UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
PROGRAMA DE PÓS GRADUAÇÃO EM ENSINO DE CIÊNCIAS EXATAS

ROBERTA MAÍRA VERDERI BRAILA

O ENSINO DE FUNÇÕES CONTEXTUALIZADO À CRIPTOGRAFIA

SOROCABA
2021

ROBERTA MAÍRA VERDERI BRAILA

O ENSINO DE FUNÇÕES CONTEXTUALIZADO À CRIPTOGRAFIA

Dissertação apresentada ao Programa de Pós Graduação em Ensino de Ciências Exatas (PPGECE) para a obtenção do título de Mestre em Ensino de Ciências Exatas.

Orientação: Prof.ª Dr.ª Silvia Maria Simões de Carvalho

SOROCABA
2021

Braila, Roberta Maíra Verderi

O ensino de funções contextualizado à criptografia / Roberta Maíra Verderi Braila -- 2021.
94f.

Dissertação (Mestrado) - Universidade Federal de São Carlos, campus Sorocaba, Sorocaba
Orientador (a): Silvia Maria Simões de Carvalho
Banca Examinadora: Magda da Silva Peixoto, Mayk Vieira Coelho
Bibliografia

1. Função. 2. Criptografia. 3. Ensino. I. Braila, Roberta Maíra Verderi. II. Título.

Ficha catalográfica desenvolvida pela Secretaria Geral de Informática (SIn)

DADOS FORNECIDOS PELO AUTOR

Bibliotecário responsável: Maria Aparecida de Lourdes Mariano - CRB/8 6979

UNIVERSIDADE FEDERAL DE SÃO CARLOS

Centro de Ciências Exatas e de Tecnologia
Programa de Pós-Graduação em Ensino de Ciências Exatas

Folha de Aprovação

Defesa de Dissertação de Mestrado da candidata Roberta Maíra Verderi Braila, realizada em 24/09/2021.

Comissão Julgadora:

Profa. Dra. Silvia Maria Simões de Carvalho (UFSCar)

Prof. Dr. Mayk Vieira Coelho (UNIFAL - MG)

Profa. Dra. Magda da Silva Peixoto (UFSCar)

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

O Relatório de Defesa assinado pelos membros da Comissão Julgadora encontra-se arquivado junto ao Programa de Pós-Graduação em Ensino de Ciências Exatas.

Dedico este trabalho ao meu esposo e aos meus pais, que sempre me entenderam e me apoiaram, não só na ausência durante o mestrado mas em todas as fases boas e ruins da minha vida.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por me dar forças para concluir mais esta etapa em minha vida acadêmica.

Ao meu esposo, por seu companheirismo, amor, apoio e por limpar as lagrimas derramadas durante o processo.

Aos meus pais, por estrarem ao meu lado sempre, me encorajando a nunca desistir.

Ao Colégio Anglo Cabreúva, pela abertura para a aplicação do trabalho.

Aos professores do Programa de Pós-Graduação em Ensino de Ciências Exatas (PPGECE) por todos os ensinamentos durante o curso de mestrado.

Agradeço principalmente à minha orientadora professora Dra. Sílvia Maria Simões de Carvalho, pela paciência e dedicação durante todo o tempo, além dos incansáveis ensinamentos que me fizeram encantar ainda mais pela área escolhida. Obrigada por tudo.

“A mente que se abre a uma nova ideia, jamais voltará ao seu tamanho original.”

(Albert Einstein)

RESUMO

O ensino da Matemática nos dias atuais vêm enfrentando grandes dificuldades com o desinteresse dos alunos em aprender o conteúdo, considerado por muitos como um trabalho árduo e sem retorno para a vida futura, tanto profissionalmente quanto pessoalmente, pois na maioria das vezes são ensinadas fórmulas e regras sem nenhuma explicação da utilidade das mesmas. Sendo as funções um dos conteúdos ignorados pelos alunos, o objetivo deste trabalho é verificar o desenvolvimento dos alunos através de uma aplicação prática envolvendo Criptografia e funções, trazendo assuntos do cotidiano como a Criptografia, encontrada em diversos meios, principalmente eletrônicos, para as aulas e a utilização de práticas diferenciadas como jogos, exercícios e ferramentas computacionais, culmina numa aprendizagem mais significativa, com melhores desempenhos e uma maior disposição por parte dos alunos durante as aulas desta disciplina.

Palavras chaves: Funções. Criptografia. Ensino

ABSTRACT

The teaching of Mathematics nowadays is facing great difficulties with disinterest of the students in learning the contents, considered for some as a hard job and no return for a future life, as professional though in person, on majority of times they are taught formulas and rules with no explanation of utility of the same subject. Being the functions one of the contents ignored by the students, the objective of this job is to check the student development through a practical application involving Cryptography and functions, bringing subjects of daily, as well as cryptography found in diverse as quite, principally electronics, the classes and the practical utilization differentiated such as game, exercises and computation tools, which culminate a learning of more significant with better performance and a bigger disposition of the students during the classes of this subject.

Keywords: Functions. Cryptography. Teaching.

LISTA DE TABELAS

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

Com o crescimento acelerado do número de aplicativos e softwares desenvolvidos atualmente, está cada vez mais difícil chamar a atenção dos alunos para aulas convencionais, principalmente na disciplina de Matemática, onde muitos possuem aversão e montam barreiras em relação ao aprendizado da mesma.

Professores devem buscar atualização constantemente, para que possam inovar em suas aulas, tornando-as mais atrativas para os alunos e para si próprios. Uma maneira simples de inovação é a introdução da tecnologia em sala de aula.

A tecnologia está presente em todos os contextos do nosso cotidiano, onde a comunicação e a interação por meio de aplicativos de bate-papo, as transações comerciais e bancárias online estão cada vez mais em alta, principalmente no período pandêmico em que estamos vivendo.

Os ensinos remoto e híbrido tomaram conta das escolas e casas em todo o mundo. Com isso, alunos e professores estão se familiarizando com o uso de ferramentas como computadores, câmeras digitais e celulares durante as aulas.

Essa inserção, principalmente dos professores, no mundo tecnológico possibilita trazer os alunos para a disciplina oferecida, de tal maneira que os mesmos tenham novos olhares em relação a determinados conteúdos e aprendam de uma forma mais leve.

A Criptografia está presente nessa tecnologia. Encontrada em aplicativos como o WhatsApp, sites bancários, compras online, chaves de automóveis e etc., pode ser utilizada em sala de aula, com a finalidade de auxiliar no processo de ensino-aprendizagem, a partir da contextualização da mesma com conteúdos que requerem uma certa atenção pela dificuldade de compreensão por parte dos alunos, principalmente a noção de função que será tratada nessa dissertação. Além do conceito de funções, a Criptografia pode ser trabalhada em outros conteúdos matemáticos, como números primos, divisibilidade, matrizes, entre outros.

A partir de exercícios diferenciados envolvendo a Criptografia para o ensino de funções, na 3ª série do Ensino Médio, tem-se o intuito de verificar a validade dessa interação dos alunos com novas práticas e analisar se o aprendizado é mais eficaz com o uso da tecnologia e assuntos do cotidiano.

O capítulo 2 apresenta um breve histórico da Aritmética e sua importância para os dias de hoje. O capítulo 3 traz as noções básicas da Aritmética e suas propriedades, que serão

utilizadas no decorrer do trabalho. O capítulo 4 trata da divisibilidade, assunto muito importante para as operações envolvendo a Criptografia no ensino, além de aprofundar em algumas propriedades do capítulo anterior, a partir de alguns exemplos. O capítulo 5 mostra o contexto histórico dos números primos, voltando-se para as principais propriedades, teoremas e operações. No capítulo 6, será tratada a congruência modular, um dos ramos mais importantes da Aritmética, encontrada em vários contextos do nosso cotidiano, até mesmo na Criptografia, tema central deste trabalho, assunto que necessita das ideias da divisibilidade e números primos, já vistos anteriormente. O capítulo 7 traz um breve resumo da história da Criptografia, desde as primeiras aparições no Egito até a Criptografia RSA, uma das variações utilizadas atualmente. No capítulo 8, serão enunciados os conceitos de função, utilizada na aplicação proposta, além de trazer informações da utilização da Criptografia em sala de aula. No capítulo 9, temos a aplicação desenvolvida em sala de aula, que envolve a introdução do tema para os alunos e atividades práticas. Por fim, no capítulo 10, encontra-se a conclusão do trabalho desenvolvido.

2. BREVE HISTÓRICO

O início da Aritmética está estritamente ligado à ideia de contagem, a partir do momento em que se tornou necessário calcular, quantificar elementos e comparar grandezas. Nesse sentido, Ifrah (1985, p. 09) afirma que o surgimento da Aritmética se deu "provavelmente resultante da necessidade de recenseamento de bens, no registro de tempo ou de inventários de terras. Supõe-se que a função primeira dos números tenha sido a de quantificar, ou seja, de atribuir uma determinada quantidade a conjuntos específicos, respondendo a uma necessidade prática".

As ferramentas utilizadas para essa contagem eram ossos, pedras, paus e até mesmo os dedos. Nos ossos eram feitos risquinhos, as pedras colocadas em sacos ou até mesmo separadas em grupos para ser comparadas com alguma grandeza, assim como os paus, onde cada unidade correspondia à um pedaço. Já os dedos, eram utilizados para indicar conjuntos. Assim, uma mão podia representar conjuntos de dois até quatorze elementos.

Segundo Dantzig (1970, p.03) o senso numérico não deve ser confundido com contagem, que provavelmente é muito posterior. Assim, nota-se que os sinais para a representação dos números, surgiram antes da escrita do número em palavras, afinal a facilidade em fazer incisões em ossos era mais conveniente do que elaborar frases bem feitas para a identificação de um número.

A necessidade de realizar cálculos mais complexos e o comércio, fez com que surgisse o número em forma de palavras, o nascimento de uma linguagem de numeração universal e de uma ciência chamada Aritmética. Onde, derivada do grego *arithmos*, a palavra aritmética significa número. Com isso, para Trajano:

> Arithmetica é a scciencia dos números e a arte de calcular por meio de algarismos. [...] Algarismos arábicos são os dez signaes seguintes, chamados: 1 (um), 2 (dois), 3 (três), 4 (quatro), 5 (cinco), 6 (seis), 7 (sete), 8 (oito), 9 (nove) e 0 (zero). (TRAJANO, s/d, p. 05).

Nesse contexto, surge a escola pitagórica, cujo lema era "tudo é número".

Assim, podemos tratar a Aritmética como o mais antigo ramo da Matemática, que estuda as operações numéricas, muito utilizado até os dias de hoje.

> A Aritmética, como usualmente é chamada a parte elementar da Teoria dos Números, teve como principal marco inicial a obra Os Elementos, de Euclides (aprox. 300 a.C), encontrando seu auge nos trabalhos de Pierre de Fermat (1601 – 1665) e Leonhard Euler (1707 – 1783), o que a levou a tornar-se um dos principais pilares da

> Matemática. A partir do início do século XIX, graças à obra de Carl Friedrich Gauss (1777 – 1855), a Aritmética transformou-se em Teoria dos Números e começa a ter um desenvolvimento extraordinário. (HEFEZ, 2016, p.VII)

A obra *Os elementos*, de Euclides, foi considerado um texto introdutório que cobre toda a matemática elementar. Composto de treze livros, onde três deles estão dedicados a Aritmética, no sentido de "teoria dos números".

Podemos dizer que a humanidade atravessou um imenso caminho para chegar à teoria citada, que segundo Dantzig (1970, p. 59), teria evoluído como uma "espécie de numerologia" e, então, passado por um "período errático de solução de charadas antes de adquirir o status de ciência". No final do período renascentista, por volta do século XVII, foram estabelecidas as técnicas de contagem e as regras de cálculos. Muitas lutas aconteceram nesse intervalo de tempo, como disputas por território e religião. Além disso, as inúmeras práticas de contar, quantificar e medir foram se modificando no decorrer dos anos. A nomenclatura também passou por mudanças. Para Dantzig (1970, p. 45), Arithmética era a Teoria do Número até o século XVII. O que atualmente denomina-se Aritmética era, para os gregos, Logística, e, na Idade Média, Algarismo.

Para Cambi (1999), o estudo da aritmética sempre esteve presente nas civilizações, desde os filósofos da antiguidade. Podemos dizer que Pitágoras (570- 497 a.C.) foi quem deu início a escrita sobre números; seguido por Nicômaco (60-120 d.C.) que deu continuidade a esse trabalho.

Em relação a cultura clássica, a maior parte do que é conhecido foi difundido para a Idade Média pelo Santo Isidoro(560-636) em sua obra *Etimologias*, composta por vinte livros, sendo o livro III, *Quadrivium: las matemáticas: arithmética, geometría, música, y astronomia.* Com isso, nota-se que a aritmética foi de grande importância também para a religião.

Inseridos nessa chamada "teoria dos números", encontram-se dois conceitos matemáticos considerados muito relevantes: Divisibilidade e Congruência.

Através da utilização de bases decimais, os critérios de divisibilidade nos permite verificar divisores de um determinado número e, até mesmo, resolver todo tipo de divisão. Esses critérios, apareceram no VII livro de Euclides, onde inicialmente foi tratada a ideia de máximo divisor comum.

Outros matemáticos muito importantes para a Teoria dos Números foram Gauss e Pierre de Fermat. Ambos tiveram várias contribuições, sendo que uma delas é o Pequeno Teorema de Fermat: *Se p é primo e a é um número não divisível por p, o número* $a^{p-1} - 1$ *é divisível por p.* A demonstração desse teorema foi publicada um século mais tarde por Leonard Euller.

Para Gauss esse teorema é considerado uma congruência do tipo: $a^p \equiv a \bmod p$.

A chamada Aritmética modular surge a partir dos conceitos de Divisibilidade e Congruência, e Gauss é conhecido como o pai dessa Aritmética pelas suas contribuições à Teoria dos Números.

2.1.Carl Friedrich Gauss

Carl Friedrich Gauss(1777-1855) nascido de uma simples família na Alemanha, em Brunswick, foi considerado um dos maiores matemáticos.

Desde pequeno sua genialidade já era percebida, pois o mesmo aprendera a ler sozinho e demonstrara uma grande habilidade em realizar cálculos complexos mentalmente, divertindo-se com isso.

Uma anedota referente aos seus começos na escola é característica. Um dia, para ocupar a classe, o professor mandou que os alunos somassem todos os números de 1 a 100, com instruções para que cada um colocasse sua lousa sobre a mesa logo que completasse a tarefa. Quase imediatamente, Gauss colocou sua lousa sobre a mesa dizendo: "Aí está!". Quando o instrutor finalmente olhou os resultados, a lousa de Gauss era a única com a resposta correta, 5050, sem nenhum outro cálculo. (BOYER e MERZBACH, 2012, p.343, 344).

Além desse episódio, ainda bem jovem, Gauss resolveu o *Paradoxo do Binômio*, onde completou o desenvolvimento do chamado Binômio de Newton, introduzindo a noção de convergência para séries infinitas, algo revolucionário para a época.

Gauss iniciou seus estudos em Aritmética com 17 anos, com o intuito de esclarecer e completar o que já havia sido feito. Aos 21 anos produz uma das maiores obras da Matemática de todos os tempos, o livro *Disquisitiones Arithmeticae*(1801), que consiste em sete secções, onde as quatro primeiras eram sobre teoria dos números, a quinta dedicada a teoria das formas quadráticas, a sexta consiste em aplicações e por fim, a sétima secção trata da resolução da equação ciclotômica geral de grau primo.

Em sua obra, Gauss nos faz perceber relações na divisão de dois ou mais números, por um outro qualquer, que independente do quociente, deixam o mesmo resto. *"Nele, [Gauss] compilou o trabalho de seus predecessores e deu à área uma vida nova, desenvolvendo as teorias de congruências quadráticas, formas e resíduos". (MOL, 2013, p. 125)*.

Em 1799, quando cursava doutorado na Universidade de Helmstedt, Gauss tinha entre seus professores Johann Friedrich Pfaff(1765-1825), que foi considerado o maior matemático alemão após Gauss. Nessa época, Gauss consegue provar o Teorema Fundamental da Álgebra e, iniciar a partir do plano cartesiano, os números complexos na Matemática.

Em 1812, aos 35 anos, estuda a convergência da série hipergeométrica, que abrangia as funções matemáticas como logarítmica e trigonométrica, além de outras da Física e Astronomia, o que lhe rendeu a inclusão na área da Análise Matemática.

Em relação à geometria, pode-se dizer que Gauss não tinha tanto apreço. Porém, em 1824, chegou a uma importante conclusão sobre as retas paralelas, não publicada. Em 1827, publicou um tratado clássico, considerado um percursor para um novo ramo da Geometria, chamado Geometria Diferencial.

Por todas as suas contribuições a matemática, Gauss é conhecido como *o príncipe das rainhas das ciências.*

Mesmo com esse "título", não tinha muitos alunos por ser ríspido em seus tratamentos e comentários, porém, não podemos subestimar a influência tida por ele nas gerações futuras. Nesse sentido, Boyer afirma que:

> Aqueles que estudaram suas publicações, os poucos que vinham se encontrar com ele, os que seguiram as novas avenidas de pesquisa que ele abriu incluem alguns dos mais bem conhecidos matemáticos do século dezenove. Quando se tratava de sua opinião expressa sobre o trabalho dos outros, no entanto, seu impacto não era sempre salutar. Perto do fim de sua vida, Gauss pode ter se tornado, de modo não característico, generoso em seus comentários; observamos a bem merecida apreciação da habilidade de Riemann e o entusiasmo questionável em relação a Eisenstein. (BOYER, 2012, p.350).

Gauss faleceu em 1855, em uma década conhecida como o fim de uma era, pelo fato da morte de outros importantes matemáticos, mas trouxe um direcionamento para os legados de Gauss, começando com a obra de Bernhard Riemann (1826-1866).

Com isso, afirmamos que Gauss mudou os rumos da matemática com os seus trabalhos revolucionários, mostrando os com perfeição, exatidão e fineza.

2.2.Pierre de Fermat

Pierre de Fermat nasceu em 1601 na Franca, na cidade de Beaumont-dLomagne, em

uma família de posses, o que possibilitou a Fermat uma educação favorecida.

Estudou no Monastério Franciscano de Grandselve e mais tarde cursou Direito em Toulouse, participando do parlamento como advogado e como conselheiro.

Mesmo tendo um trabalho em outra área do conhecimento, podemos dizer que Fermat dedicava um tempo à literatura, ciência e também matemática, onde em 1629 iniciou importantes descobertas. Por isso, é conhecido como o "príncipe dos amadores" em matemática.

Começou reconstruindo obras antigas, com base nos clássicos preservados. Primeiramente, dedicou-se aos *Lugares geométricos planos* de Apolônio, apoiado na *Coleção matemática* de Papus, onde aproximadamente em 1636 descobriu o princípio fundamental da geometria analítica. Após um ano dessa descoberta houve o aparecimento da *Geometria* de Descartes e, comparando os trabalhos, podemos dizer que houve uma contrariedade dos pensamentos em relação ao tema tratado. Baseado nisso, Boyer afirma que:

> Enquanto Descartes construíra sua *Geometria* em torno do difícil problema de Papus, Fermat limitou sua exposição, no curto tratado intitulado Ad locus planos et sólidos isagoge (Introdução ao lugares geométricos planos e sólidos), apenas aos lugares geométricos mais simples. (BOYER, 2012, p.245).

Continuando com seu trabalho sobre lugares geométricos, fez outras duas descobertas significativas. A primeira era como achar máximos e mínimos, processo que hoje é chamado de derivação. E a segunda, como calcular tangentes e áreas de curvas.

Com isso, podemos dizer que Fermat dedicara seu tempo a vários aspectos da análise infinitesimal (tangentes, quadraturas, volumes, comprimentos de curvas, centros de gravidade), da geometria analítica e também da aritmética.

No ramo da Aritmética, Fermat se tornou o fundador da moderna teoria dos números, baseando-se nos números perfeitos, números figurados, quadrados mágicos, divisibilidade, ternas pitagóricas e números primos.

Na demonstração de seus teoremas utilizou um método conhecido como "descida infinita", processo pelo qual Fermat foi o primeiro a usar, era como uma indução matemática ao contrário. A partir desse processo, conseguiu demonstrar a afirmação feita por Girard, de que todo número primo escrito da forma 4n+1 pode ser escrito de um único modo como a soma de quadrados.

Além disso, Fermat demonstrou dois grandes teoremas, o Pequeno Teorema de Fermat, descrito anteriormente, teve um destino melhor que suas conjecturas sobre números primos,

intitulado como o Último Teorema de Fermat:

Teorema 2.1. *Para todo $n \in \mathbb{Z}$, tal que n maior que 2, não existe valores inteiros positivos x, y,z, onde $x^n+y^n=z^n$.*

Fermat não deixou a demonstração desse teorema descoberto em 1637, deixou somente uma frase na margem de uma folha que dizia: “Eu tenho uma demonstração realmente maravilhosa para esta proposição mas esta margem é muito estreita para contê-la”. Com isso, o mesmo permaneceu sem solução até aproximadamente 1993. Sobre isso, Singh afirma:

> Este era Fermat no seu modo mais frustrante. Suas próprias palavras sugerem que ele estava particularmente satisfeito com sua demonstração “realmente maravilhosa” mas não se daria o incômodo de escrevê-la em detalhe, quanto mais publicá-la. (SINGH, 2008, p.80)

Fermat ficou seriamente doente em 1665 e faleceu em 12 de janeiro deste mesmo ano.

3. NOÇÕES DE ARITMÉTICA

Considerada a ciência dos números, a Aritmética é o ramo da Matemática que estuda os números e suas operações. A partir disso, Dantzig afirma que:

> A Aritmética é a base de toda a Matemática, pura ou aplicada. É a mais útil das ciências e provavelmente não existe nenhum outro ramo do conhecimento humano tão espalhado entre as massas. (Dantzig, T., 1970, p. 44.)

Podemos dizer que o conhecimento da Aritmética é indispensável para todos, afinal é a partir dele que nasce a ideia de contagem tão importante no nosso dia a dia.

A Aritmética, conhecida mais tarde como Teoria dos Números, passa por muitas transformações ao longo dos anos, baseando-se sempre no conceito de números e suas operações, a partir da ideia dos números naturais como uma sequência de números até a introdução dos números inteiros.

3.1.Números Inteiros

A ideia de número inteiro surgiu a partir dos números naturais, que tinha como um de seus objetivos, resolver problemas de contagem.

Com o advento do mercantilismo na Europa, no final da Idade Média, houve a necessidade de trabalhar com números inteiros relativos.

Somente no final do século XIX, a noção de número passou a ser baseada na teoria dos conjuntos, quando foram questionados os fundamentos da Matemática.

Giuseppe Peano (1858-1932) demonstrou toda teoria dos números naturais (N) em quatro axiomas, chamados de Axiomas de Peano.

Definição 3.1. Axiomas de Peano

1. Existe uma função $s: \mathbb{N} \to \mathbb{N}$, que associa cada elemento $n \in N$ um elemento $s(n) \in N$, chamado o sucessor de n.
2. A função $s: \mathbb{N} \to \mathbb{N}$ é injetiva.

3. Existe um único elemento, denotado por "1", no conjunto $\mathbb{N}$, tal que $1 \neq s(n), \forall\, n \in \mathbb{N}$.

4. Se um subconjunto $X \subset \mathbb{N}$ é tal que $1 \in X$ e $s(x) \in X \Rightarrow X = \mathbb{N}$.

Além dos citados números naturais, as relações de comércio motivaram a criação de um símbolo que representasse o "nada", surgindo assim o número 0.

Podemos inserir nesse contexto a ideia de inverso aditivo de um número $x \in \mathbb{N}$ como $-x$, onde $x \in (-\mathbb{N})$, ou seja, aos inversos dos números naturais, tal que $x+(-x)=0$.

A partir dessa teoria dos conjuntos, dizemos que o conjunto dos números inteiros ($\mathbb{Z}$) é composto por três subconjuntos:

$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-\mathbb{N}\}$, onde $\mathbb{N} = \{1,2,3,4, \dots\}$ e $-\mathbb{N} = \{-1,-2,-3,-4, \dots\}$, assim:

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

3.1.1. Adição e multiplicação em $\mathbb{Z}$

No conjunto dos números inteiros ($\mathbb{Z}$) são admitidas as seguintes propriedades:

- Adição:

i. Seja $a, a', b, b' \in \mathbb{Z}$, se $a = a'$ e $b = b'$, então $a + b = a' + b'$.
ii. Comutativa: Seja $a, b \in \mathbb{Z},\ a + b = b + a$.
iii. Associativa: Seja $a, b, c \in \mathbb{Z},\ (a + b) + c = a + (b + c)$.
iv. Elemento neutro: Seja $a \in \mathbb{Z}, a + 0 = a$.
v. Elementos simétricos: Existe um $b \in \mathbb{Z}$, onde $b = -a$, tal que $a + b = 0$.

- Multiplicação:

i. Seja $a, a', b, b' \in \mathbb{Z}$, se $a = a'$ e $b = b'$, então $a.b = a'.b'$.
ii. Comutativa: Seja $a, b \in \mathbb{Z}, a.b = b.a$.
iii. Associativa: Seja $a, b, c \in \mathbb{Z},\ (a.b).c = a.(b.c)$.
iv. Elemento neutro: Seja $a \in \mathbb{Z}, a.1 = a$.

Além destas, existe uma propriedade que engloba tanto a adição quanto a multiplicação:

i. Propriedade distributiva: Seja $a, b, c \in \mathbb{Z}, a.(b + c) = a.b + a.c$.

3.1.2. Outras Propriedades dos números inteiros

Além das propriedades citadas, existem outras duas muito importantes, principalmente para a demonstração de teoremas. São elas:

- Fechamento em $\mathbb{N}$: Para todos $a, b \in \mathbb{N}$, tem-se que, o conjunto $\mathbb{N}$ é fechado, tanto para a adição quanto para a multiplicação, ou seja, $a + b \in \mathbb{N}$ e $a.b \in \mathbb{N}$.

- Tricotomia: Seja $a, b \in \mathbb{Z}$, onde somente uma das propriedades é verificada:

i. $a = b$;
ii. $a < b$, se $b - a \in \mathbb{N}$;
iii. $b < a$, se $-(b - a) = a - b \in \mathbb{Z}$.

A propriedade de fechamento afirma que tanto a adição quanto a multiplicação de dois números naturais resulta sempre em um número natural. Já a tricotomia, baseia-se em três proposições, onde a demonstração somente será possível se, apenas uma delas for válida.

3.1.3. Relação "menor do que"

A relação "menor do que" é compatível com as seguintes propriedades:

- Transitiva: Seja $a, b, c \in \mathbb{Z}$ se $a < b$ e $b < c$, então $a < c$.

DEMONSTRAÇÃO:
Supondo $a < b$ e $b < c$, *temos que* $b - a \in \mathbb{N}$ e $c - b \in \mathbb{N}$.
Pelo processo aditivo, temos:
$c - a = (b - a) + (c - b) \in \mathbb{N}$,
Logo, $a < c$.

- Aditiva: Seja $a, b, c \in \mathbb{Z}$ se $a < b$ e $b < c$, se e somente se, $a + c < b + c$.

DEMONSTRAÇÃO:
($\Rightarrow$)*Supondo* $a < b$, *então* $b - a \in \mathbb{N}$.
Seja $b - a = (b + c) - (a + c) \in \mathbb{N}$, *temos que* $a + c < b + c$.
($\Leftarrow$)*Supondo* $a + c < b + c$, *temos que* $b - a = (b + c) - (a + c) \in \mathbb{N}$.

Somando $(-c)$ *em ambos os lados da desigualdade temos* $a < b$.

- Multiplicativa: Seja $a, b \in \mathbb{Z}$, para todo $c \in \mathbb{N}$, temos que, $a < b$ se, e somente se, $a.c < b.c$.

DEMONSTRAÇÃO:

$(\Rightarrow)$*Supondo* $a < b$*, então* $b - a \in \mathbb{N}$.

Multiplicando por (c) *temos,* $(b - a).c$.

Aplicando a propriedade distributiva, $bc - ac \in \mathbb{N}$.

Logo, $a.c < b.c$.

$(\Leftarrow)$*Supondo* $a.c < b.c$*, onde* $a, b \in \mathbb{Z}$ *e* $c \in \mathbb{N}$. *Pela tricotomia:*

i. $a = b$*, então* $ac = bc$. *(falso)*

ii. $b < a$*, então* $bc < ac$. *(falso)*

iii. $a < b$*, então* $ac < bc$. *(verdadeiro)*

3.1.4. Relação de ordem

A noção de relação de ordem é bastante ampla. No nosso dia a dia nos deparamos com essa relação em filas, em listas de tarefas, nas listas de chamadas escolares, no sistema de numeração, em senhas, entre outros. Quando trabalhamos com essa relação de ordem na Aritmética, isso muda um pouco, afinal nada mais é que uma propagação dos conceitos de maior ou igual e menor ou igual e está baseada em três importantes propriedades. São elas:

- Reflexiva: $\forall a \in \mathbb{Z}, a \leq a$.
- Antissimétrica: $\forall a, b \in \mathbb{Z}, a \leq b, b \leq a \Rightarrow a = b$.
- Transitiva: $\forall a, b, c \in \mathbb{Z},\ a \leq b,\ b \leq c \Rightarrow a \leq c$.

Exemplo 3.1.4.1. Mostre que a relação $\leq$ é uma relação de ordem em $\mathbb{Z}$

Solução:

Reflexividade: É óbvio que $a \leq a, \forall\, a \in \mathbb{Z}$.

Antissimetria: Se $a \leq b$ e $b \leq a$ então $(a < b$ ou $a = b)$ e $(b < a$ ou $b = a)$, o que é equivalente a $(a < b$ e $b < a)$ ou $a = b$. Portanto, pela tricotomia, temos que $a = b$.

Transitividade: Suponhamos que $a \leq b,\ b \leq c,$ então $b - a \in \mathbb{N} \cup \{0\}$ e $c - b \in \mathbb{N} \cup \{0\}$, logo $c - a = b - a + c - b \in \mathbb{N} \cup \{0\}$. Portanto, $a \leq c$.

Com isso, a relação $\leq$ é uma relação de ordem em $\mathbb{Z}$

3.2.Princípio da Boa Ordem

Definição 3.2. *Se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então S possui menor elemento.*

Dizemos que um subconjunto S de $\mathbb{Z}$ é limitado inferiormente, se existir $c \in \mathbb{Z}$ tal que $c \leq x$, para todo $x \in S$ e também, $a \in S$ é o menor elemento de S se $a \leq x$, para todo $x \in S$.

Em relação a $\mathbb{N}$, temos que como qualquer subconjunto de $\mathbb{N}$ é limitado inferiormente pelo número 1, todo subconjunto não vazio de $\mathbb{N}$ possui em menor elemento.

Se T é um subconjunto de $\mathbb{Z}$ não vazio e limitado superiormente, então T possui um maior elemento.

DEMONSTRAÇÃO:

Supondo c uma cota superior de T. Logo, $x \leq c, \forall x \in T$.

Considerando o conjunto $S = \{y \in \mathbb{Z}; y = c - x, x \in T\}$.

Dizemos que S é não vazio e como $y = c - x \geq 0, \forall x \in T$, é limitado inferiormente.

Assim, pelo Princípio da Boa ordenação, S possui um menor elemento $c - b$, com $b \in T$.

Se $x \in T$, temos que $c - x \in S$, logo $c - x \geq c - b$. Com isso, $x \leq b$, o que implica que $b = maxT$.

3.3. Princípio da Indução Matemática

No dicionário, a palavra indução está definida como: “1. Ato ou efeito de induzir. 2. Operação de estabelecer uma proposição geral com base no conhecimento de certo número de dados singulares”. (FERREIRA, 2001, p. 385)

Quando falamos de indução matemática, podemos dizer que nada mais é que uma importante ferramenta de verificação de conjecturas sobre padrões e sequências numéricas.

A partir dessa ideia de sequências, um matemático que teve muitas contribuições foi Giuseppe Peano(1858-1932).

Peano nasceu em Spinetta e foi considerado o maior matemático italiano de sua época. Foi muito importante na axiomatização, onde desenvolveu os Axiomas de Peano, citados anteriormente, considerados como sua maior contribuição para a teoria dos conjuntos, pois foi a partir daí que nasce a ideia do conjunto dos números naturais e inteiros. Para Boyer: "Os axiomas de Peano representaram a tentativa mais singular, realizada no século XIX, de reduzir a aritmética comum e, consequentemente, a maior parte d matemática, a pura essência do simbolismo formal". Além disso, Giuseppe Peano foi o percursor na ampliação da lógica.

Com essas contribuições de Peano, deu-se início a um método chamado de Princípio da Indução Matemática:

Definição 3.3. Sejam *S* um subconjunto de $\mathbb{Z}$ e $a \in \mathbb{Z}$, tais que:

i. $a \in S$

ii. S é fechado com respeito à operação de "somar 1" a seus elementos, ou seja, $\forall n, n \in S \Rightarrow n+1 \in S$.

Então, $\{x \in \mathbb{Z}; x \geq a\} \subset S$.

Uma variante do Principio da Indução é chamada de Princípio da Indução Completa ou da Indução Forte, onde consideramos a validade da propriedade para todos os números naturais menores ou iguais a outro $n \in \mathbb{N}$.

Definição 3.4. Seja $P(n)$ uma propriedade relativa ao número natural *n*. Suponhamos que:

i. $P(1)$ é válida.

ii. Para todo $n \in \mathbb{N}$, a validez de$P(k)$, para todo $k \leq n$, implica a validez de $P(n+1)$

Então $P(n)$ é válida para todo $n \in \mathbb{N}$.

A partir do Principio de Indução Matemática, segue-se o importante mecanismo para provar teoremas:

Teorema 3.3.1. Prova por indução matemática

Seja $a \in \mathbb{Z}$ e $P(n)$ uma sentença aberta em *n*. Suponha que

i. $P(a)$é verdadeiro, e que

ii. $\forall n \geq a, P(n) \Rightarrow P(n+1)\ \forall n \geq a, P(n) \Rightarrow P(n+1)$ é verdadeiro.

Então, $P(n)$ é verdadeiro para todo $n \geq a$.

DEMONSTRAÇÃO:

Seja $U = \{n \in \mathbb{Z};\ P(n)\}$*, ou seja, U é um subconjunto dos elementos de* $\mathbb{Z}$ *para os quais* $P(n)$ *é verdadeiro.*

Por (i) $a \in U$*, então, por (ii) temos que:*

$\forall n, n \in U\ \Rightarrow n+1\ \in U$,

Logo, pelo Principio de Indução Matemática $\{x \in \mathbb{Z}; x \geq a\} \subset U$.

Exemplo 3.3.1. : Mostrar que $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$

Seja $P(n) = 1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$

i. $P(1)$ é verdadeiro, já que $\frac{1(1+1)(2.1+1)}{6} = 1 = 1^2$.

ii. Suponhamos que $P(n)$ seja verdadeira, para algum $n \in N$.

iii. Verificando para $P(n+1)$ temos:

$$1^2 + 2^2 + \cdots + n^2 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2$$

$$= \frac{n(n+1)(2n+1) + 6(n+1)(n+1)}{6}$$

Colocando $(n+1)$ em evidência temos:

$\frac{(n+1)[n(2n+1)+6(n+1)]}{6} = \frac{(n+1)(2n^2+7n+6)}{6} = \frac{(n+1)(n+2)(2n+3)}{6}$.

Portanto,

$1^2 + 2^2 + \cdots + n^2 + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6}$, o que mostra que $P(n+1)$ é verdadeira.

Logo, provamos pelo Princípio da Indução Finita que $P(n)$ é verdadeira, $\forall n \in \mathbb{N}$.

4. DIVISIBILIDADE

Seja dois números inteiros *a* e *b*. Dizemos que *a* divide *b* quando existir um $c \in \mathbb{Z}$, onde $b = c.a$. Sendo assim, *b* é um múltiplo de *a*, ou então, *a* é um divisor de *b*.

Para a divisibilidade utilizamos $|$ (divide) . O símbolo não representa uma operação em $\mathbb{Z}$, nem mesmo uma fração. Assim, temos:

$a|b$, então $\exists\ c \in \mathbb{Z}$, onde $b = c.a$.

Propriedades:

Sejam $a, b, c \in \mathbb{Z}$, tem-se que:

a) $1|a, a|a\ e\ a|0$, com $a \neq 0$.

DEMONSTRAÇÃO:

É válida a partir das igualdades $a = a.1, a = 1.a\ e\ 0 = 0.a$

b) $0|a \Leftrightarrow a = 0$

DEMONSTRAÇÃO:

($\Rightarrow$)*Suponhamos que* $0|a$*, logo existe* $c \in \mathbb{Z}$ *tal que* $a = c.0$*. Com isso, conclui-se que* $a = 0$.

($\Leftarrow$)*Se* $a = 0$*, conclui-se que* $0|0$*, o que foi provado no item anterior.*

c) $a|b \Leftrightarrow |a|\ divide\ |b|$

DEMONSTRAÇÃO:

$a|b \Rightarrow \exists\ c \in \mathbb{Z}$ *tal que* $b = c.a$.

Utilizando seus módulos temos:

$|b| = |c|.|a| \Rightarrow \begin{cases} |b| = c.|a| \\ |b| = -c.|a| \end{cases}$

Em $|b| = c.|a|$*, temos que* $|a|$ divide $|b|$.

Em $|b| = -c.|a|$, *seja* $d = -c, d \in \mathbb{Z}$*. Com isso, tem-se que*$|b| = d.|a|$.

Logo, $|a|$ *divide* $|b|$.

d) Se $a|b$ e $b|c$, então $a|c$.

DEMONSTRAÇÃO:

$a|b \Rightarrow \exists d \in \mathbb{Z}$, *tal que* $b = d.a$ *(i)*

$b|c \Rightarrow \exists e \in \mathbb{Z}$, *tal que* $c = e.b$ *(ii)*

Substituindo (i) em (ii) temos:

$c = e.b$

$c = d.a.e$

Como $d, e \in \mathbb{Z}$, *pelo fechamento dos inteiros,* $d.e \in \mathbb{Z}$.

Sendo $k = d.e$:

$c = k.a, k \in \mathbb{Z}$

Logo, $a|c$.

e) Se $a|b$ e $c|d$, então $ac|bd$.

DEMONSTRAÇÃO:

$a|b \Rightarrow m \in \mathbb{Z}$, *tal que* $b = m.a$ *(i)*

$c|d \Rightarrow n \in \mathbb{Z}$, *tal que* $d = n.c$ *(ii)*

Multiplicando membro a membro (i) e (ii):

$b.d = m.a.n.c$

$b.d = a.c.(m.n)$

Seja $m.n = t$, $t \in \mathbb{Z}$, *temos:*

$b.d = a.c.t$

Logo, $ac|bd$.

f) Se $a|b$ e $a|c$, então $a|(b \pm c)$

DEMONSTRAÇÃO:

$a|b \Rightarrow \exists f \in \mathbb{Z}$, *tal que* $b = f.a$ *(i)*

$a|c \Rightarrow \exists g \in \mathbb{Z}$, *tal que* $c = g.a$ *(ii)*

Somando membro a membro (i) e (ii):

$b + c = f.a + g.a$

Colocando em evidência temos:

$b + c = a.(f + g)$

Seja $f + g = k, k \in \mathbb{Z}$*, então:*

$b + c = a.k$

Logo,$a|b + c$.

De forma análoga, prova-se que ,$a|b - c$.

g) Se $a|b$ e $a|c$, então $a|xb + yc$ para quaisquer $x, y \in \mathbb{Z}$.

DEMONSTRAÇÃO:

$a|b \Rightarrow \exists m \in \mathbb{Z}$*, tal que* $b = m.a$ *(i)*

$a|c \Rightarrow \exists n \in \mathbb{Z}$*, tal que* $c = n.a$ *(ii)*

$a|xb + yc \Rightarrow \exists k \in \mathbb{Z}$*, tal que* $xb + yc = k.a$ *(iii)*

Substituindo (i) e (ii) em (iii) temos:

$x.m.a + y.n.a = k.a$

$a(xm + yn) = k.a$

$k = (xm + yn)$

Pelo Fechamento dos inteiros $a|xb + yc$.

h) Se $a|b$ e $b \neq 0$, então $|a| \leq |b|$

DEMONSTRAÇÃO:

$a|b \Rightarrow \exists c \in \mathbb{Z}$*, tal que* $b = c.a$

Utilizando seus módulos temos:

$|b| = |c|.|a|$

Como $b \neq 0$ *, temos que* $c \neq 0$*, logo* $1 \leq |c|$.

Com isso,$|a| \leq |a|.|c| = |b|$

Logo, $|a| \leq |b|$.

i) Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a - b|a^n - b^n$.

DEMONSTRAÇÃO:

Vamos provar pelo Princípio da Indução Finita em $\mathbb{N}$

I. Verificando para n=1

$a-b|a^1-b^1$

$a-b|a-b \Rightarrow \exists c \in \mathbb{Z} \therefore a-b|c(a-b)$

Logo, a proposição é válida para n=1.

II. *Supondo que* $a-b|a^n-b^n$ *seja válida* $\forall n \in \mathbb{N}$.

III. *Provar para n+1*

$a^{n+1}-b^{n+1}=a^n.a-b^n.b$

$a^{n+1}-b^{n+1}=a^n.a-b.a^n+b.a^n-b^n.b$

$a^{n+1}-b^{n+1}=a^n(a-b)+b(a^n-b^n)$

Por hipótese, $a-b|a^n-b^n$ *e* $a-b|a-b$, *com isso* $a-b|x(a-b)+y(a^n-b^n), \forall x,y \in \mathbb{Z}, \forall x,y \in \mathbb{Z}$.

Comoa $-b|a^n(a-b)+b(a^n-b^n)$, *temos que* $a-b|a^{n+1}-b^{n+1}$.

Logo, pelo Principio da Indução Finita, a proposição é válida $\forall n \in \mathbb{N}$.

4.1. Divisão Euclidiana

Em um dos livros de sua extensa obra *Os Elementos*, Euclides enunciou a divisão euclidiana de uma forma implícita.

Inserido no conjunto dos números naturais, quando um número b≠0 não divide a, Euclides enfatiza que sempre é possível essa divisão de a por b, com resto.

Teorema 4.1.1. Sejam a e b dois números inteiros com $b \neq 0$. Existem dois únicos números inteiros q e r tais que

$$a = bq + r \text{ com } 0 \leq r < |b|$$

No teorema, a é o dividendo, b o divisor, q o quociente e r o resto. Logo, na divisão euclidiana, temos que o resto da divisão a por b é zero quando $b|a$.

DEMONSTRAÇÃO:

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

Pela Propriedade Arquimediana, existe $n \in \mathbb{Z}$ *tal que* $n(-b) > -a$, *logo* $a - nb > 0$,

que mostra que S não é vazio. Como o conjunto S é limitado inferiormente por 0, dizemos pelo Princípio da Boa Ordenação, que S possui um menor elemento r.

Suponhamos que $r = a - bq$. *Como r ≥0, vamos mostrar que* $r < |b|$.

Supondo por absurdo que $r \geq |b|$. *Com isso, existe* $s \in \mathbb{N} \cup \{0\}$, *tal quer* $= |b| + s$, *logo* $0 \leq s < r$. *Porém, isso contradiz o fato de r ser o menor elemento de S.*

Agora mostraremos a unicidade desse teorema:

Suponha que $a = bq + r = bq + r'$ *onde* $q, q', r, r' \in \mathbb{Z}$, $0 \leq r < |b|$ *e* $0 \leq r' < |b|$.

Assim temos que $-|b| < -r \leq r' - r \leq r' < |b|$. *Logo,*$|r - r'| < |b|$. *Por outro lado,* $b(q - q') = r' - r$, *o que implica que* $|b||q - q'| = |r' - r| < |b|$, *o que só é possível se* $q = q'$ *e consequentemente,* $r = r'$.

4.2.Paridade dos inteiros

Chamamos de paridade de um número inteiro, a condição desse número ser par ou ímpar.

A classificação de números pares e impares, no conjunto dos números naturais, acontece desde Pitágoras, aproximadamente 500 a.C.

Considerando $n, q \in \mathbb{Z}$, temos as seguintes possibilidades:

i. Números pares: O resto da divisão de *n* por 2 é zero. Com isso, $n = 2q$.

ii. Números impares: O resto da divisão de *n* por 2 é um. Com isso, $n = 2q + 1$.

Algumas propriedades são formadas a partir da paridade dos inteiros:

- A soma e a diferença de dois números é par se, e somente se, os dois números possuem a mesma paridade.

Exemplo 4.2.1. 4 e 8 são pares , pois 4=2.2+0 e 8=4.2+0, logo 4+8+12 é par, onde 12=2.6+0.

- O produto de dois números é par se, e somente se, pelo menos um deles é par.

Exemplo 4.2.2. 6 é par, pois 6=3.2+0. 5 é ímpar, pois 5=2.2+1. Logo 6.5=30 é par, onde 30=2.15+0.

- A potência de um número é par se, e somente se, esse número é par.

Exemplo 4.2.3. 2 é par, pois 2=2.1+0. Logo, 2^3=8 é par, onde 8=2.4+0.

- A soma de n números impares é par se, e somente se, *n* é par.

Exemplo 4.2.4. 3 é ímpar, pois 3=2.1+1. Seja n=4, temos que, 3+3+3+3=12 é par, onde 12=2.6+0.

4.3.Maior inteiro

Definição 3.3.1. Chamamos a parte inteira de um número real *x*, o maior inteiro $\lfloor x \rfloor$, onde $\lfloor x \rfloor < x$. Além disso, seja $\{x\}$ a parte fracionária de *x*, tal que $\{x\} = x - \lfloor x \rfloor$.

Exemplo 4.3.1. :

Se $x = 5 \Rightarrow \lfloor 5 \rfloor = 5$ e $\{5\} = 0$;

Se $x = 2{,}4 \Rightarrow \lfloor 2{,}4 \rfloor = 2$ e $\{2{,}4\} = 0{,}4$;

Se $x = -6{,}8 \Rightarrow \lfloor -6{,}8 \rfloor = -7$ e $\{-6{,}8\} = 0{,}2$.

Propriedades:

Seja $x, y \in \mathbb{R}$ e $m \in \mathbb{Z}$, então:

1. $\lfloor x \rfloor \leq x \leq \lfloor x \rfloor + 1$ e $0 \leq x < 1$;
2. $\lfloor x + m \rfloor = \lfloor x \rfloor + m$;
3. $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$;
4. $\left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor = \left\lfloor \frac{x}{m} \right\rfloor \in \mathbb{Z}^+$.

DEMONSTRAÇÃO (Definição 4.3.1.):

Seja $x, \lfloor x \rfloor, \{x\} \in \mathbb{R}$, *tal que* $\lfloor x \rfloor < x$ *e* $\{x\} = x - \lfloor x \rfloor$.

A partir da propriedade 3 temos:

$\lfloor x \rfloor + \lfloor \ \ \rfloor \leq \lfloor x \rfloor + \lfloor \ \ \rfloor + \lfloor \{x\} + \{\ \} \rfloor$

$\lfloor x \rfloor + \lfloor \ \ \rfloor = \left\lfloor \lfloor x \rfloor + \lfloor \ \ \rfloor + \{x\} + \{\ \} \right\rfloor$

$\lfloor x \rfloor + \lfloor \ \ \rfloor = \lfloor x + \ \rfloor$

Sabendo que $\{x\} + \{\ \} < 2$ *e* $\lfloor \{x\} + \{\ \} \rfloor \leq 1$, *então:*

$\lfloor x + \ \rfloor = \lfloor x \rfloor + \lfloor \ \ \rfloor + \lfloor \{x\} + \{\ \} \rfloor$

$\lfloor x + \ \rfloor \leq \lfloor x \rfloor + \lfloor \ \ \rfloor + 1$

Seja $\lfloor x \rfloor = qm + r$, *com* $0 \leq r < m + 1$, *pela propriedade 4 temos:*

$\left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor = \left\lfloor \frac{qm+r}{m} \right\rfloor = \left\lfloor q + \frac{r}{m} \right\rfloor = q$

A partir da propriedade 1, $0 \leq x < 1$*:*

$\left\lfloor q = q + \frac{r+\{x\}}{m} \right\rfloor = \left\lfloor \frac{qm+r+\{x\}}{m} \right\rfloor = \left\lfloor \frac{x}{m} \right\rfloor$.

Assim, sejam $a, 2a, \ldots ja$ *todos os inteiros positivos* $\leq n$*, divisíveis por a, então:*

$ja \leq n < (j+1)a$

Multiplicando ambos os termos por $\frac{1}{a}$*, temos:*

$j \leq \frac{n}{a} < j + 1 \Rightarrow j = \frac{n}{a}$.

4.4.Equações Diofantinas Lineares

Em homenagem a Diofanto de Alexandria (aprox..300d.C.), tem-se um modelo de equação ,chamada de Equação Diofantina, onde para a resolução de muitos problemas de aritmética é necessário, ao trabalharmos com números inteiros.

Definem-se como Equações Diofantinas Lineares, equações da seguinte forma:

$$aX + bY = c$$

Onde, $a, b, c \in \mathbb{R}$, com a e b não sendo simultaneamente nulos.

Vale lembrar que esse tipo de equação nem sempre possui solução, com isso temos a seguinte proposição que determina a condição de existência de Equações Diofantinas Lineares.

Proposição 4.4.1. Sejam $a, b, c \in \mathbb{Z}$. A equação $aX + bY = c$, admite solução se, e somente se, $mdc(a, b)|c$.

DEMONSTRAÇÃO:

(⇒) *Seja* (x_0, y_0) *solução da equação diofantina* $aX + bY = c$*, temos* $ax_0 + by_0 = c$ *(I)*

Ainda, seja $d = mdc(a, b)$ *então* $d|a$ *e* $d|b$*. Com isso, a partir de uma combinação linear entre a e b, tem-se que* $d|(ax_0 + by_0)$. *(II)*

De (I) e (II), $d|c$.

(⇐) *Seja* $d = mdc(a, b)$*, então* $d|a$ *e* $d|b$.

Por hipótese, $d|c$*, então* $c = t.d, t \in \mathbb{Z}$. *(I)*

Como $d = mdc(a, b)$*, temos que* $d = ma + nb, mn \in \mathbb{Z}$. *(II)*

Substituindo (II) em (I):

$c = t.d$

$c = t.(ma + nb)$

$c = a(mt) + b(nt)$

Seja $x_0 = mt$ *e* $y_0 = nt$*, onde* $(x_0, y_0) \in \mathbb{Z}$*, então* $ax_0 + by_0 = c$

Logo, (x_0, y_0) *é solução da Equação Diofantina Linear.*

Existem equações diofantinas que possuem infinitas soluções . Para essas equações temos a seguinte proposição:

Proposição 4.4.2. Seja (x_0, y_0), solução da equação $aX + bY = c$, onde $mdc(a, b) = 1$.

Então, as soluções $x, y \in \mathbb{Z}$ da equação são $x = x_0 + tb$ e $y = y_0 - ta$, $t \in \mathbb{Z}$.

Exemplo 4.4.1. Determine as soluções da equação 5X+3Y= 100.

Sendo $mdc(5,3) = 1$ e como $1|100$, a equação possui solução. Assim:

1=3-1.2 (I)

2=5-1.3 (II)

Substituindo (II) em (I) temos:

1=3-1.(5-1.3)

1=3-1.5+1.3

1=(-1).5+2.3

Multiplicando ambos os lados por 100, temos:

100=(-100).5+200.3

Com isso, $x_0 = -100$ e $y_0 = 200$. Assim:

$x = -100 + 3y, y = 200 - 5t, t \in \mathbb{Z}$.

Com isso, podemos concluir que a divisibilidade é um assunto de muita importância em Aritmética, pois a partir dela podemos analisar qualquer número inteiro, independentemente de seu tamanho, reduzindo-os em fatores primos, a partir dos critérios de divisibilidade e congruência, assunto que trataremos mais adiante. As propriedades de divisibilidade citadas anteriormente serão utilizadas frequentemente daqui para frente.

Além disso, essa função da divisibilidade em reduzir um número em fatores primos é a base da criptografia e algoritmos de segurança, muito utilizados no nosso dia a dia, em coisas simples, como por exemplo, transações online.

5. NÚMEROS PRIMOS

Como já foi dito anteriormente, os homens aprenderam a lidar com os números ao longo do tempo e com isso deu-se o surgimento dos números primos. Um tipo de números muito importantes em várias áreas da Matemática e em outros ramos do conhecimento.

São chamados de números primos todo número natural, maior ou igual a 2, que podem ser divididos apenas por um ou por ele próprio.

> "Esses números são os próprios átomos da aritmética. São os números indivisíveis que não podem ser representados pela multiplicação de dois menores...Todo número não primo pode ser formado pela multiplicação desses blocos de construção Primos. Cada uma das moléculas do mundo físico é composta por átomos da tabela periódica de elementos químicos. Uma lista de primos é a tabela periódica do Matemático." (SAUTOY, 2007, p.13)

Os primeiros indícios e resultados da ideia de primalidade deram-se através dos gregos antigos, pela Escola Pitagórica (530 a.C), mas foi Euclides de Alexandria quem tornou estes resultados como conhecemos no dia de hoje.

Em sua obra "Os Elementos", Euclides desenvolveu importantes teoremas envolvendo os números primos, dentre eles a demonstração de que existem infinitos números primos e que todos os números podem ser escritos na forma de decomposição de números primos. Esse último chamado de Teorema Fundamental da Aritmética que será demonstrado adiante.

Eratóstenes de Cirene (aproximadamente 200 a.C) também contribuiu grandemente com os números primos, desenvolvendo um dispositivo para encontrá-los. Nesse sentido, Boyer (2012, p. 122) afirma que "Eratóstenes é bem conhecido dos matemáticos pelo "crivo de Eratóstenes", um método sistemático para isolar números primos." Porém, esse método não é muito eficiente para números muito elevados.

Além destes, outros matemáticos fizeram suas contribuições para os números primos, como Fermat, Mersenne, Euler e Gauss.

Com isso, sejam p e q números primos e a um número inteiro, seguem-se as definições:

I. Se $p|q$, então $p = q$.

DEMONSTRAÇÃO:

Por hipótese $p|q$ *. Como q é primo, p=1 ou p=q.*

Porém, p é primo e com isso, $p \geq 2$.

Logo, $p = q$.

II. Se $p \nmid q$, então $mdc(a,p) = 1$

DEMONSTRAÇÃO:

Supondo $d = mdc(a,p)$*, então* $d|a$ *e* $d|p$.

Por hipótese, p é primo então, d=1 ou d=p.

Considerando d=p, como $d|a$ *então* $p|a$.

Absurdo.

Logo, d=1

Proposição 5.1. (Lema de Euclides): Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p|ab$, então $p|a$ ou $p|b$.

DEMONSTRAÇÃO:

Supondo que $p \nmid a$.

Seja $d = mdc(a,p)$*, então d=1. Com isso, existe* $x_0, y_0 \in Z$ *tal que* $ax_0 + py_0 = 1$.

Multiplicando ambos os lados por b temos:

$ab(x_0) + p(by_0) = b$

Daí, $p|ab$ *e* $p|p$*, então,* $p|b$.

De forma análoga, se $p \nmid b$ *então* $p|a$.

Teorema 5.1. (Teorema Fundamental da Aritmética): Todo número natural maior do que 1 ou é primo ou pode ser escrito de maneira única como um produto de números primos.

DEMONSTRAÇÃO:

Considerando $n \in \mathbb{N}$*. Onde n é maior que 1.*

Se n=2, verifica-se a validade do teorema, pois 2 é primo.

Se n é composto, existem $n_1, n_2 \in \mathbb{N}$*, onde* $n = n_1 \cdot n_2$ *com* $1<n_1<n$ *e* $1<n_2<n$.

Por hipótese, existem números primos $p_1, p_2, p_3, ..., p_r$ *e* $q_1, q_2, q_3, ..., q_s$*, onde* $n_1 = p_1, p_2, p_3, ..., p_r$ *e* $n_2 = q_1, q_2, q_3, ..., q_s$*., com isso* $n = p_1, p_2, p_3, ..., p_r \cdot q_1, q_2, q_3, ..., q_s$.

Para provar a unicidade da fatoração temos:

Seja $n = p_1, p_2, p_3,..., p_r$ *, com* p_i *primo e* $n = q_1, q_2, q_3,..., q_s$*, com* q_j *também primo.*

Como n=n temos que $p_1 | q_1, q_2, q_3,..., q_s$ *,com isso, podemos afirmar que* $p_1 = q_j$*, onde seguindo a sequencia temos que j=1, logo* $p_1 = q_1$*.*

Ainda, podemos afirmar que $p_2, p_3,..., p_r = q_2, q_3,...q_s$ *.Assim* $p_2 | q_2, q_3,..., q_s$ *, logo* $p_2 = q_2$*.*

Sem perda de generalidades, temos que r=s e $p_i = q_j$*.*

Tratando-se da quantidade de números primos existentes, Euclides provou em sem livro IX, utilizando uma demonstração por absurdo, demonstração esta nunca vista anteriormente, que existem infinitos números primos.

Teorema 5.2. Existem infinitos números primos

DEMONSTRAÇÂO:

Supondo que exista apenas um número finito de números primos $p_1, p_2, p_3,..., p_r$ *.*

Considerando $n \in \mathbb{N}$*, onde* $n = p_1 p_2 ... p_r + 1$*, pelo Teorema Fundamental da Aritmética, n possui um fator primo p, onde* $p | p_1 p_2 ... p_r$ *e consequentemente p divide 1, o que é um absurdo.*

Logo, existem infinitos números primos.

A demonstração citada acima, conceituada como uma das pérolas da Matemática, foi a mesma utilizada por Euclides.

5.1. Números primos especiais

Dentre os números primos existem os chamados primos especiais, que são números naturais que possuem algumas características e propriedade diferentes de outros.

5.1.1. Primos de Fermat

Foram conjecturados por Pierre de Fermat em 1640, em uma carta enviada para outro importante matemático da época, Marin Mersenne. Nessa carta Fermat afirmava que todos os números que tinham a forma $F_n = 2^{2^n} + 1$, onde $n \in \mathbb{N}$, são primos.

Porém, sua prova somente havia sido feita com *n* até quatro. Sendo assim, considerando $0 \leq n \leq 4$, temos:

$$F_0 = 2^{2^0} + 1 = 2^1 + 1 = 3$$

$$F_1 = 2^{2^1} + 1 = 2^2 + 1 = 5$$

$$F_2 = 2^{2^2} + 1 = 2^4 + 1 = 17$$

$$F_3 = 2^{2^3} + 1 = 2^8 + 1 = 257$$

$$F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65537$$

Sua afirmação foi desmentida em 1732, por Leonhard Euler, que mostrou que se *n =5* o número não é primo. Para Euler:

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297$$

Onde, $4294967297 = 641 \times 6700417$. Com isso, F_5 é composto.

Até hoje não foram descobertos mais nenhum além dos 5 primeiros, mas acredita-se que sejam infinitos.

5.1.2. Primos de Mersenne

Os primos de Mersenne são números da forma $Mp = 2^p - 1$, onde $p \geq 2$.

Marin Mersenne publicou sua relação de números primos, baseada nos valores de *p*, em meados do século XVII. Para Mersenne para o número ser primo *p* deve ser:

2,3,5,7,13,19,31,61,89,107,127,521,607,1279,2203, 2281, 3217, 4253 e 4423

O maior número primo conhecido atualmente, $2^{82.589.933}-1$, possui quase 25 milhões de dígitos e é o 51º primo de Mersenne já descoberto.

5.1.3. Números Perfeitos

Definição 5.1.3.1. Denota-se como um número perfeito $a \in \mathbb{Z}^+$, aquele que a soma de todos os seus divisores, exceto ele mesmo, resulta no próprio a.

Exemplo 5.1.3.1. Seja D(6) = $\{1,2,3,6\}$ os divisores de 6. Temos que 6 é perfeito, pois 6=1+2+3

Exemplo 5.1.3.2. Seja D(28) = $\{1,2,4,7,14,28\}$ os divisores de 28. Temos que 28 é perfeito, pois 28= 1+2+4+7+14

Os números citados nos exemplos acima são considerados os números perfeitos mais "famosos". Muitos dizem que isso é resultado de que Deus criou o universo em 6 dias e no sétimo descansou e que o 28 é a quantidade de dias que a Lua demora para completar uma volta na Terra.

Definição 5.1.3.2. Seja $n \in \mathbb{Z}^+$, e S(n) a soma dos divisores de n, tem-se que S(n)=n+1, se e somente s, n é primo.

Nota-se que sendo n primo, os únicos divisores de n são 1 e o próprio n. Logo, S(n)=n+1.

Definição 5.1.3.3. Seja $m, n \in \mathbb{Z}^+$ e S(m) a soma dos divisores de m e S(n) a soma dos divisores de n, tem-se que se $mdc\ (m,n) = 1$, então S($n.m$)=S(n).S(m).

Exemplo 5.1.3.3. Considerando n=2 e m =3, temos que mdc(2,3)=1. Além disso, S(2)=3 e S(3)=4.

Seja S(2.3)=S(6)=12, então:

S(6)=S(2).S(3)

12=3.4

12=12

Definição 5.1.3.4. Se *n* é perfeito, S(*n*)=2*n*

De fato, pois se *n* é perfeito a soma de seus divisores menos ele é igual a *n*.

Exemplo 5.1.3.4. Seja *n*=6, então:

S(6)= $\{1,2,3,6\}$

1+2+3+6=12=2.6

6. CONGRUÊNCIAS

A noção de congruência pode ser encontrada em várias situações do nosso cotidiano como, nas horas, no calendário, nos ângulos, em criptografia, além de ser encontrada nos critérios de divisibilidade nas aulas de exatas.

Os termos que veremos em abundância nesse capítulo, congruente e módulo, são derivados do latim, onde congruente significa "o que corresponde" e módulo, "modelo".

O conceito de congruência modular como uma aritmética com os restos da divisão euclidiana por um número já fixado foi introduzida por Gauss em seu livro *Disquisitiones Arithmeticae* (1801). Segundo Ore (1988), a teoria das congruências desenvolvida por Gauss fez com que seu nome fosse introduzido na chamada Teoria dos Números.

Em situações envolvendo cálculos de números excessivamente grandes, onde a utilização das operações básicas (adição, subtração, multiplicação e divisão) é muito complicada, como por exemplo, dividir 2^{48} por 9, é possível recorrer ao conceito de congruência que será proposto adiante.

Podemos dizer que dois ou mais números são congruentes quando, ao serem divididos por um mesmo número, deixam um mesmo resto.

Seja $m \in \mathbb{N}$ o divisor, r o resto, A e B números quaisquer, temos:

$$A = m \cdot q_1 + r$$

$$B = m \cdot q_2 + r$$

Dizemos que A é congruente (ou cônguo) a B, módulo d.

Em escrita Matemática, a congruência é representada pelo símbolo "≡".

Assim, o exemplo dado pode ser representado por:

$$A \equiv B mod m$$

Para tal definição consideraremos sempre $m > 1$, pois o resto da divisão de um número n qualquer, $n \in \mathbb{Z}$, por 1 é sempre 0. Ou seja, para quaisquer $a, b \in \mathbb{Z}$, podemos escrever $a \equiv b \bmod 1$.

Exemplo 6.1. :

5 ≡ 2 mod 1 (resto 0)

$7 \equiv 9 \bmod 2$ (resto 1)

Sejam $a, b, c, d \in \mathbb{Z}$, valem as seguintes propriedades:

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

b) $a \equiv b \bmod m \Rightarrow b \equiv a \bmod m$ (Antissimétrica)

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

d) Se $a \equiv b \bmod m \Rightarrow m \mid b - a$

e) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a + c \equiv b + d \bmod m$

f) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a \cdot c \equiv b \cdot d \bmod m$

g) Se $a \equiv b \bmod m \Rightarrow a^n \equiv b^n \bmod m$

DEMONSTRAÇÕES:

a) *Sendo a=a, temos que o resto da divisão de a por m será a mesma em ambos os casos.*

b) *Por hipótese,* $a \equiv b \bmod m$, ou seja, $a = m \cdot q_1 + r_1$ e $b = m \cdot q_2 + r_2$, com $r_1 = r_2$ *. Com isso, como* $r_2 = r_1$*, conclui-se que* $b \equiv a \bmod m$.

c) *Por hipótese,* $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então $a = m \cdot q_1 + r_1$, $b = m \cdot q_2 + r_1$ e $c = m \cdot q_3 + r_1$. *Logo como em ambos os casos temos o mesmo resto* r_1, *afirmamos que* $a \equiv c \bmod m$.

d) *Por hipótese* $a \equiv b \bmod m$, logo por definição $a = m \cdot q_1 + r_1$ (I) e $b = m \cdot q_2 + r_2$ (II).

Subtraindo (I) de (II) temos:

$b - a = m(q_2 - q_1) + (r_2 - r_1)$;

Como $r_1 = r_2$, $b - a = m(q_2 - q_1)$.

Seja $k = q_2 - q_1$, *então* $b - a = m \cdot k$, $k \in z$.

Logo, $m|b-a$.

e) *Por hipótese* $\begin{cases} a \equiv b \bmod m \Rightarrow m|b-a; (I) \\ c \equiv d \bmod m \Rightarrow m|d-c; (II) \end{cases}$

Por (I) e (II) temos:

$m|(b-a)+(d-c)$

$m|(b+d)-(a+c)$

Logo, $a + c \equiv b + d \bmod m$

f) *Por hipótese* $\begin{cases} a \equiv b \bmod m \Rightarrow m|b-a; (I) \\ c \equiv d \bmod m \Rightarrow m|d-c; (II) \end{cases}$

Por (I) e (II):

$m|(b-a)+(d-c)$

Multiplicando (I) por c e (II) por b, temos:

$m|bc - ac + bd - bc$

$m|bd - ac$

Logo, $ac \equiv bd \bmod m$

g) *Vamos provar por indução em* $\mathbb{N}$*:*

(I) *Para n=1:*

$a^1 \equiv b^1 \bmod m$

Por hipótese a afirmação é verdadeira.

(II) *Supondo válida* $\forall n \in \mathbb{N}$ *a proposição* $a \equiv b \bmod m \Rightarrow a^n \equiv b^n \bmod m$.

(III) *Verificando para n+1:*

De (I): $a^1 \equiv b^1 \bmod m$

Por hipótese, $a^n \equiv b^n \bmod m$

A partir da propriedade f) temos:

$a^n \cdot a^1 \equiv b^n \cdot b^1 \bmod m$

$a^{n+1} \equiv b^{n+1} \bmod m$

Logo, a proposição é válida $\forall n \in \mathbb{N}$.

A propriedade g) nos auxilia a resolver problemas que envolvem números grandes.

Exemplo 6.2. : Determine o resto da divisão de 237^{28} por 13

Como $237 \equiv 3 \bmod 13$, elevando ambos os lados a 4 temos:

$237^4 = 3^4 \bmod 13 \Rightarrow 237^4 \equiv 3 \bmod 13$ (I)

Em (I), elevando ambos os lados a 7 temos:

$(237^4)^7 \equiv 3^7 \bmod 13 \Rightarrow 237^{28} \equiv 3 \bmod 13$

Logo, o resto da divisão de 237^{28} por 13 é 3.

6.1. Critérios de Divisibilidade

Falaremos sobre os critérios de divisibilidade por alguns números primos, pois a congruência trata da divisão de números distintos e seus restos.

Em todos os critérios de divisibilidade utilizaremos os números na base decimal e a congruência de acordo com cada divisor.

6.1.1. Divisibilidade por 2

Considerando o número:

$(a_n a_{n-1} ... a_2 a_1 a_0)_{10} = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$

Então:

$10^0 \equiv 1 \bmod 2$

$10^1 \equiv 0 \bmod 2$

$10^2 \equiv 0 \bmod 2$

$10^3 \equiv 0 \bmod 2$

Com isso,

$a_0 10^0 \equiv 1 \cdot a_0 \bmod 2$

$a_1 10^1 \equiv 0 \cdot a_1 \bmod 2$

$a_2 10^2 \equiv 0 \cdot a_2 \bmod 2$

$a_3 10^3 \equiv 0 \cdot a_3 \bmod 2$

Assim por diante, até $a_n 10^n \equiv 0 \cdot a_n \bmod 2$.

Portanto, temos que o número $(a_n a_{n-1} ... a_2 a_1 a_0)_{10}$ é divisível por 2 quando o algarismo das unidades for divisível por 2.

6.1.2. Divisibilidade por 3

Considerando o número:

$(a_n a_{n-1} ... a_2 a_1 a_0)_{10} = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$

Então:

$10^0 \equiv 1 \bmod 3$

$10^1 \equiv 1 \bmod 3$

$10^2 \equiv 1 \bmod 3$

$10^3 \equiv 1 \bmod 3$

Com isso,

$a_0 10^0 \equiv 1 \cdot a_0 \bmod 3$

$a_1 10^1 \equiv 1 \cdot a_1 \bmod 3$

$a_2 10^2 \equiv 1 \cdot a_2 \bmod 3$

$a_3 10^3 \equiv 1 \cdot a_3 \bmod 3$

Assim por diante, até $a_n 10^n \equiv 1 \cdot a_n \bmod 3$.

Portanto, temos que o número $(a_n a_{n-1} ... a_2 a_1 a_0)_{10}$ é divisível por 3 quando a soma de seus algarismo for divisível por 3.

6.1.3. Divisibilidade por 5

Considerando o número:

$(a_n a_{n-1}...a_2 a_1 a_0)_{10} = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$

Então:

$10^0 \equiv 1 \bmod 5$

$10^1 \equiv 0 \bmod 5$

$10^2 \equiv 0 \bmod 5$

$10^3 \equiv 0 \bmod 5$

Com isso,

$a_0 10^0 \equiv 1 \cdot a_0 \bmod 5$

$a_1 10^1 \equiv 0 \cdot a_1 \bmod 5$

$a_2 10^2 \equiv 0 \cdot a_2 \bmod 5$

$a_3 10^3 \equiv 0 \cdot a_3 \bmod 5$

Assim por diante, até $a_n 10^n \equiv 0 \cdot a_n \bmod 5$.

Portanto, temos que o número $(a_n a_{n-1}...a_2 a_1 a_0)_{10}$ é divisível por 5 quando os algarismos das unidades for 0 ou 5.

6.1.4. Divisibilidade por 7

Considerando o número:

$(a_n a_{n-1}...a_2 a_1 a_0)_{10} = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$

Então:

$10^0 \equiv 1 \bmod 7$
$10^1 \equiv 3 \bmod 7$
$10^2 \equiv 2 \bmod 7$
$10^3 \equiv 6 \bmod 7$
$10^4 \equiv 4 \bmod 7$
$10^5 \equiv 5 \bmod 7$
$10^6 \equiv 1 \bmod 7$
$10^7 \equiv 3 \bmod 7$
$10^8 \equiv 2 \bmod 7$
$10^9 \equiv 6 \bmod 7$
$10^{10} \equiv 4 \bmod 7$
$10^{11} \equiv 5 \bmod 7$

Com isso,

$a_0 10^0 \equiv 1 \cdot a_0 \bmod 7$
$a_1 10^1 \equiv 3 \cdot a_1 \bmod 7$
$a_2 10^2 \equiv 2 \cdot a_2 \bmod 7$
$a_3 10^3 \equiv 6 \cdot a_3 \bmod 7$
$a_4 10^4 \equiv 4 \cdot a_4 \bmod 7$
$a_5 10^5 \equiv 5 \cdot a_5 \bmod 7$
$a_6 10^6 \equiv 1 \cdot a_6 \bmod 7$
$a_7 10^7 \equiv 3 \cdot a_7 \bmod 7$
$a_8 10^8 \equiv 2 \cdot a_8 \bmod 7$
$a_9 10^9 \equiv 6 \cdot a_9 \bmod 7$
$a_{10} 10^{10} \equiv 4 \cdot a_{10} \bmod 7$
$a_{11} 10^{11} \equiv 5 \cdot a_{11} \bmod 7$

Portanto, temos que o número $(a_n a_{n-1} ... a_2 a_1 a_0)_{10}$ é divisível por 7 quando $(a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5) + (a_6 + 3a_7 + 2a_8) - (a_9 + 3a_{10} + 2a_{11}) + ...$ for divisível por 7.

6.1.5. Divisibilidade por 11

Considerando o número:

$$(a_n a_{n-1}...a_2 a_1 a_0)_{10} = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$$

Então:

$$10^0 \equiv 1 \bmod 11$$
$$10^1 \equiv 10 \bmod 11$$
$$10^2 \equiv 1 \bmod 11$$
$$10^3 \equiv 10 \bmod 11$$

Com isso,

$$a_0 10^0 \equiv 1 \cdot a_0 \bmod 11$$
$$a_1 10^1 \equiv 10 \cdot a_1 \bmod 11$$
$$a_2 10^2 \equiv 1 \cdot a_2 \bmod 11$$
$$a_3 10^3 \equiv 10 \cdot a_3 \bmod 11$$

Portanto, temos que o número $(a_n a_{n-1}...a_2 a_1 a_0)_{10}$ é divisível por 11 quando os algarismos das unidades somados ao décimo dos algarismos de ordem par e impar for divisível por 11.

6.2.Teoremas de Fermat, Wilson e Euler

Alguns teoremas são de extrema importância para a congruência, dentre eles estão o Pequeno teorema de Fermat, o Teorema de Euler e o Teorema de Wilson.

Os teoremas citados baseiam- se em uma classe de números inteiros chamada de números primos. Classe essa muito importante na Teoria dos números, pois a partir dela podemos escrever números grandes de uma forma mais simples, como um produto de números primos. Ou seja, podemos escrever qualquer número diferente de 0 e ± 1 em números primos.

Para entender do que se trata essa classe de números, temos:

Definição 6.2.1. *Um número $p \in \mathbb{Z} - \{0, \pm 1\}$ diz-se primo quando seus únicos divisores são 1 e $|p|$. Caso contrário, p é dito composto.*

Com o exemplo temos os números 3 e 15, onde 3 é primo pois seus divisores são $D(3) = \{-3,1,3\}$, enquanto 15 é composto pois $D(15) = \{-15,-5,-3,1,3,5,15\}$.

6.2.1. Pequeno Teorema de Fermat

O Pequeno Teorema de Fermat é amplamente utilizado em Teoria dos números. Embora receba o nome de Fermat, foi Euler quem publicou sua demonstração.

Fermat tentou criar uma relação que gere todos os números primos, mas até hoje sua prova não teve êxito.

Teorema 6.2.1.1. (Pequeno Teorema de Fermat): *Se p é um número primo e a é um número inteiro tal que* $p \nmid a$*, então* $a^{p-1} \equiv 1 mod p$.

DEMONSTRAÇÃO: Considerando o conjunto de números inteiros:

$A = \{a,2a,3a,...,(p-1)a\}$.

Os elementos do conjunto A são incongruentes quando tomados dois a dois módulo p.

Seja $\theta, \gamma \in A$*, temos que* $\theta = \alpha_1 . a$ *e* $\gamma = a_2 . a$*, onde* $\alpha_1, \alpha_2 \in \{1,2,3, \dots (p-1)\}$*, tem-se que* $\theta \equiv \gamma mod p \Rightarrow p|(\alpha_1 - \alpha_2)a$*. Como p é primo e p não divide a, temos que* $p|\alpha_1 - \alpha_2$*, o que é impossível, pois* $|\alpha_1 - \alpha_2| < p$*. Com isso, temos que* θ *e* γ *são incongruentes módulo p, além de que nenhum elemento é congruente a 0 módulo p. Logo, notamos que cada elemento de A é congruente a apenas um elemento do conjunto B onde* $B = \{1,2,3, \dots (p-1)\}$.

Contudo, podemos supor que:

$a \equiv 1 \bmod p$

$2a \equiv 2 \bmod p$

$3a \equiv 3 \bmod p$

$4a \equiv 4 \bmod p$

.

.

.

$(p-1)a \equiv (p-1) \bmod p$

Multiplicando membro a membro, temos:

$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \bmod p$

$a^{p-1}(1 \cdot 2 \cdot 3 \cdots (p-1)) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \bmod p$

$a^{p-1}(p-1)! \equiv (p-1)! \bmod p$

Como mdc((p-1)!,p)=1:

$a^{p-1} \equiv 1 \bmod p$

Exemplo 6.2.1.1. : Determinar o resto da divisão de 14^{17} por 17

Como 17∤14, pelo Pequeno Teorema de Fermat, temos que a=14 e p=17. Assim:

$a^{p-1} \equiv 1 \bmod p$

$14^{17-1} \equiv 1 \bmod 17$

$14^{16} \equiv 1 \bmod 17$

Logo, o reto da divisão de 14^{17} por 17 é 1.

6.2.2. Teorema de Euler

Leonhard Euler nasceu na Suiça em 1707, mesma região onde nasceram importantes matemáticos do século XVIII.

Filho de um ministro religioso tinha por parte do pai certa expectativa para que o mesmo seguisse seus passos, porém Euler estudou com Jean Bernoulli, matemático respeitável de sua época, onde incorporou ao estudo da matemática temas como teologia, astronomia, medicina, física e línguas orientais.

Em sua vida profissional, ingressou em 1727 como professor na Academia de S.

Petersburgo, na área de medicina e fisiologia e em 1733, tornou-se o principal matemático da Academia, onde contribui com vários artigos. Diziam que Euler compunha esses artigos enquanto brincava com seus filhos.

Dois anos mais tarde, Euler perdeu a visão de um olho e em 1766, enfrentou uma total cegueira, o que não o impediu de continuar com suas pesquisas. Faleceu em 1783, repentinamente ao tomar chá com um de seus netos.

Ao longo de sua vida, Euler publicou mais de 500 livros e artigos. E posteriormente a sua morte apareceram listas contendo aproximadamente 886 itens.

Dentre os assuntos matemáticos escolhidos por Euler, encontra-se a Teoria dos Números. Sobre isso, Boyer afirma que:

> A teoria dos números tem atraído fortemente muitos dos maiores matemáticos, tais como Fermat e Euler, mas não interessou a outros, inclusive Newton e d'Alembert. Euler não publicou um tratado sobre o assunto, mas escreveu cartas e artigos sobre vários aspectos da teoria dos números. (BOYER, 2012, p.310).

Em 1732, Euler derrubou a afirmação feita por Fermat, que dizia que todo número na forma $2^{2^n}+1$ são sempre primos onde a partir de sua imensa habilidade computacional, provou que $2^{25}+1$ é fatorável, ou seja, não é primo.

Euler publicou em 1736 na Academia de S. Petersburgo a primeira demonstração do Pequeno Teorema de Fermat, citado anteriormente, embora Leinbniz também tenha feito essa demonstração antes dele de forma manuscrita.

Ainda em relação à Teoria dos Números, Euler contribui com um teorema importante, que recebeu seu nome. Este teorema também envolve os números primos.

Antes de enunciarmos o teorema, trataremos de alguns assuntos necessários para a demonstração.

Definição 6.2.2.1. Sistema reduzido de resíduos módulo *m*

Chamamos de sistema reduzido de resíduos módulo *m*, o conjunto de números $r_1, r_2, \dots, r_s \in \mathbb{Z}$, tais que:

i. $mdc(r_i, m) = 1, \forall i = 1,\dots,s$;

ii. r_i é incongruente a $r_j mod m$, se $i \neq j$;

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

Definição 6.2.2.2. (Função de Euler): Seja a função $\varphi: \mathbb{N} \to \mathbb{N}$, onde $\varphi(m)$ é a quantidade de números naturais compreendidos entre 0 e *m*-1, que são coprimos com *m*, tal que $\varphi(m) \leq m - 1$, para todo $m \geq 2$.

Exemplo 6.2.2.1. $\varphi(8) = 4$, pois os números 1,3,5 e 7, são menores que 8 e primos entre si com ele.

Teorema 6.2.2.1. *Sejam* $m, a \in \mathbb{Z}$, *com m>1 e mdc(a,m)=1. Então* $a^{\varphi(m)} \equiv 1 mod n$.

DEMONSTRAÇÂO: Seja $r_1, \dots, r_{\varphi(m)}$ *um sistema reduzido de resíduos módulo m, temos que* $ar_1, \dots, ar_{\varphi(m)}$ *também formam um sistema reduzido de resíduos módulo m. Assim:*

$$ar_1 \cdot ar_2 \cdots ar_{\varphi(m)} \equiv r_1 \cdot r_2 \cdots r_{\varphi(m)} \bmod m$$

Com isso,

$$a^{\varphi(m)} r_1 \cdot r_2 \cdots r_{\varphi(m)} = ar_1 \cdot ar_2 \cdots ar_{\varphi(m)} \equiv r_1 \cdot r_2 \cdots r_{\varphi(m)} \bmod m$$

Como $mdc(r_1 . r_2 \dots r_{\varphi(m)}, m) = 1$, *temos que:*

$$a^{\varphi(m)} \equiv 1 \bmod m .$$

Logo, podemos perceber que o Teorema de Euler nada mais é que uma propagação do Pequeno Teorema de Fermat, tendo em vista que se *m=p* for um número primos, então $\varphi(p) = p - 1$.

6.2.3. Teorema de Wilson

John Wilson(1741-1793) conjecturou um teorema sobre números primos, que foi provado por Lagrange(1736-1813).

Teorema 6.2.3.1. *Se p é um número primo, então* $(p - 1)! \equiv -1 mod p$.

DEMONSTRAÇÃO:

Para p=2 e p=3, o teorema é facilmente verificado:

$$(2-1)! \equiv -1 \bmod 2$$

$$(3-1)! \equiv -1 \bmod 3$$

Agora, supondo $p \geq 5$ primo, temos que $\forall i \in \{1, \dots, p-1\}$ e ainda a congruência $iX \equiv 1 mod p$, possui apenas uma solução X. Ou seja, existe um único $j \in \{1, \dots, p-1\}$, onde $ij \equiv 1 mod p$.

Além disso, temos que $i^2 \equiv 1 mod p$. Com isso, $p|i^2 - 1$, então $p|i+1$ ou $p|i-1$, o que ocorre somente se i=1 ou i=p-1.

Portanto,

$$2 \cdots (p-2) \equiv 1 \bmod p \Rightarrow 1 \cdot 2 \cdots (p-2)(p-1) \equiv -1 \bmod p$$

Exemplo 6.2.3.1. Ache o resto da divisão de $6.7.8.9 mod 5$

Sabemos que:

$$6 \equiv 1 \bmod 5$$
$$7 \equiv 2 \bmod 5$$
$$8 \equiv 3 \bmod 5$$
$$9 \equiv 4 \bmod 5$$

Multiplicando membro a membro, temos:

$$6 \cdot 7 \cdot 8 \cdot 9 \equiv 1 \cdot 2 \cdot 3 \cdot 4 \bmod 5$$
$$6 \cdot 7 \cdot 8 \cdot 9 \equiv 4! \bmod 5$$

Pelo Teorema de Wilson $4! \equiv -1 mod 5$, então:

$$6 \cdot 7 \cdot 8 \cdot 9 \equiv -1 \bmod 5$$
$$6 \cdot 7 \cdot 8 \cdot 9 \equiv 4 \bmod 5$$

Logo, o resto da divisão é 4.

6.3.Congruências Lineares

É um caso de equação envolvendo a ideia de congruência módulo m, ou seja, o intuito de resolvermos uma congruência linear é encontrar, se existirem, números inteiros *x* que satisfazem a congruência dada.

Definição 6.3.1. Dados $a, b, m \in \mathbb{Z}$, com $m > 1$, a congruência $aX \equiv b mod m$, possui solução se, e somente se, $mdc(a, m)|b$.

DEMONSTRAÇÃO:

(⇒) *Supondo que a congruência* $aX \equiv bmodm$ *possua uma solução x, ou seja,* $m|ax - b$*, o que faz com que exista um y, onde* $ax - b = my$*. Com isso, a equação* $aX - mY = b$ *têm solução.*

Logo, $mdc(a,m)|b$.

(⇐) *Supondo que* $mdc(a,m)|b$*, temos que* $aX - mY = b$ *possui uma solução x,y qualquer. Com isso, tem-se que* $ax = b + my$*, onde x é solução da congruência c*.

Exemplo 6.3.1. A congruência $3X \equiv 5mod7$ admite solução?

Sabemos que para que haja solução o $mdc(3,7)$ precisa dividir o 5.

Assim, temos que $mdc(3,7) = 1$ e, como $1|5$, podemos afirmar que $3X \equiv 5mod7$ admite solução.

Proposição 6.3.1. Sejam $a, b, m \in \mathbb{Z}$, com $m > 1$ *e* $mdc(a,m)|b$. Se x_0 é uma solução da congruência $a, b, m \in$, então $x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \dots, x_0 + (d-1)\frac{m}{d}$, onde $d = mdc(a,m)$, formam um sistema completo de soluções da congruência, duas a duas incongruentes módulo *m*.

Exemplo 6.3.2. Resolva se possível, a congruência linear$8X \equiv 4mod12$.

Seja $d = mdc(8,12) = 4$.

Como $4|4$, admite solução. Assim, seja $x_0 = 2$, uma solução, pois 16=1.12+4.

Com isso, temos que:

$$x_1 = 2 + \frac{12}{4} \Rightarrow x_1 = 5;$$

$$x_2 = 2 + 2 \cdot \frac{12}{4} \Rightarrow x_2 = 8;$$

$$x_3 = 2 + 3 \cdot \frac{12}{4} \Rightarrow x_3 = 11.$$

6.4.Teorema Chinês dos Restos

Utilizamos o Teorema Chinês dos Restos para resolver sistemas de congruências

módulo *m*. Tal teorema está definido da seguinte maneira:

Definição 6.4.1. Se $mdc(m_i, m_j) = 1$, para todo m_i, m_j, com $i \neq j$, então o sistema possui uma única solução módulo *m*, tal que $M = m_1 m_2 \ldots m_r$. As soluções são $x = M_1 y_1 c_1 \ldots . + M_r y_r c_r + yM$, onde $t \in \mathbb{Z}$, $M_i = M | m_i$ e y_i é a solução de $M_i Y \equiv 1 mod m$, *i*=1,...,*r*.

DEMONSTRAÇÃO:

Como $m_i | M_j$, *se* $i \neq j$ *e* $M_i y_i \equiv 1 \bmod m_i$, *vamos provar que x é solução simultânea do sistema. Assim, temos que:*

$$x = M_1 y_1 c_1 + \ldots + M_r y_r c_r \equiv M_i y_i c_i \equiv c_i \bmod m_i$$

Analogamente se x' é outra solução temos que:

$$x \equiv x' \bmod m_i, \forall i = 1, \ldots, r .$$

Como $mdc(m_1, m_j) = 1$, *para* $i \neq j$, *então* $mmc(m_1, \ldots, m_r) = m_1 \ldots m_r = M$. *Com isso,* $x \equiv x' \bmod M.$

Exemplo 6.4.1. Resolva o problema proposto pelo matemático Sun-Tsu: *Qual o número que deixa restos 2,3 e 2 quando dividido, respectivamente, por 3,5 e 7?*

Para resolver o problema devemos montar o seguinte sistema de congruências:

$$X \equiv 2 \bmod 3$$
$$X \equiv 3 \bmod 5$$
$$X \equiv 2 \bmod 7$$

Onde:

$$M = 3 \cdot 5 \cdot 7 = 105;$$
$$M_1 = 5 \cdot 7 = 35;$$
$$M_2 = 3 \cdot 7 = 21;$$
$$M_3 = 3 \cdot 5 = 15.$$

E ainda,

$$c_1 = 2;$$
$$c_2 = 3;$$
$$c_3 = 2.$$

Assim,

$M_1 y_1 \equiv 1 \bmod 3 \Rightarrow y_1 = 2$
$M_2 y_2 \equiv 1 \bmod 5 \Rightarrow y_2 = 1$
$M_3 y_3 \equiv 1 \bmod 7 \Rightarrow y_3 = 1$

Pelo Teorema Chinês dos Restos temos:

$x \equiv (M_1 y_1 c_1 + M_2 y_2 c_2 + M_3 y_3 c_3) mod M$
$x \equiv (35.2.2 + 21.1.3 + 15.1.2) mod 105$
$x \equiv (140 + 63 + 30) mod 105$
$x \equiv 233 mod 105$

Como o resto da divisão de 233 por 105 é 23, temos que:
$x \equiv 23 \equiv 233 mod 105$

Logo, $x = 23 + 105t, t \in \mathbb{Z}$.

O problema proposto o exemplo 6.4.1 é uma charada, muito importante para o desenvolvimento do raciocínio lógico do aluno.

7. CRIPTOGRAFIA

Derivada do grego *kriptos*, cujo significado é oculto, a palavra criptografia significa "escrita oculta".

A criptografia, muito utilizada atualmente no nosso cotidiano, em transições bancárias, celulares, computadores, compras on-line, alarmes e até mesmo em chaves de veículos, não é uma novidade. Sua utilização possui um longo histórico e diferentes métodos, que serão tratados mais a frente, todos com o intuito de ocultar mensagens e dificultar sua decodificação.

As primeiras evidências da criptografia surgiram no Egito antigo, aproximadamente 1900 a.C, quando as palavras e alguns trechos de documentos valiosos sobre localizações de tesouros, foram substituídas por símbolos, para que os mesmos não fossem encontrados. Ao longo dos anos, a criptografia foi empregada pelos militares na transmissão de segredo de Estado e da diplomacia além de questões políticas e pessoais. Além disso, em pelo menos dois milênios, a humanidade melhorou os sistemas utilizados, desenvolvendo assim a chamada criptografia moderna, baseada em sistemas computacionais cada vez mais avançados. Sobre isso, Singh afirma que:

> A natureza humana tem uma necessidade à privacidade, mesmo que seja para guardar simples segredos. É possível observar na história que a linguagem de códigos sempre foi muito usada como recurso militar, político, em questões comerciais, em guerras e até mesmo motivos sentimentais. (SINGH, 2008)

O desenvolvimento e o aperfeiçoamento da criptografia passaram por três fases, sendo elas:

i. Artesanal: Durante as idades antigas e médias, com o surgimento da escrita, técnicas que manuseavam papéis e lápis eram fáceis de serem descobertas. Como exemplo, a utilizada por Júlio César, citada mais adiante.

ii. Mecânica: No começo da idade Moderna, com a Revolução industrial e a Segunda Guerra Mundial, deu-se início a utilização das máquinas na criptografia. Como exemplo, a Máquina Enigma.

iii. Digital: A partir do desenvolvimento dos computadores, onde cálculos de números muito grandes eram feitos rapidamente, os métodos de Criptografia foram aperfeiçoados. Um exemplo é o mais utilizado atualmente chamado de RSA.

Além das fases, a criptografia é dividida em:

i. Simétrica: Chamada também de convencional, é onde a chave que criptografa uma mensagem é a mesma para descriptografar.

ii. Assimétrica: Uma chave, chamada de chave pública, criptografa a mensagem e outra, chamada de chave privada, descriptografa.

Alguns métodos utilizados em cada fase da Criptografia serão mostrados a seguir.

7.1.Histórico criptográfico

Como citado anteriormente, a criptografia nasceu há muito tempo e métodos foram desenvolvidos para o aperfeiçoamento dessa técnica. Com isso, descreveremos alguns dos principais métodos e seus respectivos autores.

7.1.1. Cifra de César

Utilizado na Roma antiga, o método de Júlio César é considerado um dos mais famosos e baseava-se na substituição de uma letra do alfabeto por outra correspondente a ela. Por isso, este método era chamado de cifra por *substituição simples*.

Seguindo um padrão predeterminado, César correspondia a letra do alfabeto com uma cifra, como na tabela abaixo:

Tabela 1- Cifra de César

Letra	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
Cifra	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

Fonte: Próprio Autor

Exemplo 7.1. Uma frase muito conhecida de Júlio César seria escrita da seguinte forma, usando-se as cifras correspondentes.

Vini, Vidi, Vici = YLQL, YLGL, YLFL

A cifra por substituição simples era falha pelo fato da mesma letra aparecer frequentemente numa mesma frase, o que facilitava a descoberta da mensagem.

Abaixo, temos a frequência das letras na língua portuguesa:

Tabela 2- Frequência das letras

A	14,63%	N	5,5%
B	1,4%	O	10,73%
C	3,88%	P	2,52%
D	4,99%	Q	1,20%
E	12,57%	R	6,53%
F	1,02%	S	7,81%
G	1,30%	T	4,34%
H	1,28%	U	4,63%
I	6,18%	V	1,67%
J	0,40%	W	0,01%
K	0,02%	X	0,21%
L	2,78%	Y	0,01%
M	4,74%	Z	0,47%

Fonte: HEFEZ, 2016, p.267

Analisando a tabela, percebemos que algumas letras aparecem mais vezes que outra e isso faz com que realmente esse método seja falho. Um exemplo dessa fragilidade é a decapitação da rainha da Escócia Maria Stuart, no século XVI, a partir de uma mensagem decifrada que tinha o intuito do assassinato da rainha Elizabeth I.

7.1.2. Formação de anagramas

Diferente do método utilizado por Júlio César, onde a quebra de um código tornava-se fácil pela frequência de determinadas letras, o chamado método da transposição ou formação de anagramas, consiste em embaralhar as letras de uma palavra ou até mesmo frases com o intuito de dificultar essa quebra. Por exemplo, uma mensagem com 100 letras formam $100!$ permutações possíveis, o que resulta em aproximadamente 9.10^{157}, número este, que torna

ilusório a decifração de um código.

Devido à dificuldade com as trocas das chaves entre os usuários, pode-se dizer que este método é inviável numa população muito grande.

7.1.3. Disco de Alberti

Em meados do século XV, durante o renascimento, Leone Battista Alberti, arquiteto italiano que era considerado um destaque em relação ao seu modo de pensar e também o pai da criptografia ocidental, sugeriu um método com um modelo diferente, chamado de *disco de Alberti* que consistia numa melhoria da cifra de César utilizando substituição polialfabética.

O modelo era formado por dois discos com diferentes diâmetros, fixados por um pino em centro comum, onde o menor era posto sobre o maior, para que o mesmo pudesse girar.

Ambos os círculos (discos) eram divididos em vinte e quatro setores de mesma medida com suas bordas preenchidas da seguinte maneira:

i. Disco maior: Seguindo o sentido horário, foram inscritas letras maiúsculas e numerais.

A, B, C, D, E, F, G, I, L, M, N, O, P, Q, R, S, T, V, X, Z, 1, 2, 3, 4

ii. Disco menor: Em ordem aleatória, foram inscritos letras minúsculas e uma palavra em latim.

a, b, c, d, e, f, g, h, i, k, l, m, n, o, p, q, r, s, t, v, x, y, z, *et*

Para ocorrer uma comunicação utilizando esse método, ambos os correspondentes possuíam cópias idênticas do disco com uma combinação feita anteriormente, onde se girava o disco menor para encontrar a letra ou o número correspondente no disco maior.

7.1.4. Blaise de Vigenère

Em 1553, Giovanni Battista Bellaso criou um novo método para cifrar e decifrar uma mensagem e o mesmo foi publicado em um curto livro, chamado *La cifra del Sig Giovan Batista Belaso*.

O método consistia na utilização de uma tabela intitulada *tabula recta*, apresentada a

seguir, e na distribuição de uma chave.

Tabela 3- Tabula Recta

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

Fonte: HEFEZ, 2016, p.276

Como a cifragem de uma palavra ou de uma mensagem acontece a partir de uma correspondência com letras da palavra chave com a do texto, analisando linha e coluna da

tabela, esse método é considerado muito difícil de ser quebrado, conhecido como cifra indecifrável, pois uma letra qualquer pode ser representada de várias maneiras, ocorrendo-se assim um grande número de possibilidades de chaves.

Blaise de Vigenère, nome o qual foi atribuído erroneamente á descoberta de Bellaso, foi um diplomata francês que em 1586 publicou um livro intitulado *Traicté des Chiffres*, onde seguindo o método apresentado anteriormente acrescentou um novo conceito, chamado de autochave, onde se utilizava o texto original como chave.

7.1.5. Era digital

A Teoria da Informação teve um avanço considerável com a vinda dos telégrafos seguida dos computadores, que utilizavam códigos binários para transmissão de dados. Com isso, com o intuito de converter todas as informações de maneira igualitária, em 1960 surge o ASCII (American Standard Code for Information Interchange), um método de tradução à linguagem binária, atribuindo significados aos 2^7=128 números binários com sete dígitos.

Em 1973, a Nation Bureal of Standards, buscando a uniformização dos padrões utilizados referente aos sistemas criptográficos escolheu como oficial americano um sistema desenvolvido pela IBM, chamado de DES (Data Encryption Standard). Utilizado até 1999, o sistema consistia na distribuição de chaves simétricas, ou seja, uma chave é definida entre os correspondentes com os padrões a serem seguidos para a cifragem e decifragem.

Mesmo com o uso da informática, para ocorrer à troca de senhas era necessário o intermédio de um portador e para pôr fim a isso, três americanos Whitfield Driffie, Martin Hellman e Ralph Merkle, introduziram a Teoria dos Números no ramo da criptografia, através da ideia de congruência, em um sistema denominado DHM. Porém, a troca de chaves só podia ser feita apenas entre dois indivíduos. E mesmo Driffie tentando tornar a troca de chaves assimétrica, esse método foi considerado não viável e insatisfatório.

7.1.6. Sistema RSA

Utilizado atualmente, o sistema RSA é o mais seguro e conhecido método criptográfico. Foi desenvolvido em 1978, por Ronald Rivest, Adi Shamir e Leonard Adleman, cujas inicias

formam o nome dado ao sistema.

A ideia proposta por Driffie em relação a chaves assimétricas foi utilizada e implantada no sistema, ou seja, cada indivíduo possui duas chaves, sendo uma pública e uma privada, para cifragem e decigrafem, respectivamente.

Tendo como base os conceitos da Teoria do Número, o sistema RSA é utilizado em vários setores que usam a comunicação e a assinatura eletrônica, como por exemplo, compras online e o uso de cartão de crédito.

> Esse código foi inventado por R.L. Rivest, A Shamir e L. Adleman, que na época trabalhavam no Massachussets Institute of Technology (M.I.T.). As letras RSA correspondem às iniciais dos inventores do código. 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 Netscape, o mais popular dos softwares de navegação da internet (COUTINHO, 2011, p.3)

Para utilizarmos o sistema RSA, devemos seguir as seguintes instruções:

i. Escolher dois números *p* e *q*, primos.

ii. Conhecer o número $n = p.q$ e $\varphi(n) = (p-1)(q-1)$.

iii. Manter *p* e *q* em sigilo, pois são as chaves de decodificação.

iv. Escolher um número *a* qualquer que faz parte da chave pública, de modo que o $mdc(a, \varphi(n)) = 1$.

v. Resolver a congruência $ab \equiv 1 \bmod \varphi(n)$, para encontrar um número b da chave privada.

vi. Utilizar uma tabela pré formulada com o intuito de transformar os caracteres da mensagem em números e dividi-los em x blocos, de modo que $1 \leq x < n$, garantindo uma única resposta na decodificação.

vii. Criptografa uma mensagem $C(x)$, de acordo com a congruência $x^a \equiv C(x) \bmod n$.

viii. Descriptografa-se uma mensagem $D(C(x))$, utilizando a congruência $C(x)^b \equiv D(C(x)) \bmod n$, com $D(C(x)) < n$.

ix. Colocar em sequência cada bloco $D(C(x))$ e converter em caracteres de acordo com a tabela pré formulada.

Consideremos a seguinte tabela de conversão:

Tabela 4- Conversão RSA

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

Fonte: Próprio Autor

Exemplo 7.1. Utilizando o sistema RSA e considerando *p*=11 e *q*=13, vamos codificar a palavra BELA.

Sendo *p*=11 e *q*=13, então *n*=11.13=143 e $\varphi(n) = (11-1)(13-1) = 120$.

Considerando *a*=7, onde $mdc(a, \varphi(n)) = 1$, temos $ab \equiv 1 \bmod \varphi(n)$. Com isso:

$7b \equiv 1 \bmod 120$

Assim, $7b = 120q + 1 \Leftrightarrow 1 = 7b - 120q$. (I)

Pelo algoritmo de Euclides:

$120 = 7.17 + 1 \Leftrightarrow 1 = 120 - 7.17$ (II)

Comparando (I) e (II) e sabendo que *b* não pode ser negativo, temos que:

b= -17+120*t* e *q*= -1-7*t*

Seja t=1, então *b*=103 (menor valor possível)

Seguindo a tabela 7.4., vamos transformar as letras em números.

B=11, E=14, L=21, A=10

Ou seja, 11-14-21-10.

Devemos agora separar em blocos *x*, onde x < 143.

11142110= 11-142-110

Utilizando $x^a \equiv C(x) \bmod n$, temos:

$11^7 \equiv 132 \bmod 143 \Leftrightarrow C(x_1) = 132$

$142^7 \equiv 142 \bmod 143 \Leftrightarrow C(x_2) = 142$

$110^7 \equiv 33 \bmod 143 \Leftrightarrow C(x_3) = 33$

Com isso, a mensagem codificada é 132-142-33.

Exemplo 7.2. Decodificar a mensagem do Exemplo 7.1.

Utilizando $C(x)^b \equiv D(C(x)) \bmod n$, temos

$132^{103} \equiv 2^{103}.2^{103}.33^{103} \bmod 143$

$132^{103} \equiv 63.63.110 \bmod 143$

$132^{103} \equiv 11 \bmod 143 \Leftrightarrow D(C(x_1)) = 11$

$142^{103} \equiv 2^{103}.71^{103} \bmod 143$

$142^{103} \equiv 63.59 \bmod 143$

$142^{103} \equiv 142 \bmod 143 \Leftrightarrow D(C(x_2)) = 142$

$33^{103} \equiv 110 \bmod 143 \Leftrightarrow D(C(x_3)) = 110$

Com isso, a mensagem decodificada é 11142110 e comparando com a Tabela 7.4., temos a mensagem original BELA.

8. APLICAÇÕES DE CRIPTOGRAFIA NO ENSINO

A criptografia está presente em vários contextos do nosso cotidiano e proporciona o desenvolvimento de inúmeras aplicações em conteúdos matemáticos que podem ser tratados na Educação Básica, levando em consideração a popularização da criptografia no mundo e o desconhecimento do significado da palavra por parte da maioria dos alunos. No entanto, como vários afirmam conhecer livros ou filmes que tem enfoque nesse assunto, fazer a utilização desse conteúdo em sala de aula facilita além do trabalho docente, a ampliação cultural e a vontade do aluno em aprender Matemática. A partir disso, os Parâmetros Curriculares Nacionais, nos mostram que:

> No ensino da Matemática, destacam-se dois aspectos básicos: um consiste em relacionar observações do mundo real com representações (esquemas, tabelas, figuras); outro consiste em relacionar essas representações com princípios e conceitos matemáticos. Nesse processo, a comunicação tem grande importância e deve ser estimulada, levando-se o aluno a falar e a escrever sobre Matemática, a trabalhar com representações gráficas, desenhos, construções, a aprender como organizar e tratar dados. [...] (PCN-MATEMÁTICA, 1997, p.19)

O ensino da criptografia na Educação Básica permite que os alunos desenvolvam habilidades e competências utilizadas no mercado de trabalho e na sociedade, por ser um tema atual e com grandes aplicações. Com isso, a inserção da criptografia nos anos finais do Ensino Fundamental ou Ensino Médio, possibilita a investigação de novos significados e o aprendizado de conceitos e conteúdos, que não estão no currículo proposto, como por exemplo, a aritmética modular, citada anteriormente, que contribui para o ensino de divisibilidade, números primos e até mesmo na resolução de equações. Além disso, as aulas contextualizadas promovem ao aluno uma nova experiência de aprendizagem.

> Percebe-se, então, a necessidade de tornar a Matemática mais interessante para o aluno, de modo que ele tenha prazer em estudá-la. Um dos caminhos possíveis para se alcançar esse objetivo é apresentar a Matemática presente no dia a dia do aluno, fazendo-o perceber que seu estudo é útil e pertinente. Ou seja, é importante contextualizar o ensino (SIQUEIRA, 2016, p. 46).

Busca-se com a contextualização no Ensino Médio, preparar o aluno para a sociedade, de modo que o mesmo saiba se comunicar claramente, trabalhar e agir com eficiência e tomar decisões de maneira assertiva. Em relação à contextualização da Matemática, o intuito é de que o aluno seja capaz de resolver problemas do cotidiano, desenvolvendo assim seu raciocínio

lógico, além de entender a relevância da matemática para o desenvolvimento cientifico e tecnológico.

Dessa forma, as finalidades para o Ensino Médio, de acordo com a Lei de Diretrizes e Bases da Educação Nacional (LDBEN) são:

> • a consolidação e o aprofundamento dos conhecimentos adquiridos no ensino fundamental, possibilitando o prosseguimento de estudos;
> • a preparação básica para o trabalho e a cidadania do educando, para continuar aprendendo, de modo a ser capaz de se adaptar com flexibilidade a novas condições de ocupação ou aperfeiçoamento posteriores;
> • o aprimoramento do educando como pessoa humana, incluindo a formação ética e o desenvolvimento da autonomia intelectual e do pensamento crítico;
> • a compreensão dos fundamentos científico-tecnológicos dos processos produtivos, relacionando a teoria com a prática, no ensino de cada disciplina.
> (BRASIL,1996, Lei 9394)

Escolher temas buscando a contextualização da Matemática com o cotidiano permite que os alunos compreendam realmente conteúdos vistos em anos anteriores, aprofundem seus conhecimentos e busquem novas estratégias para resolver problemas propostos, relacionando a teoria com a prática.

A criptografia, além de ser um tema da atualidade, está presente em vários assuntos que os alunos conhecem, como senhas de banco, compras on-line, computadores e até mesmo nos celulares, muito utilizados no dia a dia. Porém, como muito deles não sabem da existência da criptografia e da sua relação com esses assuntos, a escolha desse tema é muito relevante, pois o intuito é despertar o entusiasmo e o interesse dos alunos para aprender assuntos novos e mostrar a gama de possibilidades futuras.

Um dos conteúdos matemáticos que podem ser tratados aplicando a Criptografia no ensino são as funções, que será enunciado na Seção 8.1.

8.1.Funções

Funções podem ser entendidas como um conceito que trata de problemas de variação e quantificação de fenômenos, em outras palavras, o estudo das funções pode ser entendido como o estudo de relações entre grandezas que variam.

Definição 8.1.1. Dados dois conjuntos A e B, onde $A, B \in \mathbb{R}$, não vazios, uma relação f

de A em B recebe o nome de aplicação de A em B ou função definida em A com imagem em B se, e somente se, para todo $x \in A$ existe somente um $y \in B$ tal que, $(x, y) \in f$, ou seja:

$$f \text{ é aplicação de A em B} \Leftrightarrow \{\forall x \in A, \exists y \in B / (x, y) \in f\}$$

As funções são representações de relações de dependências entre dois conjuntos, geralmente apresentados por meio de tabelas, gráficos e equações, muito presentes no nosso cotidiano.

Os conjuntos A e B, recebem o nome de domínio e contradomínio, respectivamente. Além desses, tem-se a imagem $f(x)$ que nada mais é que valores presentes no conjunto B que correspondem a elementos de A(x), após passar por uma relação de dependência (f), denominada lei de formação. Por isso, chama-se os elementos de A de variáveis independentes e os elementos da imagem de variáveis dependentes, pois eles dependem do A para acontecer.

Exemplo 8.1.1. Considerando que o valor gasto em uma loja depende da quantidade de produtos comprados e que o custo de cada produto é R$3,00, qual o valor da conta se comprarmos 5 unidades? E 12 unidades?

Domínio x: Quantidade de produtos
Imagem $f(x)$: Valor gasto
Lei de formação: $f(x) = 3x$
Com isso, tem-se que:

Se $x = 5$, então $f(5) = 3.5 = 15$. Logo, o valor da conta será R$15,00.
Se $x = 12$, então $f(12) = 3.12 = 36$. Logo, o valor da conta será R$36,00.

Nota-se que a relação de dependência acontece, ou seja, quantidade de produtos é a variável independente e o valor gasto a dependente. Além disso, dizemos que essa relação é diretamente proporcional, pois quando x aumenta, f(x) aumenta na mesma proporção.

Na Criptografia pode ser utilizado o conceito de função. Com isso, surgiu a possibilidade de ensinar e revisar determinados conceitos de função, muito importantes para o prosseguimento da vida escolar, a partir da introdução da Criptografia no ensino.

Para que a Criptografia seja realizada a função deve ser bijetora, ou seja injetora e

sobrejetora, assim conseguimos garantir que a mensagem possa ser criptografada e descriptografada sem alteração na mesma.

Definição 8.1.2. Denomina-se função **injetora**, toda função $f: A \to B$, onde cada elemento do domínio corresponde a um único elemento do contradomínio.

Definição 8.1.3. Denomina-se função **sobrejetora**, toda função $f: A \to B$, que possui em sua imagem todos os elementos do contradomínio.

Definição 8.1.4. Denomina-se função **bijetora**, toda função $f: A \to B$, injetora e sobrejetora, simultaneamente.

Motivar o entendimento do aluno e fazer com que os mesmos se dediquem ao aprendizado é o intuito dessa contextualização, não só em Matemática, como em todas as áreas do conhecimento.

De modo análogo ao Exemplo 8.1.1. o exemplo abaixo, mostra uma das maneiras de relacionar o conceito de função a Criptografia:

Exemplo 8.1.2. Sabendo que a partir de uma mensagem original, conseguimos enviar uma mensagem criptografada, temos que:

Domínio x: Letras da mensagem original (relacionadas a números quaisquer)
Imagem f(x): Mensagem criptografada
Lei de formação: Depende de cada mensagem enviada

A ideia de enviar e receber mensagens criptografadas, utilizando o conceito de função, é uma maneira de apresentar a Criptografia aos alunos, além de auxiliá-los no aprendizado do conteúdo.

Porém, deve-se lembrar que não só a função, mas outros conteúdo matemáticos, como matrizes e números primos, podem ensinados contextualizando com a Criptografia.

9. APLICAÇÃO EM SALA DE AULA

O presente trabalho foi realizado com 14 alunos da 3ª série do Ensino Médio, do Colégio Anglo Cabreúva, onde a autora leciona nos ensinos Fundamental e Médio, as disciplinas de Matemática e Oficina de Matemática, há 8 anos.

Foi aplicado no mês de maio de 2021, durante 4 aulas, de forma totalmente remota, utilizando aplicativos e sites na internet.

O intuito era verificar se os alunos conheciam a Criptografia e se as inserções de novos conceitos chamariam a atenção dos alunos para a disciplina de Matemática, onde vários alunos apresentam dificuldade.

9.1.Descrição do local da aplicação

O Colégio Anglo Cabreúva, localizado na cidade de Cabreúva-SP, é de fácil acesso, pois se encontra na avenida principal do bairro e está próxima a grandes centros, como Jundiaí. Além disso, o bairro, é considerado um local de crescimento, atraindo indústrias, comércios e mudando a perspectiva da comunidade em relação à educação principalmente.

Possui mais de 30 anos de funcionamento, onde atua em todos os níveis da educação básica: Educação Infantil, Ensino Fundamental I e II, e Ensino Médio.

As condições físicas do colégio são excelentes, atendendo assim as condições necessárias ao desenvolvimento do projeto pedagógico. Conta com 10 salas de aulas amplas, uma sala de coordenação e uma de direção, secretaria, laboratórios de informática e de ciências, cantina, parque, quadra esportiva, além de um pátio coberto para os alunos.

Possui 201 alunos desde a Educação Infantil até o Ensino Médio, sendo no Ensino Fundamental, onde encontramos a maior parte deles.

O colégio faz parte da rede particular de ensino, e recebe alunos com perfis socioeconômico na sua maioria de classe média, média alta e alta.

9.2.Desenvolvimento do trabalho

O trabalho foi desenvolvido de forma remota, devido a pandemia da COVID-19, as aulas estão sendo ministradas através de aplicativos como ZOOM e GOOGLE MEET.

A sequência da aplicação se deu da seguinte forma:

a) Questionário inicial;
b) Explicação do conceito de Criptografia;
c) Revisão de conceitos matemáticos;
d) Exercícios para o desenvolvimento da atividade;
e) Questionário final.

9.2.1. Questionário Inicial

Antes de começar a atividade, foi proposto aos alunos um questionário inicial com o intuito de levantar informações, utilizando o Google Forms, que foi disponibilizado por meio do WhatsApp e pela plataforma digital do colégio, chamada Ultramax.

O questionário contou com perguntas simples e de fácil entendimento e resolução.

A intenção da aplicação desse questionário, era verificar se os alunos gostariam de aprender algo novo como a Criptografia que não se encontra no Currículo, mas é muito utilizada no dia a dia do estudante e também perceber qual o interesse por aulas práticas.

A seguir, encontra-se o questionário inicial proposto aos alunos:

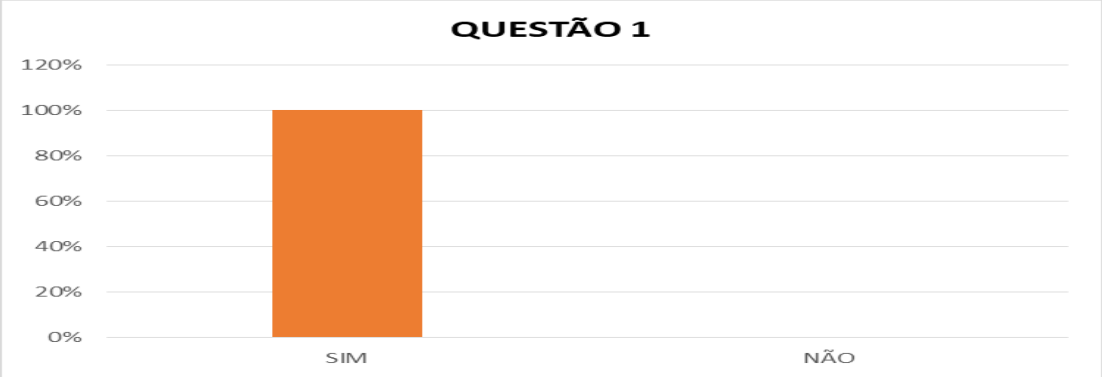
1. Acha importante aprender assuntos novos?
2. Uma aula prática seria interessante? Justifique.
3. Você já ouviu falar em criptografia? Se sim, onde?
4. Em qual conteúdo matemático, você acha que a criptografia se enquadra?
5. Você sabia que existem funções que admitem inversas?

Analisando as respostas dos alunos, temos que:

Na questão 1, 100% deles acham importante aprender novos assuntos e consideram muito bom.

“Sim, aprender assuntos novos é muito bom, conhecimento nunca é demais.”

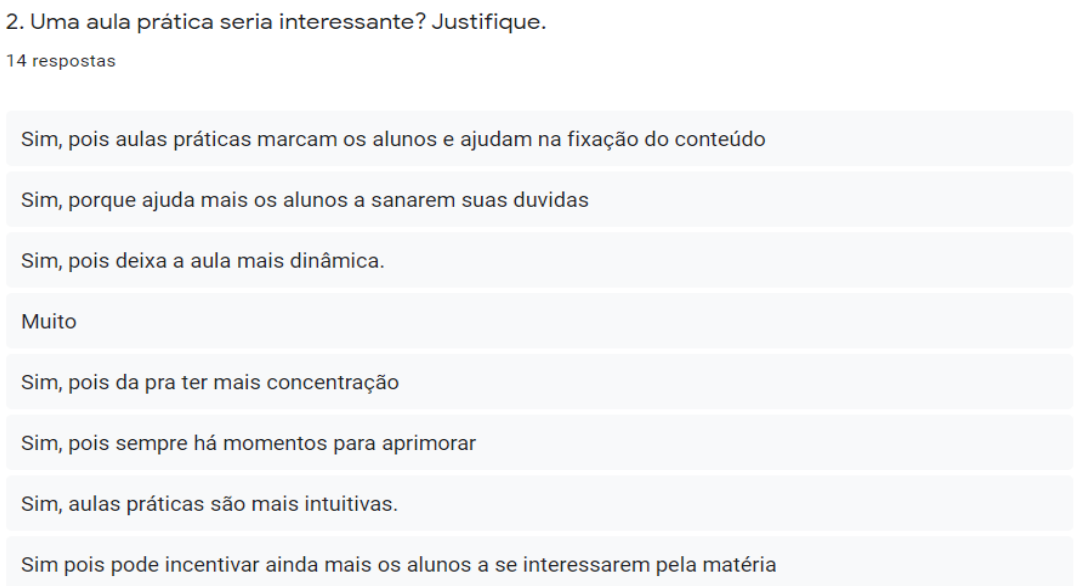
Figura 1- Questão 1: Questionário Inicial



Fonte: Próprio Autor.

Na questão 2, percebe-se que os alunos gostam muito de aulas práticas. Consideram importantes para a fixação do conteúdo e para sanar as dúvidas existentes, aprendendo de uma maneira lúdica e fácil, além de chamar a atenção dos alunos para o assunto em questão e fazer com que se interessem pela disciplina.

Figura 2- Questão 2: Questionário Inicial

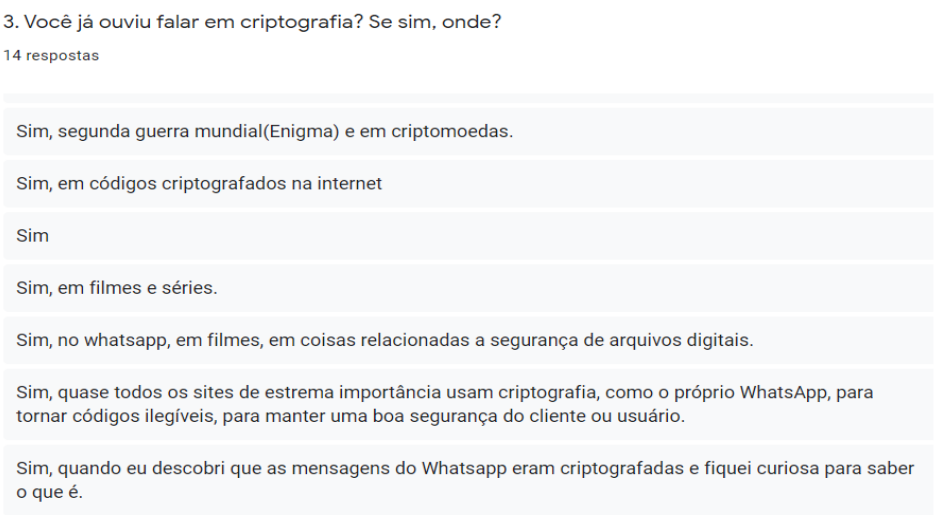


Fonte: Google Forms

Na questão 3, foi perguntado ao aluno se ele conhecia a palavra criptografia, e para a surpresa da autora, todos já tinham ao menos ouvido falar sobre o assunto. A maioria deles disseram ter conhecido através da internet e de filmes, porém alguns citaram a escola e a aula

de história ao relembrar da Máquina Enigma da 2ª Guerra Mundial.

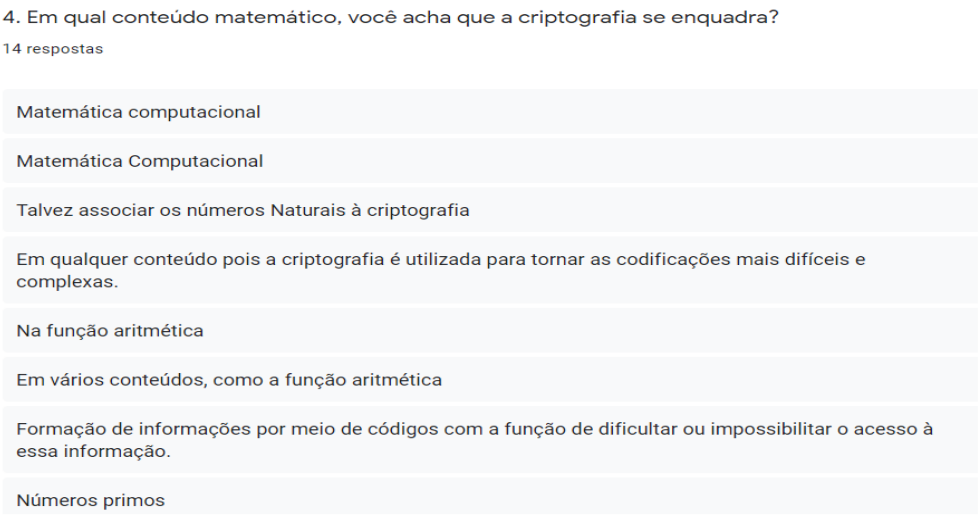
Figura 3- Questão 3: Questionário Inicial



Fonte: Google Forms.

Na questão 4, os alunos foram questionados sobre qual conteúdo matemático eles achavam que a Criptografia se encaixava, pois os mesmos não aprendem esse assunto nos níveis básicos. Muitos deles responderam Matemática Computacional, correspondendo com a questão 3, onde vários sabiam que a criptografia era encontrada na internet. A segunda resposta que mais apareceu foi Função, assunto que foi desenvolvida a atividade. Além desses, os alunos também responderam Números Naturais, Números Primos, Números Binários, Logaritmo e Matrizes.

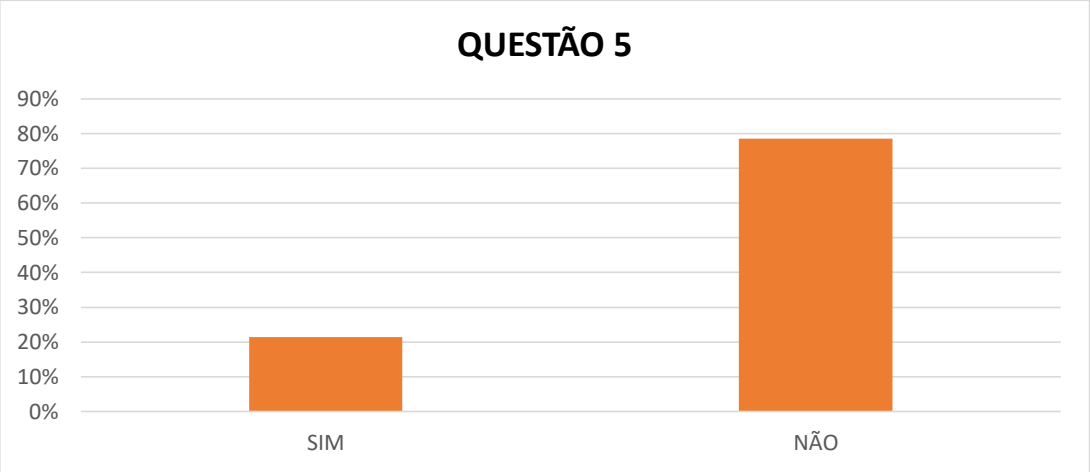
Figura 4- Questão 4: Questionário Inicial



Fonte: Google Forms.

Já a questão 5, foi pensada no fato que os alunos conhecem as funções, mas não aprenderam em anos anteriores o conceito de função inversa, pois não fazia parte do material utilizado no colégio e foi incluído a partir desse ano no material da 1ª série do Ensino Médio, seguindo a BNCC (BASE NACIONAL COMUM CURRICULAR). Como já era esperado, apenas 3 alunos responderam que sabiam que algumas funções admitiam a inversa, o que facilitou o planejamento da aula sobre os conceitos matemáticos utilizados na aplicação da criptografia em função.

Figura 5- Questão 5: Questionário Inicial



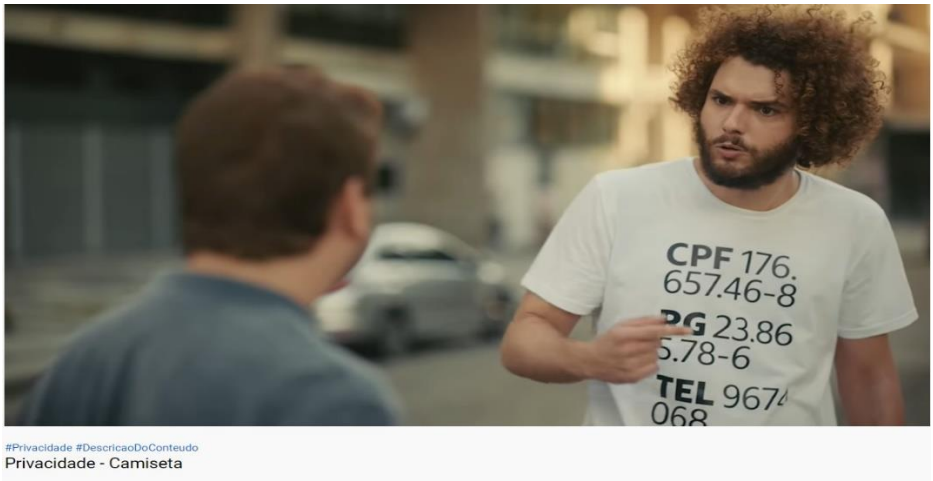
Fonte: Próprio Autor.

9.2.2. Explicação do significado de Criptografia

Após a aplicação do questionário inicial e o levantamento dos dados para dar prosseguimento no trabalho, foi utilizada uma aula expositiva com a explicação do conceito de criptografia e discussão da utilização da mesma no nosso dia a dia.

A aula foi através do aplicativo Zoom, onde primeiramente a professora compartilhou um vídeo de uma propaganda feita pelo Banco Itaú (Disponível em: https://youtu.be/BjeR1wZmI-g), onde pessoas sabiam de todas as informações pessoais importantes de uma outra, para dar início a discussão sobre o assunto de preservação dos dados.

Figura 6- Comercial Banco Itaú: Privacidade - Camiseta



Fonte: Site Youtube.

Após a discussão com os alunos, foi compartilhado um slide feito no Microsoft, contendo definições da criptografia e fases históricas, além de imagens de sites de banco, de compras e aplicativos de conversas como WhatsApp que são protegidos por sistemas de criptografia.

Durante a apresentação do slide, enquanto era apresentado a história da criptografia, o mesmo aluno que respondeu sobre a Máquina Enigma no questionário inicial, levantou esse assunto. Sabendo dessa possibilidade a professora já havia deixado preparado um vídeo explicativo sobre como era o funcionamento dessa máquina e como foi utilizada na 2ª Guerra Mundial (Disponível em **https://www.youtube.com/watch?v=5w3zDa7bgLU&t=25s**), o que gerou muito entusiasmo aos alunos.

Figura 7- Vídeo: Como Funcionou a Máquina Enigma

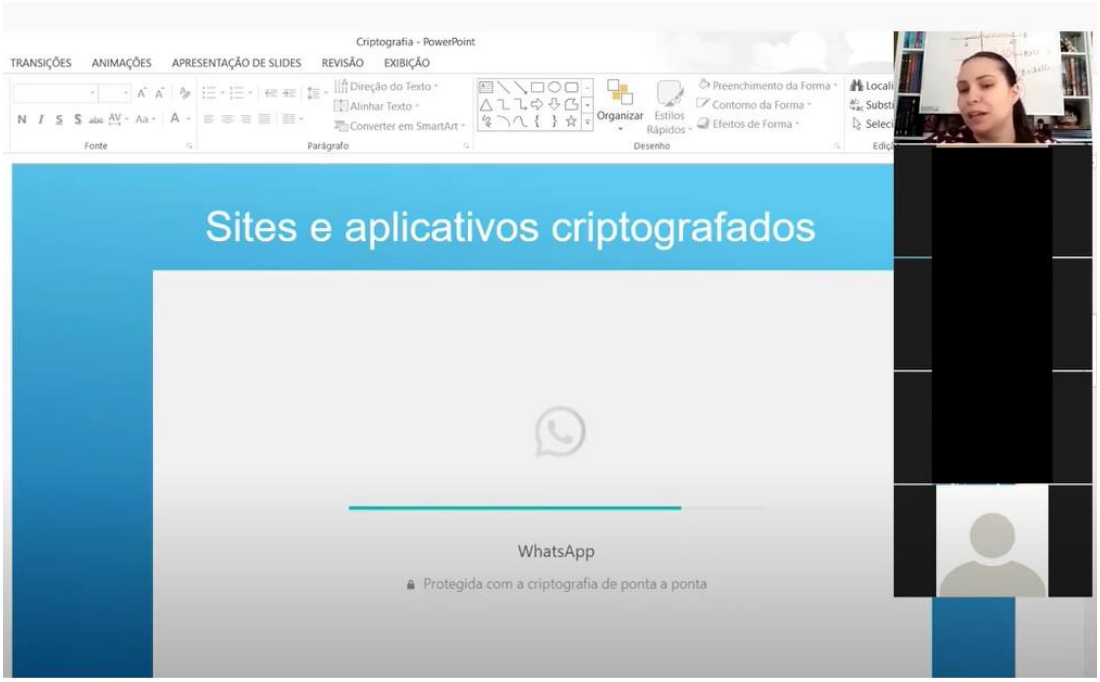
Fonte: Site Youtube.

A seguir, temos imagens da aula citada acima:

Figura 8- Aula expositiva sobre Criptografia

Fonte: Próprio autor.

Figura 9- Aula expositiva sobre Criptografia



Fonte: Próprio autor.

Figura 10- Aula expositiva sobre Criptografia

Fonte: Próprio autor.

Figura 11- Aula expositiva sobre Criptografia

Fonte: Próprio autor.

A última imagem é referente a explicação sobre a Criptografia RSA. Durante a conversa alunos que gostam e sabem utilizar a tecnologia demonstraram muito interesse no assunto.

No decorrer da aula, os alunos expuseram as suas dúvidas e opiniões.

Em uma das discussões, alunos apontaram sobre vazamentos de informações em aplicativos de mensagens como o WhatsApp e debateram sobre a segurança de aplicativos como esse. Foi muito interessante a visão de cada um sobre o assunto, onde chegou-se à conclusão que a proteção dos dados é muito maior que a exposição e com isso, a segurança é válida.

9.2.3. Revisão dos conceitos

Antes de iniciar a atividade prática, foi feito a revisão dos conceitos necessários, principalmente os de função e logaritmo, que era imprescindível para a realização da atividade e tinha sido visto pelos alunos somente na 1ª série do Ensino Médio.

Além da revisão foi necessária a explicação do conceito de Função Inversa, conteúdo novo para os alunos, que na sua maioria, achou interessante e de fácil compreensão.

Foram propostos alguns exemplos e exercícios para que os alunos praticassem um pouco

o novo conceito antes de passarmos para a próxima etapa da atividade, que era os exercícios envolvendo a ideia de criptografia com função.

9.2.4. Atividade prática

Para a realização da atividade prática foram propostos dois exercícios, com níveis de dificuldade diferentes.

Um fato curioso, é que durante a explicação de como seria desenvolvida a atividade uma aluna ficou muito animada, chegando a dizer que se soubesse que isso era possível quando era mais nova, iria mudar toda a visão dela, pois a mesma adorava códigos e brincadeiras de adivinhação, além de mensagens secretas.

Os exercícios propostos foram:

- Exercício 1: Função Afim.
- Exercício 2: Função exponencial

Ambos seguindo a mesma sequência de atividades:

- Criar tabela pré-codificada, com números a partir de dois algarismos para evitar erros de interpretação.
- Escolher em conjunto a frase a ser codificada e a função codificadora.
- Codificar e decodificar a frase.

A seguir, será mostrado o desenvolvimento do trabalho com os alunos.

Exercício 1

Para o primeiro exercício, a professora escolheu a Função Afim, pelo fato de ser um dos tipos mais fáceis de função para se trabalhar, para que os alunos consigam compreender a ideia mais rapidamente.

Começamos o exercício montando em conjunto a tabela pré-codificada.

Tabela 5- Tabela pré-codificada: Exercício 1

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**
10	11	12	13	14	15	16	17	18	19
K	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**
20	21	22	23	24	25	26	27	28	29
U	**V**	**W**	**X**	**Y**	**Z**	**Á**	**É**	**-**	
30	31	32	33	34	35	77	97	88	

Fonte: Próprio autor.

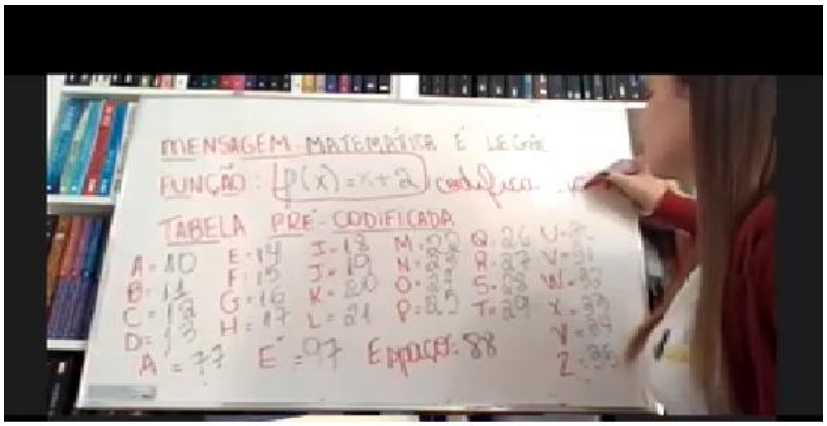
Logo após, os alunos escolheram a mensagem a ser cifrada e uma função afim, para ser a função codificadora.

- Mensagem: *A Matemática é legal*
- Função: $f(x) = x + 2$

A função escolhida pode ser vista como uma utilização da Cifra de César, com a translação de duas letras no alfabeto.

A imagem abaixo, mostra o momento da aula, citado acima:

Figura 12- Criação da tabela, função e mensagem



Fonte: Próprio Autor

Para dar continuidade, os alunos primeiramente fizeram a correspondência de cada letra da mensagem com a tabela **22102914227729181210 88 97 88 2114161021** e fizeram a codificação da mesma, utilizando a função criada por eles.

$f(22) = 22 + 2 = 24$

$f(10) = 10 + 2 = 12$

$f(29) = 29 + 2 = 31$

$f(14) = 14 + 2 = 16$

$f(22) = 22 + 2 = 24$

$f(77) = 77 + 2 = 79$

$f(29) = 29 + 2 = 31$

$f(18) = 18 + 2 = 20$

$f(12) = 12 + 2 = 14$

$f(10) = 10 + 2 = 12$

$f(88) = 88 + 2 = 90$

$f(97) = 97 + 2 = 99$

$f(88) = 88 + 2 = 90$

$f(21) = 21 + 2 = 23$

$f(14) = 14 + 2 = 16$

$f(16) = 16 + 2 = 18$

$f(10) = 10 + 2 = 12$

$f(21) = 21 + 2 = 23$

Logo, a mensagem codificada foi: **24123116247931201412 90 99 90 2316181223**.

Para fazer a decodificação, os alunos aplicaram o conceito de função inversa na função codificadora, $f(x) = x + 2$

Seja $f(x) = y$, então:

$$x = y + 2$$

$$y = x - 2$$

Com isso,

$$f^{-1}(x) = x - 2$$

A partir da função inversa, eles iniciaram o processo de decodificação.

$f^{-1}(24) = 24 - 2 = 22$

$f^{-1}(12) = 12 - 2 = 10$

$f^{-1}(31) = 31 - 2 = 29$

$f^{-1}(16) = 16 - 2 = 14$

$f^{-1}(24) = 24 - 2 = 22$

$f^{-1}(79) = 79 - 2 = 77$

$f^{-1}(31) = 31 - 2 = 29$

$f^{-1}(20) = 20 - 2 = 18$

$f^{-1}(14) = 14 - 2 = 12$

$f^{-1}(12) = 12 - 2 = 10$

$f^{-1}(90) = 90 - 2 = 88$

$f^{-1}(99) = 99 - 2 = 97$

$f^{-1}(90) = 90 - 2 = 88$

$f^{-1}(23) = 23 - 2 = 21$

$f^{-1}(16) = 16 - 2 = 14$

$f^{-1}(18) = 18 - 2 = 16$

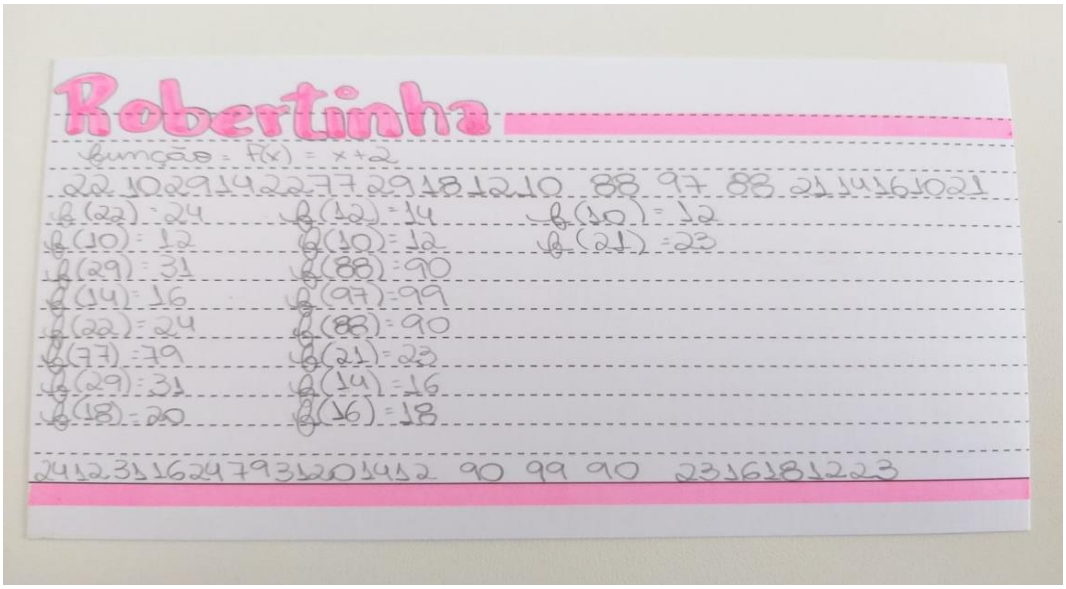
$f^{-1}(12) = 12 - 2 = 10$

$f^{-1}(23) = 23 - 2 = 21$

Assim retornaram a mensagem inicial **22102914227729181210 88 97 88 2114161021**, que significa **Matemática é legal**.

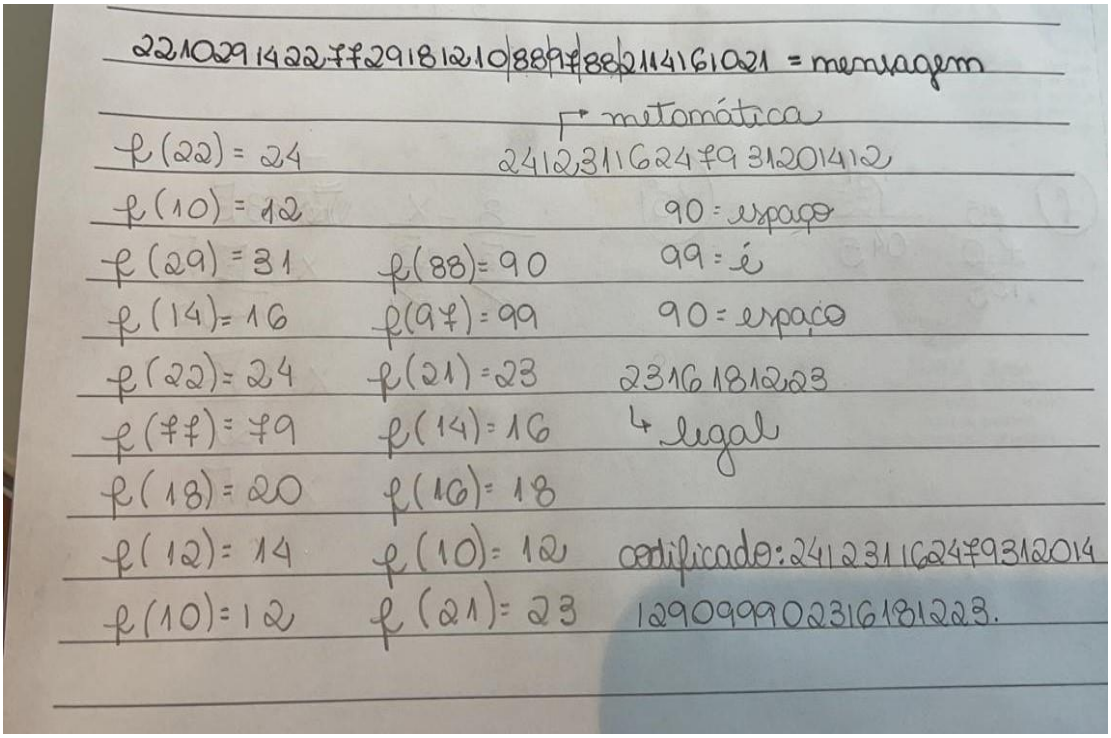
Abaixo temos algumas imagens dos exercícios realizados pelos alunos:

Figura 13- Exercício feito por aluno



Fonte: Próprio autor.

Figura 14- Exercício feito por aluno



Fonte: Próprio autor.

Exercício 2

Para a realização do exercício 2, a professora escolheu a Função Exponencial, cuja inversa é a Função Logarítmica, com o intuito de mostrar para os alunos que esses conceitos também podiam ser inseridos na Criptografia.

A atividade deu-se da mesma maneira da anterior. Primeiramente os alunos criaram uma tabela pré-codificada. Eles quiseram manter a mesma tabela fazendo pequenas alterações. Em seguida, criaram a mensagem e a função codificadora.

Tabela 6- Tabela pré-codificadora: Exercício 2

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**
10	11	12	13	14	15	16	17	18	19
K	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**
20	21	22	23	24	25	26	27	28	29
U	**V**	**W**	**X**	**Y**	**Z**	**Ú**	**-**		
30	31	32	33	34	35	38	40		

Fonte: Próprio autor.

- Mensagem: Anglo Cabreúva
- Função: $f(x) = 2^x$

Como fazia pouco tempo que os alunos tinham visto Equação exponencial, eles sabiam que quanto maior o número da base da potência, maior seria o resultado. Por isso, eles escolheram a potência de base 2.

Fizeram a correspondência da mensagem com a tabela: **1023162124 40 1210112714383110**, codificando a frase logo em seguida.

$f(10) = 2^{10} = 1.024$
$f(23) = 2^{23} = 8.388.608$
$f(16) = 2^{16} = 65.656$
$f(21) = 2^{21} = 2.097.152$
$f(24) = 2^{24} = 16.777.216$

.
.
.

Como os resultados foram grandes, os alunos estabeleceram que cada letra seria representada separadamente por meio de uma barra.

Assim a função codificada foi: **1024/ 8388608/ 65656/ 2097152/ 16777216/ 1099511627776/ 4096/ 1024/ 2048/ 134217728/ 16384/ 274877906944/ 2147483648/ 1024.**

Aplicando a função inversa, na função $f(x) = 2^x$, temos:

$$x = 2^y$$
$$y = \log_2 x$$

Com isso,

$$f^{-1}(x) = \log_2 x$$

Assim, foi feita a decodificação da mensagem:

$f^{-1}(1024) = \log_2 1024 = 10$

$f^{-1}(8388608) = \log_2 8388608 = 23$

$f^{-1}(65656) = \log_2 65656 = 16$

$f^{-1}(2097152) = \log_2 2097152 = 21$

$f^{-1}(16777216) = \log_2 16777216 = 24$

.

.

Chegando na mensagem original **1023162124 40 1210112714383110** que correspondia à **Anglo Cabreúva.**

Os alunos acharam o exercício 2 muito trabalhoso, porém gostaram muito e disseram que foi bom para desenvolver habilidades com o cálculo de logaritmos. Como os valores eram altos, para a realização da atividade, foi utilizada a calculadora científica e o celular.

9.2.5. Questionário final

Assim como no inicial, para o questionário final também foi utilizado o Google Forms e aplicativos de comunicação, como o WhatsApp.

O que diferencia os questionários, é que o final, além de questões simples, conta com uma questão prática.

O intuito desse questionário, foi a verificação do entendimento dos alunos em relação ao conceito de criptografia e a utilização da função nesse assunto.

A seguir, encontra-se o questionário proposto para os alunos:

1. A atividade mudou sua visão em relação as aulas tradicionais (giz e lousa)?
2. Você conseguiu compreender o conceito de Criptografia?
3. A Atividade despertou o seu interesse em buscar mais informações sobre o tema?
4. Atividade avaliativa:

Em uma festa junina, Ana enviou um correio elegante para Eduardo com a seguinte mensagem:

"*Sei que você gosta de gosta de Matemática, então estou mandando uma mensagem codificada 76922880 62 241264821280 42.*

Siga a tabela e a função codificadora f(x)=2x-8

Tabela 7- Tabela pré-codificadora :Atividade avaliativa

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*
10	*12*	*14*	*16*	*18*	*20*	*22*	*24*	*26*	*28*
K	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*
30	*32*	*34*	*36*	*38*	*40*	*42*	*44*	*46*	*48*
U	*V*	*W*	*X*	*Y*	*Z*	*!*	*?*	-	*Ç*
50	*52*	*54*	*56*	*58*	*60*	*15*	*25*	*35*	*45*

Fonte: Próprio autor.

Não esqueça de me enviar a sua resposta!"

As respostas para o questionário foram bem satisfatórias, algumas até surpreenderam a professora.

Na questão 1, a maioria dos alunos disseram que a atividade mudou a sua visão em relação ao modelo de aula tradicional, facilitando entendimento pelo fato da prática. Porém, dois dos alunos disseram preferir as aulas ditas "normais", pois consideram a aula expositiva mais proveitosa e conseguem aprender mais facilmente.

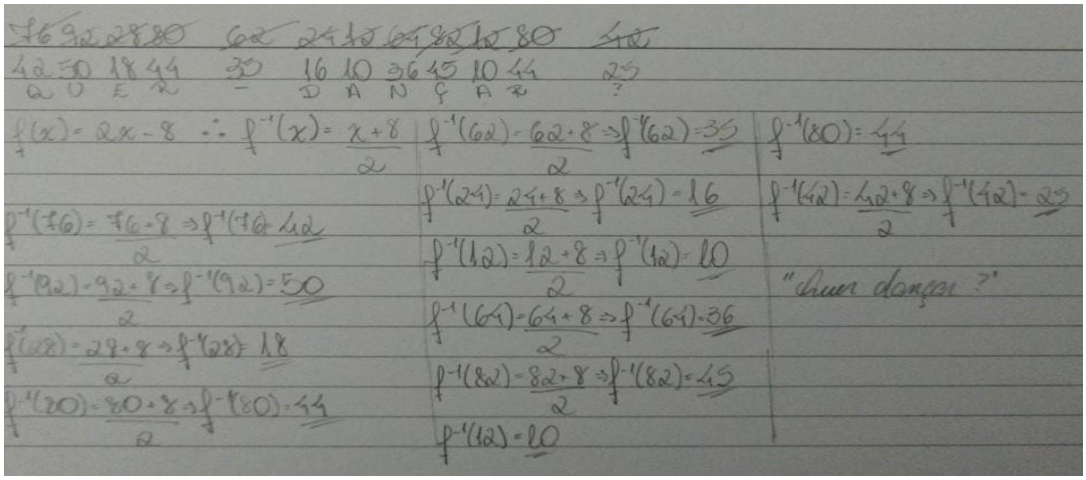
Na questão 2, 100% dos alunos disseram ter compreendido o conceito de criptografia e que abriu a visão deles em relação ao tema.

Na questão 3, todos responderam que além dessa abertura da visão em relação ao tema, despertou o interesse dos mesmos em buscar novas informações e se aprofundarem mais no assunto.

A questão 4, era uma questão prática, onde foi proposta uma mensagem a ser decodificada. Os alunos adoraram e a aluna que disse que amaria mensagens criptografada na infância, voltou a comentar sobre o assunto, afirmando que essa ideia de mandar mensagens dessa maneira poderia ser recorrente e pediu para que a professora fizesse isso sempre para que pudessem pensar mais, desenvolvendo assim, cada vez mais seu raciocínio lógico.

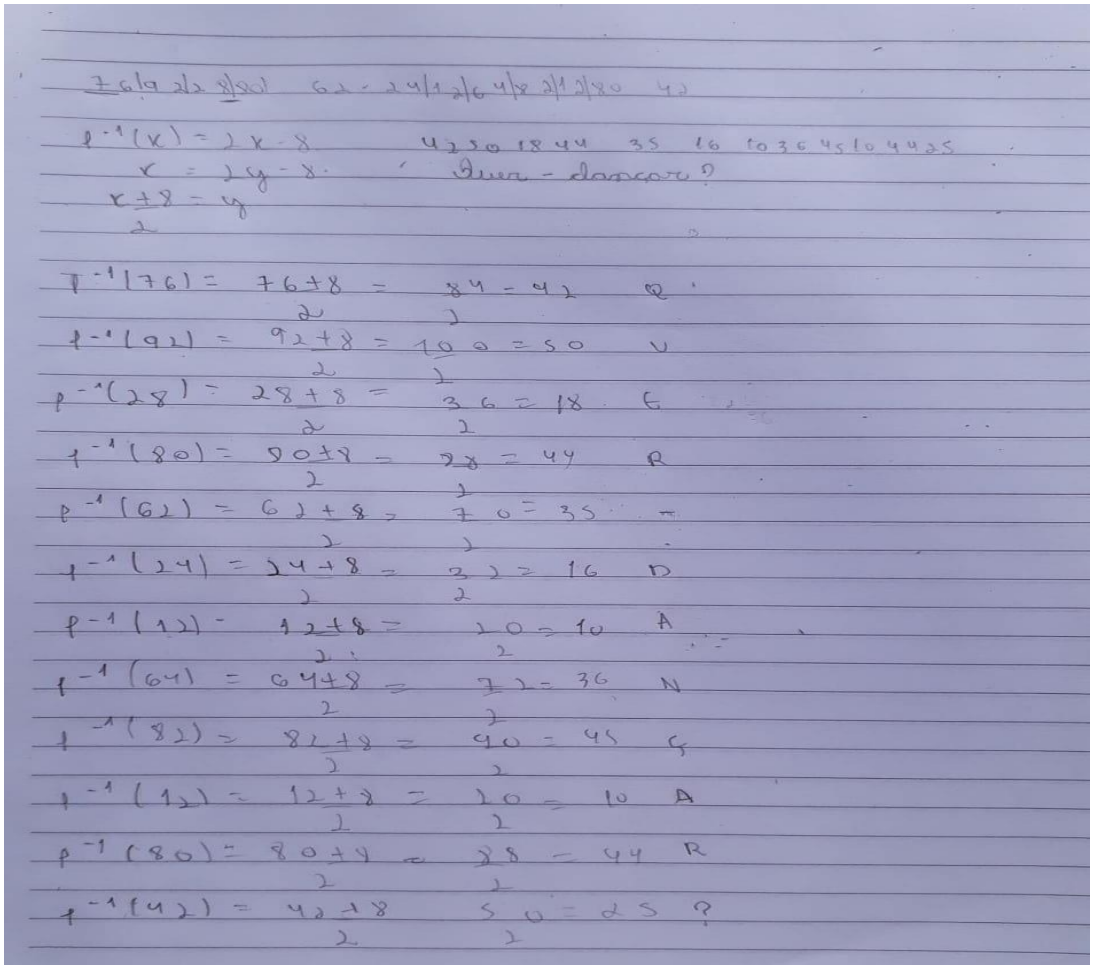
Abaixo, estão algumas imagens da questão 4, realizadas pelos alunos:

Figura 15- Exercício feito por aluno



Fonte: Próprio autor.

Figura 16- Exercício feito por aluno



Fonte: Próprio autor.

CONCLUSÃO

O trabalho teve como propósito analisar se a inserção de assuntos presentes no cotidiano, como a Criptografia durante as aulas, despertariam um interesse maior por parte dos alunos no conteúdo de funções, acarretando assim uma aprendizagem mais significativa. Para isso, foi proposta uma atividade prática envolvendo o tema citado, contendo questionários, exposições de conteúdos e exercícios diferenciados. Foi desenvolvido totalmente de forma remota, utilizando aplicativos e ferramentas como o Zoom e o Google Forms, o que dificultou um pouco o andamento das atividades, contudo os resultados foram satisfatórios.

O questionário inicial nos traz que os alunos têm muito interesse em aprender coisas novas, principalmente com aulas práticas, que para eles ajudam no aprendizado e na fixação do conteúdo proposto. Serviu como um norte para a sequência da atividade, pois foi possível perceber que todos os alunos já conheciam a palavra Criptografia, onde alguns citaram fatos importantes relacionados com a mesma, como a sua presença na 2ª Guerra Mundial. Porém, muitos não sabiam onde era utilizada na Matemática.

A explicação do significado da Criptografia e do seu contexto histórico, levantou muitas dúvidas, gerando debates durante a aula. O que nos faz perceber que trazer assuntos que não estão presentes no Currículo, mas sim no dia a dia, para a sala de aula, estimula a autonomia do estudante, tornando-os mais ativos e críticos.

A aula prática para a 3ª série do Ensino Médio, consistiu na contextualização da Criptografia para o ensino de Funções, a partir de dois exercícios diferenciados com o intuito de criptografar e descriptografar uma mensagem qualquer, escolhida pelos alunos. No desenvolvimento da atividade, muitos alunos demonstraram um maior ímpeto em relembrar os conceitos de função, vistos em anos anteriores, para que pudessem aplicar nos exercícios propostos, além da vontade de aprender conceitos novos, como a função inversa, para dar continuidade na atividade. Isso nos mostra que, quando os alunos são colocados diante de situações incomuns, buscam alternativas e se esforçam para realizá-las.

O questionário final, nos faz perceber que os alunos gostam de aulas diferenciadas e que deixar de lado, por um instante, a forma comum de ensino (giz e lousa), aumenta a motivação dos mesmos para aprender novos conceitos. Por isso, professores devem buscar cada vez mais formas atrativas de ensino, como jogos, utilização de softwares, exercícios distintos dos usuais, entre outros.

A busca por novas práticas traz dificuldades para alguns professores. Atualmente, a tecnologia é o principal canal de interação entre a escola e os alunos e com isso, além de um tempo maior gasto na preparação de novas aulas, o professor deve se dedicar constantemente a aprender a manusear as novas ferramentas digitais, para complementar sua aula.

A aplicação deste trabalho, nos mostra que todo o esforço é válido quando se trata da educação, pois mesmo encontrando as dificuldades causadas pelo ensino remoto, o objetivo foi atingido e os alunos relembraram e aprenderam novos conceitos de uma maneira lúdica. E que preparar uma aula mais atrativa, com o auxílio ou não da tecnologia, abrem novos horizontes, tanto para o professor quanto para o aluno.

A satisfação em ouvir de uma aluna durante um dos debates da aula prática: "*Amei aprender enviar mensagens criptografadas! Adoraria ter conhecido isso quando criança!"*, fez todo o esforço valer a pena.

REFERÊNCIAS

BOYER, Carl B., e MERZBACH, Uta C. **História da Matemática**. 3.ed. Traduzido por Helena Castro. São Paulo: Blucher, 2012.

BRASIL, **Ministério da Educação. Parâmetros Curriculares Nacionais:** Matemática. Brasília: MEC/SEF, 1997.

BRASIL. **Lei de Diretrizes e Bases da Educação Nacional**, LDB. 9394/1996

CAMBI, Franco. **História da pedagogia**. Traduzido por Álvaro Lorencini. São Paulo: Fundação Editora da UNESP (FEU), 1999.

COMO Funcionou a Máquina Enigma. Youtube. 01 set. 2016. 03min39seg. Em <https://www.youtube.com/watch?v=5w3zDa7bgLU&t=25s>. Acesso em 25 mai. 2021

COUTINHO, S. C. **Números Inteiros e Criptografia RSA.** 2.ed. Rio de Janeiro: IMPA, 2011.

DANTZIG, Tobias. **Número:** a linguagem da ciência. Traduzido por Sergio Goes de Paula. Rio de Janeiro: Zahar, 1970.

FERREIRA, Aurélio Buarque de Holanda. **Miniaurélio Século XXI Escolar:** O minidicionário da língua portuguesa. 4.ed. Rio de Janeiro: Nova Fronteira, 2001.

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

IFRAH, Georges. **Os números:** história de uma grande invenção. 3.ed. Traduzido por Stella M. Freitas Senra. São Paulo: Globo, 1985.

MOL, Rogério Santos. **Introdução à história da matemática.** Belo Horizonte: CAED UFMG, 2013.

ORE, Oystein. **Number Theory and its History.** New York: Dover, 1988.

PEREIRA, Nádia Marques Ikeda, **Criptografia: uma nova proposta de ensino de matemática no ciclo básico**. 78f. Dissertação de Mestrado. Universidade Estadual Paulista, 2015.Disponível em:https://repositorio.unesp.br/bitstream/handle/11449/127733/000844677.pdf;jsessionid=EE80CA2F624682D5CB96239AC82F164F?sequence=1. Acesso em: 12 mai. 2020.

PRIVACIDADE-Camiseta.Itaú. **Youtube**. 08 abr. 2021. 00min48seg. Em <https://youtu.be/BjeR1wZmI-g>. Acesso em 25 mai. 2021.

SAUTOY, Marcus du. **A Música dos Números Primos:** A história de um problema não resolvido da matemática. 1.ed. [S.l.]: Zahar, 2007.

SINGH, Simon. **O Último Teorema de Fermat:** a história do enigma que confundiu as melhores mentes durante 358 anos. 13ª.ed. Traduzido por Jorge Luiz Calife. Rio de Janeiro:

Record, 2008.

SIQUEIRA, Josué Rangel de. **A natureza sob um prisma matemático**. 95f. Monografia (Licenciatura em Matemática). Instituto Federal de Educação Ciência e Tecnologia Fluminense, 2016. Disponível em: <file:///C:/Users/Usuario/Downloads/A%20natureza%20sob%20um%20prisma%20matematico.pdf>. Acesso em: 17 jul. 2021.

TRAJANO, Antônio. **Arithmetica Primaria**. 12.ª ed. Rio de Janeiro: Livraria Francisco Alves, s/data.