qt + 7q + 3t) + 21 = 20(20qt + 7q + 3t) + 20 + 1$ que equivale a $1023 \times 247 = 20(20qt + 7q + 3t + 1) + 1$.

E assim, o resto da divisão do produto $1023 \times 247 = 252681$ por 20 é 1, exatamente o resto da divisão do produto dos restos por 20. Com essa premissa, podemos determinar o resto da divisão de $1027^2 = 1027 \times 1027$ por 20. Como 1027 deixa resto 7 na divisão por

20, então 1027^2 deixará resto igual ao resto da divisão de 7^2 por 20. Logo, $7^2 = 49$, deixa resto 9. O resto da divisão de 1027^2 por 20 é 9.
O teorema abaixo formaliza o nosso exemplo e estende para k fatores.

Teorema 2. Sejam os naturais r_1, r_2, ..., r_k os restos das divisões de a_1, a_2, ..., a_k por n, respectivamente, com $k \in \mathbb{N}$. O resto da divisão de $a_1 \times a_2 \times ... \times a_k$ por n é igual ao resto da divisão de $r_1 \times r_2 \times ... \times r_k$ por n.

Demonstração: Primeiramente, mostremos para dois naturais.
Sejam $a_1 = n.q_1 + r_1$ *e* $a_2 = n.q_2 + r_2$ *e* $0 \leq r_1, r_2 < n$ *naturais. Então,*
$a_1 \times a_2 = (n.q_1 + r_1).(n.q_2 + r_2)$
$a_1 \times a_2 = n^2 q_1 q_2 + nq_1 r_2 + nq_2 r_1 + r_1 r_2 = n(nq_1 q_2 + q_1 r_2 + q_2 r_1) + r_1 r_2$
Considere $r_1 r_2 = n.m + r$, *com* $0 \leq r < n$, *que substituindo na igualdade acima temos:*
$a_1 \times a_2 = n(nq_1 q_2 + q_1 r_2 + q_2 r_1) + n.m + r$
$a_1 \times a_2 = n(nq_1 q_2 + q_1 r_2 + q_2 r_1 + m) + \boldsymbol{r}$
Sendo $nq_1 q_2 + q_1 r_2 + q_2 r_1 + m = p$ *um natural. Então,* $a_1 \times a_2 = np + r$ *deixa resto* r *na divisão por* n. *Dessa forma, o resto da divisão do produto de dois naturais por* n *é igual ao resto da divisão do produto dos restos por* n.

Agora, vamos estender para k fatores:

Considere o produto $a_1 \times a_2 \times ... \times a_{k-1} \times a_k$. *Como os* $a_{i's}$ *são números naturais e a multiplicação é uma operação fechada no conjunto dos números naturais, temos que* $a_1 \times a_2 \times ... \times a_{k-1}$ *também é um número natural e pode ser escrito na forma* $a_1 \times a_2 \times ... \times a_{k-1} = nq + r_{k-1}$, *onde* $0 \leq r_{k-1} = a_1 \times a_2 \times ... \times a_{k-1} - nq < n$. *Sendo assim,* $a_1 \times a_2 \times ... \times a_{k-1} \times a_k = (nq + r_{k-1}).a_k$. *Sabendo que* $a_k = nq_k + r_k$, *então* $(nq + r_{k-1}).a_k = (nq + r_{k-1}).(nq_k + r_k) = n(qq_k + qr_k + q_k r_{k-1}) + r_{k-1}.r_k$. *Seja* r *o resto da divisão de* $r_{k-1}.r_k$ *por* n. *Então podemos escrever esse produto como sendo* $r_{k-1}.r_k = np + r$, $p \in \mathbb{N}$, *e substituindo na igualdade anterior temos,* $(nq + r_{k-1}).a_k = n(qq_k + qr_k + q_k r_{k-1} + p) + r$. ■

Corolário. Em particular, se r_a é o resto da divisão de a por n, então o resto da divisão de a^k por n é igual ao resto da divisão de $(r_a)^k$ por n.

Demonstração: Sejam a, n, q *e* r_a, *números naturais, tais quais,* $a = nq + r_a$ *e o natural* $k > 1$. *Fazendo* a^k, *temos* $a^k = (nq + r_a)^k$ *na qual podemos desenvolver o binômio:*

$$a^k = \binom{k}{0}(nq)^k + \binom{k}{1}(nq)^{k-1} \cdot r_a + \binom{k}{2}(nq)^{k-2} \cdot (r_a)^2 + \ldots + \binom{k}{k-1}(np)^1 \cdot (r_a)^{k-1} + \binom{k}{k}(r_a)^k$$

Perceba que podemos evidenciar n:

$a^k = n[\binom{k}{0}n^{k-1}\cdot q^k + \binom{k}{1}n^{k-2}q^{k-1}\cdot r_a + \binom{k}{2}n^{k-3}q^{k-2}\cdot (r_a)^2 + \ldots + \binom{k}{k-1}n^0 q^1 \cdot (r_a)^{k-1}] + \binom{k}{k}(r_a)^k$

Dessa forma, a^k é um múltiplo de n mais $(r_a)^k$, uma vez que $\binom{k}{k} = 1$, e podemos reescrever nossa igualdade como sendo $a^k = n.q_1 + (r_a)^k$. Considere $r_a = n.p + r$, com p natural e $0 \leq r < n$, substituindo temos $a^k = n.q_1 + (n.p + r)^k$ que, pelo desenvolvimento do binômio anterior, sabemos que $(n.p + r)^k = n.q_2 + r^k$. Então, $a^k = n.q_1 + n.q_2 + r^k$ e como $q_1 + q_2 = q_3$, temos $a^k = n.q_3 + r^k$. Sendo assim, uma vez sabendo r_a, o resto da divisão de a^k por n é igual ao resto da divisão de $(r_a)^k$ por n. ■

Vejamos um exemplo:

Obtenha o resto da divisão 13^7 **por** 35.

Fazendo $13^2 = 169$, percebemos que ele deixa resto 29 na divisão por 35 pois $169 = 4\cdot 35 + 29$. Como $13^7 = (13^2)^3.13$, o resto da divisão 13^7 por 35, fazendo o uso do Corolário, é equivalente ao resto de $(29)^3.13$, e assim, podemos escrever como sendo $29^2.29.13$. Sabendo que $29^2 = 841$ deixa resto 1 na divisão por 35 pois $841 = 35.24 + 1$, então apliquemos mais uma vez o Corolário e o resto de $29^3.13 = 29^2.29.13$ por 35 é equivalente ao resto de $1.29.13 = 377$ que deixa resto 27 na divisão por 35. Então, o número 13^7 deixa resto na divisão por 35 igual a 27.

3.2 Utilização da Calculadora na Obtenção de Restos

O uso da calculadora deve ser estimulado pelo professor em sala de aula desde que o estudante já domine os algoritmos das operações. Então, podemos utilizar a calculadora no auxílio da obtenção do resto da divisão de números grandes.

Teorema 3. Sejam n e d números naturais. Para encontrar o resto da divisão de n por d, pela calculadora, basta dividir n por d, depois subtrair a parte inteira e, em seguida, multiplicar por d.

Demonstração: Seja $n = d \cdot q + r$, com $r < d$. Façamos, na calculadora, a divisão de n por d e teremos:

$$\frac{n}{d} = \frac{dq}{d} + \frac{r}{d} = q + \frac{r}{d} \text{ onde } q \text{ é a parte inteira e } \frac{r}{d} \text{ é parte decimal pois } \frac{r}{d} < 1.$$

Logo, subtraindo a parte inteira q de $q + \frac{r}{d}$, teremos $q + \frac{r}{d} - q = \frac{r}{d}$. Agora, multipliquemos esse resultado por d e encontraremos o resto da divisão de n por d. E segue, $\frac{r}{d} \times d = \boldsymbol{r}$. ■

Vejamos alguns exemplos:

Qual o resto da divisão 18.435 por 141?

Dividindo, na calculadora, obtemos 130,7446808510638. Subtraiamos a parte inteira 130 e ficamos com 0,7446808510638. Agora, multipliquemos pelo divisor 141 e obteremos o resto: 0,7446808510638 x 141 = 105.

O resto da divisão de 18.435 por 141 é igual a 105.

Obtenha o resto da divisão 13^7 por 35.

Para encontrar a potência de 13^7, na calculadora científica, primeiramente, teclamos o 13, depois a tecla x^y, depois o expoente 7 e a tecla de igualdade (=) encontrando 62.748.517. Divida este resultado por 35 e encontraremos $1.792.814,771428571428571428571428$. Subtraindo a parte inteira 1.792.814, encontraremos $0,771428571428571428571428$. Agora, basta multiplicar esse decimal por 35 e encontraremos o resto: $0,771428571428571428571428 \times 35 = 27$.

O resto da divisão 137 por 35 é igual a 27.

É evidente que os decimais encontrados na tela da calculadora têm uma limitação de dígitos devido ao display, mas a memória tem a função de preservar a operação. Sendo assim, se a sua calculadora limita o número de dígitos da parte decimal (assim como o excel), então esta função pode ser utilizada.

4 O Método de Criptografia RSA

4.1 Codificando uma Mensagem pelo Método RSA

Partiremos da escolha da palavra que queremos codificar. Vamos escolher a palavra **RECIFE**. Antes de iniciar o processo, por razões óbvias, toda mensagem seja ela uma letra, número ou um caractere tem que ser submetido a uma pré-codificação. Utilizaremos a tabela de pré-codificação abaixo:

Tabela 3 – Pré-codificação do alfabeto

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

Fonte: Feita pelo autor

A escolha em começar essa pré-codificação pelo 10 ou 11 é arbitrária, ficando a cargo do leitor, se assim desejar, alterar a tabela e começar por outro número. Deve-se, apenas, levar em consideração a exigência de todas as letras e caracteres estarem associados a números com a mesma quantidade de dígitos para evitar confusões futuras na decodificação. Por exemplo, se começássemos a pré-codificação do 1, então, no número 12 não saberíamos dizer se temos AB ou a letra L, letra esta que está na décima segunda posição. Outro fato importante é, no caso de codificação de frases, temos os espaços em branco e a esses colocamos 99. Na frase, **"Recife é linda"**, a pré-codificação nos levará para a sequência 271412181514**99**14**99**2118231310. Dessa forma, a mensagem a ser codificada **(Recife)** será representada pelo número **271412181514**. O próximo passo é a determinação do par de números **(n, e)**, **Chave de Codificação do Sistema RSA**, com n = p·q, sendo p e q números primos e o **mdc [e, (p - 1).(q - 1)] = 1**, sendo **e** qualquer número que satisfaça este mdc. Para efeito de praticidade, utilizaremos os primos $\mathbf{p = 5}$ e $\mathbf{q = 7}$, gerando a Chave de Codificação $\mathbf{n = 35}$ e $\mathbf{e = 7}$. O processo de criptografia requer alguns critérios que devem ser seguidos e um deles é: separar a mensagem a ser criptografada em blocos, não importando se serão blocos de um, dois, três ou mais algarismos ou até mesmo tamanhos variados, exige-se que cada bloco não seja maior do que n. Tratando-se do nosso exemplo, para uma chave pequena, ficamos limitados a blocos de no máximo dois dígitos, mas, quando os primos são muito grandes gerando uma imensa chave, fica evidente a liberdade de tomarmos esses blocos de tamanhos variados. Outro critério é não iniciar os blocos por 0 e, **MUITO IMPORTANTE** é, uma vez os blocos codificados, não

poderemos juntá-los e formar um longo número. Se isso for feito, será impossível decodificar a mensagem. Dessa forma, os blocos a serem codificados são **27-14-12-18-15-14**.

Vamos, agora, codificar cada bloco por vez e, para isso, o método impõe uma regra: devemos pegar cada bloco **b** a ser codificado e elevar ao número natural **e**, obtendo o resto **a** da divisão por **n**, onde **a** será a codificação do bloco **b**. Ou seja, em termos matemáticos, nós queremos obter:

$$b^e = n \cdot q + \mathbf{a} \text{ com } 0 \leq a < n$$

Essa é a regra de codificação do método RSA!

Tomaremos o primeiro bloco 27, e assim, vamos obter o resto da divisão de 27^7 por 35.

Para um melhor aprendizado, sugerimos inicialmente, que o aluno faça manualmente esses passos e após obter habilidade suficiente, se necessário, utilize nas próximas vezes uma calculadora para efeito de praticidade e possibilitando ao estudante efetuar diretamente as potências. Fica a cargo do professor estabelecer um momento avaliativo sem o uso da calculadora e depois uma nova avaliação permitindo tal uso.

Então, tome $27^7 = (27^2)^3 \cdot 27$. Como $27^2 = 729$ deixa resto 29 na divisão por 35, nos apoiando no Corolário, podemos procurar o resto $(29)^3 \cdot 27$ que, automaticamente podemos fatorar $29^2 \cdot 29 \cdot 27$. Sabendo que $29^2 = 841$ e este deixa resto igual a 1 na divisão por 35 $(841 = 24 \cdot 35 + 1)$, podemos encontrar, nos apoiando no Teorema 2, o resto da divisão por 35 do número $1 \cdot 29 \cdot 27 = 783$ que deixa resto 13 na divisão por 35. Dessa forma, o número 27^7 deixa resto 13 na divisão por 35.
Logo, o primeiro bloco 27, criptografado é igual a 13

Vamos encriptar o segundo bloco 14 e procurar o resto da divisão de 14^7 por 35. Fatorando de maneira análoga, $(14^2)^3 \cdot 14$, como $14^2 = 196$ deixa resto 21 na divisão por 35 $(196 = 5 \cdot 35 + 21)$, usando o Corolário, podemos procurar o resto da divisão de $(21)^3 \cdot 14$ por 35 que, por sua vez, podemos escrever $21^2 \cdot 21 \cdot 14 = 441 \cdot 294$. Perceba que 441 e 294 deixam resto 21 e 14, respectivamente, na divisão por 35. Então, usando o Teorema 2, procuremos o resto da divisão de $21 \cdot 14 = 294$ por 35. Este deixa resto 14 na divisão por 35. Dessa forma, o número 14^7, ao ser dividido por 35, deixa resto 14.
Logo, o segundo bloco 14 criptografado é igual a 14.

Tomando o terceiro bloco 12, vamos buscar o resto da divisão de 12^7 por 35. Fatorando para uma potência mais simples, temos $12^7 = (12^2)^3 \cdot 12$. Como $12^2 = 144$ deixa

resto 4 na divisão por 35, utilizando o Corolário, vamos buscar o resto da divisão de $(4)^3 \cdot 12 = 768$ por 35 e obtemos 33.
Logo, o terceiro bloco 12 criptografado é igual a 33.

Agora, tome o quarto bloco 18 e vamos procurar o resto da divisão de 18^7 por 35. Fatorando $18^7 = (18^2)^3 \cdot 18$ e sabendo que $18^2 = 324$ deixa resto 9 na divisão por 35, mais uma vez usando o Corolário, vamos buscar o resto da divisão $(9)^3 \cdot 18$ por 35. Nesse caso, de maneira alternativa ao que estamos fazendo, podemos efetuar esse produto sendo igual a 13.122 e obtemos resto 32 na divisão por 35. Dessa forma, o resto da divisão de 18^7 por 35 é igual a 32.
Logo, o quarto bloco 18 criptografado é igual a 32.

Tomando o penúltimo bloco 15, vamos procurar o resto da divisão de 15^7 por 35. Como $15^7 = (15^2)^3 \cdot 15$, e sabendo que $15^2 = 225$ deixa resto 15 na divisão por 35, fazendo uso do Corolário, podemos buscar o resto da divisão de $(15)^3 \cdot 15$ e, por sua vez, $15^2 \cdot 15^2$ e como já sabemos que 225 deixa resto 15 na divisão por 35, então esse produto pode ser trocado por $15 \cdot 15 = 225$, com base no Teorema 2, que deixa resto 15 na divisão por 35. Dessa forma, 15^7 deixa resto 15 na divisão por 35.
Logo, o quinto bloco 15 criptografado é igual 15.

Chegamos ao último bloco 14 que já foi criptografado.

Sendo assim, os blocos **27-14-12-18-15-14** serão transmitidos criptografados sob os blocos **13-14-33-32-15-14.**

4.2 Decodificando uma Mensagem Codificada em RSA

Mostraremos como fazer o processo inverso, a decodificação de mensagem, utilizando como exemplo a mensagem encriptada anteriormente, no caso, **13-14-33-32-15-14**. Para decodificar precisaremos de uma chave de decodificação e essa chave é o par **(n, d)**, onde **d** é o número que multiplicado por **e** deixará resto 1 na divisão por **[(p - 1)(q - 1)]** sendo **e** expoente e **p, q** primos utilizados no processo de codificação. Ou seja, temos que encontrar o **d** que resolva a identidade $e \cdot d = t \cdot [(p-1)(q-1)] + 1$, onde t é um número natural, o quociente da divisão de $(e \cdot d)$ por $[(p-1)(q-1)]$. Como $(d \cdot e)$ deixa resto 1 na divisão por $(p-1)(q-1)$, então d é chamado de inverso de e com respeito à $(p-1)(q-1)$. Lembrando que, no exemplo que fizemos a codificação da palavra RECIFE, os primos escolhidos foram o p = 5 e q = 7 gerando a chave n = 35 e e = 7. Então, como d é o inverso de e, devemos resolver a seguinte identidade:

$$7 \cdot d = t \cdot [(5-1)(7-1)] + 1$$
$$7 \cdot d = t \cdot (24) + 1$$

Estamos procurando o primeiro número natural que multiplicado por 7 dê resto 1 na divisão por 24. Fazendo uma varredura para alguns naturais, começando de 1, percebemos que essa resposta é o 7 pois $7 \cdot 7 = 49 = 2 \cdot (24) + 1$. Logo, d = 7. Uma vez estabelecido o valor de d, vamos usar uma regra similar a que nós utilizamos na codificação:

$$a^d = k \cdot n + b$$

Onde **n** é a chave de encriptação que utilizamos para codificar, **b (mensagem original)** será o resto da divisão de a^d por **n** e, por conseguinte, a decodificação da mensagem **a (mensagem codificada)**. Precisamos esclarecer um ponto facilitador: quando falamos em "Encontrar a solução da identidade $a^d = k \cdot n + b$", significa nos limitar, apenas, a encontrar o resto b da divisão, não nos importando qual valor assumido por k, uma vez que, o objetivo do nosso trabalho é codificar e decodificar em RSA e o método exige a obtenção de restos.

Sendo assim, para o primeiro bloco 13, vamos encontrar a solução da igualdade $13^7 = k_1 \cdot 35 + b$ que é equivalente a procurar o resto da divisão de 13^7 por 35. Como $13^7 = (13^2)^3.13$, sabemos que $13^2 = 169$ e deixa resto 29 na divisão por 35 pois $169 = 4 \cdot 35 + 29$. Fazendo o uso do Corolário, podemos procurar o resto, na divisão por 35, de $(29)^3 \cdot 13$ que pode ser reescrito, para facilitar, como $(29)^2 \cdot 29 \cdot 13$. A potência $29^2 = 841$ deixa resto 1 na divisão por 35 e o produto $29 \cdot 13 = 377$ deixa resto 27 na divisão por 35. Então, se apoiando no Teorema 2, $1.27 = 27$ que deixa resto 27 na divisão por 35. Dessa forma, 13^7 deixa resto 27 na divisão por 35.

Logo, o bloco 13 decodificado é igual a 27.

Uma maneira de estimular o pensamento do estudante a buscar uma forma prática, uma vez que, não estamos usando a calculadora, é pensar que a potência 13^2 *deixa resto* -6 *na divisão por 35* ($13^2 = 5 \cdot 35 - 6$)*, e assim, buscar o resto da divisão de* $(-6)^3 \cdot 13 = -216 \cdot 13$ *por 35 que é mais prático. Perceba que* -216 *deixa resto* -6 *na divisão por 35 pois* $-216 = (-6) \cdot 35 - 6$ *(neste caso, basta assumir os valores em módulo) e assim,* $-6 \cdot 13 = -78$ *e, somando o menor múltiplo de 35* ($-78 + 3 \cdot 35$)*, encontraremos 27. Cabe ao professor estimular seu aluno a novas formas de pensar dando possibilidades de escolhas para seguir o melhor caminho.*

Tomando o segundo bloco, 14, vamos encontrar o resto da divisão de 14^7 por 35, ou seja, queremos a solução da igualdade $14^7 = k_2 \cdot 35 + b$. Sendo assim, queremos o resto da divisão de 14^7 por 35. Podemos fatorar essa potência como sendo $14^7 = (14^2)^3 \cdot 14$ e como $14^2 = 196$ deixa resto 21 na divisão por 35, e pelo Corolário, temos $(21)^3 \cdot 14$ que reescrevemos como sendo $(21)^2 \cdot 21 \cdot 14$. A potência $21^2 = 441$ deixa resto 21 na divisão por 35, e assim, pelo Corolário, podemos procurar o resto de $21 \cdot 21 \cdot 14 = 441 \cdot 14$ e, usando o Corolário novamente, $21 \cdot 14 = 294$ que deixa resto 14 na divisão por 35. Dessa forma, 14^7 deixa resto 14 na divisão por 35.
Logo, o bloco 14 decodificado é igual a 14.

Passemos para o bloco 33. Queremos encontrar o resto da divisão de 33^7 e isso é equivalente a encontrar a solução da identidade $33^7 = k_3 \cdot 35 + b$. Tomando a fatoração de $33^7 = (33^2)^3 \cdot 33$, na qual temos a potência $33^2 = 1089$ e deixa resto igual a 4 na divisão por 35. Então, pelo Corolário, basta procurar o resto de $(4)^3 \cdot 33$ na divisão por 35. Fica fácil perceber que $4^3 = 64$ e deixa resto -6 na divisão por 35 ($64 = 2 \cdot 35 - 6$) e, pelo Teorema 2, $-6 \cdot 33 = -198$ deixa resto -23 e somando 35 a este valor encontramos 12. Dessa forma, 33^7 deixa resto igual a 12 na divisão por 35.
Logo, o bloco 33 decodificado é igual a 12.

Podemos tomar outro caminho bem mais prático para esse caso. Perceba que 33 deixa resto -2 *na divisão por 35* ($33 = 1 \cdot 35 - 2$)*, então podemos, utilizando o Corolário, efetuar a busca do resto da divisão de* $(-2)^7 = -128$ *por 35. Procedendo, como já mencionado em outros exemplos, com a adição de 35 até obter uma soma positiva,* $-128 + 4 \cdot 35 = 12$*, chegamos rapidamente ao resto da divisão de* 33^7 *por 35.*

Chegamos ao bloco 32 e queremos resolver a igualdade $32^7 = k_4 \cdot 35 + b$. Fazendo uso do Corolário e do método prático mencionado anteriormente, perceba que 32 está a -3 unidade de 35, logo, vamos buscar o resto da divisão de $(-3)^7$ por 35 e, por sua vez,

essa potência é fatorável a $(-3)^4 \cdot (-3)^3 = 81 \cdot (-27)$. É fácil ver que 81 deixa resto 11 e adicionando 35 a -27 obtemos 8, o que equivale a procurar o resto da divisão de $11 \cdot 8 = 88$ por 35, conforme o Teorema 2, deixando resto 18. Dessa forma, 32^7 deixa resto igual a 18 na divisão por 35.
Logo, o bloco 32 decodificado é igual a 18.

Resta-nos o último bloco 15 uma vez que já fizemos a decodificação do 14. Tome $15^7 = (15^2)^3 \cdot 15$, como $15^2 = 225$ deixa resto 15 na divisão por 35, conforme o Corolário, podemos procurar o resto da divisão por 35 do número $(15)^3 \cdot 15 = 15^2 \cdot 15^2 = 225 \cdot 225$. Como 225 deixa resto 15 na divisão por 35, pelo Teorema 2, vamos procurar o resto de $15 \cdot 15 = 225$ por 35, e sabemos que deixa resto 15. Dessa forma, 15^7 deixa resto 15 na divisão por 35.
Logo, o bloco 15 decodificado é igual a 15.

Dessa forma, resolvendo as identidades:

$$\begin{aligned}
\mathbf{13}^7 &= k_1 \cdot 35 + \mathbf{27} \\
\mathbf{14}^7 &= k_2 \cdot 35 + \mathbf{14} \\
\mathbf{33}^7 &= k_3 \cdot 35 + \mathbf{12} \\
\mathbf{32}^7 &= k_4 \cdot 35 + \mathbf{18} \\
\mathbf{15}^7 &= k_5 \cdot 35 + \mathbf{15} \\
\mathbf{14}^7 &= k_2 \cdot 35 + \mathbf{14}
\end{aligned}$$

encontramos a mensagem original **27-14-12-18-15-14** que, de acordo com a nossa tabela de pré-codificação, corresponde a palavra **RECIFE**.

4.3 Introduzindo uma Notação muito Especial

Podemos fazer um adendo e introduzir uma notação especial para esse tipo de equação $a = k \cdot n + b$, uma vez que, a nossa intenção aqui é, como solução da equação, obter apenas o resto **b** da divisão de **a** por **n** não nos interessando o quociente $k \in \mathbb{Z}$. Dois inteiros são ditos **congruentes (ou côngruos) módulo n** quando deixam o mesmo resto **r** na divisão por **n**, sendo $\mathbf{n > 1}$. Nesse caso, o b na expressão $a = k \cdot n + b$, necessariamente, não precisa ser o resto, mas sim um número na qual a diferença de a com b seja um múltiplo de n. Em outras palavras, $a - b = k \cdot n$. Por exemplo, suponha que $a = p \cdot n + r$ e $b = q \cdot n + r$, fazendo a diferença $a - b = p \cdot n + r - (q \cdot n + r) = (p - q) \cdot n$ que, tomando $p - q = k$, temos $a - b = k \cdot n$ e, por sua vez, $a = k \cdot n + b$. Dessa forma, *dizemos que a e b são congruentes módulo n* e escrevemos $a \equiv b \mod (n)$ sendo válidos os Teoremas 1, 2 e 3 demonstrados anteriormente.

Veja como podemos introduzir essa notação nos Teoremas 1, 2 e 3:

No Teorema 1, sendo $a = n \cdot q_a + r_a$ e $b = n \cdot q_b + r_b$, temos $a + b = (n \cdot q_a + r_a) + (n \cdot q_b + r_b)$ que pode ser reescrito na forma $a + b = n \cdot (q_a + q_b) + (r_a + r_b)$ e, consequentemente, $(a + b) - (r_a + r_b) = n \cdot (q_a + q_b)$ na qual n divide a diferença $(a + b) - (r_a + r_b)$. Sendo assim, podemos escrever que $(a+b)-(r_a+r_b) \equiv 0 \mod (n)$ e, consequentemente, $(a+b) \equiv (r_a+r_b) \mod (n)$.
No Teorema 2, $a \times b = (nq_a + r_a) \cdot (nq_b + r_b) = n \cdot (nq_aq_b + q_ar_b + q_br_a) + r_ar_b$ e temos, nesse resultado, um múltiplo de n adicionado do produto dos restos. Então, podemos reescrever a sentença como $a \times b = np + r_ar_b \Rightarrow (a \times b) - (r_ar_b) = n \cdot p$, onde $p \in \mathbb{N}$, nos mostrando que a diferença é um múltiplo de n. Então, $a \times b - r_ar_b \equiv 0 \mod (n)$ e, consequentemente, $a \times b \equiv r_ar_b \mod (n)$.
No Corolário, para a potência $a^k = np + r^k$, temos $a^k - r^k = np$ denotando que a diferença $a^k - r^k$ é um número múltiplo de n, ou seja, deixa resto zero na divisão por n. Sendo assim, $a^k - r^k \equiv 0 \mod (n) \Rightarrow a^k \equiv r^k \mod (n)$.

Fica a critério do professor introduzir essa notação para os seus estudantes após o estudo do método sem o uso de tal escrita.

Abaixo, segue a codificação e decodificação da palavra RECIFE, exatamente como fizemos anteriormente, utilizando a notação de congruência.

Usando a notação de congruência, o método impõe a regra: devemos pegar cada bloco a ser codificado **(b)** e elevar ao número natural **e**, obtendo o resto **(a)** da divisão por **n**, onde **a** será a codificação do bloco **b**. Ou seja, em termos matemáticos, nós queremos obter:

$$b^e \equiv a \mod (n) \textbf{ com } 0 \leq a < n$$

Essa é a regra de codificação do método RSA!

Vamos codificar o primeiro bloco b = 27. Então, queremos a solução da congruência $27^7 \equiv a \mod (35)$, ou melhor dizendo, queremos descobrir a classe de equivalência[1] do 27^7. Em uma linguagem mais simples, queremos o resto da divisão de 27^7 por 35. Resolvendo passo a passo:

Perceba que 27 está a 8 unidades abaixo de 35, ou seja, -8. Dessa forma, podemos reescrever a congruência de maneira equivalente a $27^7 \equiv (-8)^7 \mod (35)$. O objetivo é obter potências mais simples evitando o uso de calculadoras e, nessa vertente, como $7 = 2 \times 3 + 1$, escreveremos a última congruência como sendo $27^7 \equiv [(-8)^2]^3 \cdot (-8)^1 \mod (35)$. Pode parecer que a resolução está monótona, mas o objetivo é detalhar nesse primeiro momento o passo a passo e, posteriormente, seguindo de maneira análoga a esta resolução, encurtar os passos nos próximos exemplos. Seguindo a resolução, temos $27^7 \equiv [64]^3 \cdot (-8)^1 \mod (35)$. Ao dividir 64 por 35, obteremos resto 29 e, a congruência fica $27^7 \equiv [29]^3 \cdot (-8)^1 \mod (35)$. Mas, como 29 está a 6 unidades abaixo de 35, ou seja, a – 6 unidades, podemos trocar a congruência anterior por uma equivalente, $27^7 \equiv (-6)^3 \cdot (-8)^1 \mod (35)$. Perceba que estamos trocando as potências por potências mais simples e, seguindo o método, reescreveremos a congruência como sendo igual a $27^7 \equiv (-6)^2 \cdot (-6)^1 \cdot (-8)^1 \mod (35)$ e resolvendo a potência ficaremos com $27^7 \equiv 36 \cdot (-6)^1 \cdot (-8)^1 \mod (35)$. Como 36 deixa resto 1, na divisão por 35, a congruência é equivalente a $27^7 \equiv 1 \cdot (-6)^1 \cdot (-8)^1 \mod (35)$. Seguindo o passo a passo, conseguimos reduzir a congruência de potência grande para uma congruência mais simples e equivalente, $27^7 \equiv 48 \mod (35)$. Ao dividir 48 por 35 obtemos resto igual a 13, logo $27^7 \equiv 13 \mod (35)$. Se formos colocar, em sequência, o que acabamos de fazer teremos a congruência abaixo:

$$27^7 \equiv (-8)^7 \equiv [(-8)^2]^3 \cdot (-8)^1 \equiv [64]^3 \doteq (-8)^1 \equiv [29]^3 \cdot (-8)^1 \equiv (-6)^3 \cdot (-8)^1 \equiv (-6)^2 \cdot (-6)^1 \cdot (-8)^1 \equiv 36 \cdot (-6)^1 \cdot (-8)^1 \equiv 1 \cdot (-6)^1 \cdot (-8)^1 \equiv 48 \equiv 13 \mod (35).$$

Então, como $27^7 \equiv 13 \mod (35)$, o primeiro bloco criptografado é igual a **13**.

Vamos encriptar o segundo bloco 14. Então, queremos a solução da congruência $14^7 \equiv a \mod (35)$, ou melhor dizendo, queremos descobrir a classe de equivalência do 14^7. Resolvendo passo a passo:

Podemos reescrever essa potência de maneira mais simples, $14^7 \equiv (14^2)^3 \cdot 14 \mod (35)$.

[1] Chamamos de **Classe de Equivalência de um número P módulo n** o conjunto de todos os números que são congruentes a P módulo n, e este é representado pelo menor deles. Por exemplo, $20 \equiv 8 \mod (12)$, então o conjunto $\{8, 20, 32, \ldots, (8 + 12 \cdot n)\}$ é a Classe de Equivalência do número 20 módulo 12.

Então, a nossa congruência pode ser escrita de forma equivalente a $14^7 \equiv (196)^3 \cdot 14 \mod (35)$. O múltiplo de 35 mais próximo de 196 é o 210 (6×35), ou seja, o número 196 está quatorze unidades abaixo do 210. Podemos trocar esse 196 por -14 e nossa congruência é equivalente a $14^7 \equiv (-14)^3 \cdot 14 \mod (35)$. Perceba que, 196 deixa resto 21 ao ser dividido por 35 e, dessa forma, também temos outra congruência equivalente $14^7 \equiv (21)^3 \cdot 14 \mod (35)$. A escolha de utilizar a primeira foi meramente por praticidade. Vamos reescrevê-la, $14^7 \equiv (-14)^2 \cdot (-14) \cdot 14 \mod (35)$ que por sua vez corresponde a $14^7 \equiv 196 \cdot (-14) \cdot 14 \mod (35)$. Como já visto, podemos trocar 196 por -14 e, sendo assim, $14^7 \equiv (-14) \cdot (-14) \cdot 14 \mod (35)$ que é equivalente a $14^7 \equiv 196 \cdot 14 \mod (35)$. Seguindo o processo, temos $14^7 \equiv (-14) \cdot 14 \equiv -196 \mod (35)$. Somando 210 ($6 \times 35$) teremos a congruência equivalente $14^7 \equiv 14 \mod (35)$. Dessa forma, o resto da divisão de 14^7 por 35 é 14. Colocando em sequência o que acabamos de fazer, temos:

$14^7 \equiv (14^2)^3 \cdot 14 \equiv (196)^3 \cdot 14 \equiv (-14)^3 \cdot 14 \equiv (-14)^2 \cdot (-14) \cdot 14 \equiv 196 \cdot (-14) \cdot 14 \equiv (-14) \cdot (-14) \cdot 14 \equiv 196 \cdot 14 \equiv (-14) \cdot 14 \equiv -196 \mod (35) \equiv 14 \mod (35)$.

Então, como $14^7 \equiv 14 \mod (35)$, o segundo bloco criptografado é igual ao próprio **14**.
Procederemos de maneira análoga com os demais blocos. Então, temos as seguintes congruências para resolver ou encontrar a classe de equivalência:

$$12^7 \equiv a \mod (35)$$
$$18^7 \equiv a \mod (35)$$
$$15^7 \equiv a \mod (35)$$
$$14^7 \equiv a \mod (35)$$

Colocaremos aqui de maneira mais resumida pois acreditamos que o leitor já tenha adquirido habilidade após o estudo do capítulo anterior:
$12^7 \equiv (12^2)^3 \cdot 12 \equiv (144)^3 \cdot 12 \equiv (4)^3 \cdot 12 \equiv 64 \cdot 12 \equiv (-6) \cdot 12 \equiv (-72) \equiv 33 \mod (35)$.
$18^7 \equiv (18^2)^3 \cdot 18 \equiv (324)^3 \cdot 18 \equiv (9)^3 \cdot 18 \equiv 9^2 \cdot 9 \cdot 18 \equiv 81 \cdot 162 \equiv 11 \cdot 22 \equiv 242 \equiv 32 \mod (35)$.
$15^7 \equiv (15^2)^3 \cdot 15 \equiv (225)^3 \cdot 15 \equiv (15)^3 \cdot 15 \equiv 15^2 \cdot 15 \cdot 15 \equiv 225 \cdot 225 \equiv 15 \cdot 15 \equiv 225 \equiv 15 \mod (35)$.
Dessa maneira, a mensagem pré-codificada e separada em blocos 27-14-12-18-15-14, após o processo de resolução das congruências:

$$27^7 \equiv 13 \mod (35)$$
$$14^7 \equiv 14 \mod (35)$$
$$12^7 \equiv 33 \mod (35)$$
$$18^7 \equiv 32 \mod (35)$$

$$15^7 \equiv 15 \mod (35)$$
$$14^7 \equiv 14 \mod (35)$$

será transmitida sob a sequência encriptada **13-14-33-32-15-14.** Vamos, agora, decodificar usando a notação de congruência.

Usando a notação de congruência no processo inverso, vamos decodificar a mensagem recebida sob os blocos **13-14-33-32-15-14**. Tomando a chave de decodificação, o par **(n, d)**, onde **d** é o inverso de **e** módulo **[(p - 1)(q - 1)]**, sendo **e** expoente e **p, q** primos utilizados no processo de codificação. Lembrando que, no exemplo que fizemos a codificação da palavra RECIFE, os primos escolhidos foram o $p = 5$ e $q = 7$ gerando a chave $\mathbf{n = 35}$ e $\mathbf{e = 7}$. Então, como **d** é o inverso de **e**, devemos resolver a seguinte congruência:

$$e \cdot d \equiv 1 \mod [(p-1)(q-1)]$$

que, associada aos valores utilizados na codificação do nosso exemplo, resultará:

$$7 \cdot d \equiv 1 \mod [(5-1)(7-1)]$$
$$7 \cdot d \equiv 1 \mod (24)$$

Estamos procurando o número que multiplicado por 7 dê resto 1 na divisão por 24. Percebemos que essa resposta é o 7 pois $7 \cdot 7 \equiv 1 \mod (24)$. Logo, $d = 7$. Uma vez estabelecido o valor de d, vamos usar uma regra similar a que nós utilizamos na codificação:

$$a^d \equiv b \mod (n)$$

Sendo assim, para o primeiro bloco, vamos resolver a congruência $13^7 \equiv b \mod (35)$. Nos restringiremos a efetuar as operações de maneira sucinta pois acreditamos que o leitor, através dos exemplos anteriores, já tenha criado habilidade no processo:

$13^7 \equiv (13^2)^3 \cdot 13 \equiv (169)^3 \cdot 13 \equiv (-6)^3 \cdot 13 \equiv (-6)^2 \cdot (-6) \cdot 13 \equiv 1 \cdot (-78) \equiv 27 \mod (35)$.
Logo, fazendo a decodificação do primeiro bloco igual a 13, encontramos a mensagem original que tem como bloco 27. Procederemos igualmente resolvendo as demais congruências:

$14^7 \equiv (14^2)^3 \cdot 14 \equiv (196)^3 \cdot 14 \equiv (-14)^3 \cdot 14 \equiv (-14)^2 \cdot (-14) \cdot 14 \equiv 196 \cdot (-14) \cdot 14 \equiv (-14) \cdot (-196) \equiv (-14) \cdot 14 \equiv -196 \equiv 14 \mod (35)$.

$33^7 \equiv (-2)^7 \equiv (-2)^6 \cdot (-2) \equiv 64 \cdot (-2) \equiv (-6) \cdot (-2) \equiv 12 \mod (35)$.

$32^7 \equiv (-3)^7 \equiv (-3)^4 \cdot (-3)^3 \equiv 81 \cdot (-27) \equiv 11.8 \equiv 18 \mod (35)$.

$15^7 \equiv (15^2)^3 \cdot 15 \equiv (225)^3 \cdot 15 \equiv (15)^3 \cdot 15 \equiv 15^2 \cdot 15^2 \equiv 225 \cdot 225 \equiv 15 \cdot 15 \equiv 225 \equiv 15 \mod (35)$.
Dessa forma, resolvendo as congruências:

$$\begin{aligned} 13^7 &\equiv 27 \mod (35) \\ 14^7 &\equiv 14 \mod (35) \\ 33^7 &\equiv 12 \mod (35) \\ 32^7 &\equiv 18 \mod (35) \\ 15^7 &\equiv 15 \mod (35) \\ 14^7 &\equiv 14 \mod (35) \end{aligned}$$

encontramos a mensagem original **27-14-12-18-15-14** que, de acordo com a nossa tabela de pré-codificação, corresponde a palavra **RECIFE**.

Decerto que foi mencionado anteriormente, mas o que torna o processo de criptografia RSA eficaz é o fato de não termos, até o momento, uma ferramenta de fatoração rápida que possibilite a fatoração da chave de codificação n e a obtenção dos primos p e q ainda que se conheça o n. Como o processo utiliza primos muito grandes, a fatoração levaria meses e com isso seria inviável a obtenção desses primos. E, evidentemente, sem os primos p e q não é possível encontrar (p - 1), (q - 1) e não conseguiríamos resolver a congruência $e \cdot d \equiv 1 \mod [(p-1)(q-1)]$, impossibilitando a obtenção do número d que é o expoente que aplicamos no processo de decodificação. Por isso que, o número n pode ser uma chave pública, mas as pessoas não conseguem decodificar os dados por não conhecerem o número d. Uma outra observação importante é que, sendo os primos p e q muito grandes, certamente, eles serão ímpares e (p – 1), (q – 1) serão pares e o produto deles também será par. Se escolhermos o e também um número par, no momento que precisarmos calcular o inverso de e módulo [(p – 1)(q – 1)] ($e \cdot d \equiv 1 \mod [(p-1)(q-1)]$), ou seja, o d, teremos um problema porque não existirá o inverso de e. Isso decorre do fato que, ao dividir um número par por outro número par o resto será sempre par. Então, o número e deve ser escolhido como sendo um número ímpar, mesmo assim, alguns problemas podem acontecer. Vamos imaginar que e seja igual a 3, então teremos $3 \cdot d \equiv 1 \mod (24)$ e como 24 é múltiplo de 3, nesse caso, não existe o inverso de 3 módulo 24. Com este exemplo, podemos dizer que o problema foi, exclusivamente, a escolha do $e = 3$? Evidente que não! Perceba que, no início desde capítulo, dissemos que é necessário que o mdc $[e, (p-1)(q-1)] = 1$, mas a escolha dos primos também contribui para esse problema. Devemos escolher "bons números primos" para que problemas como esse não aconteçam. A seguir, mostraremos como obter os primos p, q e o número e não conflitantes de forma a garantir que sempre exista o inverso de e.

4.4 Escolhendo os Primos (p, q) e o Número (e) não Conflitantes

A fim de não termos conflito e garantir sempre a existência do inverso de e, podemos uniformizar o seu valor e atribuir uma hipótese na escolha dos primos p e q. Conforme Framilson Carneiro(CARNEIRO, 2017), na página 93, podemos, nesse caso, particularizar para $e = 3$ e criar um algoritmo que garanta a existência desse inverso. Devemos escolher dois primos que sejam congruentes a 5 módulo 6. Dessa forma, teremos sempre 3 invertível módulo $(p - 1)(q - 1)$ e será fácil encontrar d. É preciso deixar claro que esse processo é uma limitação do método RSA. O método nos permite utilizar quaisquer dois inteiros como expoentes para codificação e decodificação desde que estabelecidas as condições já informadas.

Escolhendo p e q primos, onde $p \equiv 5 \mod (6)$ e $q \equiv 5 \mod (6)$, temos $p - 1 \equiv 4 \mod (6)$ e $q-1 \equiv 4 \mod (6)$ e multiplicando ambos os lados chegamos a $(p-1)(q-1) \equiv 16 \mod (6)$ que é equivalente a $(p-1)(q-1) \equiv 4 \mod (6)$. Então, podemos dizer que $(p-1)(q-1) = 6k+4$, com $k \in \mathbb{Z}$. Por sua vez, podemos reescrever essa igualdade como sendo $(p-1)(q-1) = 3 \cdot 2k+3+1 \Leftrightarrow (p-1)(q-1) = 3(2k+1)+1$. Isolando $3(2k+1)$ na equação temos, $3(2k+1) = (p-1)(q-1)-1$. E como $(p-1)(q-1) = 6k+4$, concluímos que $3(2k+1) = 6k+4-1$. Dessa forma, usando congruência, temos $3(2k+1) \equiv -1 \mod (6k+4)$. Multiplicando ambos os lados por (-1) ficamos com $3(-2k-1) \equiv 1 \mod (6k+4)$ e, agora, somando $3.(6k+4)$ temos por fim $3(4k+3) \equiv 1 \mod (6k+4)$. Perceba que $3(4k+3) \equiv 1 \mod (6k+4) \Leftrightarrow e \cdot d \equiv 1 \mod [(p-1)(q-1)]$, logo $(4k+3) = d$. Temos um algoritmo que nos garante a existência do inverso e nos ajuda a encontrá-lo dentro das condições da hipótese. Vejamos um exemplo:

Escolhendo dois primos, conforme a hipótese, $p = 17 \equiv 5 \mod (6)$ e $q = 29 \equiv 5 \mod (6)$, e fazendo $(p-1)(q-1) = (17-1)(29-1) = 16 \cdot 28 = 448$. Sabendo que $(p-1)(q-1) = 6k+4 = 448 \Rightarrow k = 74$. Substituindo em $d = (4k+3) = (4 \cdot 74+3) = 299$. Então, se $k = 74$ o valor de $d = 299$. Dessa forma, encontramos o valor de d com praticidade e garantimos a existência de inverso.

Então, conforme o exemplo acima, $3 \cdot 299 \equiv 1 \mod (448)$**, nos mostrando que é possível escolher** p **e** q **não conflitantes.**

No exemplo da codificação da palavra **RECIFE**, utilizamos o método RSA no caso geral, mas podemos utilizar $3(4k+3) \equiv 1 \mod (6k+4)$ porque ambos os primos $p = 17$ e $q = 29$ que escolhemos satisfazem a hipótese de serem congruentes a 5 módulo 6. Então, teremos como nova chave pública de codificação o par $(n, e) = (493, 3)$ e chave secreta de decodificação $(n, d) = (493, 299)$.

4.5 O Pequeno Teorema de Fermat (P.T.F)

Ao utilizarmos o processo de criptografia RSA, fizemos uso dos Teoremas 1, 2 e 3. Apresentaremos um elegante teorema que não foi utilizado diretamente no processo, contudo será de grande importância para justificar a eficácia do método. Estamos falando do Pequeno Teorema de Fermat que, conforme Abrahmo Hefez(HEFEZ, 2011) (2010-p.92), pelo menos 500 antes de Cristo, os chineses já sabiam que, se p é um número primo, então $p|(2^p - 2)$. Pierre de Fermat generalizou este resultado enunciando este pequeno e notável teorema. Todavia, segundo Carl B. Boyer(BOYER, 2012) (2018-p.310), Euler foi o primeiro a apresentar uma demonstração (já havendo uma demonstração mais antiga deixada por Leibniz em manuscrito). Tal demonstração proposta por Euler foi publicada em Commentarii de Petersburgo de 1736 e, conforme Boyer a descreve, é surpreendentemente elementar.

A princípio necessitaremos do lema a seguir:

Lema 1. Seja p um número primo. Então, os números binomiais $\binom{p}{i}$, onde $0 < i < p$, são todos divisíveis por p.
Demonstração: O resultado vale para $i = 1$, *pois* $\binom{p}{1} = \frac{p!}{1!\cdot(p-1)!} = \frac{p\cdot(p-1)!}{1\cdot(p-1)!} = p$ *e* $p|p$. *Como* $\binom{p}{i} = \frac{p!}{i!\cdot(p-1)!} = \frac{p\cdot(p-1)\cdot\cdots\cdot(p-i+1)\cdot(p-i)!}{i!\cdot(p-i)!} = \frac{p\cdot(p-1)\cdot\cdots\cdot(p-i+1)}{i!}$ *é um número natural (pois representa o número de maneiras de retirar* i *elementos de um grupo de* p *elementos), então* $i!|p(p-1)\cdots(p-i+1)$ *pois, como o* $(i!, p) = 1$ *(sendo* p *primo ele não é divisível por nenhum* $i, 1 < i < p$*), então decorre que* $i!|(p-1)\cdots(p-i+1)$. *Sendo assim, os binomiais* $\binom{p}{i}$ *são divisíveis por* p.

(Pequeno Teorema de Fermat). Dado um número primo p, tem-se que p divide o número $a^p - a$, para todo $a \in \mathbb{N}$.
Demonstração: Usaremos indução em a. *Para* $a = 1$, *temos* $a^p - a = 1^p - 1 = 1 - 1 = 0$ *e* $p|0$. *Supondo o resultado válido para* a, *iremos prová-lo para* $a + 1$. *Pelo desenvolvimento binomial de Newton, segue que*

$$(a+1)^p - (a+1) = \binom{p}{0}a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a + \binom{p}{p} - a - 1$$
$$(a+1)^p - (a+1) = 1 \cdot a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a + 1 - a - 1$$
$$(a+1)^p - (a+1) = a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a - a$$

que reorganizando, temos

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

Pela hipótese de indução $p|(a^p - a)$ *e* $p|\left(\binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a\right)$ *pois* p *divide todos os*

coeficientes $\binom{p}{i}$ *de cada parcela onde* $1 \leqslant i \leqslant p-1$*, então o resultado segue.*■

Finalmente, $a^p - a \equiv 0 \mod (p) \Rightarrow a^p \equiv a \mod (p)$ que, dividindo por a, temos:

$$\frac{a^p}{a} \equiv \frac{a}{a} \mod (p) \Rightarrow a^{p-1} \equiv 1 \mod (p)$$

sendo muito útil, neste último formato, para o objetivo que seguirá a frente.

4.6 Por que o Método RSA Funciona?

Vamos relembrar dos passos realizados até o momento. Para codificar uma mensagem em RSA fizemos uma pré-codificação da mensagem fazendo uso de uma tabela numerada de 10 a 35, sendo isso arbitrário, tomando apenas o cuidado de que todas as letras sejam representadas por números com a mesma quantidade de dígitos, ou seja, essa tabela pode ser numerada de 100 a 125, de 135 a 160, ou até mesmo de 1000 a 1025. Após isso, escolhemos dois primos p e q e geramos o número $n = p \cdot q$ que, juntamente com um o número e, comporá a chave pública de codificação (n, e). Por sua vez, o número e é escolhido de forma que o **mdc [e, (p - 1)(q - 1)] = 1**, podendo ser qualquer valor desde que satisfaça o mdc e, para o nosso exemplo, escolhemos $n = p \cdot q = 5 \cdot 7 = 35$ e, sendo **mdc [e, (5 - 1)(7 - 1)] = [e, 24] = 1**, escolhemos o 7 e tomamos a chave pública $(n, e) = (35, 7)$ como chave padrão e codificamos os blocos referentes a mensagem. Mostraremos o porquê da eficiência do método está garantida, desde que, todos os passos e critérios sejam obedecidos.

Cada bloco que queremos codificar b deve ser um número dentro do intervalo $1 \leqslant b < n$ de números naturais. E, para tal codificação, usamos o critério $b^e \equiv a \mod (n)$, na qual a pertence ao intervalo $0 \leqslant a < n$, onde a é a codificação da mensagem do bloco b. Quando fazemos o processo inverso, a decodificação, utilizamos como artifício critério semelhante: tomamos a mensagem recebida a e a elevamos ao número d para obter um resto na divisão por n, ou seja, tomamos $a^d \equiv c \mod (n)$, onde c está no intervalo de números naturais $0 \leqslant c < n$ e este c deve ser a mensagem original, a decodificação de a. Esse processo de codificação e decodificação só servirá de fato se $c = b$, caso contrário, o método falha, pois, toma uma mensagem a codificada e, na decodificação, o método não devolve a mensagem original. Então, precisamos mostrar que este c é, de fato, igual a informação original que foi codificada, ou seja, queremos mostrar que $(b^e)^d \equiv b \mod (n)$. Perceba que $c \equiv a^d \mod (n)$ e este a é $a \equiv b^e \mod (n)$, então, por transitividade, $c \equiv a^d \equiv (b^e)^d \mod (n)$ e isso é equivalente a $c \equiv b^{e \cdot d} \mod (n)$, sendo tal informação muito importante daqui em diante.

Sabemos que d é definido da seguinte forma: $d \cdot e \equiv 1 \mod [(p-1)(q-1)]$ e isso significa dizer que $e \cdot d = 1 + k \cdot [(p-1)(q-1)]$. Vamos substituir $e \cdot d$ em $c \equiv b^{e \cdot d} \mod (n)$ e passemos a analisar a congruência $c \equiv b^{1+k \cdot [(p-1)(q-1)]} \mod (n)$, especificamente, o $b^{1+k \cdot [(p-1)(q-1)]}$. Essa congruência pode ser escrita como sendo $c \equiv b^{1+k \cdot [(p-1)(q-1)]} \equiv b \cdot b^{k \cdot [(p-1)(q-1)]} \mod (n)$. O objetivo é mostrar que $b^{e \cdot d} \equiv b \mod (n)$ e para isso vamos dividir a demonstração em dois casos, uma vez que $n = p \cdot q$, e concluiremos no final a congruência módulo n:

Caso 1: Suponha que $(p, b) \neq 1$

Se (p, b) é diferente de 1, então resta, apenas, ao b ser um múltiplo de p, $b = \lambda p$. Ou seja,

$b \equiv 0 \mod (p)$ (pois teríamos $b = \lambda p \equiv 0 \mod (p)$) e isso implica em $b^{e \cdot d} \equiv 0 \mod (p)$. Portanto, se $(p, b) \neq 1$, então $b^{e \cdot d} \equiv b \mod (p)$, chegando ao nosso objetivo.

Caso 2: Suponha que $(p, b) = 1$

Neste caso, b não é múltiplo de p. Tomaremos o que mencionamos no início do parágrafo: sabemos que $b^{e \cdot d} = b \cdot b^{k \cdot [(p-1)(q-1)]}$ e vamos escrever, convenientemente, como $b^{e \cdot d} \equiv b \cdot [b^{(p-1)}]^{k \cdot (q-1)} \mod (p)$. Percebamos, pelo Pequeno Teorema de Fermat que, $b^{p-1} \equiv 1 \mod (p)$ (uma vez que $(p, b) = 1$), então, $b^{e \cdot d} \equiv b \cdot [b^{(p-1)}]^{k \cdot (q-1)} \equiv b \cdot [1]^{k \cdot (q-1)} \mod (p)$ que implica em $b^{e \cdot d} \equiv b \mod (p)$. Para o primo q é análogo e chegamos a mesma conclusão de que $b^{e \cdot d} \equiv b \mod (q)$. Como $b^{e \cdot d} \equiv b \mod (p)$ e $b^{e \cdot d} \equiv b \mod (q)$, essa conclusão nos leva a um sistema de congruências:

$$\begin{cases} X \equiv b \mod (p) \\ \\ X \equiv b \mod (q) \end{cases} \textbf{, sendo } X = b^{e \cdot d}$$

vamos procurar os números X's que satisfaçam ao sistema.

Pelo sistema, sabemos que $X = b + t_1 \cdot p$ e $X = b + t_2 \cdot q$, ou seja, $X - b = t_1 \cdot p$ e $X - b = t_2 \cdot q$. Dessa forma, $X - b$ é múltiplo de p e q, mas como p e q são distintos, consequentemente, $X - b$ é múltiplo do produto pq, ou seja, $X - b = t_3 \cdot pq$. Sendo $X - b = t_3 \cdot pq$, isso nos diz que $X - b \equiv 0 \mod (pq)$ e, consequentemente, $X \equiv b \mod (pq)$. Mas, lembre-se de que $pq = n$, chave pública de codificação, e por fim, $X \equiv b \mod (n)$. Como $X = b^{e \cdot d}$, então, concluímos que $b^{e \cdot d} \equiv b \mod (n)$.

Acabamos de mostrar que $b^{e \cdot d} \equiv b \mod (n)$. Mas, $b^{e \cdot d} \equiv c \mod (n)$, como foi dito no início, então, $c \equiv b \mod (n)$. O fato do b e do c serem congruentes módulo n, não quer dizer que sejam iguais. Entretanto, como $0 \leq c < n$ e $1 \leq b < n$, então, necessariamente, essa congruência implica a igualdade. Dessa forma, $c = b$. Lembre-se que **c** é a decodificação do bloco **b**. Isso nos garante que, ao decodificar o bloco **a**, o que iremos encontrar, de fato, é a informação inicial, o bloco **b**.

4.7 A segurança do Método RSA

Vimos que o sistema de criptografia é de chave pública e que a dupla (n, e) é a chave de codificação ou chave pública. Sendo assim, todos os usuários têm acesso a chave de codificação e o que torna o método seguro é a dificuldade em fatorar n e, por isso, o método exige números primos p e q grandes para que essa fatoração seja extremamente difícil mesmo com o uso dos atuais computadores.

Para calcular d precisamos de $[(p-1)(q-1)]$ e e, o que nos obriga a saber os valores de p e q, mas para isso precisamos fatorar n, uma vez que, os primos escolhidos ficam em total sigilo. E é por esse fato, a fatoração, que o método se torna altamente seguro. Não temos um algoritmo rápido de fatoração. Contudo, ainda não provaram que exista um algoritmo de fatoração rápido e eficiente a ponto de fatorar n em tempo hábil e, assim, quebrar o código. Encontrar esse algoritmo e fatorar n é considerado, pelos analistas, um problema equivalente a quebra do RSA. Portanto, para números primos suficientemente grandes, o RSA é seguro, dado esse problema da fatoração de inteiros grandes.

A tabela abaixo, divulgada pelos próprios criadores do RSA, mostra o tempo estimado para um computador atual, levando em consideração o número de dígitos e o número de operações matemáticas necessárias para tal.

Tabela 4 – Tempo estimado da fatoração por um computador

Quantidade de dígitos do número **n**	Número de operações	Tempo estimado
50	$1,4 \times 10^{10}$	3,9 horas
70	$9,0 \times 10^{12}$	104 dias
100	$2,3 \times 10^{15}$	74 anos
200	$1,2 \times 10^{23}$	$3,8 \times 10^{9} anos$
300	$1,5 \times 10^{29}$	$4,9 \times 10^{15}$ anos
500	$1,3 \times 10^{39}$	$4,2 \times 10^{25}$ anos

Fonte: A method for obtaining digital signature

5 As Sequências Didáticas

A sequência didática baseada na teoria de Dolz, Noverraz e Schneuwly(DOLZ NOVERRAZ, 2004) é uma metodologia de ensino que busca desenvolver a competência comunicativa dos alunos, permitindo que eles aprendam a produzir e compreender textos em diferentes gêneros textuais. Embora seja comumente utilizada no ensino da língua portuguesa, essa abordagem também pode ser aplicada ao ensino da matemática, contribuindo para o desenvolvimento de habilidades essenciais nessa disciplina.

Uma das principais vantagens da sequência didática é que ela permite aos alunos aprender a comunicar seus pensamentos matemáticos de forma clara e precisa, por meio da produção de textos como relatórios, resenhas e outros tipos de produção textual. Além disso, essa abordagem também favorece a construção de significados e a compreensão de conceitos matemáticos, por meio da discussão e revisão conjunta dos textos produzidos pelos alunos.

De acordo com Machado(MACHADO, 2009), a sequência didática pode ser utilizada para trabalhar diversos gêneros textuais na disciplina de matemática, tais como o relatório de experimento, a resenha crítica de artigos científicos e a produção de textos explicativos. Ao utilizar esses gêneros textuais, os alunos são estimulados a pensar de forma crítica sobre os conceitos matemáticos aprendidos em sala de aula, e a construir significados a partir de suas próprias experiências e vivências.

Outra vantagem da sequência didática para o ensino da matemática é que ela permite que os alunos aprendam a argumentar e justificar suas respostas e soluções matemáticas de forma coerente e fundamentada. Segundo Santos(SANTOS, 2018), a produção de textos argumentativos, como cartas de opinião e debates, pode ser uma forma eficiente de estimular o pensamento crítico dos alunos e favorecer a construção de argumentos sólidos e bem fundamentados.

Em resumo, a sequência didática baseada na teoria de Dolz, Noverraz e Schneuwly pode ser uma ferramenta valiosa para o ensino da matemática, contribuindo para o desenvolvimento de habilidades comunicativas e críticas essenciais para a vida pessoal e profissional dos alunos. Ao permitir que os alunos aprendam a produzir e compreender textos em diferentes gêneros textuais, essa abordagem favorece a construção de significados e a compreensão dos conceitos matemáticos, além de estimular o pensamento crítico e a argumentação fundamentada.

A seguir, temos a sequência construída e aplicada na escola pública estadual de Pernambuco, Escola de Aplicação do Recife, nas três únicas turmas do Ensino Médio.

.

Tabela 5 – Sequência Didática

<table>
<tr><th colspan="4">APRESENTAÇÃO</th></tr>
<tr><td colspan="4">A sequência Didática se destina aos estudantes do Ensino Médio como forma de introduzir os conteúdos da aritmética dos restos no processo da criptografia RSA. A partir de três blocos com duas aulas de 50 minutos cada, e com poucos itens como piloto, quadro branco, papel, projetor, caneta e calculadora, os estudantes compreenderão como obter restos de divisões entre números, incalculáveis manualmente, através do estudo de quatro teoremas e/ou com uso da calculadora, tendo por atividade prática a criptografia de mensagens para o entendimento de como esse processo acontece naturalmente no cotidiano.</td></tr>
<tr><th>AUTOR</th><th>COMPONENTE</th><th>SÉRIE</th><th>AULAS PREVISTAS</th></tr>
<tr><td>Eliton Mendes</td><td>Matemática</td><td>1º, 2º e 3º anos do Ensino Médio</td><td>6 Aulas de 50 minutos</td></tr>
<tr><th colspan="2">TEMA</th><th colspan="2">CONTEÚDOS</th></tr>
<tr><td colspan="2">Criptografia RSA</td><td colspan="2">- Teorema 1 – Obtenção do resto da soma de dois números naturais;
- Teorema 2 – Obtenção do resto do produto de dois números naturais;
- Corolário – Obtenção do resto de potências;
- Teorema 3 – Obtenção do resto com uso da calculadora;
- Codificação de mensagem com uso do método RSA;
- Decodificação de mensagem com uso do método RSA.</td></tr>
<tr><th colspan="4">OBJETIVOS GERAIS</th></tr>
<tr><td colspan="4">- Compreender a obtenção de restos da soma de dois números naturais;
- Compreender a obtenção de restos do produto de dois números naturais;
- Compreender a obtenção de restos com o uso da calculadora;
- Compreender a obtenção de restos com o uso da calculadora;
- Compreender o processo de encriptação de mensagens através do método RSA;
- Compreender o processo de decriptação de mensagens do método RSA.</td></tr>
<tr><th colspan="4">OBJETIVOS ESPECÍFICOS</th></tr>
<tr><td colspan="4">Desenvolver a habilidade e o entendimento do processo de criptografia RSA.</td></tr>
<tr><th colspan="4">CONHECIMENTOS PRÉVIOS NECESSÁRIOS</th></tr>
<tr><td colspan="4">Conhecer o processo da divisão euclidiana.</td></tr>
</table>

Fonte: Feita pelo autor

Tabela 6 – Desenvolvimento das atividades - Aulas 1 e 2

DESENVOLVIMENTO DAS ATIVIDADES
Aulas 1 e 2
Assunto: Problematização e apresentação dos Teoremas 1, 2, 3 e do Corolário. Duração: 100 minutos
Metodologia: Iniciaremos apresentando, superficialmente, um exemplo de envio de mensagem pelo método RSA e, para isso, explicaremos aos estudantes como o processo se baseia em restos de divisões. Com isso, deixaremos claro para o aluno a importância da obtenção dos restos, uma vez que, o processo necessita. Em seguida, pediremos para os estudantes responder a primeira pergunta da lista de atividades. Após isso, apresentaremos a demonstração e exemplificação dos teoremas 1, 2, 3, Corolário e aplicaremos as atividades.
Atividades: 01) Quais dos problemas abaixo você acha que consegue responder? 02) Mostre que o ***Teorema 1 vale para k parcelas;*** 03) Sabendo que o resto da divisão de 2473 por 10 é 3, e sendo 9 o resto da divisão de 8799 por 10, qual o resto da divisão 2473 + 8799 por 10? 04) Sabendo que o resto da divisão de 8799 por 10 é 9, e o resto da divisão de 2473 por 10 é igual a 3, obtenha o resto da divisão de 8799 – 2473 por 10. 05) Encontre o resto da divisão de 7257 e 361 por 50. Qual o resto da divisão 2.619.777 (7257 x 361) por 50? 06) Sabendo que o resto da divisão 127 por 41 é 4, então qual é o resto da divisão de 1274 por 41? 07) Obtenha o resto da divisão de 27^7 por 35. 08) Utilizando uma calculadora, obtenha o resto da divisão de 19.897 por 41. 09) Utilizando uma calculadora, obtenha o resto de 13^{13} por 85.

Fonte: Feita pelo autor

Tabela 7 – Desenvolvimento das atividades - Aulas 3 e 4

Aulas 3 e 4
Assunto: Codificação de uma mensagem pelo método RSA. **Duração: 100 minutos**
Objetivos Específicos: - Compreender o processo de encriptação de mensagens através do método RSA.
Metodologia: Apresentaremos o processo de criptografia RSA com a utilização dos teoremas já estudados nas aulas 1 e 2, bem como a criação da chave pública de criptografia. Em seguida, aplicaremos as atividades.
Atividades: 10) Utilizando os primos 17 e 19 obtenha a chave de codificação *(n, e).* 11) Obtenha uma chave de codificação segundo os critérios de criptografia RSA.
(Confira com os seus colegas e padronize uma chave comum para todos).
12) Sem o uso de calculadoras e, utilizando a chave obtida no item anterior e o método de criptografia RSA, obtenha a mensagem encriptada da frase
"*AMO A MATEMÁTICA" e* confira se a sua criptografia é a mesma obtida pelos
seus colegas.
13) A partir dessa chave padronizada, escolha uma pequena mensagem, codifique-a e
transmita a um(a) colega e peça para que ele(a) a guarde para decodificar mais tarde.

Fonte: Feita pelo autor

Tabela 8 – Desenvolvimento das atividades - Aulas 5 e 6

Aulas 5 e 6
Assunto: Decodificação de uma mensagem pelo método RSA. **Duração: 100 minutos**
Objetivos Específicos: - Compreender o processo de decriptação de mensagens do método RSA.
Metodologia: Apresentaremos o processo de decodificação RSA com a utilização dos teoremas já estudados, bem como a obtenção da chave de decodificação. Em seguida, aplicaremos as atividades.
Atividades: 14) Resolva a igualdade $7.d = k.40 + 1$ e encontre o valor de d, inverso de 7. 15) Suponha que uma mensagem foi codificada utilizando os primos $p = 11$ e $q = 13$, encontrando a chave de codificação $(143, 17)$. Fazendo o uso dos métodos de decodificação e de uma calculadora, encontre o valor de d. 16) Encontre o valor de d (inverso de e) da chave de codificação acordada pela sua turma. 17) Tome a mensagem que você recebeu do seu colega e, utilizando a chave de decodificação (e, d) e o método de decodificação RSA, decodifique-a.

Fonte: Feita pelo autor

Tabela 9 – Ficha do aluno - Aulas 1 e 2

FICHA DO ALUNO		
Data:	**Escola:**	**Aluno 01**
Assunto: Problematização e apresentação dos Teoremas 1, 2, 3 e do Corolário.		**Duração:** 100 minutos
Objetivos Específicos: - Compreender a obtenção de restos da soma de dois números naturais; - Compreender a obtenção de restos do produto de dois números naturais; - Compreender a obtenção de restos de potências; - Compreender a obtenção de restos com o uso da calculadora.		**Aulas 1 e 2**
01)Quais dos problemas abaixo você consegue responder?		
02) Mostre que o ***Teorema 1 vale para k parcelas;***		
03) Sabendo que o resto da divisão de 2473 por 10 é 3, e sendo 9 o resto da divisão de 8799 por 10, qual o resto da divisão 2473 + 8799 por 10?		
04) Sabendo que o resto da divisão de 8799 por 10 é 9, e o resto da divisão de 2473 por 10 é igual a 3, obtenha o resto da divisão de 8799 – 2473 por 10.		
05) Encontre o resto da divisão de 7257 e 361 por 50. Qual o resto da divisão 2.619.777 (7257 x 361) por 50?		
06) Sabendo que o resto da divisão 127 por 41 é 4, então qual é o resto da divisão de 127^4 por 41?		
07) Obtenha o resto da divisão de 27^7 por 35.		
08) Utilizando uma calculadora, obtenha o resto da divisão de 19.897 por 41		
09) Utilizando uma calculadora, obtenha o resto de 13^{13} por 85.		

Fonte: Feita pelo autor

Tabela 10 – Ficha do aluno - Aulas 3 e 4

FICHA DO ALUNO		
Data:	**Escola:**	**Aluno 01**
Assunto: Codificação de uma mensagem pelo método RSA		**Duração:** 100 minutos
Objetivos Específicos: - Compreender o processo de encriptação de mensagens através do método RSA.		**Aulas 3 e 4**
10) Utilizando os primos 17 e 19 obtenha a chave de codificação *(n, e).*		
11) Obtenha uma chave de codificação segundo os critérios de criptografia RSA. *(Confira com os seus colegas e padronize uma chave comum para todos).*		
12) Sem o uso de calculadoras e, utilizando a chave obtida no item anterior e o método de criptografia RSA, obtenha a mensagem encriptada da frase "*AMO A MATEMÁTICA" e*conf ira se a sua criptografia é a mesma obtida pelos seus colegas.		
13) A partir dessa chave padronizada, escolha uma pequena mensagem, codifique-a e transmita a um(a) colega e peça para que ele(a) a guarde para decodificar mais tarde.		

Fonte: Feita pelo autor

Tabela 11 – Ficha do aluno - Aulas 5 e 6

FICHA DO ALUNO		
Data:	**Escola:**	**Aluno 01**
Assunto: Decodificação de uma mensagem pelo método RSA.		**Duração:** 100 minutos
Objetivos Específicos: - Compreender o processo de decriptação de mensagens do método RSA.		**Aulas 5 e 6**
14) Resolva a igualdade $7.d = k.40 + 1$ e encontre o valor de d, inverso de 7.		
15) Suponha que uma mensagem foi codificada utilizando os primos $p = 11$ e $q = 13$, encontrando a chave de codificação (143, 17). Fazendo o uso dos métodos de decodificação e de uma calculadora, encontre o valor de d.		
16) Encontre o valor de d (inverso de e) da chave de codificação acordada pela sua turma.		
17) Tome a mensagem que você recebeu do seu colega e, utilizando a chave de decodificação (e, d) e o método de decodificação RSA, decodifique-a.		

Fonte: Feita pelo autor

5.1 Análises dos Resultados

A sequência didática referente as aulas 1 e 2 foi entregue aos estudantes e foi solicitado que eles fizessem uma verificação minuciosa em cada item sem resolvê-los. Foi dado um tempo e depois foi solicitado que eles respondessem, livremente, o primeiro item. A princípio, a ideia é verificar os conhecimentos dos estudantes sobre a obtenção de restos e, para que não sofressem influência dos teoremas que seriam enunciados, que eles pudessem avaliar quais itens seriam capazes de responder com os conhecimentos já adquiridos ao longo da vida escolar até o momento. Feito isso, utilizando o Power Point, foi explicado o tema da dissertação, o contexto histórico sobre a criptografia e do sistema de criptografia RSA, a motivação que levou ao estudo do assunto aplicado ao ensino médio e as contribuições esperadas do tema no aprendizado dos estudantes. Os teoremas 1, 2, 3 e 4 foram expostos, através de slides para otimizar o tempo, e demonstrados em sua integralidade utilizando quadro e piloto e aplicando a cada um, no mínimo, dois exemplos. Alguns alunos fizeram perguntas e outros exemplos surgiram no decorrer da explicação. Esta primeira sequência didática foi aplicada em 28 de outubro de 2022 nas únicas turmas de 1º, 2º e 3º anos do Ensino Médio da Escola de Aplicação do Recife, onde leciono, e, devido ao calendário apertado entre as provas letivas e as avaliações externas como ENEM, SSA e SAEPE, as demais sequências só foram aplicadas recentemente em março e abril de 2023. Dessa forma, como a turma do 3º de 2022 já não estava mais na escola, esta primeira sequência foi aplicada aos alunos do 1º ano de 2023 para completar as três turmas do ensino médio. Abaixo, temos os resultados percentuais desta primeira sequência didática.

1º Ano do Ensino Médio

A turma é composta por 37 alunos e participaram da aplicação 21 estudantes. Todos que estavam presentes participaram da atividade. Observemos o resultado do primeiro item da sequência da aula 1 e 2:

01.Quais dos problemas abaixo você acha que consegue responder?

Tabela 12 – 1o Ano: Respostas da questão 1.

Aluno	Respostas
1, 3, 4, 5, 6, 7, 11, 12, 13, 14, 15, 17, 18, 19, 20, 21	Nenhum.
2	O problema 3, 4, 5, 6, 8, 9.
9	6
16	Alguns.
8	Nenhum que envolva números grandes.
10	Pelo menos metade.

Fonte: Elaborada pelo autor.

Estamos diante de alunos recém-saídos do fundamental II, o que julgo terem menos maturidade na escrita matemática, e podemos ver que 16 estudantes declararam não saber

responder nenhum problema. Todos que participaram não informaram saber responder o problema 02. Pouquíssimos estudantes julgaram saber responder algum problema. Após as demonstrações dos teoremas, tivemos, conforme podemos ver na tabela 12, 2 acertos dos 10 que tentaram responder o problema 2. Contudo, de acordo com a figura 7, há imaturidade no que se refere a demonstrações, onde o aluno deixa lacunas e falta de conclusão em sua resposta.

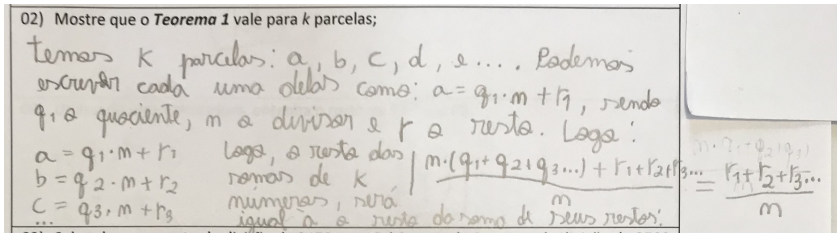


Figura 7 – Resposta do Aluno 13.

Tabela 13 – 1o Ano: Acertos da primeira Sequência Didática

PROBLEMA	CERTOS	PARCIALMENTE CERTOS	ERRADOS	SEM RESPOSTA
02	2	4	4	11
03	21	0	0	0
04	19	0	0	2
05	14	1	2	4
06	14	2	0	5
07	11	2	4	4
08	18	0	0	3
09	9	0	6	6

Fonte: Elaborada pelo autor.

Os percentuais que veremos foram com base na média aritmética por questão. Podemos ver que tivemos, aproximadamente, 73% de acertos por questão quando analisamos do problema 03 ao 09. Esse percentual diminui para, aproximadamente, 65% de acertos quando consideramos o problema 02. Aproximadamente, 5% de parcialidade no acerto. Vemos, também, que, aproximadamente, 8% erraram algum problema e esse percentual se concentra nos problemas 7 e 9 que se referem a aplicação dos teoremas 3 e 4, respectivamente. E, 21%, aproximadamente, desses alunos deixaram algum problema sem resposta, concentrando nos problemas 5, 6, 7, 8 e 9, referentes aos teoremas 3 e 4. Quando incluímos o problema 02, onde tivemos a maioria (11) sem resposta, o percentual de questões sem resposta, em média, sobe para 21% do alunado, aproximadamente. Tivemos 100% dos alunos sinalizando não terem condições de responder o problema 02, mesmo o aluno 10, subjetivamente, dizendo saber responder "pelo menos metade". Mesmo após apresentação dos teoremas, tivemos 20% de acertos, aproximadamente, nesse item dentre aqueles que tentaram responder, 40% de parcialidade no acerto do item e 40% de erro,

aproximadamente. Destacando que, aproximadamente, 52% da turma deixou este item sem resposta.

2º Ano do Ensino Médio

A turma é composta por 40 alunos e participaram da aplicação 27 estudantes. Alguns alunos optaram em não participar devolvendo a atividade em branco, por isso, há a ausência de alguns alunos. Observemos o resultado do primeiro item da sequência aula 1 e 2:

01. Quais dos problemas abaixo você acha que consegue responder?

Tabela 14 – 2o Ano: Respostas da questão 1.

Aluno	Respostas
3, 4, 9, 11, 12, 14, 21, 22, 23, 25, 31, 33, 37, 40,	*Nenhum.*
24, 28, 36, 39	Em branco.
15	Algun's.
17	Algumas.
18	Nem uma.
20	7, 8 e 9
27	No máximo 4 ou 5.
32	Conseguiria fazer da maneira tradicional (dividindo), mas, por isso, demoraria mais.
34	Algumas.
35	Alguns deles.
38	Alguns.

Fonte: Elaborada pelo autor.

Percebemos que 19 estudantes, destes 4 sem resposta, 15 julgaram não saber responder nenhuma questão. Daqueles que se dizem saber responder algum problema, nenhum deles informaram saber responder o problema 2. Podemos, também, ver algumas respostas como "Algun's" e "Nem uma" que denota falta de letramento. Esses estudantes não sabem a ortografia vigente. Mesmo eles não informando saber responder o item 2, poderemos ver na tabela 14 que 14 estudantes tentaram resolver e, desses, 6 acertaram e 7 estavam com suas respostas faltando a parte final, a conclusão. Tivemos respostas bem-organizadas e, um caso interessante: o estudante 18, que escreveu "Nem uma", apresentou, conforme a figura 8, uma solução organizada e coerente. Isso nos mostra que, mesmo o estudante demonstrando lacunas no letramento, a matemática tem sua linguagem própria.

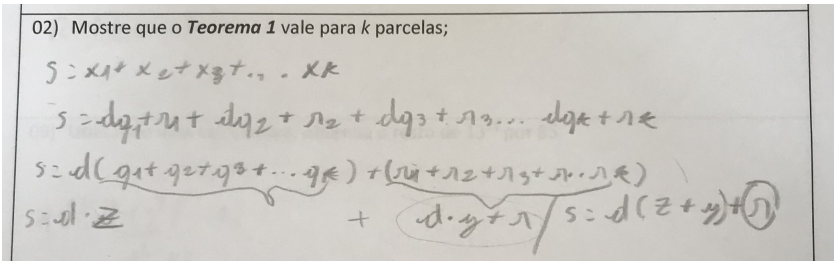


Figura 8 – Resposta do Aluno 18.

Tabela 15 – 2o Ano: Acertos da primeira Sequência Didática

PROBLEMA	CERTOS	PARCIALMENTE CERTOS	ERRADOS	SEM RESPOSTA
02	6	7	1	13
03	23	4	0	0
04	25	0	2	0
05	20	1	2	4
06	19	0	3	5
07	20	1	0	6
08	19	0	0	8
09	9	0	11	7

Fonte: Elaborada pelo autor.

Os percentuais que veremos foram com base na média aritmética por questão. Podemos ver que tivemos, aproximadamente, 71% de acertos por questão quando analisamos do problema 03 ao 09. Esse percentual diminui para 65%, aproximadamente, de acertos quando consideramos o problema 02. Analisando sem o problema 2, aproximadamente, 3% de parcialidade no acerto. Vemos, também, que, aproximadamente, 10% erraram algum problema e esse percentual se concentra no problema 9 que se refere a aplicação do teorema 4, uso da calculadora. E, aproximadamente, 16% desses alunos deixaram algum problema sem resposta, concentrado nos problemas 5, 6, 7, 8 e 9, referentes aos teoremas 3 e 4. Quando incluímos o problema 02, onde tivemos a maioria (13) sem resposta, o percentual de questões sem resposta, em média, sobe para 20% do alunado. Tivemos 100% dos alunos sinalizando não terem condições de responder o problema 02, mas, após apresentação dos teoremas e, mesmo o problema exigindo uma demonstração, prática não corriqueira em sala de aula, tivemos, aproximadamente, 43% de acertos nesse item dentre aqueles que tentaram responder, 50% de parcialidade no acerto do item e 7% de erro, aproximadamente. E, vale ressaltar, que 48% da turma deixou este item sem resposta.

3º Ano do Ensino Médio

A turma é composta por 36 alunos e participaram da aplicação 26 estudantes. Os estudantes 4 e 8 devolveram suas atividades em branco. Observemos o resultado do primeiro item da sequência aula 1 e 2:

01. Quais dos problemas abaixo você acha que consegue responder?

Tabela 16 – 3o Ano: Respostas da questão 1.

Aluno	Respostas
1, 2, 3, 4, 6, 9, 11, 13, 14, 17, 27	Nenhuma
10	Nenhuma, eu acho.
12	Não sei, provavelmente nenhuma.
18	Nenhum, porque sou péssimo em matemática.
21	Eu creio que o problema 3, 4 e 5 eu conseguiria responder com meus conhecimentos.
23	Conseguiria responder apenas os problemas 3 e 4 apenas com os meus conhecimentos.
24	Acredito que saberia responder as questões 8 e 9 apenas.
20	3, 4 e a 8 sem auxílio algum.
25	3, 4, 5, 6, 8, 9.
26	Problema 8 e 9 apenas.
28	3, 4, 5, 6, 7, 8, 9.
15	3 e 4
7	Somente a 05.
22	03, 04, 08 e 09.
5	6, 7, 8 e 9.
16	Os problemas 3, 4, 5, 8 e 9.
19	A questão 7 e 8.

Fonte: Elaborada pelo autor.

Podemos ver que 15 estudantes declararam não saber responder nenhum problema e 100% da turma não informaram saber responder o problema 02. É perceptível que, mesmo eles não tendo acesso aos teoremas, julgaram saber responder algum problema, exceto o problema 02. Acreditamos que esse percentual decorre do fato dos estudantes não terem uma prática em problemas que exijam demonstrações. Há de se aprofundar na problemática. Contudo, após as demonstrações dos teoremas, tivemos, conforme podemos ver na tabela 16, 8 acertos no problema 02 e, dentre eles, demonstrações bem-organizadas, conforme a figura abaixo.

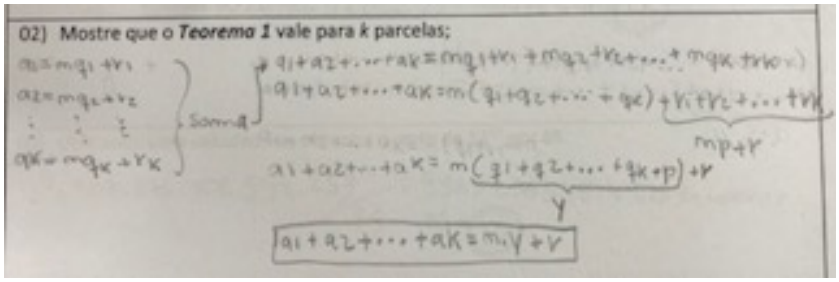


Figura 9 – Resposta do Aluno 5.

Tabela 17 – 3o Ano: Acertos da primeira Sequência Didática

PROBLEMA	CERTOS	PARCIALMENTE CERTOS	ERRADOS	SEM RESPOSTA
02	8	1	1	16
03	25	1	0	0
04	25	1	0	0
05	20	3	3	0
06	14	3	4	5
07	19	4	1	2
08	24	1	0	1
09	23	1	1	1

Fonte: Elaborada pelo autor.

Os percentuais que veremos foram com base na média aritmética por questão. Podemos ver que tivemos, aproximadamente, 82% de acertos por questão quando analisamos do problema 03 ao 09. Esse percentual diminui para 76%, aproximadamente, de acertos quando consideramos o problema 02. Sem incluir o problema 02, aproximadamente, 8% de parcialidade no acerto por questão e que tinham pequenos comprometimentos na escrita, o que nos sugere que uma intervenção sobre como escrever matematicamente pode ajudar no momento de o estudante pensar, inferir e colocar no papel. Vemos, também, que, aproximadamente, 5% erraram algum problema (sem incluir o problema 02) e esse percentual se concentra nos problemas 5, 6 e 7 que se referem a aplicação dos teoremas 2 e 3. E, 5% desses alunos deixaram algum problema sem resposta, concentrando nos problemas 6, 7, 8 e 9, referente aos teoremas 3 e 4. Quando incluímos o problema 02, onde tivemos a maioria (16) sem resposta, o percentual de questões sem resposta, em média, sobe para 12% do alunado. Tivemos 100% dos alunos sinalizando não terem condições de responder o problema 02, mas, após apresentação dos teoremas e, mesmo o problema exigindo uma demonstração, prática não corriqueira em sala de aula, tivemos 80% de acertos nesse item dentre aqueles que tentaram responder, 10% de parcialidade no acerto do item e 10% de erro. Vale salientar que, aproximadamente, 61,5% da turma deixou este item sem resposta. Isso mostra que é possível inserir a prática das demonstrações de teoremas e propor exercícios na qual os estudantes façam tal demonstração.

Para a aplicação da sequência didática 3 e 4, expus o processo de codificação de mensagens utilizando o RSA através dos teoremas já estudados e do método imposto pelo RSA. Não utilizamos calculadoras nesse processo e sim rascunhos com lápis em papel. A ideia é tentar desenvolver a habilidade do cálculo mental na aplicação do método, consequentemente, dos teoremas. Utilizei, como critério de participação para esta sequência didática, o estudante que participou da aplicação da primeira sequência. Foi perceptível, nessa segunda sequência didática, um trabalho extenuante por parte dos alunos do primeiro ano. Foi a turma que eu mais precisei inferir, cobrar participação e agilidade nos processos.

1º Ano do Ensino Médio

A turma é composta por 37 alunos e participaram da aplicação os mesmos 21 estudantes.

Tabela 18 – 1o Ano: Acertos da Segunda Sequência Didática

PROBLEMA	CERTOS	PARCIALMENTE CERTOS	ERRADOS	SEM RESPOSTA
10	21	0	0	0
11	21	0	0	0
12	10	8	0	3
13	8	10	0	3

Fonte: Elaborada pelo autor.

É perceptível o baixo percentual de acertos nessa turma. Tivemos, em média, 71% de acertos. Os percentuais mais baixos se concentraram nos itens 12 e 13 com 48% e 38%, respectivamente. Acredito que a razão para tal se deu em virtude de os itens exigirem mais cálculos por parte dos alunos, uma vez que, essa turma apresentou índices de aproveitamento menores dos que as demais turmas na aplicação da primeira sequência didática.

2º Ano do Ensino Médio

A turma é composta por 40 alunos e participaram da aplicação os mesmos 27 estudantes.

Tabela 19 – 2o Ano: Acertos da Segunda Sequência Didática

PROBLEMA	CERTOS	PARCIALMENTE CERTOS	ERRADOS	SEM RESPOSTA
10	27	0	0	0
11	26	1	0	0
12	26	1	0	0
13	20	5	0	2

Fonte: Elaborada pelo autor.

A turma de segundo ano apresentou um excelente rendimento na segunda sequência didática. O percentual de acertos ficou em, aproximadamente, 92% denotando um bom rendimento. O item 13 apresentou o menor percentual de acerto, aproximadamente, 74%. Mesmo assim, apenas 7%, aproximadamente, entregaram o item em branco.

3º Ano do Ensino Médio

A turma é composta por 36 alunos e participaram da aplicação os mesmos 26 estudantes que participaram da atividade anterior.

Tabela 20 – 3o Ano: Acertos da Segunda Sequência Didática

PROBLEMA	CERTOS	PARCIALMENTE CERTOS	ERRADOS	SEM RESPOSTA
10	26	0	0	0
11	26	0	0	0
12	21	5	0	0
13	26	0	0	0

Fonte: Elaborada pelo autor.

Todos os alunos mostraram comprometimento com a atividade e isso acarretou um bom número de acertos. Em média, 95% de acertos na atividade.

Como já estávamos na última sequência didática (aulas 5 e 6), deixei-os livres para usar a calculadora se eles julgassem necessário. Percebi alguns estudantes usando a calculadora para conferir seus cálculos e outros a utilizaram diretamente para resolver os problemas, principalmente, nas turmas de terceiro e segundo ano. Fiz a exposição do processo de decodificação pelo método RSA, encontrando o inverso do **e** e, por conseguinte, mostrei a decodificação da palavra RECIFE, antes codificada na aplicação da sequência didática das aulas 3 e 4. Feito isso, entreguei a ficha do aluno e pedi para que eles as respondessem e usassem os dados necessários, guardados por eles, da atividade anterior, neste caso, a chave de codificação e a mensagem recebida por eles do seu colega. No caso do terceiro ano, não tivemos maiores problemas. No segundo ano, houve uma interação maior entre eles na resolução dos itens de maneira superficial. Mas, a turma de primeiro ano, mostrou certa imaturidade não lembrando de regras básicas já estudadas e, de longe, deu para eu perceber que muitos esqueceram e/ou perderam a mensagem recebida, sendo necessário minha intervenção em sugerir que olhassem nos seus rascunhos qual foi a mensagem enviada ao colega, uma vez que, eu não estava de posse da sequência das aulas 3 e 4 e a ficha do aluno não traz identificação. Foi necessário eu intervir e identificar aluno por aluno qual a mensagem e para quem foi enviada. Nesta turma, o tempo se estendeu mais do que o normal e foi necessário eu tomar a aula seguinte para concluir a tarefa.

1º Ano do Ensino Médio

A turma é composta por 37 alunos e participaram da aplicação os mesmos 21 estudantes.

Tabela 21 – 1o Ano: Acertos da Terceira Sequência Didática

PROBLEMA	CERTOS	PARCIALMENTE CERTOS	ERRADOS	SEM RESPOSTA
14	15	2	4	0
15	9	6	6	0
16	13	4	4	0
17	14	5	2	0

Fonte: Elaborada pelo autor.

A atividade aplicada nesta turma não trouxe resultados significativos de aprendizagem. Podemos ver que, em média, tivemos 61% de acertos ficando bem distante dos percentuais alcançados nas atividades anteriores.

2º Ano do Ensino Médio

A turma é composta por 40 alunos e participaram da aplicação os mesmos 27 estudantes.

Tabela 22 – 2o Ano: Acertos da Terceira Sequência Didática

PROBLEMA	CERTOS	PARCIALMENTE CERTOS	ERRADOS	SEM RESPOSTA
14	20	0	7	0
15	19	1	7	0
16	20	0	7	0
17	20	1	6	0

Fonte: Elaborada pelo autor.

Esta turma se mostrou, nesta sequência didática, com um índice razoável de acertos, aproximadamente, 73%. Como esta turma foi a última a passar pela terceira sequência didática, acredito que o tempo (intervalo entre uma sequência e outra) foi preponderante na alavancagem desse percentual. Contudo, a turma vem com percentuais muito próximos quando comparamos com a primeira sequência didática.

3º Ano do Ensino Médio

A turma é composta por 36 alunos e participaram da aplicação os mesmos 26 estudantes que participaram da atividade anterior.

Tabela 23 – 3o Ano: Acertos da Terceira Sequência Didática

PROBLEMA	CERTOS	PARCIALMENTE CERTOS	ERRADOS	SEM RESPOSTA
14	26	0	0	0
15	26	0	0	0
16	24	1	1	0
17	26	0	0	0

Fonte: Elaborada pelo autor.

A atividade aplicada na turma do terceiro ano trouxe resultados incríveis. Podemos ver que, em média, tivemos 98% de acertos.

5.2 Consolidação dos dados

A tabela a seguir, Consolidação dos dados, traz o Índice Médio por Turma (IMT) de acertos de cada sequência didática e, também, o Índice Médio por Sequência Didática (IMS) de cada turma, no que se refere aos percentuais de acertos de cada sequência didática por turma. Nesses dois índices, IMT e IMS, a média utilizada continua sendo a aritmética. Vale ressaltar que tais índices é uma estimativa numérica criada com a intenção de trazer um dado numérico mas com a observância que tal avaliação envolve muito mais fatores cognitivos no que tange aos critérios da aprendizagem.

Tabela 24 – Consolidação dos dados

	1o Ano	**2o Ano**	**3o Ano**	**IMS (%)**
Primeira Sequência Didática	73	71	82	75,3
Segunda Sequência Didática	71	92	95	86
Terceira Sequência Didática	61	73	98	77,3
IMT (%)	68,3	78,7	91,7	

Fonte: Elaborada pelo autor. IMS (Índice Médio por Sequência); IMT (Índice Médio por Turma)

É possível ver que o primeiro ano apresentou o menor IMT, 68,3%, que pode ser atribuído ao fato de termos estudantes recém chegados no Ensino Médio e, ainda há de levar em consideração o grau de amadurecimento desses alunos advindos de um momento de pandemia onde, em 2020, permaneceram com sua educação remota, iniciando o sétimo ano do Ensino Fundamental II em plena pandemia da covid. No Encontro Gaúcho de Educação Matemática, em 2021, foi apresentado o estudo: O Ensino de Matemática e os Desafios dos Professores Frente à Pandemia, pela UFPel, onde os pesquisadores Thalita Fagundes Leal, Filipe Henrique Ramos e Luana Leal Alves trazem resultados concretos de uma pesquisa qualitativa com professores de matemática da rede pública da cidade de Pelotas, no ensino de matemática no período da pandemia, com o objetivo de investigar e identificar os desafios enfrentados pelos professores.[1].

> *"De acordo com Senhoras (2020) à Pandemia apresenta alguns efeitos críticos sobre a Educação, que referem-se aos impactos negativos manifestado pelo comprometimento do processo de ensino e aprendizagem e pelo aumento da evasão escolar, já que muitos estudantes não possuem acesso aos meios tecnológicos".*

Dessa forma, acredito que os resultados apresentados pela turma do 1o Ano do Ensino Médio, podem ser revalidados a posteriori, intervindo e reforçando pontos que possam ser elencados pelos estudantes sobre o tema a fim de sanar possíveis dúvidas.

[1] Ver no sítio https://wp.ufpel.edu.br/egem2021/files/2021/07/027.pdf

Conclusão

Este trabalho foi idealizado com o objetivo de levar ao conhecimento dos estudantes ferramentas matemáticas significativas, apresentadas em forma de teoremas aplicados à criptografia, tema importante que vivemos, cotidianamente, mostrando sua relevância prática e de como a matemática fornece o devido suporte ao desenvolvimento de diversas áreas do conhecimento.

O método proposto tem, como ferramentas, conteúdos apropriados para a educação básica, envolvendo características e propriedades da teoria dos números, o uso de ferramentas de suporte como a calculadora e o contexto histórico da evolução da criptografia, oportunizando ao estudante manipular uma das mais belas aplicações da aritmética na contemporaneidade.

Os resultados colhidos, em forma de índices de aprendizagem, foram satisfatórios levando em consideração o grau de amadurecimento de cada turma do Ensino Médio e, talvez, com sensíveis adaptações, poderemos aplicar em forma de oficina para as séries finais do Ensino Fundamental.

Decerto, como não obtemos resultados satisfatórios com a turma do primeiro ano, pois percebemos que ela não acompanhou no mesmo nível as séries seguintes, o processo necessita de alguns ajustes. Acreditamos que o resultado esteja ligado ao grau de maturidade da turma e aos anos anteriores vividos em plena pandemia.

Uma forma de melhoria dos processos seria dispor de mais tempo, em cada sequência didática, e inserir mais itens com diversos outros exemplos com a finalidade de desenvolver habilidades sobre a temática.

Referências

BOYER, C. *História da Matemática*. Rio de Janeiro: Blucher, 2012.

CARNEIRO, F. J. F. *Criptografia e Teoria dos Números*. Rio de Janeiro: Editoda Ciência Moderna Ltda, 2017.

COUTINHO, S. C. *Números Inteiros e Criptografia RSA*. Rio de Janeiro: IMPA, 2014.

DOLZ NOVERRAZ, S. *Sequências didáticas para o oral e a escrita: apresentação de um procedimento*. Campinas: Mercado de Letras, 2004.

G1. *Pai da computação, Turing recebe o perdão real 59 anos após morrer*. São Paulo: Tecnologia e Games. http://glo.bo/JX9sAd, 2013.

HEFEZ, A. *Elementos de Aritmética*. Rio de Janeiro: SBM, 2011.

HISTóRIA, A. da. *Por que a Rainha Elizabeth II concedeu seu perdão real ao pai da computação?* São Paulo: Notícias. https://bit.ly/3W0hqhq, 2022.

MACHADO, A. R. *A Sequência Didática no Ensino de Matemática*. Rio Claro: Educação Matemática em Revista, 2009.

PERNAMBUCO, S. *Secretaria de Educação e Esportes. Currículo de Pernambuco*. Pernambuco: Ensino Médio, 2021.

SANTOS, D. M. F. *Utilização da Sequência Didática no Ensino da Matemática*. Rio Claro: Encontro Nacional de Educação Matemática, 2018.

SINGH, S. *O livro dos códigos*. Rio de Janeiro: Record, 2001.

SINGH, S. *Os Segredos Matemáticos dos Simpsons*. Rio de Janeiro: Record, 2016.