Universidade Federal de Goiás (UFG)
Instituto de Matemática e Estatística (IME)
Programa de Pós-Graduação em Matemática em Rede Nacional
(PROFMAT/UFG)

Aline Márcia dos Santos

A MATEMÁTICA DAS CRIPTOGRAFIAS

Goiânia
2025

UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO (TECA) PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TESES

E DISSERTAÇÕES NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), regulamentada pela Resolução CEPEC nº 832/2007, sem ressarcimento dos direitos autorais, de acordo com a Lei 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo das Teses e Dissertações disponibilizado na BDTD/UFG é de responsabilidade exclusiva do autor. Ao encaminhar o produto final, o autor(a) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do material bibliográfico

[x] Dissertação [ ] Tese [ ] Outro*:_____

*No caso de mestrado/doutorado profissional, indique o formato do Trabalho de Conclusão de Curso, permitido no documento de área, correspondente ao programa de pós-graduação, orientado pela legislação vigente da CAPES.

Exemplos: Estudo de caso ou Revisão sistemática ou outros formatos.

2. Nome completo do autor

Aline Márcia dos Santos

3. Título do trabalho

A Matemática das Criptografias

4. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador)

Concorda com a liberação total do documento [X] SIM [ ] NÃO[1]

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante:
a) consulta ao(à) autor(a) e ao(à) orientador(a);
b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo da tese ou dissertação.
O documento não será disponibilizado durante o período de embargo.
Casos de embargo:
- Solicitação de registro de patente;
- Submissão de artigo em revista científica;
- Publicação como capítulo de livro;
- Publicação da dissertação/tese em livro.

Obs. Este termo deverá ser assinado no SEI pelo orientador e pelo autor.

Documento assinado eletronicamente por **Paulo Henrique De Azevedo Rodrigues**, **Professor do Magistério Superior**, em 10/07/2025, às 16:38, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Aline Márcia Dos Santos**, **Discente**, em 11/07/2025, às 14:10, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5490131** e o código CRC **CFF9EB19**.

Referência: Processo nº 23070.031205/2025-75 SEI nº 5490131

Aline Márcia dos Santos

A MATEMÁTICA DAS CRIPTOGRAFIAS

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional (PROFMAT/UFG), do Instituto de Matemática e Estatística(IME), da Universidade Federal de Goiás(UFG), como requisito para obtenção do título de Mestra em Matemática. **Área de concentração:** Matemática do Ensino Básico. **Orientador:** Prof. Dr. Paulo Henrique de Azevedo Rodrigues.

Goiânia
2025

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Santos, Aline Márcia dos
A Matemática das Criptografias [manuscrito] / Aline Márcia dos Santos. - 2025.
108 f.

Orientador: Prof. Dr. Paulo Henrique de Azevedo Rodrigues.
Dissertação (Mestrado) - Universidade Federal de Goiás, Instituto de Matemática e Estatística (IME), PROFMAT - Programa de Pós graduação em Matemática em Rede Nacional - Sociedade Brasileira de Matemática (RG), Goiânia, 2025.
Bibliografia. Apêndice.
Inclui siglas, abreviaturas, símbolos, tabelas, algoritmos.

1. Criptografia.. 2. Aritmética Modular.. 3. Divisões Euclidianas.. 4. Segurança Cibernética.. 5. Matemática Prática BNCC.. I. Rodrigues, Paulo Henrique de Azevedo, orient. II. Título.

CDU 51:37

UNIVERSIDADE FEDERAL DE GOIÁS

INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

ATA DE DEFESA DE DISSERTAÇÃO

Ata nº 16 da sessão de Defesa de Dissertação de Aline Márcia dos Santos, que confere o título de Mestra em Matemática, na área de concentração em **Matemática do Ensino Básico.**

Aos oito dias do mês de julho de dois mil e vinte e cinco, a partir das 10h30m por meio de videoconferência, realizou-se a sessão pública de Defesa de Dissertação intitulada "A Matemática das Criptografias". Os trabalhos foram instalados pelo Orientador, Professor Doutor Paulo Henrique de Azevedo Rodrigues (IME/UFG) com a participação dos demais membros da Banca Examinadora: Professor Doutor Mário José de Souza (IME/UFG) e o membro titular externo Sandro Ricardo Pinto da Silva (UFAC). Durante a arguição os membros da banca **não fizeram** sugestão de alteração do título do trabalho. A Banca Examinadora reuniu-se em sessão secreta a fim de concluir o julgamento da Dissertação, tendo sido a candidata **aprovado** pelos seus membros. Proclamados os resultados pelo Professor Doutor Paulo Henrique de Azevedo Rodrigues, Presidente da Banca Examinadora, foram encerrados os trabalhos e, para constar, lavrou-se a presente ata que é assinada pelos Membros da Banca Examinadora, aos oito dias do mês de julho de dois mil e vinte e cinco.

TÍTULO SUGERIDO PELA BANCA

Documento assinado eletronicamente por **Paulo Henrique De Azevedo Rodrigues**, **Professor do Magistério Superior**, em 08/07/2025, às 12:21, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Mario Jose De Souza**, **Professor do Magistério Superior**, em 08/07/2025, às 12:22, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **SANDRO RICARDO PINTO DA SILVA**, **Usuário Externo**, em 08/07/2025, às 13:49, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5440873** e o código CRC **0E48E013**.

Referência: Processo nº 23070.031205/2025-75 SEI nº 5440873

Dedico este trabalho ao meu marido, pelo apoio incondicional e por cuidar com dedicação do nosso lar durante o período em que estive imersa neste projeto. À minha filha, pela valiosa colaboração na revisão gramatical e pelas orientações prestadas na língua inglesa, minha sincera gratidão.

Agradecimentos

Em primeiro lugar, agradeço a Deus por ter-me sustentado em cada etapa desta caminhada, desde minha aprovação no processo seletivo até a conclusão desta dissertação.

Registro minha gratidão ao amigo Wallisson, companheiro de jornada no mestrado, cuja ajuda foi essencial nos momentos mais desafiadores. Ao professor Paulo Henrique, meu orientador, agradeço profundamente pela paciência, orientação e apoio constante ao longo do desenvolvimento deste trabalho.

Agradeço, ainda, ao meu marido e ao meu filho, que se reorganizaram com generosidade durante minha ausência. À minha filha Carolina, agradeço pelo apoio na estruturação desta dissertação e pela colaboração cuidadosa na revisão do texto.

"A matemática é a linguagem em que Deus escreveu o Universo."
Galileu Galilei (1564-1642).

Resumo

A Aritmética Modular é sistematicamente empregada no desenvolvimento de tecnologias contemporâneas a fim de promover a segurança cibernética, a exemplo da necessidade de proteção de dados em transações bancárias e em plataformas de redes sociais. Considerando o contexto hodierno, em que a comunicação digital é elemento fundamental para a segurança da informação, o presente estudo objetiva mostrar a estudantes e professores de Matemática do Ensino Médio uma utilização prática da Aritmética Modular no cenário atual em que vivemos, através do uso da Criptografia, por meio de uma revisão de literatura acerca do tema. Diante disso, o trabalho volta-se para a elaboração de um material direcionado especificamente para o ensino da Aritmética Modular no Ensino Médio, de forma a validar sua aplicação prática. Para mais, realiza-se uma breve análise histórica que evidencia a recorrente utilização de métodos criptográficos em diferentes civilizações. Ao relacionar conteúdos clássicos, como Divisões Euclidianas, com situações concretas de proteção de dados e segurança da informação, foi possível construir uma ponte entre o conhecimento matemático e o cotidiano dos estudantes. Por fim, é proposta uma sequência didática com treze atividades em consonância com a Base Nacional Comum Curricular (BNCC) por meio da qual busca-se otimizar a aprendizagem matemática conectada à prática, em detrimento de um ensino mecânico e desconectado com a realidade.

Palavras-chave: Criptografia; Aritmética Modular; Segurança Cibernética; Divisões Euclidianas; Matemática Prática BNCC.

Abstract

Modular arithmetic is systematically employed in the development of contemporary technologies in order to promote cybersecurity, such as the need for data protection in banking transactions and on social media platforms. Considering the contemporary scenario, in which digital communication is a fundamental element for information security, this study aims to demonstrate to high school mathematics students and teachers a practical application of modular arithmetic in the current context, through the use of cryptography, through a literature review on the topic. Therefore, the work focuses on developing a material specifically aimed at teaching modular arithmetic in high school, in order to validate its practical application. Furthermore, a brief historical analysis is conducted to highlight the recurring use of cryptographic methods in different civilizations. By relating classical content, such as Euclidean divisions, to concrete data protection and information security situations, it was possible to build a bridge between mathematical knowledge and the daily lives of students. Finally, a teaching sequence is proposed with thirteen activities aligned with the National Common Curricular Base. This sequence seeks to optimize mathematical learning by connecting it to practice,in detriment of a teaching method disconnected from reality.

Keywords: Cryptography; Modular Arithmetic; Cybersecurity; Euclidean Divisions; Practical Mathematics BNCC.

Sumário

Introdução

"A Criptografia é a arte de se escrever em códigos"(SILVA, 2005).

Na contemporaneidade, a compreensão da Criptografia como uma ciência de codificação e decodificação é essencial para a proteção e salvaguarda de dados cibernéticos.

Nesse sentido, o presente trabalho constrói uma revisão bibliográfica com a elaboração de material específico de uma proposta de ensino em Aritmética modular para turmas do Ensino Médio da Educação Básica. Tem, ainda, como objetivo demonstrar aos professores e estudantes uma utilização prática da Teoria dos Números.

Levando em consideração que a tecnologia moderna de comunicação tem como base a Criptografia e a Teoria dos Códigos, estudaremos tópicos de aritmética modular que serão usados em mensagens criptografadas, mostrando ao estudante aplicações matemáticas que contribuem para os avanços da comunicação.

Conforme será demonstrado, ao longo da história, a Criptografia é responsável por criar cifras que possibilitam a comunicação entre fontes autorizadas, ao mesmo tempo impedindo que fontes não autorizadas tenham acesso ao conteúdo dessas mensagens.

Foi muito usada durante a Segunda Guerra Mundial pelos alemães; com isto, os criptógrafos da época foram desafiados a descodificar as mensagens por eles enviadas, surgindo então máquinas decodificadoras (KRISCHER, 2013).

A Criptografia é um método usado há milênios, mas a partir do século XX, com o uso intensivo da internet, sua aplicação se popularizou e acabou tornando-se cada vez mais necessária no mundo atual, isto por causa da segurança e da transmissão de informações nos sistemas digitais e hoje possui teoria própria.

No entanto, para trabalhar habilidades encontradas na Base Nacional Comum Curricular - BNCC (BRASIL, 2018), desenvolver-se-á uma sequência didática contendo treze atividades com duração média de 50 minutos cada.

1 Contextualização Histórica

Segundo o artigo "Um pouco da Teoria dos Números: da Antiguidade até os Dias Atuais", de Cristiana Abud da Silva Fusco e Sônia Pitta Coelho(FUSCO; COELHO, 2014), publicado na Revista Matemática em Debate, o uso da Criptografia é uma ferramenta antiga: existem relatos históricos datados desde 1900 a.C. em mensagens do Egito antigo, esculpidas em hieróglifos nas paredes de um túmulo. Já na

Mesopotâmia, foram encontrados tabletes de argila que continham, supostamente, receitas secretas de esmaltes cerâmicos, isso por volta de 1500 a.C..

Os espartanos usavam um bastão cifrador, o scytale, que era uma espécie de disco que embaralhava as letras criando mensagens codificadas em suas comunicações militares, por volta do século V a.C. (FIARRESGA, 2010). Em Roma, durante o grande império romano, entre os anos 60 a 44 antes de Cristo, o imperador Júlio César usou códigos que ficaram conhecidos como a Cifra de César, a fim de mandar e receber mensagens dentro do exército romano (FUSCO; COELHO, 2014).

Porém, o termo "CRIPTOGRAFIA"como conhecemos hoje, só foi usado pela primeira vez no século XIX, na obra O Escaravelho de Ouro, de Edgar Allan Poe (POE, 2011).

Em 1918, Arthur Scherbius desenvolveu a Enigma, uma máquina que codificava mensagens e foi usada pela marinha alemã em 1926 durante a Segunda Guerra Mundial (FUSCO; COELHO, 2014). Alan Turing um matemático e criptógrafo, junto com uma equipe de também matemáticos e criptógrafos, criaram uma outra máquina que conseguia decodificar a Enigma. Esse foi um passo definitivo para a Teoria da Informação e a criação dos computadores (KRISCHER, 2013).

Uma das mais importantes criações na Criptografia foi apresentada por Diffie e Hellman em 1976, chamada de Criptografia simétrica, que permite a codificação com duas chaves: uma pública e outra privada (SHOKRANIAN, 2005).

A pública é usada para criptografar a mensagem e pode ser compartilhada livremente; a privada, por sua vez, é mantida em segredo e serve para descriptografar a mensagem - sobre o tópico, discorreremos no capítulo 3.

2 Justificativa

Observando os conteúdos de aritmética encontrados em nossos livros didáticos, podemos perceber que, ao longo das últimas décadas, o estudo da aritmética vem se resumindo em regras e algoritmos que são entregues ao estudante de forma pronta. Sendo assim, não é dada a oportunidade para que possam pensar e encontrar o porquê de tais regras e como surgem os chamados algoritmos. Além disto, na maior parte das atividades realizadas por eles, não se vê estímulos para que cheguem de forma racional a uma determinada resposta, mas sim, essa resposta é encontrada de forma mecânica, utilizando ferramentas, muitas vezes sem reflexão. Tudo isso faz com que a Matemática da sala de aula se distancie da Matemática aplicada no mundo tecnológico e o estudante não é contemplado com uma aprendizagem significativa.

Segundo a BNCC (BRASIL, 2018), a aprendizagem significativa acontece quando o estudante consegue relacionar conhecimentos prévios em uma determinada atividade proposta pelo professor. De uma forma geral, os estudantes devem encontrar sentido e significados a respeito de suas aprendizagens.

Para mais, o Documento Curricular para Goiás - DCGO determina:

> "O professor, ao trabalhar o conteúdo de forma significativa, proporciona ao estudante sentir o que é importante saber, qual a importância do que está sendo ensinado para a tomada de decisão na vida em sociedade, ou para entender melhor o mundo em que vive, valorizando a experiência acumulada dentro e fora da instituição escolar"(GOIÁS, 2018).

A aprendizagem significativa é a interação entre conhecimentos prévios e conhecimentos novos (MASINI; MOREIRA, 2017). Nesse processo, os novos conhecimentos adquirem significado para o estudante, e os conhecimentos prévios adquirem novos significados ou maior estabilidade cognitiva.

Já David Ausubel (AUSUBEL, 1982) chamava de subsunçor, ou ideia-âncora, o conhecimento específico existente na estrutura de conhecimentos do indivíduo, que permite dar significado a um novo conhecimento que lhe é apresentado ou por ele descoberto. Contudo, o novo conhecimento se modifica, adquirindo novos significados.

No entanto, o uso da aritmética, segundo Abramo (HEFEZ, 2013), até o século passado, era considerado uma das áreas mais abstratas da Matemática e, com o desenvolvimento da Teoria da Informação, esse conceito tem mudado completamente, possibilitando um sentido acerca do que será estudado.

Diante deste cenário, serão propostos desafios que mostram como a aritmética modular pode ser útil nesse mundo das tecnologias a fim de manter a privacidade dos usuários em redes sociais, transações bancárias e em vários outros aplicativos, inclusive no sistema eleitoral brasileiro.

Ao usar a aritmética modular para codificar e decodificar mensagens, damos a ela uma aplicação prática e atual, podendo despertar em nossos estudantes uma aprendizagem significativa.

3 Hipótese

Como a Criptografia na sala de aula pode contribuir para incentivar a curiosidade dos estudantes a compreender a Matemática como ferramenta indispensável à evolução de outras ciências?

4 Objetivos

O objetivo geral desse trabalho é mostrar aos estudantes e professores de Matemática a utilização prática da Aritmética Modular no contexto atual em que vivemos.

Integram, ainda, os objetivos específicos da presente dissertação:

- Aplicar as operações modulares na codificação e decodificação de mensagens criptografadas;
- Operar na decodificação de uma mensagem com o uso de chaves simples, chaves vetores e chaves matrizes;
- Criar mensagens criptografadas com um certo nível de dificuldade;

- Relacionar o uso da Criptografia com os sistemas de segurança com chaves públicas, como por exemplo o RSA que, é um sistemas de Criptografia de chave pública, usado para transmissão segura de dados.

5 Estrutura do Trabalho

No capítulo 1, falaremos sobre Divisões Euclidianas e Máximo Divisor Comum, conteúdos que, apesar de serem muito usados pelos estudantes, sempre aparecem dúvidas e aqui propomos estudar de uma forma mais racional e menos automática.

A definição de números inteiros primos entre si é bastante trabalhada nas turmas do Ensino Fundamental, assim como a Divisão Euclidiana. Os múltiplos e divisores de um número são facilmente encontrados nos livros didáticos do ensino básico e, neste capítulo, exploraremos seus conceitos e proposições. Definições de números inteiros primos e compostos também são bastante exploradas durante a formação dos estudantes e serão contempladas neste capítulo.

No capítulo 2, vamos estudar a aritmética modular com uma linguagem acessível tanto para os professores quanto para os estudantes do Ensino Médio. Estudaremos os critérios de divisibilidade, que na grande maioria das vezes são decorados pelos estudantes com o incentivo dos professores, mas que dificilmente são construídos utilizando conceitos da aritmética.

Sendo assim, este capítulo usará congruência para entender as regras de divisibilidade. Iremos, também, apresentar as Equações Diofantinas, que possibilitarão aos estudantes determinarem valores possíveis para variáveis que se encontram em equações com duas incógnitas.

Após esses estudos preliminares, abordaremos o conceito de congruência modular, ferramenta essencial para a compreensão de diversos tópicos da Teoria dos Números. Em seguida, exploraremos o Teorema Chinês do Resto, utilizando exemplos curiosos e instigantes com o objetivo de despertar o interesse dos estudantes. Por fim, estudaremos operações no conjunto dos inteiros módulo m, sendo m pertencente aos números inteiros, sempre destacando como esses conhecimentos são fundamentais para aplicações práticas, especialmente na área da Criptografia.

No capítulo 3, vamos abordar o conteúdo de Criptografia, de forma a desenvolver uma apresentação sobre as hipóteses de uso da Criptografia; mostraremos, pois, aos professores e estudantes diferentes formas de codificar uma mensagem e de como conseguimos decodificá-las.

Para isso, usaremos a Cifra de César, além de chaves vetores e chaves matrizes. Esse processo envolverá algumas estratégias matemáticas como, por exemplo, resolução de sistemas e multiplicações de matrizes.

Posto isso, traremos uma breve informação sobre codificação com chave pública usando o sistema RSA (Rivest-Shamir-Adleman), que foi o primeiro sistema criptográfico com uso desse tipo de chave.

Com efeito, o capítulo 4 será reservado para o relato de experiência referente às aplicações das atividades contidas na sequência didática apresentada. Essas atividades foram realizadas com estudantes do Ensino Médio da segunda série de um colégio estadual do estado de Goiás onde lecionei a disciplina Estudo Orientado em Matemática. Teremos, também, o relato da minha participação no vigésimo primeiro

Congresso de Pesquisa, Ensino e Extensão - CONPEEX, realizado pela Universidade Federal de Goiás.

No capítulo 5, serão apresentadas as considerações finais deste trabalho, com uma breve análise do percurso desenvolvido ao longo da pesquisa, destacando os principais resultados obtidos e as contribuições alcançadas.

Por outro lado, o Apêndice A apresenta o desenvolvimento de uma sequência didática composta por treze atividades aplicadas a estudantes da segunda série do Ensino Médio, com o objetivo de aprofundar e consolidar os conteúdos abordados ao longo do trabalho.

No Apêndice B temos, por fim, os materiais apresentados no CONPEEX.

Capítulo 1

Fundamentação Teórica

1.1 Divisões Euclidianas

A fim de desenvolver habilidades importantes, é interessante que o estudante consiga entender o processo de divisibilidade de uma forma mais geral, para que depois possa usar de maneira específica. Também é importante que ele entenda o raciocínio envolvido nas divisões para, somente depois disso, utilizar-se de algoritmos; afinal, eles podem facilitar muito os cálculos de divisões com números maiores.

Segundo o Documento Curricular para Goiás, etapa Ensino Médio (DC-GOEM), temos como objetivo de aprendizagem:

> "(GO-EMMAT405A):Compreender a ideia básica de algoritmos como sequência finita de passos (instruções), registrando representações matemáticas (algébrica, geométrica, estatística, computacional, entre outras) referentes a situações cotidianas (rotineiras ou não) para organizar o processo e utilizar conceitos iniciais de linguagem de programação na implementação de algoritmos escritos em linguagem corrente e/ou matemática."(GOIÁS, 2018)

De acordo com esse pensamento, é importante o esclarecimento aos estudantes dos processos mentais envolvidos na construção de um algoritmo e de sua utilização prática.

Sendo assim, quando queremos falar sobre divisões de números inteiros não exatas, buscamos na Teoria dos Números o que chamamos de algoritmo da divisão. Esse algoritmo é fundamental para a representação de divisões que deixam restos diferentes de zero, tornando fácil a compreensão do algoritmo de Euclides, muito utilizado no Ensino Fundamental para cálculo do Máximo Divisor Comum entre dois ou mais números inteiros. E sobre ele, encontramos a seguinte proposição:

Proposição 1. *Se a e b são números inteiros, sendo b diferente de zero, então existem dois únicos inteiros q e r tais que: $a = bq + r$, onde $0 \leq r < |b|$.*

Demonstração. Primeiramente vamos considerar $a > 0$ e $b > 0$.

Se consideramos $a < b$, faça $q = 0$ e $r = a$ assim teremos,

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

Consideremos agora $a \geq b$, nesse caso, existe um inteiro $q_1 > 0$ tal que $a \geq q_1 b$. (Por exemplo $q_1 = 1$). Logo:

$$a = q_1.b + r_1.$$

Com isso $r_1 \geq 0$.

Se $r_1 < b$ tome $q = q_1$ e $r = r_1$ assim obtemos o resultado sobre sua existência.

Por outro lado, se $r_1 \geq b$ tome $q_2 > 0$ tal que $r_1 \geq q_2 b$ e escreva:

$$q_2 b + r_2 = r_1.$$

Nota-se que $r_1 > r_2$ e que:

$$\begin{aligned} r_2 &= r_1 - q_2 b, \\ &= (a - q_1 b) - q_2 b, \\ &= a - b(q_1 + q_2). \end{aligned}$$

Logo, teremos:

$$a = b(q_1 + q_2) + r_2.$$

Caso $r_2 < b$, faça $q_1 + q_2 = q$ e $r = r_2$. Fica provado que $a = bq + r$, com $0 \leq r < |b|$.

Mas se $r_2 \geq b$, repetiremos o processo acima obtendo $q_3 > 0$, tal que $r_2 \geq q_3 b$, $r_1 >$r$_2 > r_3$.

$$\begin{aligned} r_3 &= r_2 - q_3 b, \\ &= a - b(q_1 + q_2 + q_3). \end{aligned}$$

Se $r_3 < b$, faça $q_1 + q_2 + q_3 = q$ e $r = r_3$. Fica provado que $a = bq + r$, com $0 \leq r < |b|$.

Caso contrário, repetindo o processo n vezes, obteremos uma sequência de inteiros positivos que satisfaçam a equação:

$$r_n = a - (q_1 + q_2 + q_3 + \ldots + q_n)b,$$

e $r_1 > r_2 > r_3 > \ldots >$ r$_{\text{n}}$, assim podemos escolher n tal que r$_{\text{n}} < b$.

Façamos $q = (q_1 + q_2 + q_3 + \ldots + q_n)$ e $r = r_n$ e teremos:
$a = qb + r$, com $0 \leq r < |b|$.

Devemos, então, demonstrar os outros casos, ou seja:
Caso 2: quando $a < 0$ e $b > 0$;
Caso 3 : quando $a > 0$ e $b < 0$;

Caso 4: quando $a < 0$ e $b < 0$.

1. Se $a < 0$ e $b > 0$ então $-a$ é um inteiro positivo, logo existem q_1 e r_1, tais que,$-a = bq_1 + r_1$, com $0 \leq r_1 < |b|$.

Se $r_1 = 0$,

$$\begin{aligned} -a &= b.q_1, \\ a &= b(-q_1). \end{aligned}$$

Façamos $q = -q_1$ e $r = 0$. Assim $a = bq + r$, com $0 \leq r < |b|$.

Se $r_1 \neq 0$,

$$\begin{aligned} -a &= bq_1 + r_1, \\ a &= -bq_1 - r_1, \\ &= -bq_1 - r_1 - b + b, \\ &= b(-q_1 - 1) + b - r_1. \end{aligned}$$

Fazendo $q = -q_1 - 1$ e $r = b - r_1$.
Nota-se que $0 < r < b$, pois como $r_1 < b$, então $b - r_1 > 0$ e $-r_1 < 0$, logo $b - r_1 < b$.
Temos que $a = bq + r$, com $0 \leq r < |b|$.

2. Se $a > 0$ e $b < 0$, então $-b$ é um inteiro positivo, logo, existem q_1 e r_1, tais que $a = -bq_{\ 1} + r_1$, com $0 \leq r_1 < |b| = -b$. Daí,

$$\begin{aligned} a &= -bq_1 + r_1, \\ a &= b(-q_1) + r_1. \end{aligned}$$

Façamos $q = -q_1$ e $r = r_1$. Então $a = bq + r$, com $0 \leq r < |b|$.

3. Se $a < 0$ e $b < 0$, então $-a$ e $-b$ são inteiros positivos, logo, existem q_1 e r_1, tais que $-a = -bq_1 + r_1$, com $0 \leq r_1 < |b| = -b$.

Se $r_1 = 0$, então $a = bq_1$. Façamos $q = q_1$ e $r = 0$.

Se $r_1 \neq 0$,

$$\begin{aligned} a &= bq_1 - r_1, \\ &= bq_1 - r_1 - b + b, \\ &= b(q_1 + 1) - b - r_1, \\ &= b(q_1 + 1) + (-b - r_1). \end{aligned}$$

Façamos $q = q_1 + 1$ e $r = -b - r_1$.

Nota-se que $0 < r < -b$, pois $r_1 < -b$, então $-b - r_1 > 0$ e $-r_1 < 0$, logo $-b - r_1 < -b$.

Então $a = bq + r$, com $0 \leq r < |b| = -b$.

Agora, provaremos a unicidade desses números. Para isso, suponhamos existir inteiros q' e r' que também satisfaçam esse algoritmo.

$$a = qb + r = q'b + r',$$

com

$$0 \leq r <\mid b \mid \text{ e } 0 \leq r' <\mid b \mid .$$

Então:

$$qb - q'b = r' - r,$$

$$b(q - q') = r' - r.$$

Sendo assim $r' - r$ é múltiplo de b.

Como

$$0 \leq r <\mid b \mid \text{ e } 0 \leq r' <\mid b \mid,$$

temos

$$-b < r' - r < b.$$

Então,

$$r' - r = 0, \text{ ou seja, } r' = r.$$

Com isso,

$$b(q - q') = 0.$$

Como $b \neq 0$, temos:

$$q - q' = 0, \text{ e daí } q = q'.$$

Provando assim a unicidade de q e r para essa proposição.

□

Esse algoritmo é muito utilizado no ensino da matemática básica mas, na maioria das vezes, não é explorado de forma clara e consciente. Isto reflete na forma dos estudantes lidarem com as atividades apresentadas, que acaba sendo uma forma mecânica e sem consciência do raciocínio matemático que acompanha todo o processo.

Exemplo 1: Tomando $a = 90$ e $b = 12$, existem dois inteiros tais que $a = bq + r$, onde $0 \leq r < |b|$.

Vejamos:

$$\begin{aligned} 90 &= 12.q + r, \\ 90 &= 12.2 + 66, \\ 66 &= 12.6 + 18, \\ 18 &= 12.1 + 6. \end{aligned}$$

Nota-se que: $90 = 12.(2 + 6 + 1) + 6$.

$$90 = 12.(9) + 6.$$

Obs. 1. *Podemos escolher aleatoriamente o quociente q, desde que ele seja um inteiro que, ao ser multiplicado pelo divisor, não resulte em um número maior do que o dividendo. E assim, realizar sucessivas divisões até o resto ser menor do que o divisor. Porém, se escolhermos um quociente de forma a ser o maior possível, conseguiremos chegar ao menor resto possível com apenas uma etapa; isso tornará o processo mais prático e rápido.*

Exemplo 2: Sendo $a = 51$ e $b = 8$, encontremos q e r na divisão de a por b usando o algoritmo da divisão.

Solução:

$51 = 8q + r$ então $51 = 8.6 + 3$.

Podemos observar que $q = 6$ e $r = 3$.

Exemplo 3: Sendo $a = 51$ e $b = -8$, encontremos q e r na divisão de a por b usando o algoritmo da divisão.

Solução:

$$51 = -8q + r.$$

Então,

$$51 = -8.(-6) + 3.$$

Podemos observar que $q = -6$ e $r = 3$.

Exemplo 4: Sendo $a = -51$ e $b = 8$, encontremos q e r na divisão de a por b usando o algoritmo da divisão.

Solução:

$$-51 = 8q + r, \text{ então } -51 = 8(-7) + 5.$$

Podemos observar que $q = -7$ e $r = 5$.

Exemplo 5: Sendo $a = -51$ e $b = -8$, encontremos q e r na divisão de a por b usando o algoritmo da divisão.

Solução:

$$-51 = -8q + r, \text{ então } -51 = -8.(7) + 5.$$

Podemos observar que $q = 7$ e $r = 5$.

Definição 1. *Se na Divisão Euclidiana de um número inteiro a por um número inteiro b não nulo o resto for igual a zero, ou seja $a = qb$, diremos que a é múltiplo de b ou que b divisor é de a. Usamos a notação $b \mid a$ (Leia b divide a).*

Exemplo 6: Temos que $5 \mid 10$ pois $10 = 5 \cdot 2$.

Proposição 2. *Sejam a, b, c, x e $y \in \mathbb{Z}$ então:*

1. *$b \mid a$ se, somente se $b \mid |a|$;*
2. *$b \mid a$ se, somente se $-b \mid a$;*
3. *Se $b \mid a$ então $b \mid ax$;*
4. *Se $b \mid a$ e $b \mid c$ então $b \mid (ax + cy)$;*
5. *Se $b \mid a$ e $x \neq 0$, então $bx \mid ax$;*
6. *Se $b \mid a$ e $a \neq 0$, então $|b| \leq |a|$;*
7. *Se $b \mid a$ e $a \mid c$ então $b \mid c$;*
8. *Se $b \mid a$ e $a \mid b$ então $a = b$ ou $a = -b$.*

Demonstração.

1. Se $b \mid a$, então $a = qb$ logo $|a| = |q|.|b|$;
Caso 1: Se $b \geq 0$ temos $|b| = b$, daí $|a| = |q|b$ então $b \mid |a|$;
Caso 2: Se $b < 0$ temos $|b| = -b$, daí $|a| = |q|(-b)$, então $|a| = -|q|.b$ logo $b \mid |a|$.

Vemos que nos dois casos $b \mid |a|$.

Reciprocamente: Se $b \mid |a|$ então $|a| = qb$.
Caso 1: Se $a \geq 0$ temos $|a| = a$, daí $a = qb$ então $b \mid a$;
Caso 2: Se $a < 0$ temos $|a| = -a$, daí $-a = qb$ então $a = -qb$ então $b \mid a$.

Vemos que nos dois casos $b \mid a$.

2. $b \mid a$ se, somente se, $a = qb$, daí $a = (-q)(-b)$, portanto $-b \mid a$.

3. $b \mid a$, então $a = qb$, assim $ax = qxb$, logo $b \mid ax$.

4. Se $b \mid a$ e $b \mid c$, então $a \mid qb$ e $c = q_1 b$, daí $ax = (qx)b$ e $cy = (q_1 y)b$.
Logo, a soma $ax + cy$ resulta: $ax + cy = qxb + q_1 yb = b(qx + q_1 y)$.
Mas se $ax + cy = (qx + q_1 y)b$, então $b \mid ax + cy$.

5. Se $b \mid a$ temos que $a = qb$ logo $ax = q(xb)$ então $bx \mid ax$.

6. Se $b \mid a$, então $a = qb$ logo $|a| = |q||b|$, e como $a \neq 0$ temos $|q| > 0$.
Mas $a.b = a(b-1) + a$ se $a \neq 0$. Logo, $|a| = (|q| - 1)|b| + |b|$.
Temos também que se $a = x + b$ com $x \geq 0$, então $b \leq a$. Fazendo $(|q| - 1)|b| = x$, temos $|a| = x + |b|$, logo $|b| \leq |a|$.

7. Se $b \mid a$ e $a \mid c$, então $a = qb$ e $c = q_1 a$, logo $c = q_1(qb)$, desta forma temos que $b \mid c$.

8. Se $b \mid a$ e $a \mid b$, então $a = qb$ e $b = q_1 a$.
Portanto, $a = q(q_1 a)$, sendo assim, $qq_1 = 1$, então $|q||q_1| = 1$.
Desta forma, teremos que $|q| = |q_1| = 1$, logo $q = 1$ ou $q = -1$, então $a = b$ ou $a = -b$.

□

Obs. 2. *Temos, também, algumas situações que são triviais como:*
$1 \mid a$*, para todo inteiro não nulo;*
$a \mid a$*, já que* $a = a.1$*, sendo a um inteiro não nulo;*
$a \mid 0$ *, já que* $0 = 0.a$*, sendo a um inteiro não nulo.*

1.2 Máximo Divisor Comum (MDC)

No documento da Base Nacional Comum Curricular (BRASIL, 2018), encontramos algumas habilidades que contemplam conteúdos relacionados à aritmética que iremos estudar:

> "(EF06MA06):Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisores. [...] (EF07MA01): Resolver e elaborar problemas com números naturais, envolvendo as noções de divisor e de múltiplo, podendo incluir máximo divisor comum ou mínimo múltiplo comum, por meio de estratégias diversas, sem a aplicação de algoritmos"(BRASIL, 2018, p.303, p.309).

Tradicionalmente, em nossa experiência no exercício do magistério, percebemos que os livros didáticos, ao longo dos últimos anos, colocam uma ênfase muito grande na aplicação do algoritmo, sem se preocupar com o processo existente antes de sua finalização; assim, tornamos o cálculo do MDC e MMC totalmente automáticos, sem muito raciocínio. Porém, a nova proposta da BNCC é fazer com que o próprio estudante construa caminhos para tal algoritmo.

O MDC é conteúdo indispensável para o ensino da Matemática básica, ele abre muitas possibilidades de atividades criativas e, quando bem explorado, serve como pilar para o avanço no campo da aritmética durante o Ensino Fundamental e Médio.

Exemplo 7: Considerando os números 30 e 50, de forma intuitiva vamos verificar quais são os divisores positivos desses números:

O conjunto dos divisores positivos de 30 é $\{1, 2, 3, 5, 6, 10, 15, 30\}$.

O conjunto dos divisores positivos de 50 é $\{1, 2, 5, 10, 25, 50\}$.

Os divisores positivos comuns entre esses dois números são: $\{1, 2, 5, 10\}$.

Definição 2. *Sejam a e b dois inteiros, não ambos nulos. O Máximo Divisor Comum entre a e b é o inteiro positivo d que satisfaz as seguintes condições:*

- $d \mid a$ *e* $d \mid b$*;*
- *Se existe* $c \in \mathbb{Z}$ *tal que* $c \mid a$ *e* $c \mid b$*, então* $c \leq d$*.*

Usaremos a notação $MDC(a, b) = d$ para indicar o Máximo Divisor Comum entre a e b.

Exemplo 8: $MDC(a, 0) = |a|$, pois $a \mid a$, $a \mid 0$, $-a \mid a$ e $-a \mid 0$.

Sabemos que o MDC sempre existe, já que $1 \mid a$, para todo inteiro não nulo, então o inteiro 1 será divisor de todos os demais inteiros, além disto, o conjunto dos divisores de um número é limitado superiormente por $|a|$. Para calcular o MDC de números maiores, podemos usar o algoritmo de Euclides com divisões sucessivas, a fim de facilitar os cálculos.

Obs. 3. *Observando o conjunto dos divisores de um número, podemos verificar que o maior deles é o seu valor absoluto, sendo assim, esse conjunto é finito. Logo, os divisores comuns entre dois ou mais números sempre serão conjuntos finitos, ou seja, terão um valor máximo, que é o maior divisor comum entre eles.*

Proposição 3. *Se* $MDC(a, b) = d$*, então* $MDC(\frac{a}{d}, \frac{b}{d}) = 1$.

Demonstração. Se $MDC(a, b) = d$, isso significa que $a = d \cdot a_1$ e $b = d \cdot b_1$, onde a_1 e b_1 são inteiros e $MDC(a_1, b_1) = 1$.

Observe que,

$$MDC(\frac{a}{d}, \frac{b}{d}) = MDC(a_1, b_1) = 1.$$

□

Exemplo 9: $MDC(15, 25) = 5$, então $MDC(\frac{15}{5}, \frac{25}{5}) = MDC(3, 5) = 1$.

Proposição 4. *Sejam a e b números inteiros, e r o resto da Divisão Euclidiana de a por b então:* $MDC(a, b) = MDC(b, r)$**.**

Demonstração. Se $MDC(a, b) = d$ e $a = qb + r$. Verificaremos que $d = MDC(b, r)$, ou seja:

- $d \mid b$ e $d \mid r$;
- Se $c \mid b$ e $c \mid r$, então $c \leq d$.

Usando a proposição 2.4, teremos: $d \mid a$ e $d \mid b$ então $d \mid (ax+by)$, para todo $x, y \in \mathbb{Z}$. Portanto:

$$d \mid (a.1 + q(-b)),$$
$$d \mid (a - qb).$$

Nota-se que,

$$r = a - qb, \text{ daí } d \mid r.$$

Por outro lado, se $c \mid b$ e $c \mid r$ então $c \mid (qb+r)$ ou seja $c \mid a$, pois $a = qb+r$.
Mas se $c \mid b$ e $c \mid a$, então $c \leq d$, pois $MDC(a, b) = d$.
Desta forma, concluímos que: $MDC(b, r) = d$. Logo $MDC(a, b) = MDC(b, r)$.
Reciprocamente: se $MDC(b, r) = d_1$ e $a = qb + r$. Verificaremos que $d_1 = MDC(a, b)$, ou seja:

- $d_1 \mid a$ e $d_1 \mid b$;
- Se $c \mid a$ e $c \mid b$, então $c \leq d_1$.

$d_1 \mid b$ e $d_1 \mid r$ então $d_1 \mid (bx + ry)$, para todo $x, y \in \mathbb{Z}$.

$$d_1 \mid (b.q + r.1),$$
$$d_1 \mid (qb + r), \text{ daí } d_1 \mid a.$$

Por outro lado, se $c \mid a$ e $c \mid b$, então $c \mid (a.1 - bq)$ ou seja $c \mid r$, pois $r = a - qb$.
Mas se $c \mid b$ e $c \mid r$, então $c \leq d_1$, pois $MDC(b, r) = d_1$. Desta forma, concluímos que $MDC(a, b) = d_1$.
Logo, $MDC(b, r) = MDC(a, b)$.

□

Esse tipo de comparação entre MDCs costuma ser feita de forma intuitiva pelos estudantes e até mesmo por professores, sem que se analise o processo de Divisões Euclidianas usadas sucessivamente.

Exemplo 10: Encontrando o MDC entre 1340 e 395.

Usando o algoritmo da divisão, sucessivamente teremos:

$$\begin{aligned} 1340 &= 395.3 + 155, \\ 395 &= 155.2 + 85, \\ 155 &= 85.1 + 70, \\ 85 &= 70.1 + 15, \\ 70 &= 15.4 + 10, \\ 15 &= 10.1 + 5, \\ 10 &= 5.2 + 0. \end{aligned}$$

Desta forma, fica fácil visualizar a proposição 3:

$$MDC(1340, 395) = MDC(395, 155) = MDC(155, 85) = MDC(85, 70) = MDC(70, 15) = MDC(15, 10) = MDC(10, 5) = MDC(5, 0) = 5.$$

Podemos, agora, usar uma tabela prática para encontrarmos o MDC:

Quociente:	-	3	2	1	1	4	1	2
Dividendo:	1340	395	155	85	70	15	10	5
Resto:	155	85	70	15	10	5	0	

A seguir veremos algumas propriedades em forma de proposição:

Proposição 5. *Se a, b e k são números inteiros, diferentes de zero, então:*

1. *O $MDC(a, b) = MDC(|a|, |b|)$.*

2. *O $MDC(ka, kb) = |k|MDC(a, b)$.*

Demonstração.

1. Se $MDC(a, b) = d$ então $d \mid a$ e $d \mid b$, é imediato verificar que $d \mid |a|$ e $d \mid |b|$, além disto, se $c \mid |a|$ e $c \mid |b|$, então $c \mid a$ e $c \mid b$, daí $c \leq d$.

Desta forma, $MDC(|a|, |b|) = d$. Logo $MDC(a, b) = MDC(|a|, |b|)$.

2. De acordo com o algoritmo euclidiano:

$$\begin{aligned} a &= q_1 b + r_1, 0 \leq r_1 < |b|, \\ b &= q_2 r_1 + r_2, 0 \leq r_2 < r_1, \\ r_1 &= q_3 r_2 + r_3, 0 \leq r_3 < r_2 < r_1, \\ &\vdots \end{aligned}$$

Logo, existe n tal que, $r_{n+1} = 0$, $r_n \neq 0$ e $0 = r_{n+1} \leq r_n \ldots < r_2 < r_1$ então:

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

$$MDC(a, b) = MDC(r_n, 0).$$

Considerando $k > 0$ e multiplicando k a cada linha temos:

$$\begin{aligned} ka &= kq_1 b + kr_1, \\ kb &= kq_2 r_1 + kr_2, \\ kr_1 &= kq_3 r_2 + kr_3, \\ &\vdots \\ kr_{n-1} &= kq_{n-1} . r_n + 0. \end{aligned}$$

Então:

$$MDC(ka, kb) = kr_n = k.MDC(a, b) = |k|MDC(a, b).$$

Logo:

$$MDC(ka, kb) = |k|MDC(a, b).$$

Por outro lado se $k < 0$, então $|k| > 0$ e temos pelo item 1.

$$\begin{aligned} MDC(ka, kb) &= MDC(|ka|, |kb|) \\ &= MDC(|k||a|, |k||b|) \\ &= |k|MDC(|a|, |b|) \\ &= |k|MDC(a, b). \end{aligned}$$

□

Exemplo 11 $MDC(-50, 22) = MDC(|-50|, |22|) = MDC(50, 22) = 2.$

Quociente:	-	2	3	1	2
Dividendo:	50	22	6	4	2
Resto:	6	4	2	0	

Exemplo 12: $MDC(42, 18) = MDC(6.7, 6.3) = |6|MDC(7, 3) = |6|.1 = 6.$

Quociente:	-	2	3
Dividendo:	42	18	6
Resto:	6	0	

Quociente:	-	2	3
Dividendo:	7	3	1
Resto:	1	0	

Teorema 1. *(Teorema de Bézout) : Sejam a e b inteiros, ambos não nulos. Se $d = MDC(a, b)$, então existem inteiros x e y tais que $d = ax + by$.*

Demonstração. Defina o conjunto : $S = \{ax + by \mid x, y \in \mathbb{Z}\}$.

Como $|a| = Ka + b.0 \in S$ em que $K = 1$ ou $K = -1$, dependendo do sinal de a, temos que $S \cap \mathbf{Z}^+ \neq \varnothing$, logo S possui um menor elemento positivo que chamamos de d.

Afinal, pelo Princípio da Boa Ordem (PBO): Todo conjunto não vazio de inteiros positivos contém um elemento mínimo (SANTOS, 1998).

Mostraremos agora que $d = MDC(a, b)$. Como $d \in S$, suponhamos $d = ax_0 + by_0$; sendo x_0 e y_0 inteiros. Seja r o resto na divisão de a por d, pelo algoritmo da divisão podemos escrever: $a = q.d + r$, com $0 \leq r < d$, e daí:

$$\begin{aligned} r &= a - qd, \\ &= a - q(ax_0 + by_0), \\ &= a(1 - qx_0) + b(-qy_0). \end{aligned}$$

Portanto, $r \in S$, se $r \neq 0$ teríamos $r < d = min(S)$, o que é um absurdo. Então, o único caso é $r = 0$, desta forma $a = qd$. Logo, $d \mid a$ e analogamente $d \mid b$. Suponhamos, então, que $c > 0$ é um outro divisor comum de a e b, assim temos $c \mid ax_0 + by_0 = d$, o que implica $c \leq d$ e, portanto, d é, por definição, o maior divisor comum entre a e b.

□

Exemplo 13: No exemplo 9, temos que $MDC(50, 22) = 2$. Então, existem x e $Y \in \mathbb{Z}$ tais que $50x+22y = 2$ (esse tipo de equação, chamamos de Equação Diofantina).

Nem sempre é fácil determinar x e y por tentativa e erro neste tipo de equação. Então, apresentaremos no capítulo 2 um método para tal resolução.

Definição 3. *Se a e b são números inteiros tais que $MDC(a, b) = 1$ diremos a e b são primos entre si.*

Proposição 6. *Sejam a, b e c números inteiros tais que $MDC(a, b) = 1$.*
1- Se $a \mid c$ e $b \mid c$, então $ab \mid c$.
2- Se $a \mid bc$, então $a \mid c$.

Demonstração.

1. De acordo com o teorema 1, se $MDC(a, b) = 1$ então existem $x, y \in \mathbb{Z}$ tais que, $ax + by = 1$, logo $cax + cby = c$.

Se $a \mid c$ e $b \mid c$, então $ab \mid bc$ e $ab \mid ac$. Daí, $ab \mid (acx + bcy)$ ou $ab \mid c$.

2. Se $a \mid bc$, então $a \mid (acx + bcy)$, mas $acx + cby = c$, logo $a \mid c$.

□

Proposição 7. *Sejam a e b números inteiros não nulos, e d um número inteiro positivo. Logo, $d = MDC(a, b)$ se, somente se,*

- *$d \mid a$ e $d \mid b$;*
- *Se $c \in \mathbb{Z}$ tal que $c \mid a$ e $c \mid b$, então $c \mid d$.*

Demonstração. Seja $MDC(a, b) = d$, então $d = ax + by$, para $x, y, \in \mathbb{Z}$.

Se $c \mid a$ e $c \mid b$ temos que $c \mid (ax + by)$, então $c \mid d$.

Reciprocamente, se d satisfaz,

- $d \mid a$ e $d \mid b$;
- Se $c \in \mathbb{Z}$ tal que $c \mid a$ e $c \mid b$, então $c \mid d$.

Basta provar que se $c \mid a$ e $c \mid b$, então $c \leq d$. Mas pelo segundo item $c \mid d$, logo $\mid c \mid \leq \mid d \mid$.

Como $d > 0$, $\mid d \mid = d$, sendo assim, $c \leq \mid c \mid \leq d$.

□

Diante das definições e propriedades fundamentais da Divisão Euclidiana e do Máximo Divisor Comum, evidenciou-se o potencial formativo desses conteúdos quando abordados de forma racional, além de seu papel estruturante na teoria dos números. Aprofundar essa base é essencial para a compreensão do próximo capítulo, em que exploraremos a aritmética modular e os conceitos de congruência. Tais ferramentas serão fundamentais para a construção de códigos criptográficos e, mais adiante, para formulação de propostas pedagógicas aplicáveis ao Ensino Médio.

Capítulo 2

Congruência

2.1 A aritmética dos restos

Para analisar a aplicação da aritmética modular, também conhecida como a aritmética dos restos, faz-se necessária a compreensão dos fenômenos cíclicos na Matemática. Nesse sentido, Jhone Caldeira Silva e Olimpio Ribeiro Gomes dissertam:

> "Existem na natureza e no cotidiano diversas situações envolvendo contagem que são cíclicas. Por exemplo, as horas do dia são as mesmas a cada 24 horas, os dias da semana são os mesmos a cada 7 dias, o cometa Halley passa por seu periélio (ponto da sua órbita mais próximo do Sol) a cada 76 anos. Consideremos, por exemplo, o problema de saber que horas do dia serão daqui a 134 horas, ou que dia da semana será daqui a 73 dias, ou, ainda, sabendo que o cometa Halley passou por aqui em 1986, qual será a sua primeira aparição depois do ano 2481? É em situações cíclicas como essas que surge a chamada aritmética modular, a aritmética dos fenômenos cíclicos"(SILVA; GOMES, 2020)

A noção de congruência linear módulo m, sendo m um número inteiro, foi criada por Gauss e, na sala de aula, podemos usá-la para desenvolver importantes habilidades em nossos estudantes.

De acordo com a BNCC (BRASIL, 2018), entre as competências específicas de Matemática e as habilidades a serem desenvolvidas, encontramos:

> "Competência 2: Desenvolver o raciocínio lógico, o espírito de investigação e a capacidade de produzir argumentos convincentes, recorrendo aos conhecimentos matemáticos para compreender e atuar no mundo"(BRASIL, 2018, p.269).

> "(EM13MAT306): Resolver e elaborar problemas em contextos que envolvem fenômenos periódicos reais (ondas sonoras, fases da lua, movimentos cíclicos, entre outros) e comparar suas representações com as funções seno e cosseno, no plano cartesiano, com ou sem apoio de aplicativos de álgebra e geometria"(BRASIL, 2018, p.546).

Sendo assim, torna-se bastante relevante o uso de congruências lineares para desenvolver, nos estudantes, tais habilidades e competências.

Definição 4. *Sejam a, b e m inteiros tais que $a - b$ é divisível por m, dizemos que a e b são congruentes módulo m. E para tal definição, usaremos a notação $a \equiv b(mod\ m)$. (Leia a é congruente a b módulo m).*

Exemplo 14: $20 \equiv 2(mod\ 6)$, pois $20 - 2 = 6 \cdot 3$,
$20 \equiv -4(mod\ 6)$, pois $20 + 4 = 6 \cdot 4$,
$20 \equiv 80(mod\ 6)$, pois $20 - 80 = 6 \cdot (-10)$,
$24 \equiv 0(mod\ 6)$, pois $24 - 0 = 6 \cdot 4$.

Proposição 8. *Seja m um número inteiro maior do que 1 então a é congruente a b módulo m se, somente se a e b deixam restos iguais quando divididos por m.*

Demonstração. Se $a \equiv b(mod\ m)$, então $a - b = qm$.

Sejam r_1 e r_2 restos das divisões de a e b por m, então $a = q_1m + r_1$, com $0 \leq r_1 < m$ e $b = q_2m + r_2$, com $0 \leq r_2 < m$.

Então:

$$q_1m + r_1 - q_2m - r_2 = qm;$$
$$q_1m - q_2m - qm = r_2 - r_1;$$
$$m(q_1 - q_2 - q) = r_2 - r_1.$$

Logo:

$$m \mid r_2 - r_1.$$

Nota-se que $-m < r_2 - r_1 < m$, então $r_1 = r_2$.

Assim, conseguimos mostrar que a e b quando divididos por m deixam restos iguais.

Agora, demonstraremos a recíproca:
Se $r_1 = r_2$, podemos escrever, $a = q_1m + r_1$ e $b = q_2m + r_1$.
Então, $a - b = q_1m + r_1 - q_2m - r_1 = m(q_1 - q_2)$.
Fazendo $q_1 - q_2 = q$, temos $a - b = qm$, ou seja, $a \equiv b(mod\ m)$.

□

Exemplo 15: $151 \equiv 26(mod\ 5)$, pois $26 = 5 \cdot 5 + 1$ e $151 = 30 \cdot 5 + 1$.

Proposição 9. *Sejam m um inteiro positivo, para todo $a, b, c \in \mathbb{Z}$ tem-se que:*

1. $a \equiv a(mod\ m)$; (propriedade reflexiva).
2. $a \equiv b(mod\ m)$ se, e somente se, $b \equiv a(mod\ m)$; (propriedade simétrica).
3. Se $a \equiv b(mod\ m)$ e $b \equiv c(mod\ m)$, então $a \equiv c(mod\ m)$; (propriedade transitiva).
4. $a \equiv b(mod\ m)$ se, e somente se, $a \equiv b(mod\ (-m))$.

Demonstração.

1 e 2. São triviais e seguem da definição.

3. Se $a \equiv b(mod\ m)$, temos:

$$a - b = q_1 m,$$
$$a = q_1 m + b.$$

Se $b \equiv c(mod\ m)$, temos:

$$b - c = q_2 m,$$
$$-c = q_2 m - b,$$
$$c = -q_2 m + b.$$

Calculando $a - c$ temos:

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

$$\text{Fazendo } q_1 + q_2 = q,$$
$$a - c = mq,$$
$$a \equiv c(mod\ m).$$

4. Como $a \equiv b(mod\ m)$, então $a - b = q.m$, logo $a - b = -q(-m)$, assim:

$$a \equiv b(mod\ (-m)).$$

Por outro lado, se $a \equiv b(mod\ (-m))$, então $a - b = q(-m)$, que é igual a $a - b = -q(m)$, logo:

$$a \equiv b(mod\ m).$$

□

Uma conclusão muito importante que ajudará a resolver vários problemas envolvendo restos de divisões é:

Sendo r o resto da divisão de a por m, temos que $a \equiv r(mod\ m)$, e como $0 \leq r < m$, o resto r poderá ser qualquer número inteiro entre 0 e $m - 1$, ou seja, $r \in \{0, 1, 2, 3, \ldots, m - 1\}$ e esse conjunto chamamos de um sistema completo de restos.

Exemplo 16: Um número qualquer quando dividido por 3 poderá ter resto igual a $0, 1$ ou 2.

Um número divisível por 3 pode ser escrito da forma $3k$. Logo, um número não divisível por 3 pode ser escrito da forma $3k + 1$ ou $3k + 2$.

Exemplo 17: Um número qualquer, quando dividido por 7 poderá ter resto igual a $0, 1, 2, 3, 4, 5$ ou 6.

Um número divisível por 7 pode ser escrito da forma $7k$. Logo, um número não divisível por 7 pode ser escrito da forma $7k + 1, 7k + 2, 7k + 3, 7k + 4, 7k + 5$ ou $7k + 6$.

Exemplo 18:

- Se $a \equiv 12(mod\ 3)$, então $a \equiv 0(mod\ 3)$.
- Se $a \equiv 13(mod\ 3)$,então $a \equiv 1(mod\ 3)$.
- Se $a \equiv 14(mod\ 3)$, então $a \equiv 2(mod\ 3)$.
- Se $a \equiv 15(mod\ 3)$, então $a \equiv 0(mod\ 3)$.

Observamos que os restos encontrados na divisão de a por 3 são iguais a $0, 1$ ou 2.

Obs. 4. *A congruência é uma relação de equivalência, assim como a igualdade. Desta forma, existem compatibilidades entre ela e algumas operações elementares, como por exemplo a multiplicação e a adição. Que serão apresentadas na proposição a seguir.*

Proposição 10. *Sejam a, b, c, d e m números inteiros, então:*

1. *Se $a \equiv b(mod\ m)$, então $a + c \equiv b + c(mod\ m)$.*
2. *Se $a \equiv b(mod\ m)$, então $ac \equiv bc(mod\ m)$.*
3. *Se $a \equiv b(mod\ m)$ e $c \equiv d(mod\ m)$, então $a + c \equiv b + d(mod\ m)$.*
4. *Se $a \equiv b(mod\ m)$ e $c \equiv d(mod\ m)$, então $ac \equiv bd(mod\ m)$.*
5. *Se $a \equiv b(mod\ m)$, então $a^k \equiv b^k(mod\ m)$, sendo k um inteiro maior do que zero.*

Demonstração.

1. Se $a \equiv b(mod\ m)$, então $a - b = qm$, logo $a - b + c - c = qm$.
Mas se $a + c - (b + c) = qm$, então $a + c \equiv b + c(mod\ m)$.

2. Se $a \equiv b(mod\ m)$, então $a - b = qm$, logo $(a - b)c = qmc$, sendo assim $ac - bc = (qc)m$ e $ac \equiv bc(mod\ m)$.

3. Se $a \equiv b(mod\ m)$, então $a - b = q_1m$, logo $a = q_1m + b$.
Por outro lado, se $c \equiv d(mod\ m)$, então $c - d = q_2m$, logo $c = q_2m + d$.
Agora, calculando $a + c$ temos:
$a + c = q_1m + b + q_2m + d$;
$a + c = m(q_1+q_2) + b + d$;
$a + c - (b + d) = m(q_1+q_2)$, fazendo $q_1 + q_2 = q$;
$a + c - (b + d) = mq$, então $a + c \equiv b + d(mod\ m)$.

4. Se $a \equiv b(mod\ m)$, então $a - b = q_1m$, logo $a = q_1m + b$.
Por outro lado, se $c \equiv d(mod\ m)$, então $c - d = q_2m$, logo $c = q_2m + d$.
Agora, calculando ac temos:
$ac = (q_1m + b).(q_2m + d)$;
$ac = q_1q_2m^2; + q_1dm + q_2bm + bd$;

$ac = m(q_1q_2mq_1d + q_2b) + bd$.
Fazendo $q_1q_2m + q_1d + q_2b = q$ $ac = mq + bd$;
então $ac - bd = qm$, logo $ac \equiv bd(mod\ m)$.

5. Basta aplicarmos repetidas vezes o item 4 já provado.
Se $a \equiv b(mod\ m)$, tome $c = a$ e $d = b$, então $aa \equiv bb(mod\ m)$.
Logo, $a^k \equiv b^k\ (mod\ m)$.

□

Toda essa construção aritmética modular nos ajuda a encontrar restos de divisões que seriam extremamente desgastantes e inviáveis por métodos tradicionais encontrados nos nossos livros de Matemática básica.

Exemplo 19: Encontremos o resto da divisão de 2^{54} por 7.
Sabemos que $2^3 \equiv 1(mod\ 7)$, pois $8 - 1 = 7$.
Logo:

$$\begin{aligned} (2^3)^{18} &\equiv 1^{18}(mod\ 7); \\ 2^{54} &\equiv 1(mod\ 7); \end{aligned}$$

Assim, o resto da divisão de 2^{54} por 7 é igual a 1.

Exemplo 20: Encontremos o resto da divisão de 2^{56} por 7.
Sabemos que $2^3 \equiv 1(mod\ 7)$, pois $8 - 1 = 7$.
Logo:

$$\begin{aligned} (2^3)^{18} &\equiv 1^{18}(mod\ 7); \\ 2^{54} &\equiv 1(mod\ 7); \\ (2^{54}) \cdot 2^2 &\equiv 1 \cdot 2^2(mod\ 7); \\ 2^{56} &\equiv 4(mod\ 7). \end{aligned}$$

Assim, o resto da divisão de 2^{56} por 7 é igual a 4.

Exemplo 21: Encontremos o resto da divisão de 5^{1381} por 14.
Sabemos que $5^3 \equiv -1(mod\ 14)$, pois $125 + 1 = 14 \cdot 9$.
Logo:

$$\begin{aligned} (5^3)^{460} &\equiv (-1)^{460}(mod\ 14); \\ 5^{1380} &\equiv 1(mod\ 14); \\ 5^{1380} \cdot 5 &\equiv 1 \cdot 5(mod\ 14); \\ 5^{1381} &\equiv 5(mod\ 14). \end{aligned}$$

Sendo assim, o resto da divisão de 5^{1381} por 14 é igual a 5.

Proposição 11. *Sejam a, b, c e m números inteiros, sendo $m > 1$ e $c \neq 0$.*

1. *Se $ac \equiv bc(mod\ m)$ e $MDC(c, m) = 1$, então $a \equiv b(mod\ m)$.*

2. Se $ac \equiv bc(mod\ mc)$*, então* $a \equiv b(mod\ m)$*.*

Demonstração.

1. Se $ac \equiv bc(mod\ mc)$, então $m \mid ac - bc$, logo $m \mid c(a-b)$. Como $MDC(c,m) = 1$, pela proposição 5.2, temos que $m \mid a - b$, logo $a \equiv b(mod\ m)$.

2. Se $ac \equiv bc(mod\ mc)$, existe q tal que $ac - bc = qmc$, então $c(a-b) = qmc$, e como $c \neq 0$, temos $a - b = qm$, contudo $a \equiv b(mod\ m)$.

□

2.2 Usando Congruência para entender as Regras de Divisibilidade

No documento da Base Nacional Comum Curricular (BRASIL, 2018), encontramos mais uma habilidade que pode ser contemplada com o estudo da aritmética modular.

> "(EF06MA05): Classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos "é múltiplo de", "é divisor de", "é fator de", e estabelecer, por meio de investigações, critérios de divisibilidade por 2, 3, 4, 5, 6, 8, 9, 10, 100 e 1000"(BRASIL, 2018, p.303).

Para aprofundarmos neste assunto, vamos falar a seguir sobre as regras de divisibilidade que sempre estão presentes nos livros do 6º ano do Ensino Fundamental.

Com efeito, no início dos estudos de aritmética no Ensino Fundamental, nos deparamos com várias regras de divisibilidade que nós, professores, quase sempre induzimos nossos estudantes a decorarem sem que se tenha uma explicação consistente.

Uma das regras básicas de divisibilidade é a divisibilidade por 2: um inteiro é divisível por dois se ele for par e podemos escrevê-lo da forma $2k$.

Outra regra muito conhecida é a da divisibilidade por 3: um inteiro é divisível por três quando a soma de seus algarismos for um número divisível por três; além disto, ele pode ser escrito da forma $3k$.

Outrossim, muito usados são os critérios de divisibilidade por cinco e por dez: é divisível por cinco todo número terminado em cinco ou zero e é divisível por dez todo número terminado em zero.

Posto isso, vamos usar a aritmética modular para explicar o porquê de todas essas regras de divisibilidade que quase sempre são decoradas pelos estudantes, sem que as compreendam, tornando esse processo totalmente mecânico e sem nenhum tipo de raciocínio lógico.

Não obstante, o objetivo desse trabalho não é listar várias regras de divisibilidade, mas sim mostrar como se constroem essas regras através das propriedades das congruências.

Divisibilidade por 3.

Proposição 12. *O resto da divisão de um número por três é igual ao resto da divisão da soma de seus algarismos por três.*

Demonstração. Seja x um número inteiro positivo escrito na base 10,

$x = a_0.10^0 + a_1.10^1 + a_2.10^2 + \ldots + a_n.10^n$, sendo $0 \leq a_i < 10$ e $a_n \neq 0$.

Sabemos que $10 \equiv 1(mod\ 3)$, logo $10^k \equiv 1^k(mod\ 3)$, então $10^k \equiv 1(mod\ 3)$, sendo k um inteiro positivo. Isso significa que qualquer que seja o expoente de uma potência de base dez, sempre o resto da sua divisão por três será igual a um.

Daí:

$$\begin{aligned} a_0.10^0 &\equiv a_0(mod\ 3); \\ a_1.10^1 &\equiv a_1(mod\ 3); \\ a_2.10^2 &\equiv a_2(mod\ 3); \\ &\vdots \\ a_n.10^n &\equiv a_n(mod\ 3). \end{aligned}$$

Somando os termos dessas congruências, temos:

$x \equiv a_0 + a_1 + a_2 + \ldots + a_n\ (mod\ 3)$.

Logo, $a_0 + a_1 + a_2 + \ldots + a_n$ é divisível por 3 se, e somente se, x também o é.

□

O mesmo acontece de forma análoga para os números divisíveis por 9.

Divisibilidade por 9.

Proposição 13. *Um número é divisível por 9 se, e somente se, a soma dos seus algarismos for divisível por 9.*

Demonstração. Observa-se que: $10^1 \equiv 1(mod\ 9)$.

$$\begin{aligned} a_0.10^0 &\equiv a_0(mod\ 9); \\ a_1.10^1 &\equiv a_1(mod\ 9); \\ a_2.10^2 &\equiv a_2(mod\ 9); \\ &\vdots \\ a_n.10^n &\equiv a_n(mod\ 9). \end{aligned}$$

Então:

$$x \equiv a_0 + a_1 + a_2 + \ldots + an(mod\ 9).$$

Logo, se $a_0 + a_1 + a_2 + \ldots + a_n$ é divisível por 9 se, e somente se, x também o é.

□

Divisibilidade por 2.

Proposição 14. *Um número é divisível por 2 se ele for um número par.*

Demonstração. Sabemos que:

$$\begin{aligned} 10^0 &\equiv 1(mod\ 2);\\ 10^1 &\equiv 0(mod\ 2);\\ 10^2 &\equiv 0(mod\ 2);\\ &\vdots\\ 10^n &\equiv 0(mod\ 2). \end{aligned}$$

Então:

$$\begin{aligned} a_0 10^0 &\equiv a_0\ (mod\ 2);\\ a_1 10^1 &\equiv 0(mod\ 2);\\ a_2 10^2 &\equiv 0(mod\ 2);\\ &\vdots\\ a_n 10^n &\equiv 0(mod\ 2). \end{aligned}$$

Somando os termos dessas congruências:

$$x \equiv a_0(mod\ 2).$$

Logo, x é divisível por 2 se, somente se a_0 também o é, ou seja, ele será divisível se terminar com os algarismos $0, 2, 4, 6$, ou 8.

□

Analogamente, temos a divisibilidade por 5 e por 10.

Divisibilidade por 5.

Proposição 15. *Um número é divisível por 5 quando termina com os algarismos 5 ou 0.*

Demonstração. Sabemos que:

$$\begin{aligned} 10^0 &\equiv 1(mod\ 5);\\ 10^1 &\equiv 0(mod\ 5);\\ 10^2 &\equiv 0(mod\ 5);\\ &\vdots\\ 10^n &\equiv 0(mod\ 5). \end{aligned}$$

Então:

$$\begin{aligned} a_0 10^0 &\equiv a_0\ (mod\ 5);\\ a_1 10^1 &\equiv 0(mod\ 5);\\ a_2 10^2 &\equiv 0(mod\ 5);\\ &\vdots\\ a_n 10^n &\equiv 0(mod\ 5). \end{aligned}$$

Somando os termos dessas congruências:

$$x \equiv a_0 (mod\ 5).$$

Portanto, x é divisível por 5 se, somente se, a_0 também o é, ou seja, se o último algarismo for divisível por 5, então esse algarismo só poderá ser 0 ou 5.

□

Divisibilidade por 10.

Proposição 16. *Um número é divisível por 10 quando termina com o algarismo 0.*

Demonstração. Sabemos que:

$$\begin{gathered} 10^0 \equiv 1 (mod\ 10); \\ 10^1 \equiv 0 (mod\ 10); \\ 10^2 \equiv 0 (mod\ 10); \\ \vdots \\ 10^n \equiv 0 (mod\ 10). \end{gathered}$$

Então:

$$\begin{gathered} a_0 10^0 \equiv a_0\ (mod\ 10); \\ a_1 10^1 \equiv 0 (mod\ 10); \\ a_2 10^2 \equiv 0 (mod\ 10); \\ \vdots \\ a_n 10^n \equiv 0 (mod\ 10). \end{gathered}$$

Somando os termos dessas congruências:

$$x \equiv a_0 (mod\ 10).$$

Logo, x é divisível por 10 se, somente se, a_0 for divisível por 10, ou seja, se o último algarismo for igual a 0.

□

Divisibilidade por 8.

Proposição 17. *Um número é divisível por 8 se o número formado pelos seus três últimos algarismos for divisíveis por 8.*

Demonstração. Sabemos que:

$$\begin{gathered} 10^0 \equiv 1 (mod\ 8); \\ 10^1 \equiv 2 (mod\ 8); \\ 10^2 \equiv 4 (mod\ 8); \\ 10^3 \equiv 0 (mod\ 8); \\ 10^4 \equiv 0 (mod\ 8); \\ \vdots \\ 10^n \equiv 0 (mod\ 8). \end{gathered}$$

Então:

$$\begin{gathered} a_0\ 10^0 \equiv a_0 (mod\ 8); \\ a_1\ 10^1 \equiv 2a_1 (mod\ 8); \\ a_2 10^2 \equiv 4a_2 (mod\ 8); \\ a_3 10^3 \equiv 0 (mod\ 8); \\ \vdots \\ a_n 10^n \equiv 0 (mod\ 8). \end{gathered}$$

Somando os termos dessas congruências:

$$x \equiv a_0 + 2a_1 + 4a_2 (mod\ 8).$$

Portanto, x é divisível por 8 se, somente se $a_0 + 2a_1 + 4a_2$ é divisível por 8.

O critério que aparece nos livros didáticos usa a seguinte estratégia:

$$\begin{aligned} a_0 + 2a_1 + 4a_2 (mod\ 8) &\equiv a_0 + 2a_1 + 4a_2 + 8a_1 + 96a_2 (mod\ 8); \\ &\equiv a_0 + 10a_1 + 100a_2 (mod\ 8). \end{aligned}$$

Como $8a_1 \equiv 0 (mod\ 8)$ e $96a_2 \equiv 0 (mod\ 8)$, podemos somá-los sem que altere o resultado.

Logo, se $a_0 + 10a_1 + 100a_2$ for divisível por 8, então x também será.

□

Exemplo 22: Verificando se $x = 85314$ é divisível por 8.

Sabemos que $x \equiv a_0 + 2a_1 + 4a_2\ (mod\ 8)$;

Então $a_0 + 2a_1 + 4a_2 = 4 + 2.1 + 4.3 = 18$.

Como 18 não é divisível por 8, então 85314 também não é.

Ressaltando que basta verificar os três últimos algarismos do número em questão.

De forma análoga, podemos definir os critérios de divisibilidade por 4.

Divisibilidade por 4.

Proposição 18. *Um número é divisível por 4 se o número formado pelos seus dois últimos algarismos for também divisível por 4.*

Demonstração. Sabemos que:

$$\begin{gathered} 10^0 \equiv 1 (mod\ 4); \\ 10^1 \equiv 6 (mod\ 4); \\ 10^2 \equiv 0 (mod\ 4); \\ 10^3 \equiv 0 (mod\ 4); \\ \vdots \\ 10^n \equiv 0 (mod\ 4). \end{gathered}$$

Então:

$$
\begin{aligned}
a_0 10^0 &\equiv a_0 \ (mod\ 4);\\
a_1 10^1 &\equiv 6a_1 (mod\ 4);\\
a_2 10^2 &\equiv 0 (mod\ 4);\\
a_3 10^3 &\equiv 0 (mod\ 4);\\
&\vdots\\
a_n 10^n &\equiv 0 (mod\ 4).
\end{aligned}
$$

Somando os termos dessas congruências:

$$x \equiv a_0 + 6a_1 (mod\ 4).$$

Logo, x é divisível por 4 se, somente se $a_0 + 6a_1$ é divisível por 4.

$$
\begin{aligned}
a_0 + 6a_1 (mod\ 4) &\equiv a_0 + 6a_1 + 4a_1 (mod\ 4)\\
&\equiv a_0 + 10a_1 (mod\ 4).
\end{aligned}
$$

Como $4a_1 \equiv 0 (mod\ 4)$, podemos somá-lo sem que altere o resultado. Então, se $a_0 + 10a_1$ for divisível por 4, x também o é.

Exemplo 23: Verificando se $x = 52316$ é divisível por 4.
Sabemos que: $x \equiv a_0 + 10a_1 (mod\ 4)$. Logo, $a_0 + 10a_1 = 6 + 10.1 = 16$.
Como 16 é divisível por 4, então 52316 também é.

□

Divisibilidade por 11.

Proposição 19. *Um número é divisível por 11 quando a diferença entre a soma dos algarismos de ordem par e a soma dos algarismos de ordem ímpar é um número divisível por 11.*

Demonstração. Sabemos que:

$$
\begin{aligned}
10^0 &\equiv 1 (mod\ 11);\\
10^1 &\equiv -1 (mod\ 11);\\
10^2 &\equiv 1 (mod\ 11);\\
10^3 &\equiv -1 (mod\ 11);\\
10^4 &\equiv 1 (mod\ 11);\\
&\vdots
\end{aligned}
$$

Então:

$$
\begin{aligned}
a_0\ 10^0 &\equiv a_0 (mod\ 11);\\
a_1\ 10^1 &\equiv -a_1 (mod\ 11);\\
a_2 10^2 &\equiv a_2 (mod\ 11);\\
a_3 10^3 &\equiv -a_3 (mod\ 11);\\
a_4 10^4 &\equiv a_4 (mod\ 11).\\
&\vdots
\end{aligned}
$$

Somando os termos dessas congruências:

$$x \equiv a_0 - a_1 + a_2 - a_3 + a_4 (mod\ 11).$$

Portanto, x é divisível por 11 se, somente se $a_0 - a_1 + a_2 - a_3 + a_4$ é divisível por 11.

□

Exemplo 24: Verificando se $x = 52316$ é divisível por 11.

Vejamos que:

$$5 + 3 + 6 = 14,$$

$$2 + 1 = 3.$$

Calculando a diferença, temos $14 - 3 = 11$. Logo, $x = 52316$ é divisível por 11.

Divisibilidade por 6.

Proposição 20. *Um número é divisível por 6 quando for divisível por 2 e 3 ao mesmo tempo.*

Demonstração. Decompondo o número 6 em fatores primos, encontramos $2 \cdot 3 = 6$, como 2 e 3 são primos entre si, temos que:

Se $x \equiv 0 \pmod 2$ e $x \equiv 0 \pmod 3$ então, $x \equiv 0 \pmod 6$.

Logo, um número x é divisível por 6 se, e somente se, ele for divisível por 2 e por 3 ao mesmo tempo.

□

2.3 Equações Diofantinas

O Documento Curricular para Goiás Etapa Ensino Médio - DC-GOEM (GOIÁS, 2018) dispõe, dentre os objetivos de aprendizagens:

> "(GO-EMMAT302C) - Modelar problemas que envolvem variáveis que se relacionam por meio de duas grandezas específicas, investigando informações apresentadas em textos que trazem dados decorrentes de situações socioeconômicas, técnico-científicas, etc.; para resolver problemas relativos à realidade do/a estudante"(GOIÁS, 2018).

Neste contexto, compreender e até mesmo solucionar Equações Diofantinas, pode ajudar a alcançar tal objetivo.

Definição 5. *Equação Diofantina é uma equação para a qual se busca soluções inteiras.*

Definição 6. *Uma Equação Diofantina linear com duas incógnitas é uma equação do tipo: $ax + by = c$, onde a, b, c são inteiros conhecidos.*

Esse tipo de equação pode ter infinitas soluções ou não ter nenhuma solução, conforme será demonstrado no presente capítulo.

Exemplo 25: Considerando a equação $2x + 5y = 9$, buscaremos soluções inteiras.

Nessa equação, podemos verificar que $2 \cdot 2 + 5 \cdot 1 = 9$.

Logo, $x_0 = 2$ e $y_0 = 1$ é uma solução particular, que indicaremos por $(x_0, y_) = (2, 1)$. Com tudo, se considerarmos o conjunto dos números inteiros, teremos várias outras soluções como, por exemplo:

$$2 \cdot (7) + 5 \cdot (-1) = 9.$$
$$2 \cdot (-3) + 5 \cdot (3) = 9.$$
$$2 \cdot (-8) + 5 \cdot (5) = 9.$$
$$2 \cdot (12) + 5 \cdot (-3) = 9.$$

Sendo assim, temos como soluções desta equação $(7, -1), (-3, 3), (-8, 5), (12, -3) \ldots$

Exemplo 26: Já na equação $4x + 2y = 5$, que é equivalente a $2(2x + y) = 5$, podemos observar que $2(2x+y)$ sempre será um número par, portanto, essa equação não terá solução, quaisquer que sejam x e y inteiros.

Exemplo 27: A equação $3x + 6y = 5$ corresponde a $3(x + 2y) = 5$ e $3(x + 2y)$ sempre será um número múltiplo de 3, logo, essa equação não terá solução inteira.

Proposição 21. *Sejam $a, b, c \in \mathbb{Z}$ e $MDC(a, b) = d$, a Equação Diofantina linear $ax + by = c$, terá solução se, e somente se, o $MDC(a, b) \mid c$.*

Demonstração. Pelo Teorema 1 (Teorema de Bézout), sabemos que existem inteiros r e s tais que $ar + bs = d$. E como $d \mid c$, existe um inteiro q tal que $c = qd$.

E como $d \mid c$, existe um inteiro q tal que $c = qd$. Multiplicando a igualdade por q temos: $a(rq) + b(sq) = dq$, assim $x_0 = rq$ e $y_0 = sq$ formam uma solução da equação $ax + by = c$.

Reciprocamente, seja (x_0, y_0) uma solução da equação, logo $ax_0 + by_0 = c$. Como $d \mid a$ e $d \mid b$, então pela proposição 2.4, $d \mid ax_0 + by_0 = c$.

□

De fato, encontrar todas as soluções em Equações Diofantinas pode ser difícil, se usarmos somente a intuição e cálculos mentais. Desse modo, usaremos as proposições e exemplos a seguir para simplificar ao máximo esse processo.

Proposição 22. *Seja (x_0, y_0) inteiros, uma solução da equação $ax + by = c$, onde $MDC(a, b) = 1$. Então, as soluções x, y em $\mathbb{Z}$ da equação são:*

$$\begin{cases} x = x_0 - tb. \\ y = y_0 + ta. \end{cases} , t \in \mathbb{Z}.$$

Demonstração. Seja (x_0, y_0) uma solução de $ax + by = c$.

Logo, para determinar, devemos ter x e y, $ax_0 + by_0 = ax + by = c$, consequentemente:

$$a(x_0 - x) = b(y - y_0).$$

Como $MDC(a, b) = 1$, então $b \mid (x_0 - x)$, logo $x_0 - x = tb$ daí:

$$x = x_0 - tb, t \in \mathbb{Z}.$$

Substituindo em $a(x_0 - x) = b(y - y_0)$, teremos, $at = (y - y_0)$, e finalmente:

$$y = y_0 + at, t \in \mathbb{Z}.$$

Reciprocamente, se $t \in \mathbb{Z}$ e $x = x_0 - tb, y = y_0 + at$, temos:

$$a(x_0 - bt) + b(y_0 + at) = ax_0 - abt + by_0 + abt = ax_0 + by_0 = c.$$

□

Exemplo 28: Retomando ao exemplo 24:

$$2x + 5y = 9.$$

Após encontrarmos uma solução particular $(x_0, y_0) = (2, 1)$ dessa equação, para chegar à solução geral, basta fazer:

$$x_0 = 2 - 5t \text{ e}$$
$$y_0 = 1 + 2t.$$

Se em uma equação $ax + by = c$, a condição do $MDC(a, b) = d$ tal que $d \mid c$, for satisfeita, podemos reescrevê-la da seguinte forma:

$$\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}.$$

Por fim, será possível encontrar uma solução particular para ela.

Exemplo 29: Encontrando uma solução particular para a equação $125x+70y = 15$ e depois generalizando-a.

Primeiro vamos calcular o MDC entre 125 e 70, usando os algoritmos da divisão de Euclides:

$$\begin{aligned} 125 &= 1 \cdot 70 + 55, \\ 70 &= 1 \cdot 55 + 15, \\ 55 &= 3 \cdot 15 + 10, \\ 15 &= 1 \cdot 10 + 5, \\ 10 &= 2 \cdot 5 + 0. \end{aligned}$$

De forma prática:

Quociente:	-	1	1	3	1	2
Dividendo:	125	70	55	15	10	5
Resto:	55	15	10	5	0	

O MDC é igual a 5 e $5 \mid 15$, logo, a equação admite solução. Dividindo-a por 5, temos uma equação equivalente a ela:

$$25x + 14y = 3.$$

Agora, isolaremos todos os restos:

$$\begin{aligned} 55 &= 125 - 1 \cdot 70, \\ 15 &= 70 - 1 \cdot 55, \\ 10 &= 55 - 3 \cdot 15, \\ 5 &= 15 - 1 \cdot 10, \\ 0 &= 10 - 2 \cdot 5. \end{aligned}$$

Façamos a substituição: $10 = 55 - 3 \cdot 15$,

$$\begin{aligned} 5 &= 15 - 1 \cdot (55 - 3 \cdot 15), \\ 5 &= (15) - 1(55) + 3(15), \\ 5 &= 4(15) - 1(55). \end{aligned}$$

Façamos a substituição: $15 = 70 - 1 \cdot 55$,

$$\begin{aligned} 5 &= 4(70 - 1 \cdot 55) - 1(55), \\ 5 &= 4(70) - 4(55) - 1(55), \\ 5 &= 4(70) - 5(55). \end{aligned}$$

Façamos a substituição: $55 = 125 - 1 \cdot 70$,

$$\begin{aligned} 5 &= 4(70) - 5(125 - 1 \cdot 70), \\ 5 &= 4(70) - 5(125) + 5(70), \\ 5 &= 9(70) - 5(125). \end{aligned}$$

Como o resultado da nossa equação é igual a 15, e 15 dividido pelo $MDC(125, 70) = 5$ é igual a 3, temos que multiplicar por 3 a última substituição:

$$5 = 27(70) - 15(125).$$

Deste modo, uma solução particular será $x_0 = -15, y_0 = 27$. Então a solução geral para essa equação será, $x = -15 - 14t$ e $y = 27 + 25t$.

Exemplo 30: Determinando as duas menores frações positivas que tenham 15 e 17 como denominadores e cuja soma seja igual a $\frac{314}{255}$.

Sabemos que as frações serão $\frac{x}{15}$ e $\frac{y}{17}$.

Então:

$$\frac{x}{15} + \frac{y}{17} = \frac{17x + 15y}{255} = \frac{314}{255}.$$

A solução consiste em encontrar os menores valores de x e y , inteiros positivos, que satisfaçam a igualdade $17x + 15y = 314$.

Usando o algoritmo da divisão de Euclides:

$$\begin{aligned} 17 &= 15 \cdot 1 + 2; \\ 15 &= 2 \cdot 7 + 1. \end{aligned}$$

Isolando os restos e substituindo:

$$\begin{aligned} 1 &= 15 - 2 \cdot 7, \\ 1 &= 15 - (17 - 15 \cdot 1) \cdot 7, \\ 1 &= 17(-7) + 15(8), \\ 314 &= 17(-7 \cdot 314) + 15(8 \cdot 314), \\ 314 &= 17(-2198) + 15(2512). \end{aligned}$$

As soluções são: $x = -2198 + 15t$ e $y = 2512 - 17t, t \in \mathbb{Z}$. Como x e y são inteiros positivos, $x > 0$ e $y > 0$, então:

$$-2198 + 15t > 0,$$

$$t > 146.$$

e

$$2512 - 17t > 0,$$

$$t < 148.$$

Então, $t = 147$. Portanto, temos como solução $x = -2198 + 15.147 = 7$ e $y = 2512 - 17.147 = 13$.

E as frações são:

$$\frac{7}{13}, \frac{13}{17}.$$

2.4 Congruência Linear

Definição 7. *Seja $m, a, b \in \mathbb{Z}$ e $m > 1$. Uma congruência do tipo $ax \equiv b(mod\ m)$, na incógnita x, é chamada de congruência linear.*

Exemplo 31: A congruência $16x \equiv 2(mod\ 7)$ é linear e admite como solução $x = -13, -6, 1, 8, \ldots$ entre outros, de fato,

$$\begin{aligned} 16(-13) &\equiv 2(mod\ 7); \\ 16(-6) &\equiv 2(mod\ 7); \\ 16(1) &\equiv 2(mod\ 7); \\ 16(8) &\equiv 2(mod\ 7). \\ &\vdots \end{aligned}$$

Observamos que congruências lineares podem ser escritas em forma de Equações Diofantinas, por exemplo, a congruência $16x \equiv 2(mod\ 7)$, pode ser escrita como $16x-2 \equiv 0(mod\ 7)$ que corresponde a $7 \mid 16x-2$, isso significa que deve existir $y \in \mathbb{Z}$ tal que $16x-2 = 7y$, logo $16x-7y = 2$. Desta forma, assim como as Equações Diofantinas, as congruências lineares podem ter várias soluções ou nenhuma solução.

Exemplo 32: A congruência $16x \equiv 7(mod\ 4)$ é linear, mas não admite solução inteira.

Observamos que $16x - 7 \equiv 0(mod\ 4)$ é equivalente à Equação Diofantina $16x - 4y = 7$, mas essa não tem solução, uma vez que o $MDC(16, 4) = 4$ e $4 \nmid 7$. Sendo assim, a congruência não tem solução.

Proposição 23. *Sejam $a, m \in \mathbb{Z}, m > 1$ e $MDC(a, m) = d$, então a congruência linear $ax \equiv b(mod\ m)$ tem solução se, e somente se, $d \mid b$.*

Demonstração. Se $ax \equiv b(mod\ m)$ admitir solução x_0 então $ax_0 \equiv b(mod\ m)$, logo, existe um número inteiro y_0 tal que $ax_0 - b = my_0$, que é equivalente a $ax - my = b$, e pela proposição 19, terá solução se, somente se, $d \mid b$.

Reciprocamente, se $MDC(a, m) \mid b$, pela proposição 19, a equação $ax - my = b$ admite solução (x_0, y_0). Assim $ax_0 = b + my_0$, que é o mesmo que $ax_0 - b = my_0$ e, portanto, $ax_0 \equiv b(mod\ m)$ que terá solução inteira.

□

Exemplo 33: Determinando a solução geral para as congruências lineares elencadas:

a) $x \equiv 2(mod\ 3)$;

Primeiramente, encontraremos a Equação Diofantina que corresponde a essa congruência:

$$x - 3y = 2.$$

O $MDC(3, 1) = 1$, sendo assim, a equação admite solução inteira.
Pelo algorítimo de Euclides, temos:

$$\begin{aligned} 3 &= 3(1) + 0, \\ 1 &= 1(1) + 3(1) - 3(1), \\ 1 &= 1(1) + 3(0). \end{aligned}$$

Multiplicado por 2:

$$2 = 1(2) + 3(0).$$

Logo, uma solução particular será $x_0 = 2$ e $y_0 = 0$ e a solução geral será:

$$x = 2 - 3t \text{ e } y = -t.$$

Voltando à congruência $x \equiv 2(mod\ 3)$, a solução geral é $x = 2 - 3t$; sendo $t \in \mathbb{Z}$.

b) $25x \equiv 15(mod\ 10)$;

Basta resolver $25x - 10y = 15$.

O $MDC(25, 10) = 5$, logo, $5 \mid 15$, então, a equação admite solução inteira. Dividindo a equação pelo $MDC(25, 10)$, temos $5x - 2y = 3$.

Pela divisão de Euclides:

$$\begin{aligned} 5 &= 2(2) + 1, \\ 2 &= 1(2) + 0. \end{aligned}$$

Isolando os restos:

$$1 = 5(1) - 2(2).$$

Multiplicado por 3:

$$3 = 5(3) - 2(6).$$

Logo, uma solução particular será $x_0 = 3$ e $y_0 = 6$ e a solução geral será: $x = 3 + 2t$ e $y = 6 + 5t$.

Voltando à congruência, a solução geral é $x = 3 + 2t$.

c) $156x \equiv 1(mod\ 11)$.

Basta resolver $156x - 11y = 1$.

Como $MDC(156, 11) = 1$, a equação admite solução inteira.

Quociente:	-	14	5	2
Dividendo:	156	11	2	1
Resto:	2	1	0	

$156 = 14 \cdot 11 + 2$, então $2 = 156(1) - 14(11)$.
$11 = 5 \cdot 2 + 1$ então, $1 = 11(1) - 5(2)$.

Substituindo as igualdades:

$$\begin{aligned} 1 &= 1(11) - 5(2), \\ 1 &= 1(11) - 5[156(1) - 14(11)], \\ 1 &= 1(11) + 156(-5) + 70(11), \\ 1 &= 156(-5) + 71(11), \\ 1 &= 156(-5) + 11(71). \end{aligned}$$

Então uma solução particular será $x_0 = -5$ e $y_0 = 71$ e a solução geral da Equação Diofantina é $x = -5 + 11t$ e $y = -71 + 156t$.

Voltando à congruência, a solução geral é $x = -5 + 11t, t \in \mathbb{Z}$.

2.5 O Teorema Chinês do Resto

O matemático chinês Sun-Tsu Ching, por volta do século I, apresentou a problemática: "Qual é o número que deixa resto $2, 3$ e 2 quando dividido por $3, 5$ e 7 respectivamente?"(HEFEZ, 2013).

Usando congruências lineares, conseguimos representar esse problema de forma relativamente simples:

$$\begin{aligned} x &\equiv 2(mod\ 3). \\ x &\equiv 3(mod\ 5). \\ x &\equiv 2(mod\ 7). \end{aligned}$$

Para solucionar esse problema, podemos começar resolvendo a congruência $x \equiv 2(mod\ 3)$, cuja solução geral é $x = 2 + 3t$, com $t \in \mathbb{Z}$, e depois substituir na segunda congruência:

$$\begin{aligned} 2 + 3t &\equiv 3(mod\ 5); \\ 3t &\equiv 1(mod\ 5); \\ t &= 2 + 5q, q \in \mathbb{Z}. \end{aligned}$$

Então, substituindo em x:

$$\begin{aligned} x &= 2 + 3(2 + 5q), \\ &= 8 + 15q; q \in \mathbb{Z}. \end{aligned}$$

Logo, substituindo na terceira congruência, temos:

$$\begin{aligned} 8 + 15q &\equiv 2(mod\ 7); \\ 1 + 1q &\equiv 2(mod\ 7); \\ q &\equiv 1(mod\ 7). \end{aligned}$$

A solução é, pois:

$$q = 1 + 7k, k \in \mathbb{Z}.$$

Assim:

$$\begin{aligned} x &= 8 + 15(1 + 7k); \\ x &= 23 + 105k. \end{aligned}$$

Observa-se que essa equação possui infinitas soluções do tipo $x = 23+105k$, sendo $k \in \mathbb{Z}$. Tomemos $k = 1$ e teremos $x = 128$, dessa forma 128 é um dos números que deixa resto 2 quando dividido por 3, resto 3 quando dividido por 5 e resto 2 quando dividido por 7.

Entretanto, esse método de substituição torna-se enfadonho quando tem-se mais de três congruências, razão pela qual a aplicação do Teorema Chinês do Resto possibilita a resolução desses tipos de problemas de forma mais práticas.

Definição 8. *O inverso multiplicativo de a módulo m é um número b tal que,* $ab \equiv 1(mod\ m)$.

Proposição 24. *O inverso multiplicativo de a módulo m existe se, e somente se,* $mdc(a, m) = 1$.

Demonstração. Se $mdc(a, m) = 1$, significa que existe uma combinação linear inteira de a e m que é igual a 1, ou seja, existem inteiros x e y tal que, $ax + my = 1$. Logo, x é o inverso multiplicativo de a módulo m, pois $ax \equiv 1(mod\ m)$.

Reciprocamente, se existe um inverso multiplicativo de a módulo m, então $ax \equiv 1(mod\ m)$ tem solução, logo, a equação $ax - my = 1$ terá solução e isso implica que $MDC(a, m) = 1$.

□

Proposição 25. *Toda congruência* $ax \equiv b(mod\ m)$ *que possui solução é equivalente a uma congruência da forma* $x \equiv c(mod\ n)$.

Demonstração. Se $ax \equiv b(mod\ m)$ possui solução, então, $d = MDC(a, m)$ divide b.

Façamos:

$$a' = \frac{a}{d}, b' = \frac{b}{d}, n = \frac{m}{d}.$$

Temos que a equação $ax \equiv b(mod\ m)$ é equivalente a $a'x \equiv b'(mod\ n)$, usando a proposição 3, $MDC(a', n) = 1$; logo, existe inverso multiplicativo de a' modulo n. Digamos que t seja esse inverso, sabemos que $ta'x \equiv tb'(mod\ n)$, mas $ta' \equiv 1(mod\ n)$. Assim $x \equiv tb'(mod\ n)$, ou seja, $x \equiv c(mod\ n)$.

□

Teorema 2. *(Teorema Chinês do Resto): Se* $MDC(m_i, m_j) = 1$, *para todo par de inteiros,* m_i, m_j *com* $i \neq j$, *sendo* $a_1, a_2, a_3, \ldots, a_s, b_1, b_2, b_3, \ldots, b_s \in \mathbb{Z}$. *Então, o sistema de congruências:*

$$\begin{aligned} a_1x &\equiv b_1(mod\ m_1); \\ a_2x &\equiv b_2(mod\ m_2); \\ a_3x &\equiv b_3(mod\ m_3); \\ &\vdots \\ a_sx &\equiv b_s(mod\ m_s); \end{aligned}$$

possui uma única solução módulo $M = m_1m_2 \ldots m_s$. *As soluções são* $x = M_1y_1r_1 + M_2y_2r_2 \ldots + M_sy_sr_s$, *onde* $M_i = M/m_i$ *e* y_i *são soluções de* $M_iY \equiv 1(mod\ m_i)$, *sendo* $i = 1, 2, \ldots, s$.

Demonstração. Pela proposição 22, temos um sistema de congruência equivalente ao apresentado:

$$\begin{aligned} x &\equiv c_1(mod\ n_1); \\ x &\equiv c_2(mod\ n_2); \\ x &\equiv c_3(mod\ n_3); \\ &\vdots \\ x &\equiv c_s(mod\ n_s). \end{aligned}$$

Seja $N = n_1 n_2 \dots n_s$, provaremos que x é uma solução simultânea do sistema. Como $n_i \mid N_i$, se $i \neq j$,e $N_i y_i \equiv 1(mod\ m_i)$, temos:

$$x = N_1 y_1 r_1 + N_2 y_2 r_2 \dots + N_s y_s r_s \equiv N_i y_i r_i \equiv r_i(mod\ n_i).$$

Por outro lado, se x' é outra solução do sistema, então $x \equiv x'(mod\ n_i)$, tal que $i = 1, 2, \dots, s$. Como $n_i \mid (x - x')$ e $n_j \mid (x - x')$, sendo $MDC(n_i, n_j) = 1$, para $i \neq j$, n_i e n_j são primos entre si, logo, $n_i.n_j \mid (x - x')$. Portanto, $N \mid (x - x')$ e $x \equiv x'(mod\ N)$.

□

Resolveremos, pois, o mesmo problema anteriormente anunciado usando o Teorema Chinês do Resto.

Façamos $M = 3 \cdot 5 \cdot 7 = 105$, ou seja, a multiplicação entre os módulos apresentados.

Encontrando M_1, M_2 e M_3, usamos:

$$M_1 = \frac{M}{3} = \frac{105}{3} = 35.$$
$$M_2 = \frac{M}{5} = \frac{105}{5} = 21.$$
$$M_3 = \frac{M}{7} = \frac{105}{7} = 15.$$

Posteriormente encontraremos y_1, y_2 e y_3, de forma que:

$$M_1 y_1 \equiv 1(mod\ 3).$$
$$M_2 y_2 \equiv 1(mod\ 5).$$
$$M_3 y_3 \equiv 1(mod\ 7).$$

Isso é:

$$35 y_1 \equiv 1(mod\ 3).$$
$$21 y_2 \equiv 1(mod\ 5).$$
$$15 y_3 \equiv 1(mod\ 7).$$

Buscando a menor solução positiva para y_1, y_2 e y_3, temos :

$$y_1 = 2, y_2 = 1, y_3 = 1$$

.

Ademais, para encontrar o valor do número x referido no problema de Sun-Tsu, usamos a seguinte congruência linear:

$$\begin{aligned} x &\equiv M_1 y_1 r_1 + M_2 y_2 r_2 + M_3 y_3 r_1 (mod\ M), \\ x &\equiv 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 (mod\ 105), \\ x &\equiv 140 + 63 + 30 (mod\ 105), \\ x &\equiv 233 (mod\ 105), \\ x &\equiv 23 (mod\ 105). \end{aligned}$$

Logo, $x = 23 + 105t$, sendo $t \in \mathbb{Z}$, é a solução procurada, destacamos, ainda, que essa equação não tem uma única solução.

Destarte, notamos que O Teorema Chinês do Resto está historicamente associado a aplicações em problemas de Astronomia e podemos utilizá-lo para resolver problemas e desafios com os nossos estudantes, vide o exemplo 34 e 35.

Exemplo 34: A professora Aline arrecadou dinheiro para realizar um passeio escolar. Se o valor arrecadado fosse dividido entre 11 turmas, sobraria 1 real; se a distribuição fosse feita entre 12 turmas, sobrariam 2 reais; e, por fim, se a distribuição fosse feita entre 13 turmas do colégio, então sobrariam 3 reais. Sabendo que a arrecadação foi menor do que 3000 reais, qual foi o valor arrecadado pela professora Aline?

Solução:

Observamos que, neste caso, temos:

$$x \equiv 1(mod\ 11).$$
$$x \equiv 2(mod\ 12).$$
$$x \equiv 3(mod\ 13).$$

Multiplicando m_1, m_2 e m_3 :

$$M = 11 \cdot 12 \cdot 13 = 1716.$$

Encontrando M_1, M_2 e M_3:

$$M_1 = \frac{M}{11} = \frac{1716}{11} = 156.$$

$$M_2 = \frac{M}{12} = \frac{1716}{12} = 143.$$

$$M_3 = \frac{M}{13} = \frac{1716}{13} = 132.$$

Encontraremos, então, y_1 , y_2 e y_3, de forma que:

$$M_1 y_1 \equiv 1(mod\ 11).$$
$$M_2 y_2 \equiv 1(mod\ 12).$$
$$M_3 y_3 \equiv 1(mod\ 13).$$

Ou seja:

$$156 y_1 \equiv 1(mod\ 11).$$
$$143 y_2 \equiv 1(mod\ 12).$$
$$132 y_3 \equiv 1(mod\ 13).$$

Posteriormente, buscaremos a menor solução positiva para y_1, y_2 e y_3:

$$y_1 = 6, y_2 = 11 \text{ e } y_3 = 7.$$

Utilizando a congruência linear:

$$\begin{aligned} x &\equiv M_1 y_1 r_1 + M_2 y_2 r_2 + M_3 y_3 r_1 (mod\ M). \\ x &\equiv 156 \cdot 6 \cdot 1 + 143 \cdot 11 \cdot 2 + 132 \cdot 7 \cdot 3 (mod\ 1716). \\ x &\equiv 936 + 3146 + 2772 (mod\ 1716). \\ x &\equiv 6854 (mod\ 1716). \end{aligned}$$

Temos, então:

$$x \equiv 1706(mod\ 1716).$$

Desta forma, o valor de x poderá ser $1706 + 1716t$, sendo t um número inteiro.

Se $t = 0$, temos $1706 + 1716 \cdot 0 = 1706$

Se $t = 1$, temos $1706 + 1716 \cdot 1 = 3422$ e $3422 > 3000$.

No entanto, como o valor foi menor do que 3000 reais: o único valor possível é 1706 reais.

Exemplo 35: (UFRJ) Seu Almeida possuía uma quantidade de azulejos maior do que 150 e menor do que 250. Ele arrumou os azulejos em várias caixas, cada uma contendo 17 azulejos. Sobraram 15 azulejos. Ele, então, resolveu guardar tudo em caixas menores, cada uma contendo 11 azulejos. Dessa vez, sobraram 4 azulejos. Determine quantos azulejos seu Almeida possuía (GIOVANNI; CASTRUCCI, 2002).

É possível resolver a questão utilizando o Teorema Chinês do Resto.

Primeiramente é necessário encontrar um inteiro entre 150 e 250 que, dividido por 17, tem resto 15 e, dividido por 11, tem resto 4.

Então:

$$x \equiv 15(mod\ 17).$$
$$x \equiv 4(mod\ 11).$$

Fazendo : $M = 11 \cdot 17 = 187$.

Para encontrar, M_1e M_2 usamos:

$$M_1 = \frac{M}{17} = \frac{187}{17} = 11.$$
$$M_2 = \frac{M}{11} = \frac{187}{11} = 17.$$

Posteriormente encontraremos y_1 e y_2, de forma que:

$$M_1 y_1 \equiv 1(mod\ 17).$$
$$M_2 y_2 \equiv 1(mod\ 11).$$

Isto é:

$$11y_1 \equiv 1(mod\ 17).$$
$$17y_2 \equiv 1(mod\ 11).$$

Buscaremos, pois, a menor solução positiva para y_1 e y_2.

Sendo assim, $y_1 = 14$, $y_2 = 2$:

$$\begin{aligned} x &\equiv M_1 y_1 r_1 + M_2 y_2 r_2 (mod\ M). \\ x &\equiv 11 \cdot 14 \cdot 15 + 17 \cdot 2 \cdot 4 (mod\ 187). \\ x &\equiv 2310 + 136 (mod\ 187). \\ x &\equiv 2446 (mod\ 187). \end{aligned}$$

Temos, então:

$$x \equiv 15(mod\ 187).$$
$$\text{e } 15 + 187t,$$

Usando $t = 1$:

$$15 + 187 = 202.$$

Usando $t = 2$:

$$15 + 374 = 389.$$

Como o número de azulejos está entre 150 e 250, ele só pode ser igual a 202:

$$\begin{aligned} 191 : 17 &= 11 \cdot 17 + 4; \\ 191 : 11 &= 11 \cdot 17 + 4; \\ 202 : 17 &= 187 + 15; \\ 202 : 11 &= 18 \cdot 11 + 4. \end{aligned}$$

2.6 Operações módulo m

Ao dividimos um número por dois, podemos encontrar como resto 0 ou 1. Já se a divisão for por três, encontraremos resto 0, 1 ou 2. Na divisão por cinco, encontramos como resto 0,1,2,3 ou 4. Nesse sentido, percebemos que em uma Divisão Euclidiana por m, sendo $m \in \mathbb{Z}$ e $m > 1$, encontraremos resto $0, 1, 2, \ldots, m-1$.

Definição 9. *Seja $m \in \mathbb{Z}, m > 1$. O conjunto $\{0, 1, 2, \ldots, m-1\}$ é chamado de Sistema Padrão Completo de Resíduos módulo m e usaremos a notação $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$.*

Exemplo 36: Considerando a congruência $x \equiv r(mod\ 3)$, os valores que o inteiro r poderá assumir em um Sistema Padrão Completo de Resíduos módulo 3 são $\{0, 1, 2\}$, logo, $\mathbb{Z}_3 = \{0, 1, 2\}$.

Isto é:

$$\begin{aligned} x &\equiv 0(mod\ 3); \\ x &\equiv 1(mod\ 3); \\ x &\equiv 2(mod\ 3). \end{aligned}$$

Obs. 5. *Em congruências do tipo $x \equiv 3(mod\ 3)$ ou $x \equiv 5(mod\ 3)$, em que o resto não pertence ao Sistema Padrão Completo de Resíduos módulo 3, podemos realizar divisões, objetivando encontrar o resto correspondente pertencente a esse conjunto:*

$$x \equiv 3(mod\ 3),\ \textit{corresponde a}\ x \equiv 0(mod\ 3);$$
$$x \equiv 5(mod\ 3),\ \textit{corresponde a}\ x \equiv 2(mod\ 3).$$

Por conseguinte, podemos definir sobre o conjunto $\mathbb{Z}_m$ operações de adição e multiplicação da seguinte forma:

Definição 10.

1-Adição módulo m: $r_1 + r_2$ = *resto da Divisão Euclidiana de* $r_1 + r_2$ *por m.*

2-Multiplicação módulo m: $r_1 \cdot r_2$ = *resto da Divisão Euclidiana de* $r_1 \cdot r_2$ *por m.*

Exemplo 37: No conjunto $\mathbb{Z}_m$, temos $2 + 3 = 0$, uma vez que 5 dividido por 5 deixa resto 0 e $2 \cdot 3 = 1$, porque 6 dividido por 5 deixa resto 1.

Assim, como no conjunto $\mathbb{Z}$, essas operações que supra definimos para o conjunto $\mathbb{Z}_m$, também possuem propriedades.

Proposição 26. *Sejam* r_1, r_2 *e* $r_3 \in \mathbb{Z}_m$, *restos de divisões módulo m, temos:*

1- Comutativa da adição: $r_1 + r_2 = r_2 + r_1$;

2- Associativa da adição: $(r_1 + r_2) + r_3 = r_1 + (r_2 + r_3)$;

3- Existe elemento neutro da adição: $r_1 + 0 = r_1$;

4- Existe elemento oposto da adição: Se $r_1 \in \mathbb{Z}_m$, $r_1 + (m - r_1) = 0$;

5- Comutativa da multiplicação: $r_1 \cdot r_2 = r_2 \cdot r_1$;

6- Associativa da multiplicação: $(r_1 \cdot r_2) \cdot r_3 = r_1 \cdot (r_2 \cdot r_3)$;

7-Existe elemento neutro da multiplicação: $r_1 \cdot 1 = r_1$;

8- Distributiva: $r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_1 \cdot r_3$.

Demonstração.

$$\begin{aligned} 1)\ r_1 + r_2 &= \text{resto da divisão de } r_1 + r_2 \text{ por } m; \\ &= \text{resto da divisão de } r_2 + r_1 \text{ por } m; \\ &= r_2 + r_1. \end{aligned}$$

$$\begin{aligned} 2)\ (r_1 + r_2) + r_3 &= \text{resto da divisão de } (r_1 + r_2) + r_3 \text{ por } m; \\ &= \text{resto da divisão de } r_1 + (r_2 + r_3) \text{ por } m; \\ &= r_1 + (r_2 + r_3). \end{aligned}$$

$$\begin{aligned} 3)\ 0 + r_1 &= \text{resto da divisão de } 0 + r_1 \text{ por m}; \\ &= \text{resto da divisão de } r_1 \text{ por } m; \\ &= r_1. \end{aligned}$$

$$
\begin{aligned}
4)\ r_1 + (m - r_1) &= \text{resto da divisão de } r_1 + (m - r_1) \text{ por } m;\\
&= \text{resto da divisão de } m \text{ por } m;\\
&= 0.
\end{aligned}
$$

$$
\begin{aligned}
5)\ r_1 \cdot r_2 &= \text{resto da divisão de } r_1 \cdot r_2 \text{ por } m;\\
&= \text{resto da divisão de } r_2 \cdot r_1 \text{ por } m;\\
&= r_2 \cdot r_1.
\end{aligned}
$$

$$
\begin{aligned}
6)\ (r_1 \cdot r_2) \cdot r_3 &= \text{resto da divisão de } (r_1 \cdot r_2) \cdot r_3 \text{ por } m;\\
&= \text{resto da divisão de } r_1 \cdot (r_2 \cdot r_3) \text{ por } m;\\
&= r_1 \cdot (r_2 \cdot r_3).
\end{aligned}
$$

$$
\begin{aligned}
7)\ r_1 \cdot 1 &= \text{resto da divisão de } r_1 \cdot 1 \text{ por m};\\
&= \text{resto da divisão de } r_1 \text{ por } m;\\
&= r_1.
\end{aligned}
$$

$$
\begin{aligned}
8)\ r_1 \cdot (r_2 + r_3) &= \text{resto da divisão de } r_1 \cdot (r_2 + r_3) \text{ por } m;\\
&= \text{resto da divisão de } r_1 \cdot r_2 + r_1 \cdot r_3 \text{ por } m;\\
&= r_1 \cdot r_2 + r_1 \cdot r_3.
\end{aligned}
$$

□

Obs. 6. *Se $b(mod\ m) \cdot d(mod\ m) = 1(mod\ m)$, então, dizemos que $b(mod\ m)$ é a inversa de $d(mod\ m)$.*

Exemplo 38:

Tabela de adição em $\mathbb{Z}_3$:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Tabela de multiplicação em $\mathbb{Z}_3$:

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Tabela de adição em $\mathbb{Z}_5$:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Tabela de multiplicação em $\mathbb{Z}_5$:

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Posto isso, observamos que, em uma multiplicação do conjunto dos números inteiro, não seria possível multiplicar dois números não nulos e obter zero. Porém, em uma operação módulo m, isso é possível.

Quando usadas na codificação e decodificação de mensagens criptografadas, as tábuas de multiplicação e de adição colacionadas são de grande valia, uma vez que essa modalidade de operação limita os resultados a um Sistema Padrão Completo de Resíduos, elemento fundamental para a Criptografia, que estudaremos no próximo capítulo.

A partir da análise detalhada da aritmética dos restos e das propriedades de congruência, podemos compreender como os números se comportam em estruturas cíclicas. Essa compreensão é vital para a construção de sistemas criptográficos. Com base nisso, no próximo capítulo investigaremos como esses conhecimentos matemáticos são aplicados em técnicas de codificação de mensagens, desde cifras clássicas até sistemas modernos de criptografia com chave pública, como o RSA.

Capítulo 3

Criptografia: A escrita oculta

3.1 Introdução

A palavra Criptografia vem do grego *kryptos* que significa culto ao secreto, e, por sua vez, *graphein* significa escrever (HEFEZ, 2013). A finalidade do uso dessa técnica milenar é esconder e proteger mensagens, técnica que, no decorrer dos anos, foi, gradativamente, aprimorada de forma a dificultar a decodificação dos códigos.

Nesse contexto, Salahoddin Shokranian, professor de Matemática na Universidade de Brasília, discorre: "Um sistema de criptos é um método de comunicação secreto num canal de comunicação pública entre um grupo de fontes (pessoas, usuários)"(**??**).

É possível verificar a utilização de ferramentas criptográficas diariamente. Na contemporaneidade, os aplicativos de comunicação e troca de mensagens, sejam essas escritas ou de voz, são protegidos por Criptografia. É comum, pois, a exibição de mensagens como: "As mensagens e as ligações são protegidas com Criptografia de ponta a ponta e ficam somente entre você e os participantes"(*WhatsApp*).

Não obstante, a Teoria dos Números, da qual a Aritmética é a parte mais elementar, era, anteriormente, considerada uma das áreas mais puras e abstratas da Matemática, desprovida de aplicações práticas. Esse panorama muda completamente a partir do desenvolvimento da Teoria da Informação, motivada pela evolução e popularização dos computadores além da facilidade de conexão com grandes redes mundiais. Abrangendo, assim, dentre outros assuntos, a Criptografia (HEFEZ, 2013).

É importante que os estudantes compreendam como a Matemática tem sido utilizada como uma ferramenta no avanço das tecnologias empregadas no desenvolvimento da humanidade.

Atualmente, a Criptografia é uma ciência fundamental no contexto virtual. Através dela, é possível autenticar os usuários para lhes fornecer acesso aos sites, possibilitar proteção em transações financeiras e segurança na troca de mensagens.

Para compreensão do funcionamento de alguns modelos de Criptografia, primeiramente associaremos a cada letra do nosso alfabeto um número natural:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

R	S	T	U	V	W	X	Y	Z
18	19	20	21	22	23	24	25	26

Usaremos o zero para simbolizar os espaços vazios entre as letras e, assim, teremos uma sequência de elementos em $\mathbb{Z}_{27}$.

Posteriormente, tentaremos decifrar o código a seguir:

$$(17, 21, 5, 0, 12, 5, 7, 1, 12).$$

Solução: Associando as letras com os números, encontramos a frase **QUE LEGAL.**

Entretanto, esse tipo de associação é muito simples e torna a decodificação muito fácil. Então, para uma melhor proteção da mensagem, poderemos usar o que chamamos de chave x.

3.2 Cifra de César

O notório imperador romano Júlio César usava um código de substituição no qual cada letra da mensagem original era substituída pela letra que a seguia em três posições no alfabeto: a letra A era substituída por D, a letra B por E, e assim sucessivamente. Podemos, então, concluir que ele usava uma chave $x = 3$ para se comunicar com seus generais; por esse motivo, essa codificação ficou conhecida como a Cifra de César(HEFEZ, 2013).

Júlio César pegava o código que queria passar e adicionava 3 em cada número, por exemplo, a mensagem **QUE LEGAL** seria trocada pelos números naturais: $(17, 21, 5, 0, 12, 5, 7, 1, 12)$; conforme a tabela e, logo depois, seriam realizadas as devidas adições. Assim, os novos números seriam : $(20, 24, 8, 3, 15, 8, 10, 4, 15)$ e, para terminar a codificação, ele trocava novamente esses números naturais por letras: **TXHCOHJDO**.

O procedimento anterior pode ser apresentado em forma de um fluxograma:

.

$$\text{QUE LEGAL} \rightarrow$$
$$(17, 21, 5, 0, 12, 5, 7, 1, 12) \rightarrow$$
$$+3(mod\ 27) \rightarrow$$
$$(20, 24, 8, 3, 15, 8, 10, 4, 15) \rightarrow$$
$$\text{TXHCOHJDO}$$

Para decodificar as mensagens, trocaremos as letras TXHCOHJDO pelos números $(20, 24, 8, 3, 15, 8, 10, 4, 15)$ e, como a chave usada para codificar foi $x = 3$, usaremos o oposto de 3 no conjunto $\mathbb{Z}_{27}$, isso é, o número que somado a 3 resultará 0:

$$3 + 24 = 0.$$

.

$$\text{TXHCOHJDO} \rightarrow$$

$$(20, 24, 8, 3, 15, 8, 10, 4, 15) \rightarrow$$
$$+24(mod\ 27) \rightarrow$$
$$(17, 21, 5, 0, 12, 5, 7, 1, 12) \rightarrow$$
$$\text{QUE LEGAL}$$

Demostraremos, então como essa técnica pode ser utilizada para a codificação e decodificação de mensagens com chaves diferentes de $x = 3$, vide exemplo 39.

Exemplo 39: Codificando uma mensagem usando a cifra de César, mas, dessa vez usando uma chave $x = 10$, a mensagem é "Vencemos".

Substituindo as letras por números:

22	5	14	3	5	13	15	19
V	E	N	C	E	M	O	S

$$22 + 10 = 32 \equiv 5(mod\ 27).$$
$$5 + 10 \equiv 15(mod\ 27).$$
$$14 + 10 \equiv 24(mod\ 27);$$
$$3 + 10 \equiv 13(mod\ 27);$$
$$5 + 10 \equiv 15(mod\ 27);$$
$$13 + 10 \equiv 23(mod\ 27);$$
$$15 + 10 \equiv 25(mod\ 27);$$
$$19 + 10 \equiv 2(mod\ 27).$$

A sequência agora é $(5, 15, 24, 13, 15, 23, 25, 2)$, que corresponde a EOXMOWYB.

Temos o fluxograma:

.

$$\text{VENCEMOS} \rightarrow$$
$$(22, 5, 14, 3, 5, 13, 15, 19) \rightarrow$$
$$+10(mod\ 27) \rightarrow$$
$$(5, 15, 24, 13, 15, 23, 25, 2) \rightarrow$$
$$\text{EOXMOWYB}$$

Para decodificá-la, devemos usar a chave oposta à que foi usada para codificar, ou seja, $x = 17$.

Encontrando os números correspondentes a cada letra:

E	O	X	M	O	W	Y	B
5	15	24	13	15	23	25	2

$$\begin{aligned} 5+17 &\equiv 22(mod\ 27);\\ 15+17 &\equiv 5(mod\ 27);\\ 24+17 &\equiv 14(mod\ 27);\\ 13+17 &\equiv 3(mod\ 27);\\ 15+17 &\equiv 5(mod\ 27);\\ 23+17 &\equiv 13(mod\ 27);\\ 25+17 &\equiv 15(mod\ 27);\\ 2+17 &\equiv 19(mod\ 27). \end{aligned}$$

A nova sequência é $(22, 5, 14, 3, 5, 13, 15, 19)$, que substituindo por letras, será VENCEMOS.

Observemos o fluxograma: .

$$\text{EOXMOWYB} \rightarrow$$

$$(5, 15, 24, 13, 15, 23, 25, 2) \rightarrow$$

$$+17(mod\ 27) \rightarrow$$

$$(22, 5, 14, 3, 5, 13, 15, 19) \rightarrow$$

$$\text{VENCEMOS}$$

No entanto, se não soubéssemos qual chave foi usada para codificar a mensagem, ficaria muito difícil quebrar esse código e encontrar a mensagem correta.

Sem a utilização da chave para decodificar, encontraríamos: EOXMOWYB, o que não faria sentido algum. Mas, por outro lado, se a chave for revelada, a mensagem seria facilmente encontrada.

3.3 Chave Vetor

A Cifra de César, contudo, se tornou muito fácil de ser decodificada com o passar do tempo, sendo assim, outras formas de dificultar a quebra da codificação começaram a ser usadas. Neste contexto, temos, por exemplo, a chave vetor $v = (x, y, z)$, que é mais complexa do que uma simples chave x.

Para codificar com uma chave vetor $v = (x, y, z)$,, escrevemos a mensagem, depois trocamos as letras por números, em seguida separamos de três em três e, então, adicione x ao primeiro, y ao segundo e z ao terceiro. Para finalizar, trocamos os novos números pelas letras correspondentes.

Exemplo 40: Codificando a mensagem **QUE LEGAL**, usando a chave vetor $v = (1, 5, 3)$.

Solução:

$$\begin{gathered}17 + 1 \equiv 18(mod\ 27);\\ 21 + 5 \equiv 26(mod\ 27);\\ 5 + 3 \equiv 8(mod\ 27);\\ 0 + 1 \equiv 1(mod\ 27);\\ 12 + 5 \equiv 17(mod\ 27);\\ 5 + 3 \equiv 8(mod\ 27);\\ 7 + 1 \equiv 17(mod\ 27);\\ 1 + 5 \equiv 6(mod\ 27);\\ 12 + 3 \equiv 15(mod\ 27).\end{gathered}$$

Nota-se que, soma foi feita de três em três, usando sempre a sequência de números 1, 5, 3.

O código será, então: $(18, 26, 8, 1, 17, 8, 17, 6, 15)$.

Vejamos o fluxograma:

.

$$\begin{gathered}\text{QUE LEGAL} \rightarrow\\ (17, 21, 5); (0, 12, 5); (7, 1, 12) \rightarrow\\ +(1, 5, 3)(mod\ 27) \rightarrow\\ (18, 26, 8); (1, 17, 8); (17, 6, 15) \rightarrow\\ \text{RZHAQHQFO}\end{gathered}$$

Para decodificar essa mensagem, temos que usar a chave oposta $v = (26, 22, 24)$:

.

$$\begin{gathered}\text{RZHAQHQFO} \rightarrow\\ (18, 26, 8); (1, 17, 8); (17, 6, 15) \rightarrow\\ +(26, 22, 24)(mod\ 27) \rightarrow\\ (17, 21, 5); (0, 12, 5); (7, 1, 12) \rightarrow\\ \text{QUE LEGAL}\end{gathered}$$

Observamos que, quanto mais aumentarmos o número de coordenadas do vetor v, maior será a segurança do sistema e mais difícil será a quebra da codificação.

Em um sistema de codificação com Criptografia de ponta a ponta, não é possível quebrar o sigilo. Nem mesmo os melhores *hackers* conseguem quebrar códigos protegidos por Criptografia, isso se ela for bem codificada, ou seja, bem protegida com uma chave mais complexa, e quanto mais complexa for a chave, mais difícil é a sua decodificação.

3.4 Chave Matriz

Outra forma de proteger essas mensagens é usando multiplicação de matrizes.

Por exemplo, vamos codificar a mensagem **QUE LEGAL**, mas agora com o uso de matrizes.

Primeiramente, vamos observar os números que estão associados às letras do nosso alfabeto, ressaltando que, justamente por isto, usaremos $\mathbb{Z}_{27}$:

Q	U	E		L	E	G	A	L
17	21	5	0	12	5	7	1	12

Posteriormente, devemos agrupar as letras da mensagem conforme a chave que iremos usar, neste caso, usaremos uma matriz dois por dois: $M = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$, que será multiplicada pelas matrizes dois por um formadas com as letras da mensagem.

Agrupemos, pois, as letras de dois em dois, sem esquecer do espaço entre as palavras:

$$\begin{pmatrix} x & y \\ z & t \end{pmatrix} \cdot \begin{pmatrix} Q \\ U \end{pmatrix},$$

$$\begin{pmatrix} x & y \\ z & t \end{pmatrix} \cdot \begin{pmatrix} E \\ 0 \end{pmatrix},$$

$$\begin{pmatrix} x & y \\ z & t \end{pmatrix} \cdot \begin{pmatrix} L \\ E \end{pmatrix},$$

$$\begin{pmatrix} x & y \\ z & t \end{pmatrix} \cdot \begin{pmatrix} G \\ A \end{pmatrix},$$

$$\begin{pmatrix} x & y \\ z & t \end{pmatrix} \cdot \begin{pmatrix} L \\ 0 \end{pmatrix}.$$

Façamos as multiplicações e troquemos os resultados novamente por letras.

Exemplo 41: Codificando a mensagem "QUE LEGAL", usando a matriz $M = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}$.

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} Q \\ U \end{pmatrix},$$

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} .E \\ 0 \end{pmatrix},$$

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} L \\ E \end{pmatrix},$$

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} G \\ A \end{pmatrix},$$

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} L \\ 0 \end{pmatrix}.$$

Substituamos as letras por números, realizemos as multiplicações e ao final, substituamos novamente por letras:

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 17 \\ 21 \end{pmatrix} = \begin{pmatrix} 2.17 + 5.21 \\ 1.17 + 3.21 \end{pmatrix} = \begin{pmatrix} 139 \\ 80 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 26 \end{pmatrix} (mod\ 27) = \begin{pmatrix} D \\ Z \end{pmatrix}.$$

Analogamente:

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 5 \\ 0 \end{pmatrix} = \begin{pmatrix} 2.5 + 5.0 \\ 1.5 + 3.0 \end{pmatrix} \equiv \begin{pmatrix} 10 \\ 5 \end{pmatrix} (mod\ 27) = \begin{pmatrix} J \\ E \end{pmatrix};$$

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 12 \\ 5 \end{pmatrix} = \begin{pmatrix} 2.12 + 5.5 \\ 1.12 + 3.5 \end{pmatrix} = \begin{pmatrix} 49 \\ 27 \end{pmatrix} \equiv \begin{pmatrix} 22 \\ 0 \end{pmatrix} (mod\ 27) = \begin{pmatrix} V \\ 0 \end{pmatrix};$$

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 1 \end{pmatrix} = \begin{pmatrix} 14 + 5 \\ 7 + 3 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 10 \end{pmatrix} (mod\ 27) = \begin{pmatrix} S \\ J \end{pmatrix};$$

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 12 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 24 \\ 12 \end{pmatrix} (mod\ 27) = \begin{pmatrix} X \\ L \end{pmatrix}.$$

Por fim temos a mensagem codificada com a chave matriz:

$$M = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}$$

.

E se transformou em: $DZJEV\_SJXL$.
Obs.: Usaremos _ para o zero.

Para decodificar essa mensagem, será necessário encontrar uma matriz que, quando multiplicada pela matriz $M = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}$, resultará em cada uma das matrizes codificadas com letras como, por exemplo:

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} D \\ Z \end{pmatrix};$$

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 4 \\ 26 \end{pmatrix} (mod\ 27).$$

$$\begin{cases} 2a + 5b = 4(mod\ 27) \\ a + 3b = 26(mod\ 27) \end{cases}$$

Solucionando o sistema de equações, encontraremos $a = -118 \equiv 17(mod\ 27)$ e $b = 48 \equiv 21(mod\ 27)$.

Então, a matriz decodificada será: $\begin{pmatrix} 17 \\ 21 \end{pmatrix} = \begin{pmatrix} Q \\ U \end{pmatrix}$.

Analogamente, deve-se realizar o mesmo procedimento para as demais matrizes letras que foram codificadas.

Porém, a forma mais rápida e eficaz de encontrar as letras que foram usadas é com a utilização da matriz inversa de $M = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}$. É interessante encorajar os estudantes para que decodifiquem a mensagem usando a matriz inversa, pois isto dará significado ao aprendizado de matrizes, além de tornar mais fácil a realização desta tarefa.

Calculando a inversa de $M = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}$, ou seja, M^{-1}.

Como a matriz M é uma matriz quadrada da forma dois por dois, então usaremos uma matriz identidade dois por dois. $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Sabemos que $M^{-1} \cdot M = M \cdot M^{-1} = I$.

Logo:

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 2a + 5c & 2b + 5d \\ 1a + 3c & 1b + 3d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Assim, teremos:

$$\begin{gathered} 2a + 5c = 1(mod\ 27), \\ 2b + 5d = 0(mod\ 27), \\ a + 3c = 0(mod\ 27), \\ b + 3d = 1(mod\ 27). \end{gathered}$$

Portanto:

$$\begin{cases} 2a + 5c = 1(mod\ 27), \\ a + 3c = 0(mod\ 27). \end{cases}$$

Então, $a \equiv 3(mod\ 27)$ e $c = -1 \equiv 26(mod\ 27)$.

Analogamente:

$$\begin{cases} 2b + 5d = 0(mod\ 27), \\ b + 3d = 1(mod\ 27). \end{cases}$$

Então, $b = -5 \equiv 22(mod\ 27)$ e $d \equiv 2(mod\ 27)$.

Agora, montando a matriz inversa $M^{-1}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 3 & 22 \\ 26 & 2 \end{pmatrix}$.

Retomando a mensagem $DZJEV\_\ SJXL$, organizaremos as letras em matrizes dois por um e multiplicaremos a inversa da matriz chave por cada uma delas:

$$\begin{pmatrix} 3 & 22 \\ 26 & 2 \end{pmatrix} \cdot \begin{pmatrix} D \\ Z \end{pmatrix} =$$

$$\begin{pmatrix} 3 & 22 \\ 26 & 2 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 26 \end{pmatrix} = \begin{pmatrix} 12 + 572 \\ 104 + 52 \end{pmatrix} = \begin{pmatrix} 584 \\ 156 \end{pmatrix} \equiv \begin{pmatrix} 17 \\ 21 \end{pmatrix} (mod\ 27) = \begin{pmatrix} Q \\ U \end{pmatrix}.$$

De forma análoga, faremos:

$$\begin{pmatrix} 3 & 22 \\ 26 & 2 \end{pmatrix} \cdot \begin{pmatrix} J \\ E \end{pmatrix}.$$

$$\begin{pmatrix} 3 & 22 \\ 26 & 2 \end{pmatrix} \cdot \begin{pmatrix} V \\ - \end{pmatrix}.$$

$$\begin{pmatrix} 3 & 22 \\ 26 & 2 \end{pmatrix} \cdot \begin{pmatrix} S \\ J \end{pmatrix}.$$

$$\begin{pmatrix} 3 & 22 \\ 26 & 2 \end{pmatrix} \cdot \begin{pmatrix} X \\ L \end{pmatrix}.$$

Ao final, o destinatário encontrará as matrizes: $\begin{pmatrix} Q \\ U \end{pmatrix} \begin{pmatrix} E \\ - \end{pmatrix} \begin{pmatrix} L \\ E \end{pmatrix} \begin{pmatrix} G \\ A \end{pmatrix} \begin{pmatrix} L \\ - \end{pmatrix}$.

Posto isso, o resultado é a frase: **QUE LEGAL**.

Vejamos o fluxograma para codificação:

.

$$\text{QUE LEGAL} \rightarrow$$
$$\begin{pmatrix} Q \\ U \end{pmatrix} \begin{pmatrix} E \\ - \end{pmatrix} \begin{pmatrix} L \\ E \end{pmatrix} \begin{pmatrix} G \\ A \end{pmatrix} \begin{pmatrix} L \\ - \end{pmatrix} \rightarrow$$
$$\begin{pmatrix} 17 \\ 21 \end{pmatrix} \begin{pmatrix} 5 \\ 0 \end{pmatrix} \begin{pmatrix} 12 \\ 5 \end{pmatrix} \begin{pmatrix} 7 \\ 1 \end{pmatrix} \begin{pmatrix} 12 \\ 0 \end{pmatrix} \rightarrow$$
$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \left[\begin{pmatrix} 17 \\ 21 \end{pmatrix} \begin{pmatrix} 5 \\ 0 \end{pmatrix} \begin{pmatrix} 12 \\ 5 \end{pmatrix} \begin{pmatrix} 7 \\ 1 \end{pmatrix} \begin{pmatrix} 12 \\ 0 \end{pmatrix} \right] \rightarrow$$
$$\begin{pmatrix} 4 \\ 26 \end{pmatrix} \begin{pmatrix} 10 \\ 5 \end{pmatrix} \begin{pmatrix} 22 \\ 0 \end{pmatrix} \begin{pmatrix} 19 \\ 10 \end{pmatrix} \begin{pmatrix} 24 \\ 12 \end{pmatrix} \rightarrow$$
$$\text{DZJEV\_SJXL}$$

Para decodificação:

$$\text{DZJEV\_SJXL} \rightarrow$$
$$\begin{pmatrix} D \\ Z \end{pmatrix}\begin{pmatrix} J \\ E \end{pmatrix}\begin{pmatrix} V \\ - \end{pmatrix}\begin{pmatrix} S \\ J \end{pmatrix}\begin{pmatrix} X \\ L \end{pmatrix} \rightarrow$$
$$\begin{pmatrix} 4 \\ 26 \end{pmatrix}\begin{pmatrix} 10 \\ 5 \end{pmatrix}\begin{pmatrix} 22 \\ 0 \end{pmatrix}\begin{pmatrix} 19 \\ 10 \end{pmatrix}\begin{pmatrix} 24 \\ 12 \end{pmatrix} \rightarrow$$
$$\begin{pmatrix} 3 & 22 \\ 26 & 2 \end{pmatrix} \cdot \left[\begin{pmatrix} 4 \\ 26 \end{pmatrix}\begin{pmatrix} 10 \\ 5 \end{pmatrix}\begin{pmatrix} 22 \\ 0 \end{pmatrix}\begin{pmatrix} 19 \\ 10 \end{pmatrix}\begin{pmatrix} 24 \\ 12 \end{pmatrix}\right] \rightarrow$$
$$\begin{pmatrix} 17 \\ 21 \end{pmatrix}\begin{pmatrix} 5 \\ 0 \end{pmatrix}\begin{pmatrix} 12 \\ 5 \end{pmatrix}\begin{pmatrix} 7 \\ 1 \end{pmatrix}\begin{pmatrix} 12 \\ 0 \end{pmatrix} \rightarrow$$
$$\text{QUE LEGAL}$$

Lembrando que, para que seja possível a multiplicação de duas matrizes, o número de colunas da primeira tem que ser igual ao número de linhas da segunda. Poderíamos usar, então, uma matriz chave três por três, assim agruparíamos as letras de três em três, formando uma matriz letra três por um. Ou quatro por quatro com matriz letra quatro por um, e assim sucessivamente. No entanto, para que esse processo seja exitoso, temos que usar como chave matriz somente matrizes que sejam inversíveis.

Definição 11. *Seja A uma matriz quadrada. Dizemos que A é inversível se existir uma matriz A^{-1} tal que:*

$$A \cdot A^{-1} = A^{-1} \cdot A = I_n,$$

onde I_n é a matriz identidade de ordem n.

De forma prática, para que uma matriz seja inversível, seu determinante deve ser diferente de zero.

$$\det(A) \neq 0.$$

Exemplo 42: Considerando a matriz:

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}.$$

O determinante é:

$$\det(A) = 1 \cdot 4 - 2 \cdot 3 = 4 - 6 = -2 \neq 0.$$

Logo, a matriz A é inversível.

Definição 12. *Seja $A \in \mathbb{Z}_{27}^{n\times n}$ uma matriz quadrada, dizemos que A é inversível em $\mathbb{Z}_{27}$ se existir uma matriz $A^{-1} \in \mathbb{Z}_{27}^{n\times n}$ tal que:*

$$A \cdot A^{-1} \equiv I_n (mod\ 27),$$

onde I_n é a matriz identidade de ordem n, e todas as operações são feitas módulo 27.

A matriz A é inversível em $\mathbb{Z}_{27}$ se, somente se, $MDC(\det(A), 27) = 1$.

Exemplo 43: Considerando a matriz:

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in \mathbb{Z}_{27}^{2\times 2}.$$

O determinante de A é:

$$\det(A) = 1 \cdot 4 - 2 \cdot 3 = 4 - 6 = -2 \equiv 25 (mod\ 27).$$

Como $MDC(25, 27) = 1$, o número 25 tem inverso em $\mathbb{Z}_{27}$ e, portanto, a matriz A é inversível em $\mathbb{Z}_{27}$.

É evidente que, quanto maior for o número de linhas e colunas da matriz chave, maior será a dificuldade de decodificação da mensagem.

Outra operação matemática mais elaborada que pode ser usada para dificultar a quebra de sigilo, é a equação exponencial que, para a decodificação, será necessário o uso de logaritmos, uma vez que estes correspondem à sua operação inversa.

Para este sistema ser utilizado com segurança, é necessário que as partes interessadas em trocar informações confidenciais combinem previamente quais chaves irão utilizar.

Durante a Segunda Guerra Mundial, os alemães tinham uma máquina chamada de Enigma que podia ser configurada de 15.896.255.521.782.636.000 maneiras diferentes; essa máquina foi adquirida pelos ingleses, que levaram muito tempo para conseguir quebrar o sistema de Criptografia alemão. Essa quebra de sistema foi fundamental para a vitória dos Aliados(KRISCHER, 2013).

3.5 Criptografia com chave pública: O RSA

A ideia de Criptografia com chave pública foi inicialmente proposta, de maneira teórica, por Diffie e Hellman em 1976,(SHOKRANIAN, 2005) O mais conhecido dos métodos de Criptografia de chave pública é o RSA. Este código foi inventado em 1977 por R. L. Rivest, A. Shamir e L. Adleman, que, na época, trabalhavam no *Massachusetts Institute of Technology* (M.I.T.), uma das melhores universidades americanas. As letras RSA correspondem às iniciais dos inventores do código, e vem sendo largamente empregado para garantir segurança em transações eletrônicas(COUTINHO, 2023).

Nesse sistema, são usados vários tipos de operações matemáticas baseadas nos conceitos elementares da Teoria dos Números. Nos tópicos anteriores discutimos

formas muito antigas de Criptografias, já aqui estamos falando de uma Criptografia moderna que teve início por volta de 1976, como já mencionamos.

Atualmente, podemos encontrar vários outros códigos de chave pública, mas o RSA continua sendo o mais usado em aplicações comerciais, e a Matemática necessária para entender esse sistema vai um pouco além da Teoria dos Números.

Entenderemos, então, como funciona esse tipo de Criptografia.

1. Escolheremos dois números primos distintos p_1 e p_2.
2. Calcularemos $n = p_1 \cdot p_2$.
3. Calcularemos $\varphi(n) = (p_1 - 1)(p_2 - 1)$.
4. Escolheremos um inteiro x tal que $1 < x < \varphi(n)$, seja $MDC(x, \varphi) = 1$. Este será o expoente público.

Chave pública: (x, n).

Exemplo 44: Sejam $p_1 = 7$ e $p_2 = 11$ dois primos, daí $n = p_1 \cdot p_2 = 7 \cdot 11 = 77$. Assim $\varphi(n) = (7 - 1)(11 - 1) = 6 \cdot 10 = 60$.

Escolheremos um número x tal que $MDC(x, \varphi) = 1$, por exemplo $x = 7$. As chaves públicas serão x e $p_1 \cdot p_2$. Nesse caso, os números 7 e 77.

Chave pública: $(7, 77)$.

Exemplo 45: Codifiquemos a mensagem "QUE LEGAL"com chave pública $(7, 77)$.

Q	U	E		L	E	G	A	L
17	21	5	0	12	5	7	1	12

$$(17, 21, 5, 0, 12, 5, 7, 1, 12)$$

Elevemos cada um desses números à potência x, módulo 77. No nosso caso, como $x = 7$, obtemos:

$$17^7 \equiv 52 (mod\ 77);$$
$$21^7 \equiv 21 (mod\ 77);$$
$$5^7 \equiv 47 (mod\ 77);$$
$$0^7 \equiv 0 (mod\ 77);$$
$$12^7 \equiv 12 (mod\ 77);$$
$$5^7 \equiv 47 (mod\ 77).$$
$$7^7 \equiv 28 (mod\ 77).$$
$$1^7 \equiv 1 (mod\ 77).$$
$$12^7 \equiv 17 (mod\ 77).$$

Teremos, assim, uma nova sequência de números: $(52, 21, 47, 0, 12, 47, 28, 1, 12)$.

Exemplo 46: Para decifrar a mensagem criptografada no exemplo anterior, é preciso conhecer o número φ que, no caso, sabemos ser igual a 60, e determinar um número y tal que

$$x \cdot y \equiv 1(mod\ \varphi)$$

Como $x = 7$, $y = 43$ satisfaz $7 \cdot 43 \equiv 1(mod\ 60)$.

Deciframos a mensagem da seguinte forma: elevemos cada termo da sequência de números associada à mensagem criptografada à potência x módulo 77.

$$52^{43} \equiv 17(mod\ 77)$$
$$21^{43} \equiv 21(mod\ 77)$$
$$47^{43} \equiv 5(mod\ 77)$$
$$0^{43} \equiv 0(mod\ 77)$$
$$12^{43} \equiv 12(mod\ 77)$$
$$47^{43} \equiv 5(mod\ 77)$$
$$28^{43} \equiv 7(mod\ 77)$$
$$1^{43} \equiv 1(mod\ 77)$$
$$12^{43} \equiv 12(mod\ 77)$$

Temos, então, $(17, 21, 5, 0, 12, 5, 7, 1, 12)$ que corresponde a "QUE LEGAL".

No sistema de chave pública, divulgamos os números x e $p_1 \cdot p_2$, que são utilizados para codificar a mensagem a ser enviada. Portanto, qualquer pessoa pode enviar uma mensagem criptografada para o receptor, que detém o número y, utilizado para decifrar a mensagem. A segurança do RSA baseia-se na dificuldade de fatorar o número n em seus fatores primos p_1 e p_2. O tamanho dos primos p_1 e p_2 utilizados está diretamente relacionado ao tamanho da chave RSA.

A recomendação atual para seguranças mais sensíveis, como por exemplo, em transações financeiras, é que se use primos com no mínimo 615 dígitos (OLIVEIRA, 2021). Quando n é suficientemente grande, a fatoração se torna computacionalmente inviável com os métodos atuais.

A seguir, veremos teoremas que ajudarão na compreensão de sistemas de Criptografia com chave pública.

Teorema 3. *(O Pequeno Teorema de Fermat). Seja p um número primo e $a \in \mathbb{Z}$ tal que $a \not\equiv 0(mod\ p)$, então:*

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

Demonstração. Consideremos o conjunto dos inteiros $\{1, 2, 3, \ldots, p-1\}$, que contém todos os inteiros positivos menores que p. Como p é primo, todos esses números são relativamente primos a p, ou seja, $MDC(k, p) = 1$ para $1 \leq k < p$.

Agora, multiplicaremos cada elemento do conjunto por um número a tal que $a \not\equiv 0(mod\ p)$; isto é, a e p também são primos entre si. O conjunto resultante será:

$$\{a \cdot 1, a \cdot 2, a \cdot 3, \ldots, a \cdot (p-1)\}.$$

Como $MDC(a, p) = 1$, então a possui um inverso multiplicativo módulo p, ou seja, existe $a^{-1} \in \mathbb{Z}$ tal que:

$$a \cdot a^{-1} \equiv 1 (mod\ p).$$

Suponhamos que existam $i, j \in \{1, 2, \ldots, p-1\}$ tais que:

$$ia \equiv ja (mod\ p).$$

Multiplicando ambos os lados por a^{-1}, obtemos:

$$i \equiv j (mod\ p).$$

Como i e j estão entre 1 e $p-1$, concluímos que $i = j$.

Portanto, os elementos do conjunto $\{a, 2a, 3a, \ldots, (p-1)a\}$ são todos distintos módulo p, o que mostra que a multiplicação por a define uma bijeção no conjunto $\{1, 2, \ldots, p-1\}$.

Assim, os dois produtos são congruentes módulo p:

$$a \cdot 1 \cdot a \cdot 2 \cdot \cdots \cdot a \cdot (p-1) = a^{p-1} \cdot (p-1)! \equiv (p-1)! (mod\ p).$$

Como $(p-1)! \not\equiv 0 (mod\ p)$, podemos cancelar $(p-1)!$ dos dois lados da congruência:

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

Teorema 4. *(O Teorema de Euler). Seja $n \in \mathbb{N}$ com $n \geq 1$, e seja $a \in \mathbb{Z}$ tal que $MDC(a, n) = 1$. Então:*

$$a^{\varphi(n)} \equiv 1 (mod\ n),$$

onde $\varphi(n)$ é a função totiente de Euler.

Demonstração. Sejam os inteiros positivos $r_1, r_2, \ldots, r_{\varphi(n)}$ os representantes do conjunto dos elementos invertíveis módulo n, ou seja, o conjunto:

$$\mathbb{Z}_n^* = \{r \in \{1, 2, \ldots, n-1\} \mid MDC(r, n) = 1\}.$$

Como $MDC(a, n) = 1$, então $a \cdot r_i (mod\ n) \in \mathbb{Z}_n^*$ para cada i. Além disso, a multiplicação por a é uma bijeção em $\mathbb{Z}_n^*$, ou seja, o conjunto $\{ar_1, ar_2, \ldots, ar_{\varphi(n)}\} (mod\ n)$ é apenas uma reordenação de $\mathbb{Z}_n^*$.

Logo, temos:

$$ar_1 \cdot ar_2 \cdots ar_{\varphi(n)} \equiv r_1 r_2 \cdots r_{\varphi(n)} (mod\ n).$$

O lado esquerdo é:

$$a^{\varphi(n)} \cdot (r_1 r_2 \cdots r_{\varphi(n)}) \equiv r_1 r_2 \cdots r_{\varphi(n)} (mod\ n).$$

Como $r_1 r_2 \cdots r_{\varphi(n)}$ e n são primos entre si, podemos cancelar este produto (pois é invertível módulo n). Assim, obtemos:

$$a^{\varphi(n)} \equiv 1(mod\ n).$$

□

Teorema 5. *(Teorema da Corretude do RSA) Sejam p_1, p_2 números primos e $\varphi = \varphi(p_1 p_2) = (p_1 - 1)(p_2 - 1)$. Escolha $x \in \mathbb{Z}$ tal que $MDC(x, \varphi) = 1$. Seja $y \in \mathbb{Z}$ satisfazendo $x \cdot y \equiv 1(mod\ \varphi)$. Então, para cada inteiro t satisfazendo $1 \leq t \leq p_1 p_2$ temos,*

$$t^{x \cdot y} \equiv t(mod\ p_1 p_2).$$

Demonstração. Como p_1 e p_2 são primos distintos, o produto $n = p_1 p_2$ é composto, e podemos usar propriedades da aritmética modular com respeito a cada primo separadamente, usando o Teorema 2 (Teorema Chinês do Resto).

Sabemos que $x \cdot y \equiv 1(mod\ \varphi)$, ou seja, existe um inteiro k tal que:

$$x \cdot y = 1 + k\varphi.$$

Queremos provar que:

$$t^{x \cdot y} = t^{1+k\varphi} = t \cdot (t^{\varphi})^k \equiv t(mod\ p_1 p_2).$$

Caso 1: Se $MDC(t, p_1 p_2) = 1$.

Neste caso, temos $MDC(t, p_1) = 1$ e $MDC(t, p_2) = 1$.

Pelo Teorema 3 (Pequeno Teorema de Fermat):

$$t^{p_1 - 1} \equiv 1 \pmod{p_1}, \quad t^{p_2 - 1} \equiv 1 \pmod{p_2}.$$

Como $\varphi = (p_1 - 1)(p_2 - 1)$, então $t^{\varphi} \equiv 1 \pmod{p_1}$ e $\pmod{p_2}$.

Logo:

$$t^{xy} = t^{1+k\varphi} = t \cdot (t^{\varphi})^k \equiv t \cdot 1^k \equiv t(mod\ p_1).$$

Analogamente:

$$t^{xy} \equiv t \pmod{p_2}.$$

Assim, pelo Teorema 2 (Teorema Chinês do Resto):

$$t^{xy} \equiv t(mod\ p_1 p_2).$$

Caso 2: Se $MDC(t, p_1 p_2) \neq 1$.

Isso significa que t é múltiplo de algum dos primos p_1 ou p_2. Suponhamos, sem perda de generalidade, que $p_1 \mid t$. Então:

$$t \equiv 0(mod\ p_1),$$

$$t^{xy} \equiv 0 \equiv t(mod\ p_1).$$

Se $p_2 \mid t$, então $t \equiv 0(mod\ p_2)$, logo $t^{xy} \equiv 0 \equiv t(mod\ p_2)$.

Se $p_2 \nmid t$, então $MDC(t, p_2) = 1$ e pelo Teorema 4 (O Teorema de Euler):

$$t^{\varphi(p_2)} \equiv 1(mod\ p_2),$$
$$t^{k\cdot\varphi(p_2)} \equiv 1(mod\ p_2),$$
$$t^{x\cdot y} = t^{1+k\varphi} \equiv t \cdot 1 \equiv t(mod\ p_2).$$

Portanto, em todos os casos:

$$t^{x\cdot y} \equiv t(mod\ p_1) \quad \text{e} \quad t^{x\cdot y} \equiv t(mod\ p_2).$$

Novamente, pelo Teorema 2 (Teorema Chinês do Resto), concluímos que:

$$t^{x\cdot y} \equiv t \pmod{p_1 p_2}.$$

□

De forma geral, quando temos uma mensagem codificada com chave RSA, já vimos que a chave pública é (x, n), e n é a multiplicação de $p_1 p_2$, porém, para decodifica-lá, não basta ter os valores de x e de n, é necessário encontrar o valor exato de p_1 e de p_2 para encontrar o valor de $\varphi(n)$, e só então encontrar o valor de y.

Exemplo 47: Em uma codificação com chave pública onde $n = 14.558.801$ sabemos que $p_1 \cdot p_2 = 14.558.801$, mas seria totalmente inviável encontrar os número p_1 e p_2 de forma mental ou manual, no entanto hoje em dia temos computadores capazes de conseguir encontrar os primos, $p_1 = 4093$ e $p_2 = 3557$. Logo $\varphi = 4092 \cdot 3556 = 14.551.152$.

Contudo, se pensarmos em um primo com mais de 615 dígitos, multiplicado por outro primo também com mais de 615 dígitos, essa fatoração se torna computacionalmente inviável com os métodos atuais, tornando a codificação segura, como mencionamos anteriormente.

Ao percorrer o universo da Criptografia, desde a Cifra de César até o sistema RSA, demonstramos que a Matemática desempenha papel central na proteção de informação em nosso tempo. Tais conteúdos, além de historicamente significativos, revelam-se férteis para a abordagem pedagógica de temas abstratos como congruências, $(mod\ m)$ e multiplicação de matrizes. No próximo capítulo, relatamos como essas ideias foram levadas à sala de aula por meio de uma sequência didática estruturada, com ênfase no protagonismo dos estudantes e na promoção de uma aprendizagem significativa.

Capítulo 4

Experiência Didática

4.1 Introdução

Para colocar em prática parte dos estudos realizados nesse trabalho, foi elaborada uma sequência didática pensando no desenvolvimento de habilidades gerais e específicas. Nesse contexto, baseamos-nos na Base Nacional Comum Curricular, cujas competências visam o desenvolvimento de habilidades matemáticas essenciais para a resolução de problemas em diversos contextos, com ênfase na interpretação, construção de modelos e análise de soluções.

A habilidade de utilizar conceitos e procedimentos matemáticos de forma crítica e reflexiva é fundamental para a construção de argumentação consistente e a adequação dos resultados obtidos. Nesse cenário, a aritmética, com seus conceitos como divisibilidade, congruência e matrizes, se torna uma ferramenta poderosa para a resolução de problemas práticos, como é o caso da Criptografia, que visa proteger informações e garantir a segurança nas comunicações digitais.

O objetivo deste projeto é, portanto, aplicar esses conhecimentos aritméticos para codificar e decodificar mensagens criptografadas, proporcionando aos estudantes uma experiência prática e interdisciplinar, que une Matemática, Tecnologia e Comunicação.

Por meio de uma sequência didática composta por treze atividades, buscamos ampliar o entendimento dos estudantes sobre conteúdos já estudados, como Divisão Euclidiana, multiplicação de matrizes e matrizes inversas, além de introduzir o conceito de aritmética modular. Este processo de aprendizagem foi conduzido de forma dinâmica, com desafios que incentivaram a curiosidade e a aplicação da Matemática em situações reais, reforçando a importância do pensamento lógico e analítico na resolução de problemas do cotidiano.

4.2 Sobre a elaboração da sequência

A sequência de atividades que se encontra no Apêndice A foi pensada de forma a proporcionar aos estudantes do Ensino Médio uma experiência prática de aprendizado, focada na aplicação de conceitos matemáticos em um contexto desafiador e envolvente: a Criptografia. O uso de aritmética, divisibilidade, congruência

modular e matrizes, temas fundamentais para o desenvolvimento de habilidades matemáticas, foi integrado com o processo de codificação e decodificação de mensagens criptografadas. O objetivo central dessas atividades foi, então, permitir que os estudantes não apenas dominassem os algoritmos de divisões e operações matemáticas, mas também compreendessem sua aplicação em situações reais, como a segurança das informações no mundo digital.

Com efeito, a competência 3 da BNCC determina:

> "Utilizar estratégias, conceitos, definições e procedimentos matemáticos para interpretar, construir modelos e resolver problemas em diversos contextos, analisando a plausibilidade dos resultados e a adequação das soluções propostas, de modo a construir argumentação consistente."(BRASIL, 2018).

O objetivo é, pois, desenvolver habilidades matemáticas, usando a aritmética. Aplicar conhecimentos adquiridos como divisibilidade, congruência e matrizes para codificar e descodificar mensagens criptografadas usando cálculos matemáticos.

Para isso, adotaremos como metodologia a aplicação de uma sequencia didática que permite a recapitulação de conteúdos previamente lecionados aos discentes e ampliar os conhecimentos em aritmética, além de introduzir o conceito de aritmética modular.

Segundo Pais, uma sequência didática é formada por um certo número de aulas planejadas e analisadas previamente com a finalidade de observar situações de aprendizagem, envolvendo os conceitos previstos na pesquisa didática (PAIS, 2016).

Para Barbosa, uma sequência didática pode ser composta por uma série de atividades (tarefas) que permitam que o ensino da Matemática ocorra em um ambiente mais atrativo. Essas atividades são planejadas para serem interligadas e desenvolvidas etapa por etapa, tendo em vista seus objetivos específicos (BARBOSA, 2016).

Nesse sentido, foram elaboradas atividades com duração média de cinquenta minutos cada, atividades essas que foram construídas, primeiramente, de forma a despertar a curiosidade dos estudantes, realizando pesquisas sobre o tema em questão. Retomamos conteúdos já estudados, como, por exemplo, Divisão Euclidiana de números inteiros, multiplicação de matrizes e matrizes inversas. Em meio a essa retomada, introduzimos conteúdos sobre aritmética modular. Por fim, foram lançados desafios que consistem em codificar e descodificar mensagens trocadas entre estudantes, tudo, é claro, com o uso de muita Matemática.

4.3 Relato de experiência

A sequência de atividades foi cuidadosamente planejada para abordar de forma gradual e dinâmica o uso da Matemática na Criptografia, começando com a revisão de conceitos básicos, como a divisão de números inteiros e o uso de módulos, até alcançar a aplicação de matrizes para a Criptografia um pouco mais avançada. Além disso, o desenvolvimento de habilidades práticas foi combinado com

o incentivo ao raciocínio lógico e criativo, criando um ambiente de aprendizado ativo e colaborativo.

As aulas escolhidas para realização dessa experiência foram as aulas de estudo orientado de Matemática nas turmas da segunda série do Ensino Médio, nas quais ministrei durante o ano de 2024. A escolha foi feita devido à flexilidade de conteúdos da disciplina.

O processo de ensino-aprendizagem foi permeado por desafios que estimulavam a reflexão sobre os conceitos, proporcionando momentos de superação das dificuldades, como o domínio da divisão algorítmica e a compreensão do conceito de congruência modular. A participação dos estudantes foi estimulada por atividades práticas, que envolviam a troca de mensagens criptografadas, resultando em uma experiência enriquecedora para todos os envolvidos.

Apresento, portanto, um breve relato sobre as experiências vivenciadas em sala de aula com estudantes da segunda série do Ensino Médio. As atividades encontram-se no Apêndice A, e foram entregue aos estudantes com o cabeçalho padrão da escola, numa configuração adequada, contendo uma linguagem clara e coerente ao nível de desenvolvimento da turma.

Atividade 1: O algoritmo da divisão.

Habilidade da BNCC desenvolvida:

> "(EF07MA01): Resolver e elaborar problemas com números naturais, envolvendo as noções de divisor e de múltiplo, podendo incluir máximo divisor comum ou mínimo múltiplo comum, por meio de estratégias diversas, sem a aplicação de algoritmos"(BRASIL, 2018, p.309).

Ao realizar essa atividade com os estudantes da 2ª série do Ensino Médio, observei uma certa dificuldade na realização das operações de divisão usando somente números inteiros. Alguns tentaram usar a calculadora que, por sua vez, apresentava respostas em números decimais.

Então, passaram a usar outra estratégia, relembrando dos estudos de divisão do fundamental anos iniciais. Percebi que, usualmente, os estudantes realizam operações com auxilio de calculadora e, desta forma, o algorítimo da divisão já estava em desuso.

Outra observação interessante refere-se ao desconhecimento dos estudantes sobre a forma de utilização do algorítimo da divisão. Apegavam-se à crença de complexidade da divisão, alegando que tinham lembranças do Ensino Fundamental séries iniciais, quando não conseguiam realiza-lá. Contudo, separei a turma em grupos de quatro estudantes, o que proporcionou o encorajamento por aqueles que tinham conhecimento da matéria.

Posto isso, mesmo os estudantes com maior dificuldade e que, em seus estudos do Ensino Fundamental anos iniciais não conseguiam compreender de forma alguma os algorítimos, tiveram maior facilidade na realização das operações.

Nessa oportunidade, apresento o relato de uma estudante: "Nossa professora, eu nunca tinha entendido isso. Pensei que era difícil. Era só isso?."

Também pude observar que, depois de feitas as divisões, as outras questões foram solucionadas de forma mais tranquila, porque os discentes conseguiram

relacioná-las com as divisões anteriormente respondidas.

Em conclusão, o resultado alcançado foi positivo, pois a maioria compreendeu o algorítimo da divisão. Para mais, em média 50 por cento dos estudantes conseguiram realizar toda a atividade sem a intervenção da professora ou de algum colega.

Atividade 2: Divisibilidade com números negativos.

Habilidade da BNCC desenvolvida:

> "(EF06MA06): Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor"(BRASIL, 2018, p.303).

Nesta atividade, foi necessário o desenvolvimento de um raciocínio matemático referente às divisões de números inteiros, principalmente quando tínhamos um dividendo negativo e um divisor positivo.

Alguns, observando os exemplos dados, logo entenderam que, se dividissem os números sem o sinal e depois aumentassem o quociente em uma unidade, conseguiriam realizar a divisão de forma correta, encontrando seu resto e escrevendo os algorítimos da divisão.

Foi necessário fazer uma rápida revisão sobre módulo de um número e sobre intervalo, pois, na questão de número quatro, eles tinham conhecimento de quais seriam os restos possíveis.

Porém, tiveram um pouco de dificuldade de formalizar o resultado na forma de intervalos como pedia a questão. Uma média de 80 por cento dos estudantes precisou de auxílio, nunca vez que desconheciam a possibilidade de realização da operação nesses moldes e, novamente, a calculadora não apresentava o resultado esperado.

Achei o resultado incrível, pois, apesar de ser fácil, os estudantes tiveram que pensar sobre a divisão e não simplesmente realizar contas de forma automática. Também foi interessante ver o caminho reflexivo no tocante aos restos das divisões, sendo esses sempre menores do que o divisor.

Atividade 3: Aprendendo congruências.

Competência do Ensino Fundamental da BNCC desenvolvida:

> "Competência 2: Desenvolver o raciocínio lógico, o espírito de investigação e a capacidade de produzir argumentos convincentes, recorrendo aos conhecimentos matemáticos para compreender e atuar no mundo"(BRASIL, 2018, p.267).

A princípio, fiquei um pouco apreensiva com o fato de introduzir o conceito de congruência modular para os estudante de Ensino Médio, mas fui surpreendida pela receptividade. Os discentes não questionaram o fato deste conteúdo não estar nos livros didáticos como eu temia; ao contrário, por ser uma atividade de fácil entendimento, houve uma participação efetiva por parte deles.

Um fato interessante aconteceu em uma das turma onde, inicialmente, deixei que eles respondessem a primeira questão e, somente depois, quando fiz explicações sobre a segunda questão, um estudante me questionou: "Professora, mas por que a senhora não disse antes que bastava subtrair os dois números? Desta forma fica bem mais fácil."

Respondi, então, que a princípio queria observar como verificariam as congruências sozinhos, sem ajuda de algoritmos ou de qualquer tipo de método, ou seja, simplesmente usando a lógica e as divisões com números negativos. Dessa madeira, desta forma não estariam realizando contas de forma mecânica e sem pensarem no que estão fazendo, Mas desenvolvendo um raciocínio matemático. Foi, portanto, uma atividade leve e a maioria dos estudantes não tiveram grandes dificuldades.

Atividade 4: Um pouco mais sobre congruências.

Competência do Ensino Fundamental da BNCC desenvolvida:

> "Competência 2: Desenvolver o raciocínio lógico, o espírito de investigação e a capacidade de produzir argumentos convincentes, recorrendo aos conhecimentos matemáticos para compreender e atuar no mundo"(BRASIL, 2018, p.267).

No primeiro momento, ficou claro para os estudantes as passíveis formas de se escrever um número, levando em consideração o módulo de divisão e os possíveis restos. Quando falamos de números pares e ímpares, também ficou claro a relação com a divisibilidade por dois.

Já na segunda questão, a maioria dos estudantes se lembrou das relações de congruências estudadas na aula anterior e, por isto, conseguiu encontrar os valores esperados. Não obstante, encontraram dificuldades com os valores negativos que foram solicitados no item b, para os quais foi necessária a minha interferência.

Na questão três, que foi colocada como desafio, tivemos uma média de dois estudantes por sala que conseguiram chegar à expressão desejada, sem que lhes fosse dado qualquer tipo de explicação.

Por fim, os problemas das questões quatro e cinco foram entendidos e solucionados com algumas intervenções.Destaco que achei proveitosa a utilização da congruência modular para resolver um problema relativamente simples que poderia estar presente no conidiano dos estudantes.

Atividade 5: Equações Diofantinas.

Objetivos do DC-GO almejados:

> "Modelar problemas que envolvem variáveis que se relacionam por meio de duas grandezas específicas, investigando informações apresentadas em textos que trazem dados decorrentes de situações socioeconômicas, técnico-científicas etc, para resolver problemas relativos à realidade do/a estudante"(GO-EMMAT302C).

Não houve aplicação da atividade 5, uma vez que após realizar a atividade 4 e perceber que os estudantes foram capazes de encontrar o valor de x

em congruências do tipo $x \equiv b (mod\ m)$, optei por não adentrar no conteúdo das Equações Diofantinas. Logo, essa atividade fica como sugestão para uma ampliação da sequência didática em questão.

Atividade 6: Operações com módulo m.

Competência da BNCC desenvolvida:

> "Competência 2 : Desenvolver o raciocínio lógico, o espírito de investigação e a capacidade de produzir argumentos convincentes, recorrendo aos conhecimentos matemáticos para compreender e atuar no mundo"(BRASIL, 2018, p.306).

Habilidade da BNCC desenvolvida:

> "(EM13MAT306): Resolver e elaborar problemas em contextos que envolvem fenômenos periódicos reais (ondas sonoras, fases da lua, movimentos cíclicos, entre outros) e comparar suas representações com as funções seno e cosseno, no plano cartesiano, com ou sem apoio de aplicativos de álgebra e geometria."(BRASIL, 2018).

Começamos a atividade relembrando as aulas anteriores em que conseguimos determinar os restos possíveis para cada divisor e a forma como podemos escrever os números conforme o módulo que iremos usar. Desta forma, a compreensão dos estudantes sobre restos residuais foi facilitada.

Porém, quando da realização das operações, ocorreram alguns erros como, por exemplo, a soma e multiplicação por 0, além de dúvidas sobre a forma de utilização dos restos residuais para substituir os resultados das operações.

Acredito, contudo, que essa aula foi fundamental para o processo de codificação e decodificação das mensagens criptografadas.

Atividade 7: Você já ouviu falar em Criptografia?

Competência da BNCC desenvolvida:

> "Competência 1: Reconhecer que a Matemática é uma ciência humana, fruto das necessidades e preocupações de diferentes culturas, em diferentes momentos históricos, e é uma ciência viva, que contribui para solucionar problemas científicos e tecnológicos e para alicerçar descobertas e construções, inclusive com impactos no mundo do trabalho"(BRASIL, 2018, p.267).

Primeiramente apresentei o tema Criptografia, expondo seu conceito e como tem sido usada ao longo do tempo, depois fiz a exibição de um vídeo sobre o assunto (TECMUNDO, 2024). Ao final, expliquei como usaríamos os restos das divisões para trocar por letras do nosso alfabeto.

Foi um momento muito produtivo; durante as explicações, retomei as aulas anteriores de forma a facilitar o processo de compreensão; os estudantes perceberam como pode ser feita a codificação e decodificação das mensagens. Avaliei de forma

positiva a participação em todas as turmas.

Atividade 8: A Criptografia de César.

Competência da BNCC desenvolvida:

> "Competência 2: Desenvolver o raciocínio lógico, o espírito de investigação e a capacidade de produzir argumentos convincentes, recorrendo aos conhecimentos matemáticos para compreender e atuar no mundo"(BRASIL, 2018, p.267).

Ao realizarem as questões um e dois da atividade, a maioria dos estudantes não teve dúvidas e conseguiu encontrar a mensagem sem dificuldades, porém, quando foram codificar as mensagens para trocarem com os colegas, houve confusão.

Nas duas primeiras turmas onde apliquei essa atividade, não obtive o resultado esperado. Os estudantes não entenderam que, ao final da adição, deveriam trocar as letras novamente, também não havia ficado claro para eles que deveriam codificar para que o colega tentasse decodificar.

Com certa dificuldade, houveram estudantes que conseguiram codificar da forma correta, mas, quando a decodificação foi iniciada, nos deparamos com outro problema. As divisões negativas, embora já tivessem sido objeto de uma atividade anterior, identificaram-se como um grande obstáculo.

Portanto, quando entrei na terceira turma, mudei um pouco a estratégia e expliquei de forma mais clara e incisiva o que deveria ser feito. Exemplifiquei com mais detalhes no quadro como deveria ser feita a codificação, realizando passo a passo e desta vez os resultados foram positivos. Em vista disso, reproduzi o mesmo processo na quarta e quinta turma nas quais apliquei essa atividade, obtendo, então, o resultado esperado.

Cada mencionar que alguns estudantes descobriram uma forma diferente de encontrar as letras que correspondiam a números negativos sem ter que fazer as tão temidas divisões, o que facilitou a resolução para a turma toda. Usaram, pois, a barra de relação entre letras e números que estava na atividade.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

R	S	T	U	V	W	X	Y	Z
18	19	20	21	22	23	24	25	26

Nesse sentido localizaram a letra codificada, começaram a contar usando a chave oposta até chegar na letra esperada. Mas quando a barra acabava antes da letra ser encontrada, voltavam ao início e continuavam a contagem formando um ciclo, remetendo à técnica o bastão cifrador dos espartanos e ao disco de César.

Os estudantes se divertiram e até mencionaram que iriam utilizar a Criptografia como método de cola nas provas. Acredito que gostaram da experiência e um estudante, inclusive disse que agora iria se comunicar secretamente dessa forma.

Após a realização dessa atividade, foram feitos alguns ajustes a fim de melhorar a compreensão dos estudantes e pude aplicar novamente em duas turmas de

primeira série, turmas essas que também estavam realizando as atividades anteriores.

Atividade 9: Criptografia com chave vetor.

Competência desenvolvida:

> "Competência 2: Desenvolver o raciocínio lógico, o espírito de investigação e a capacidade de produzir argumentos convincentes, recorrendo aos conhecimentos matemáticos para compreender e atuar no mundo"(BRASIL, 2018, p.267).

Posteriormente, foi o momento de introduzir maiores complexidades na forma de criptografar. Expliquei como deveriam ser feita a codificação usando vetores e reforcei o fato de que quanto maior a quantidade de números contidos no vetor, maior será a segurança dos dados.

Desta vez, a realização da atividade, foi mais tranquila , porque mesmo usando vetores, o que em um primeiro momento acreditei que dificultaria o entendimento por parte dos estudantes, eles já haviam compreendido a ideia da codificação e quase não tiveram dúvidas. Outro sim, foi corrente a decodificação e, sem maiores dificuldades as mensagens foram decifradas.

Antes de realizarmos a atividade 10 que traz uma revisão sobre matrizes, achei interessante mostrar a eles o filme "Enigma, o jogo da imitação". A obra mostra a utilização da Criptografia durante a Segunda Guerra Mundial e, através dela, o surgimento de uma máquina idealizada por um Matemático que deu origem ao que chamamos hoje de computador.

Enquanto os estudantes assistiam ao filme, pude perceber a importância dos nossos estudos para a compreensão de várias cenas onde é possível observar o uso da Criptografia. Alguns estudantes fizeram, ainda, comentários do tipo "Era isso que a gente estava fazendo".

Atividade 10: Revisando multiplicação de matrizes.

Habilidade da BNCC desenvolvida:

> "(EM13MAT301): Resolver e elaborar problemas do cotidiano, da Matemática e de outras áreas do conhecimento, que envolvem equações lineares simultâneas, usando técnicas algébricas e gráficas, com ou sem apoio de tecnologias digitais"(BRASIL, 2018, p.306).

A atividade 10 faz uma revisão sobre multiplicação de matrizes, conteúdo que foi trabalhado com os estudantes no primeiro semestre do ano.

O processo transcorreu sem dificuldades, e percebi que os discentes tiveram tranquilidade em realizar as multiplicações comparado ao início do ano letivo. Acredito que tal fato se deve à maturidade adquirida em relação ao conteúdo.

Atividade 11: Revisando matriz inversa.

Habilidade da BNCC desenvolvida:

> "(EM13MAT301): Resolver e elaborar problemas do cotidiano, da Matemática e de outras áreas do conhecimento, que envolvem equações lineares simultâneas, usando técnicas algébricas e gráficas, com ou sem apoio de tecnologias digitais"(BRASIL, 2018, p.306).

Nessa atividade, os estudantes foram desafiados a encontrar a matriz inversa à matriz dada. A maior dificuldade encontrada foi na resolução dos sistemas que surgiram através da multiplicação das matrizes inversas igualadas à matriz identidade. Sendo assim, ficou clara a importância do domínio de conteúdos anteriores para o avanço nos cálculos da aritmética.

Atividade 12: Criptografia com chave matriz.

Competência da BNCC desenvolvida:

> "Competência 2: Desenvolver o raciocínio lógico, o espírito de investigação e a capacidade de produzir argumentos convincentes, recorrendo aos conhecimentos matemáticos para compreender e atuar no mundo"(BRASIL, 2018, p.267).

Durante a atividade de número doze, os estudantes tiveram que codificar e decodificar mensagens usando como chave de codificação algumas matrizes e, conforme previsto tiveram dificuldades e precisaram do auxílio da professora. No entanto, ao finalizar a atividade, mais da metade da turma conseguiu decifrar corretamente a Criptografia com o uso da chave matriz.

Atividade 13: A Criptografia no sistema eleitoral brasileiro.

Competência da BNCC desenvolvida:

> "Competência 1: Utilizar estratégias, conceitos, definições e procedimentos matemáticos para interpretar, construir modelos e resolver problemas em diversos contextos, analisando a plausibilidade dos resultados e a adequação das soluções propostas, de modo a construir uma argumentação consistente"(BRASIL, 2018, p.267).

> "Competência 4: Fazer observações sistemáticas de aspectos quantitativos e qualitativos presentes nas práticas sociais e culturais, de modo a investigar, organizar, representar e comunicar informações relevantes, para interpretá-las e avaliá-las crítica e eticamente, produzindo argumentos convincentes"(BRASIL, 2018, p.267).

Nessa atividade, falamos sobre a segurança das urnas eletrônicas, que são aparelhos criptografados. Por conseguinte, apresentado aos estudantes recortes do site do TSE - Tribunal Superior Eleitoral onde é falado sobre a criptografia.

Segundo o Tribunal Superior Eleitoral:

"A criptografia digital é um mecanismo de segurança para o funcionamento dos programas computacionais. Como os dados tornam-se embaralhados, eles ficam inacessíveis a pessoas não autorizadas.
O Tribunal Superior Eleitoral usa algoritmos proprietários de cifração simétrica e assimétrica, de conhecimento exclusivo do TSE.
O boletim de urna é criptografado de forma segmentada, assinado digitalmente e transmitido.
Além da Criptografia, existe a descriptografia, que é o processo pelo qual são recuperados os dados previamente criptografados, isto é, eles são desembaralhados. É um mecanismo de segurança para o funcionamento dos programas computacionais.
No recebimento do boletim de urna ocorre:

- a validação da compatibilidade da chave pública de assinatura digital do boletim de urna com a chave privada do Totalizador;
- a descriptografia do boletim de urna de forma segmentada;
- a leitura do boletim de urna descriptografado;
- O armazenamento do boletim de urna criptografado e descriptografado"(BRASIL, 2024).

Posto isso a turma foi dividida em grupos e fizemos uma simulação de uma votação na qual o resultado seria entregue em forma de mensagens criptografadas. Alguns estudantes se dispuseram em fazer papel de *hackers* que tentavam decodificar as mensagens.

O desafio foi o uso da Criptografia de formas variadas, podendo o estudante usar o método que achar melhor para codificar sua mensagem. Neste momento, com a turma dividida em grupos, os estudantes escolheram entre cifra de Cézar, chave vetor ou chave matriz.

Encontrei grupos mais ousados que se arriscaram na chave matriz, alguns ainda inseguros, usaram a cifra de Cézar, porém, a maioria optou pela chave vetor. Na entrega de mensagens aos estudantes - *hackers*, nenhum conseguiu descifrar as mensagens, a decodificação só aconteceu posteriormente após a revelação das chaves.

4.4 21° Congresso de Pesquisa, Ensino e Extensão

Após a elaboração e aplicação da sequência didática, tive a oportunidade de apresentar este trabalho no CONPEEX 2024 na modalidade Mostra da Pós-Graduação *Stricto Sensu* e *Lato Sensu*. Esse momento foi bastante enriquecedor, contando com a presença de professores e estudantes do mestrado profissional em Matemática em Rede Nacional (PROFMAT).

Inicialmente, foi apresentado um resumo do trabalho desenvolvido, disponível no Apêndice B, publicado nos Anais do Congresso. Em seguida, foi enviado um *banner*, elaborado conforme os padrões estipulados pela comissão organizadora do evento, que também se encontra no Apêndice B. Durante a apresentação do trabalho, o *banner* ficou em exposição para a explanação.

O relato da aplicação da sequência didática mostrou como é possível articular teoria e prática, integrando saberes matemáticos e históricos com o cotidiano

dos estudantes. A vivência escolar, alinhada ao envolvimento em eventos como o CONPEEX, fortaleceu o propósito da pesquisa: demonstrando que a Criptografia pode ser uma ponte entre a Matemática escolar e os desafios do mundo digital. No próximo capítulo, sintetizaremos os principais resultados alcançados, refletindo sobre as contribuições do trabalho e caminhos futuros.

Capítulo 5

Considerações finais

A realização deste trabalho possibilitou uma reflexão aprofundada sobre a importância da Aritmética Modular e suas aplicações no contexto da Criptografia, revelando o potencial da Matemática enquanto ferramenta, não apenas teórica, mas também prática e atual. Ao relacionar conteúdos clássicos, como Divisões Euclidianas, com situações concretas de proteção de dados e segurança da informação, foi possível construir uma ponte entre o conhecimento matemático e o cotidiano dos estudantes.

Conforme demonstrado, a Matemática é usada para codificar e descodificar mensagens; possibilitando uma maior proximidade com o mundo tecnológico e proporcionando à aritmética um lugar de destaque no cenário contemporâneo.

Para mais, restou evidente que aplicações matemáticas contribuíram para os avanços da comunicação no decorrer da história humana. Seu desenvolvimento está, pois, associado à criação da Teoria dos Códigos e de máquinas codificadoras que, atualmente, identificamos como computadores.

Mostramos que o uso da Criptografia, apesar de antigo, tem aplicabilidade atual e é uma ciência fundamental para um bom desenvolvimento da Teoria da Informação.

A proposta de sequência didática apresentada demonstrou-se eficaz para tornar o ensino da Matemática mais significativo, uma vez que proporcionou aos estudantes o contato com temas desafiadores de forma acessível e contextualizada. As atividades desenvolvidas, alinhadas à Base Nacional Comum Curricular (BNCC) (BRASIL, 2018), permitiram o desenvolvimento de competências e habilidades essenciais à formação integral dos estudantes do Ensino Médio.

No decorrer do processo os estudantes puderam constatar grande aplicabilidade na proteção de informações sigilosas. Foram sanadas várias dúvidas referentes às divisões usando números negativos e sobre a utilização da aritmética modular, possibilitando a construção de uma nova perspectiva de resolução de questões ferramenta útil para o desempenho em Olimpíadas de Matemática e até mesmo no Exame Nacional do Ensino Médio - ENEM.

Almejamos utilizar a presente dissertação como material complementar em futuras aulas de Matemática. Acreditando no valor pedagógico da abordagem exposta, nosso objetivo é enriquecer a prática docente com estratégias que aproximem os conteúdos escolares da realidade dos estudantes, despertando o interesse e favorecendo uma aprendizagem mais crítica, reflexiva e conectada com as demandas do

mundo contemporâneo.

Além disso, teorizamos a possibilidade de expandir este trabalho para outros contextos educacionais, de forma a contribuir para o fortalecimento do ensino da Matemática por meio de temas interdisciplinares e aplicados, como a Criptografia. Assim, reafirmamos nosso compromisso com uma educação matemática que ultrapasse a engessada estrutura de memorização de fórmulas e promova a construção de sentido, a valorização do saber e a formação de cidadãos mais preparados para os desafios da sociedade moderna.

Nesse diapasão Simon Singh asseverou em sua obra O Livro dos Códigos:

> "Já se falou que a Primeira Guerra Mundial foi a guerra dos químicos, devido ao emprego, pela primeira vez, do gás mostarda e do cloro, que a Segunda Guerra Mundial foi a guerra dos físicos devido à bomba atômica. De modo semelhante, se fala que uma Terceira Guerra Mundial seria a guerra dos matemáticos, pois os matemáticos terão o controle sobre a próxima grande arma de guerra, a informação"(SINGH, 2003, p.13).

Acreditamos que a proposta desenvolvida possa contribuir para estudos futuros voltados à inserção prática da Criptografia no Ensino Médio, ampliando o repertório dos estudantes e mostrando que a Matemática está longe de ser um saber meramente teórico. Pelo contrário, temas como a Aritmética Modular e a Teoria dos Números ainda reservam grande potencial para aplicações educacionais e tecnológicas, especialmente no contexto crescente da segurança da informação.

Apêndice A

Atividade 1:

O algoritmo da divisão.

Dizemos que um número inteiro a é divisível por um número inteiro b quando o resto dessa divisão for igual a zero.

1- Resolva as seguintes divisões usando somente números inteiros no quociente e não se esqueça de escrever o resto dessas divisões.

Ex: 52 dividido por 3:

$$\begin{array}{r|l} 52 & 3 \\ \hline 1 & 17 \end{array}$$ Lembre-se que 52 é o dividendo, 3 é o divisor, 17 é o quociente e 1 é o resto.

a)37 dividido por 5.
b) 150 dividido por 4.
c) 282 dividido por 6.
d) 1345 dividido por 2.
e) 360 dividido por 11.

2- Usando o algoritmo da divisão, escreva todas as divisões que você resolveu usando a operação inversa a multiplicação e depois adicione o resto para que a igualdade seja satisfeita.

Ex: 52 dividido por 3, temos que $52 = 17.3 + 1$

a) 37 dividido por 5.
b) 150 dividido por 4.
c) 282 dividido por 6.
d) 1345 dividido por 2.
e) 360 dividido por 11.

3- Agora, pense e responda às seguintes questões:

a) É possível encontrar um resto maior do que o divisor?
b) O que acontece se tivéssemos um resto maior do que o divisor?

c) O resto pode ser igual ao divisor?

d) O que aconteceria se o resto fosse igual ao divisor?

e) Sendo assim você sabe dizer quais são os restos possíveis na divisão por 2? E por 3? E por 10?

4- João comprou um saco de balinhas e dividiu entre seus 25 colegas de classe. Primeiramente, ele deu 5 a cada um de seus colegas, mas logo ele percebeu que havia sobrado 53 balinhas no saco e resolveu continuar com a distribuição até que não sobrasse mais balinhas, porém a quantidade recebida por eles deve ser igual.

a)Quantas balinhas João ainda poderá entregar a cada colega?

b) Depois dessa última distribuição, quantas balinhas sobraram no saco?

c) Quantas balinhas a mais seriam necessárias para que João conseguisse entregar mais uma para cada um?

d) Quantas balinhas tinham dentro do saco?

e) Escreva o algoritmo da divisão da quantidade de balinhas presentes no saco pela quantidade de colegas que tinha na classe de João.

Atividade 2:

Divisibilidade com números negativos.

Sabemos que a divisão não é uma operação comutativa como acontece nos casos da adição e da multiplicação. Então $10 : 2 \neq 2 : 10$. E quando falamos de divisão com números inteiros, podemos também usar os números negativos, mas nesse caso usaremos sempre como resto um número positivo.

Ex.$_1$: 52 dividido por -3.

52	-3
1	-17

Logo $52 = (-17).(-3) + 1$.

Ex.$_2$: -52 dividido por 3.

-52	3
2	-18

Logo $-52 = (-18).(3) + 2$.

1- Resolva as seguintes divisões usando números inteiros no quociente e não se esqueça de que o resto sempre deve ser um número inteiro positivo.

a) 37 dividido por -5.

b) -37 dividido por 5.

c) -150 dividido por 4.

d) -282 dividido por 6.

e) -1345 dividido por 2.

f) -1345 dividido por -2.

g) -360 dividido por 11.

h) -360 dividido por -11.

2- Usando o algorítimo da divisão, escreva todas as divisões que você resolveu usando a operação inversa a multiplicação e depois adicione o resto para que a igualdade seja satisfeita.

3- Agora, pense e responda as seguintes questões:

a) É possível encontrar um resto maior do que o módulo do divisor?
b) O que acontece se tivéssemos um resto maior do que o módulo do divisor?
c) O resto pode ser igual ao módulo do divisor?
d) O que aconteceria se o resto fosse igual ao módulo do divisor?
e) Sendo assim, você sabe dizer quais são os restos possíveis na divisão por 2? E por 3? E por 10?

4-Portanto, podemos concluir que o conjunto dos restos r da divisão de um número inteiro por x será:
$0 \leq r < x$, sendo r um inteiro positivo.
Agora escreva o conjunto dos restos possíveis na divisão de:

a) Um inteiro por 5.
b) Um inteiro por -5.
c) Um inteiro por 7.
d) Um inteiro por -7.

Atividade 3:

Aprendendo congruências.

Observe a definição a seguir: sejam a, b e m números inteiros, se os restos das divisões de a e de b por m são iguais, então dizemos que a e b são congruentes módulo m.
E quando isso acontecer usaremos a seguinte notação: $a \equiv b(mod\ m)$.
Ex.$_1$: 151 dividido por 5.

151	5
1	30

26 dividido por 5.

26	5
1	5

Nesse caso, o resto da divisão de 151 e de 26 por 5 são iguais a 1, logo:

$$151 \equiv 26(mod\ 5).$$

Ex.$_2$: 20 dividido por 6 deixa resto 2.
Enquanto 2 dividido por 6 também deixa resto 2.

2	6
2	0

Logo, $20 \equiv 2(mod\ 6)$.
Observe que -4 dividido por 6 também deixa resto 2.

-4	6
2	-1

Logo, $20 \equiv -4(mod\ 6)$.
E 80 dividido por 6 deixa resto 2.

80	6
2	13

Logo, $20 \equiv 80(mod\ 6)$.

Agora é a sua vez

1- Verifique se as congruências a seguir estão corretas e assinale v para verdadeiro e f para falso.

a)$53 \equiv 3(mod\ 5)$ ( ).
b)$53 \equiv 8(mod\ 5)$ ( ).
c)$53 \equiv 14(mod\ 5)$ ( ).
d)$53 \equiv -2(mod\ 5)$ ( ).
e)$53 \equiv -3(mod\ 5)$ ( ).
f)$-53 \equiv 2(mod\ 5)$ ( ).
g)$-53 \equiv -2(mod\ 5)$ ( ).
h)$55 \equiv 0(mod\ 5)$ ( ).
i)$55 \equiv 5(mod\ 5)$ ( ).
j)$55 \equiv 16(mod\ 5)$ ( ).
k)$55 \equiv 20(mod\ 5)$ ( ).
l)$-55 \equiv 20(mod\ 5)$ ( ).
m)$-55 \equiv -20(mod\ 5)$ ( ).

Observe que quando temos uma congruência $151 \equiv 26(mod\ 5)$ então,

$$151 - 26 \equiv 0(mod\ 5).$$

Isso significa que, para verificar a veracidade de uma congruência, basta subtrair os dois dividendos e obter resto 0. Neste caso, $151 - 26 = 125$ que é divisível por 5, logo deixa resto 0 na sua divisão por 5.

2- Veja se você respondeu de forma correta aos itens da questão anterior. Fazendo as subtrações necessárias e se a congruência não for verdadeira, encontre o resto diferente de zero que a tornaria possível.

a)$53 \equiv 3(mod\ 5)$ então:
b)$53 \equiv 8(mod\ 5)$ então:
c)$53 \equiv 14(mod\ 5)$ então:
d)$53 \equiv -2(mod\ 5)$ então:
e)$53 \equiv -3(mod\ 5)$ então:
f)$-53 \equiv 2(mod\ 5)$ então:
g)$-53 \equiv -2(mod\ 5)$ então:

h)$55 \equiv 0(mod\ 5)$ então:
i)$55 \equiv 5(mod\ 5)$ então:
j)$55 \equiv 16(mod\ 5)$ então:
k)$55 \equiv 20(mod\ 5)$ então:
l)$-55 \equiv 20(mod\ 5)$ então: m)$-55 \equiv -20(mod\ 5)$ então:

Atividade 4:

Um pouco mais sobre congruências.

Sendo r o resto da divisão de a por m, temos que $a \equiv r(mod\ m)$ e como $0 \leq r < m$ o nosso resto r poderá ser qualquer número natural entre 0 e $m-1$, ou seja $r \in \{0, 1, 2, 3, \ldots, m-1\}$ e esse conjunto é um sistema completo de restos.

Ex.: Um número qualquer, quando dividido por três, poderá ter resto igual a $0, 1$ ou 2.

Então, um número divisível por 3 pode ser escrito da forma $3k$. Logo, um número não divisível por 3 pode ser escrito da forma $3k+1$ ou $3K+2$.

1- Seguindo o mesmo raciocínio, responda:

a) Quando dividimos um número por 7, quais serão as formas que podemos escrevê-lo?

b) Quando um número for par de qual forma podemos escrevê-lo?

c) Quando um número for ímpar, de que forma podemos escrevê-lo?

Outro fato importante é quando temos, por exemplo, um número x tal que $x \equiv 12\ (mod\ 3)$, sabemos que o resto da divisão de 12 por 3 é igual ao resto da divisão de x por 3, então o resto da divisão de x por 3 é igual a 0. Logo $x \equiv 0(mod\ 3)$

Como os restos das divisões de um número por três serão sempre: 0, 1, 2 ou 3, observe que:

- Se $x \equiv 12(mod\ 3) \Rightarrow x \equiv 0(mod\ 3)$ e pode ser escrito da forma $3k$.
- Se $x \equiv 13(mod\ 3) \Rightarrow x \equiv 1(mod\ 3)$e pode ser escrito da forma $3k+1$.
- Se $x \equiv 14(mod\ 3) \Rightarrow .\ x \equiv 2(mod\ 3)$e pode ser escrito da forma $3k+2$.
- Se $x \equiv 15(mod\ 3) \Rightarrow x \equiv 0(mod\ 3)$e pode ser escrito da forma $3k$.

Sendo que k pertence aos números inteiros.

2- Agora, tente descobrir :

a)Quais os valores possíveis de x sabendo que $x\equiv 85(mod\ 10)$ sendo x menor do que 100 e maior que 0. Lembre-se que o resto da divisão de 85 por 10 é igual a 5.

b)Quais são os valores possíveis de x sabendo que $x\equiv 43(mod\ 10)$ sendo x menor do que 50 e maior que -20 .

3- Desafio: Escreva uma expressão algébrica que possa encontrar qualquer valor possível para x dentro do universo dos números inteiros, sendo $x \equiv 43 (mod\ 10)$.

4- Construa uma expressão algébrica parecida com a que você encontrou na questão anterior para o seguinte problema:

A turma da 3ª série fez uma festa a fim de arrecadar dinheiro para o pagamento das becas dos 45 estudantes formandos. Porém, após a festa, o tesoureiro da turma não quis revelar o valor arrecadado, dissendo apenas que o dinheiro pagará o aluguel de todas as becas e ainda sobrará 135 reais. Além disso, já tinha sido estimado pela turma e confirmado pelo tesoureiro que o valor arrecadado teria sido acima de 4500 e a baixo de 5000. Sendo x o valor arrecadado, quais são os possíveis valores para x ?

5- Usando a expressão que você construiu, encontre a solução desse problema.

6- Ainda em relação ao problema apresentado, se o aluguel de cada beca custa mais do que 105 reais, quais serão os valores possíveis para x?

Atividade 5:

Equações Diofantinas.

Agora que você já sabe sobre congruências, vamos entender o que é uma Equação Diofantina e como resolvê-la. Considere a congruência:

$$16x \equiv 2 (mod\ 7),$$

Ela pode ser escrita como $16x - 2 \equiv 0 (mod\ 7)$ que corresponde a $16x - 7y = 2$, chamamos esse tipo de equação de Equações Diofantinas.

1- Sendo assim, escreva as seguintes congruências em forma de Equações Diofantinas:

a) $21x \equiv 1 (mod\ 5)$.
b) $53x \equiv 3 (mod\ 2)$.
c) $20x \equiv -4 (mod\ 6)$.
d) $-2x \equiv 5 (mod\ 3)$.
e) $20x \equiv 3 (mod\ -2)$.
f) $-32x \equiv 4 (mod\ -8)$.

Agora, vamos tentar encontrar soluções para essas equações. Usaremos como exemplo a equação.

$$2x + 5y = 9.$$

Primeiramente temos que verificar se ela realmente admite solução e, para isso, temos que encontrar o MDC entre 2 e 5, que sabemos ser igual a 1.

Se o MDC dividir o resultado da equação, no caso 9, a equação admite solução. Como 1 divide 9, ela terá solução.

2- Observe as equações a seguir e verifique se elas possuem solução, se sim assinale com S se não assinale com N.

a) $3x + 2y = 3$ ( ).
b) $3x + 6y = 5$ ( ).
c)$5x + 6y = 5$ ( ).
d)$3x + 6y = 1$ ( ).
e) $3x + 2y = 1$ ( ).
f)$5x + 6y = 1$ ( ).

Voltando à nossa equação $2x + 5y = 9$, quando calculamos o MDC entre 2 e 5, usamos os algorítimos de Euclides sucessivamente.

Quociente:	-	2	2
Dividendo:	5	2	1
Resto:	1	0	

Assim, podemos verificar que $5 = 2 \cdot 2 + 1$ então $1 = 5(1) - 2(2)$.
Logo, $x = 2$ e $y = 1$.
Então, se substituirmos na equação $2x + 5y = 9$ teremos:

$$2(2) + 5(1) = 9.$$

Mas se considerarmos o conjunto dos números inteiros, teremos várias outras soluções como, por exemplo:

- $2 \cdot (7) + 5 \cdot (-1) = 9$, Logo $x = 7$ e $y = -1$.
- $2 \cdot (-3) + 5 \cdot (3) = 9$, Logo $x = -3$ e $y = 3$.
- $2 \cdot (-8) + 5 \cdot (5) = 9$, Logo $x = -8$ e $y = 5$.
- $2 \cdot (12) + 5 \cdot (-3) = 9$, Logo $x = 12$ e $y = -3$.

Desta forma, $(2, 1)$ é apenas uma solução particular de $2x + 5y = 9$.

Verifique que quando:

- $x = 2 - 5(0) = 2$ e $y = 1 + 2(0) = 1 \Rightarrow (2, 1)$.
- $x = 2 - 5(-1) = 7$ e $y = 1 + 2(-1) = -1. \Rightarrow (7, -1)$.
- $x = 2 - 5(1) = -3$ e $y = 1 + 2(1) = 3. \Rightarrow (-3, 3)$.
- $x = 2 - 5(2) = -8$ e $y = 1 + 2(2) = 5. \Rightarrow (-8, 5)$.
- $x = 2 - 5(-2) = 12$ e $y = 1 + 2(-2) = -3. \Rightarrow (12, -3)$.

podemos escrever como solução geral de uma Equação Diofantina:

$$x = x_0 - tb,\ y = y_0 + ta; t \in \mathbb{Z}.$$

Então, para essa equação, temos: $x = 2 - 5t$ e $y = 1 + 2t$, sendo t pertencente ao conjunto dos números inteiros.

3- Agora é a sua vez, encontre uma solução particular para as equações a seguir e depois generalize-a.

a) $2x - 3y = 1$.

b) $21x - 5y = 1$.

c) $156x - 11y = 1$.

Atividade 6:

Operações com módulo m.

Quando dividimos um número por dois, podemos encontrar como resto 0 ou 1. Já se a divisão for por três, encontraremos resto 0, 1 ou 2. Na divisão por cinco, encontramos como resto 0,1,2,3 e 4. Assim fica fácil perceber que em uma Divisão Euclidiana por m, sendo $m \in \mathbb{Z}$ e $m > 1$, encontraremos resto $0, 1, 2, \ldots, m - 1$.

Obs.: Os restos de uma divisão módulo cinco pertencem ao conjunto $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Agora, se somarmos dois desses restos, ex: $2 + 3 = 5$, veremos que o 5 não faz parte do conjunto de restos, logo dividindo novamente pelo módulo 5, encontraremos resto 0. Se $3+4 = 7$, dividindo por 5 encontraremos resto 2.

Veja agora alguns exemplos de tabelas de adição e multiplicação de resto em $\mathbb{Z}_m$.

Tabela de adição em $\mathbb{Z}_3$ (só pode ser usado resto 0,1,2):

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Observe que em uma adição do conjunto dos números inteiros não seria possível somar dois números positivos e obter zero. Porém, em uma operação módulo m isso é possível.

Tabela de multiplicação em $\mathbb{Z}_4$ (só pode ser usado resto 0,1,2,3):

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

1- Construa a tabela de adição em $\mathbb{Z}_4$.

2- Construa a tabela de multiplicação em $\mathbb{Z}_3$.

Atividade 7:

Você já ouviu falar em Criptografia?

Trabalhando com aprendizagem significativa.

1-Após a exibição do vídeo pelo professor, discussão sobre o assunto e curiosidades sobre o tema.

2- Em duplas, usem os *chromebooks*, computadores disponibilizados pela escola, ou o próprio celular para que realizar uma pesquisa sobre Criptografia. Vocês poderão escolher um dos temas a seguir:

- O origens da Criptografia;
- Ligação da Criptografia com a Matemática;
- O uso da Criptografia nos dias de hoje;
- Curiosidades sobre a Criptografia;
- A história da Criptografia;
- Uso da Criptografia em guerras.

Depois, escrevam um pequeno texto com o que eles encontraram de interessante.

Atividade 8:

A Criptografia de César.

Primeiramente, para que possamos entender como funciona a Criptografia, vamos associar às letras do nosso alfabeto números naturais.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

R	S	T	U	V	W	X	Y	Z
18	19	20	21	22	23	24	25	26

Usaremos o zero para simbolizar os espaços vazios entre as letras, e assim teremos uma sequência de elementos em $\mathbb{Z}_{27}$.

1- Agora tente decifrar o código a seguir:

$$17, 21, 5, 0, 12, 5, 7, 1, 12.$$

O famoso imperador romano Júlio César, usava esse tipo de codificação, porém, por ser muito fácil de decodificar, César usava chave 3 para se comunicar com seus generais e, por esse motivo, esse tipo de codificação ficou conhecido como a cifra de César.

Vamos entender como isso era feito. Júlio César pegava o código que queria passar e adicionava 3 em cada número, por exemplo, a mensagem 17, 21, 5, 0, 12, 5, 7, 1, 12 se transformaria em 20, 24, 8, 3, 15, 8, 10, 4, 15.

2- Pense um pouco e tente descodificar essa mensagem passada por Júlio César a um de seus generais (lembre-se que no conjunto $\mathbb{Z}_{27}$ não usamos números negativos).

$$4, 23, 4, 20, 24, 8, 3, 22, 4, 5, 4, 7, 18.$$

3- Porém, Júlio César, para dificultar ainda mais a decodificação da mensagem, trocava os números que foram adicionados pelas novas letras correspondentes. Sendo assim, descubra essa mensagem passada por ele:

YHQFHPRV.

4- Vamos agora usar a chave $x = 10$ para codificar uma mensagem, siga os passos:

- Você escolhe a mensagem e codifica;
- Depois troque essa mensagem com a do colega ao lado;
- Então, tente descodificar a mensagem que você recebeu do seu colega;

Não esqueça que quando o número é maior do que 26 você terá que usar a classe residual desse número em $\mathbb{Z}_{27}$.

Atividade 9:

Criptografia com chave vetor.

Vimos na atividade anterior que podemos codificar mensagens usando a cifra de César, mas existem formas de dificultar ainda mais a quebra da codificação, como por exemplo, usando uma chave vetor $v = (x, y, z)$ no lugar de uma simples chave x.

Ex_1.: Vamos codificar a Mensagem QUE LEGAL usando a chave vetor $v = (1, 5, 3)$.

Primeiramente, use a tabela de numeração de letras para encontrar:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

R	S	T	U	V	W	X	Y	Z
18	19	20	21	22	23	24	25	26

Q	U	E		L	E	G	A	L
17	21	5	0	12	5	7	1	12

Agora vamos somar de três em três usando sempre a sequência de números do vetor 1, 5, 3.

$$17 + 1 = 18.$$

$$21 + 5 = 26.$$

$$5 + 3 = 8.$$

$$0 + 1 = 1.$$

$$12 + 5 = 17.$$

$$5 + 3 = 8.$$

$$7 + 1 = 8.$$

$$1 + 5 = 6.$$

$$12 + 3 = 15.$$

E o código será: 18, 26, 8, 1, 17, 8, 8, 6, 15.

1- Quando usamos a chave vetor $v = (1, 5, 3)$ para codificar, poderíamos usar a chave $v = (-1, -5, -3)$, mas isso não será possível pois estamos considerando somente o universo dos números naturais módulo 27. Desta forma, você terá que usar o vetor $v = (26, 22, 24)$. Sabendo disto, descodifique a mensagem que foi codificada com a chave vetor $v = (1, 5, 3)$:

$$2, 17, 8, 8, 23, 12, 2.$$

Ex_2.: Agora vamos codificar a Mensagem QUE LEGAL usando a chave vetor $v = (10, 27, 20)$:

$17 + 10 = 27$ que é igual a 0 em $\mathbb{Z}_{27}$.
$21 + 27 = 48$ que é igual a 21 em $\mathbb{Z}_{27}$.
$5 + 20 = 25$.
$0 + 10 = 10$.
$12 + 27 = 39$ que é igual a 12 em $\mathbb{Z}_{27}$.
$5 + 20 = 25$.
$7 + 10 = 17$.
$1 + 27 = 28$ que é igual a 1 em $\mathbb{Z}_{27}$.
Teremos: $0, 21, 25, 10, 12, 25, 17, 1$.

2-Quando usamos a chave vetor $v = (10, 27, 20)$ para codificar a mensagem, qual será a chave vetor para decodifica-la? Decodifique essa mensagem.

3- Explique como você conseguiu encontrar a chave vetor que descodifica a mensagem.

4- Descodifique as mensagens a seguir que foram codificadas com chave vetor $v = (10, 27, 20)$:

a)$14, 5, 14, 10, 3, 25, 1, 20, 8$.

b) VIVADUNE.

Quanto mais aumentarmos o número de coordenadas do vetor, v maior será a segurança do sistema e mais difícil será a quebra da codificação.

5- Vamos agora usar chave vetor $v = (8, 12, 5, 2)$ para codificar uma mensagem, siga os passos:

- Você escolhe a mensagem e codifica;
- Depois, troque essa mensagem com a do colega ao lado;
- Agora tente descodificar a mensagem que você recebeu do seu colega;

Não esqueça que, quando o número é maior do que 26, você terá que usar a classe residual desse número em $\mathbb{Z}_{27}$.

Atividade 10:

Revisando multiplicação de matrizes.

Agora vamos usar matrizes para codificar mensagens. Primeiramente, vamos lembrar que, quando uma matriz é representada na forma $M_{2\cdot 3}$, significa que ela possui duas linhas e três colunas, por exemplo:

$$M_{2\cdot 3} = \begin{pmatrix} 2 & 5 & 1 \\ 1 & 3 & 0 \end{pmatrix}.$$

Mas para ser possível a multiplicação entre duas matrizes, o número de colunas da primeira tem que ser exatamente igual ao número de linhas da segunda e, ao final, teremos uma matriz com o número de linhas da primeira e o número de colunas da segunda, por exemplo:

$$M_{2\cdot 3} \cdot M_{3\cdot 1} = M_{2\cdot 1}.$$

Outro fato importante e fundamental é sempre multiplicamos uma linha da primeira por uma coluna da segunda, por exemplo:

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 17 \\ 21 \end{pmatrix} = \begin{pmatrix} 2.17 + 5.21 \\ 1.17 + 3.21 \end{pmatrix} = \begin{pmatrix} 139 \\ 80 \end{pmatrix}.$$

1- Calcule as multiplicações das matrizes a seguir:

a)$\begin{pmatrix} 3 & 7 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 5 \\ 9 \end{pmatrix} =$

b) $\begin{pmatrix} 10 & 2 & 1 \\ 3 & 8 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 5 \\ 7 \end{pmatrix} =$

c) $\begin{pmatrix} 2 & 0 & 9 \\ 1 & 5 & 10 \\ 3 & 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} 11 \\ 2 \\ 5 \end{pmatrix} =$

d) $\begin{pmatrix} 12 & 1 & 6 \\ 3 & 8 & 1 \\ 15 & 5 & 2 \end{pmatrix} \cdot \begin{pmatrix} 20 \\ 10 \\ 15 \end{pmatrix} =$

e) $\begin{pmatrix} 1 & 5 & 2 & 1 \\ 8 & 4 & 0 & 2 \\ 2 & 10 & 3 & 0 \\ 0 & 2 & 1 & 10 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 2 \\ 5 \end{pmatrix} =$

Atividade 11:

Revisando matriz inversa.

Definindo uma matriz identidade.

Matriz identidade é a matriz quadrada em que os elementos da diagonal principal são iguais a 1 e os demais elementos são iguais a 0. Sendo ela sempre uma matriz quadrada. Ex:

$$I_{2\cdot 2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} I_{3\cdot 3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Para encontrar a Matriz inversa M^{-1} de uma matriz M devemos usar:
$M \cdot M^{-1} = I$, sendo todas as matrizes quadradas com as mesmas dimensões.
Exemplificando: Vamos encontrar a matriz inversa de $M \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}$, ou seja:

$$M^{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

.

Como a matriz M é uma matriz quadrada da forma $2 \cdot 2$, então também usaremos uma matriz identidade $2 \cdot 2$.

Logo:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Sabemos que $M \cdot M^{-1} = I$, então:

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix};$$

$$\begin{pmatrix} 2a + 5c & 2b + 5d \\ 1a + 3c & 1b + 3d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Assim:

$$2a + 5c = 1.$$
$$2b + 5d = 0.$$
$$a + 3c = 0.$$
$$b + 3d = 1.$$

Logo, teremos:

$$\begin{cases} 2a + 5c = 1 \\ a + 3c = 0 \end{cases}$$

Então:

$$a = -3c;$$
$$2(-3c) + 5c = 1;$$
$$-6c + 5c = 1;$$
$$-c = 1;$$
$$c = -1.$$

Então:

$$a = -3.(-1) = 3.$$

Analogamente:

$$\begin{cases} 2b + 5d = 0 \\ b + 3d = 1 \end{cases}$$

Assim:

$$b = 1 - 3d;$$
$$2(1 - 3d) + 5d = 0;$$
$$2 - 6d + 5d = 0;$$
$$2 - d = 0;$$
$$-d = -2;$$
$$d = 2.$$

Então:

$$b = 1 - (3.2) = 1 - 6 = -5.$$

Montamos então a matriz inversa $M^{-1}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 3 & -5 \\ -1 & 2 \end{pmatrix}$.

Faça agora a atividade a seguir.

1- Encontre as inversas das seguintes matrizes:
a)$A = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$.

b) $B = \begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix}$.

c) $C = \begin{pmatrix} 1 & 4 \\ 0 & 2 \end{pmatrix}$.

d) $D = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{pmatrix}$.

e) $E = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 3 & 1 \\ 1 & 2 & 0 \end{pmatrix}$.

Atividade 12:

Criptografia com chave matriz.

Outra forma de proteger mensagens criptografadas é usando multiplicação de matrizes.

Por exemplo, vamos codificar a mensagem **QUE LEGAL**, agora com o uso de matrizes.

Primeiro, vamos observar os números que estão associados às letras do nosso alfabeto, lembrando que justamente por isto usaremos $\mathbb{Z}_{27}$.

Q	U	E		L	E	G	A	L
17	21	5	0	12	5	7	1	12

Depois, devemos agrupar as letras da mensagem conforme a chave que iremos usar. Neste caso, iremos usar uma matriz dois por dois que será multiplicada por uma matriz dois por um e, ao final, teremos uma matriz dois por um. Sendo assim, vamos agrupar as letras de dois em dois, sem esquecer do espaço entre as palavras:

Para codificar, usaremos a matriz $\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}$.

Então faremos:

$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} Q \\ U \end{pmatrix}$.

$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} E \\ 0 \end{pmatrix}$.

$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} L \\ E \end{pmatrix}$.

$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} G \\ A \end{pmatrix}$.

$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} L \\ 0 \end{pmatrix}$.

1- Agora é com você, substitua as letras por números e realize a multiplicação, depois substitua novamente por letras.

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} ? \\ ? \end{pmatrix} = \begin{pmatrix} ?+? \\ ?+? \end{pmatrix} \equiv \begin{pmatrix} ? \\ ? \end{pmatrix} (mod\ 27), = \begin{pmatrix} letra \\ letra \end{pmatrix}.$$

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} ? \\ ? \end{pmatrix} = \begin{pmatrix} ?+? \\ ?+? \end{pmatrix} = \begin{pmatrix} ? \\ ? \end{pmatrix} (mod\, 27) = \begin{pmatrix} letra \\ letra \end{pmatrix}.$$

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} ? \\ ? \end{pmatrix} = \begin{pmatrix} ?+? \\ ?+? \end{pmatrix} = \begin{pmatrix} ? \\ ? \end{pmatrix} (mod\, 27) = \begin{pmatrix} letra \\ letra \end{pmatrix}.$$

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} ? \\ ? \end{pmatrix} = \begin{pmatrix} ?+? \\ ?+? \end{pmatrix} = \begin{pmatrix} ? \\ ? \end{pmatrix} (mod\, 27) = \begin{pmatrix} letra \\ letra \end{pmatrix}.$$

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} ? \\ ? \end{pmatrix} = \begin{pmatrix} ?+? \\ ?+? \end{pmatrix} = \begin{pmatrix} ? \\ ? \end{pmatrix} (mod\, 27) = \begin{pmatrix} letra \\ letra \end{pmatrix}.$$

Pronto, nossa mensagem foi codificada com a chave matriz $\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}$.

2-Então, escreva a mensagem codificada:

3-E agora? Se mandarmos essa mensagem codificada para alguém e entregarmos a chave matriz, como essa pessoa fará para descodificar?

a)Para descodificar essa mensagem, ela terá que encontrar a matriz inversa da matriz chave $\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}$. Então, encontre a matriz inversa.

b) Após encontrar a matriz inversa, multiplique-a pelas matrizes letras que foram codificadas.

$\begin{pmatrix} ? & ? \\ ? & ? \end{pmatrix} \cdot \begin{pmatrix} letra \\ letra \end{pmatrix} =$

Ao final, o destinatário encontrará as matrizes $\begin{pmatrix} Q \\ U \end{pmatrix} \begin{pmatrix} E \\ - \end{pmatrix} \begin{pmatrix} L \\ E \end{pmatrix} \begin{pmatrix} G \\ A \end{pmatrix} \begin{pmatrix} L \\ - \end{pmatrix}$.

Resultado na frase **QUE LEGAL**.

Claro que quanto maior for o número de linhas e colunas da matriz chave, maior será a dificuldade de descodificação da mensagem.

Obs.: Poderíamos usar então uma matriz chave 3 por 3, assim agruparíamos as letras de três em três, formando uma matriz letra 3 por 1. Ou 4 por 4 com matriz letra 4 por 1, e assim sucessivamente. Porém, a matriz chave deve ser sempre uma matriz quadrada.

4-Vamos usar uma matriz chave igual a $\begin{pmatrix} 1 & 2 \\ 4 & 0 \end{pmatrix}$ para codificar uma mensagem, siga os passos:

- Você escolhe a mensagem e codifica;
- Lembre-se que para que seja possível a multiplicação de duas matrizes o número de colunas da primeira tem que ser igual ao número de linhas da segunda. Então você deve usar uma matriz letra 2 por 1 para multiplicar com a matriz chave;
- Depois, troque essa mensagem com a do colega ao lado;
- Agora tente descodificar a mensagem que você recebeu do seu colega;

Lembre-se de encontrar a matriz inversa e não se esqueça que, quando o número for maior do que 26, você terá que usar a classe residual desse número em $\mathbb{Z}_{27}$.

Atividade 13:

A Criptografia no sistema eleitoral brasileiro.

Segundo o Tribunal Superior Eleitoral:

> "A criptografia digital é um mecanismo de segurança para o funcionamento dos programas computacionais. Como os dados tornam-se embaralhados, eles ficam inacessíveis a pessoas não autorizadas.
> O Tribunal Superior Eleitoral usa algoritmos proprietários de cifração simétrica e assimétrica, de conhecimento exclusivo do TSE.
> O boletim de urna é criptografado de forma segmentada, assinado digitalmente e transmitido.
> Além da Criptografia, existe a descriptografia, que é o processo pelo qual são recuperados os dados previamente criptografados, isto é, eles são desembaralhados. É um mecanismo de segurança para o funcionamento dos programas computacionais.
> No recebimento do boletim de urna ocorre:
>
> - a validação da compatibilidade da chave pública de assinatura digital do boletim de urna com a chave privada do Totalizador;
> - a descriptografia do boletim de urna de forma segmentada;
> - a leitura do boletim de urna descriptografado;
> - O armazenamento do boletim de urna criptografado e descriptografado". (BRASIL, 2024).

As urnas não são conectadas à internet. Após o encerramento da votação, os boletins de cada urna são transportados de forma física.

1- Vamos, então, fazer uma simulação do uso de Criptografia no sistema eleitoral. Em nossa simulação, teremos hackers que tentarão descodificar o boletim de urna. Siga os passos:

- Primeiro escolham 5 estudantes que serão os *hackers*.
- Depois, dividam-se em cinco grupos, esses representarão os colégios eleitorais de diferente estados.
- Escolham dois candidatos. Ex: candidato A e candidato B.
- Cada grupo terá que escolher uma chave para codificar o resultado da votação.
- O número de votos de cada candidato deverá aparecer no resultado codificado pelo grupo.
- A chave de codificação deve ser entregue somente ao professor que representará o cartório eleitoral.

- Os estudantes escolhidos como *hackers* deverão tentar descodificar o resultado, (cada um em um estado diferente, ou seja em um grupo diferente), antes que chegue até o professor.

  E boa sorte!

Apêndice B

Resumo CONPEEX

A Criptografia é uma técnica milenar que tem sido utilizada ao longo da história a fim de codificar e proteger mensagens importantes, principalmente em tempos de guerras. Porém, atualmente, com a popularização da *internet*, ela passou a ser usada em redes sociais, bancos digitais, proteção de senhas e vários outros aplicativos para garantir a privacidade de seus usuários. No mundo virtual, a Criptografia tem sido bastante explorada, tornando-se fundamental para nossa segurança digital.

Pensando nisto, o presente trabalho traz como proposta o desenvolvimento de habilidades matemáticas em estudantes do ensino básico, através da codificação e decodificação de mensagens criptografadas, usando como base de cálculos a aritmética modular.

O objetivo de trazer o assunto "A Matemática das Criptografias" é mostrar aos estudantes a utilização prática da Teoria dos Números que, até pouco tempo, era considerada uma das áreas mais abstratas da Matemática e que, com o desenvolvimento da Teoria da Informação, esse conceito tem mudado completamente.

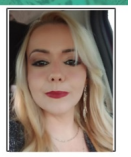
No entanto, para trabalhar tais habilidades, desenvolver-se-á uma sequência didática contendo 13 atividades com duração média de 50 minutos cada. Essas atividades foram construídas, primeiramente, de forma a aguçar a curiosidade dos estudantes, realizando pesquisas sobre o tema em questão.

No segundo momento, será feita uma retomada de conteúdos já estudados como, por exemplo, Divisão Euclidiana de números inteiros, multiplicação de matrizes e matrizes inversas. Em meio a essa retomada, introduziremos conteúdos sobre aritmética modular. Por fim, serão lançados desafios que consistem em codificar e descodificar mensagens trocadas entre estudantes, tudo, é claro, com o uso de muita Matemática.

Tal sequência didática deverá ser aplicada em turmas de Ensino Médio, de forma a produzir um relato de conclusões empíricas. No decorrer desse processo, espera-se ampliar o conhecimento dos discentes em aritmética, mostrando aplicações práticas para o tema e, ao final, o resultado almejado é a compreensão do uso da Matemática para a codificação e decodificação de mensagens.

21º CONPEEX 2024 Congresso de Pesquisa, Ensino e Extensão
BIOMAS DO BRASIL: DIVERSIDADE, SABERES E TECNOLOGIAS SOCIAIS
6 A 8 NOVEMBRO 2024
UFG UNIVERSIDADE FEDERAL DE GOIÁS

A MATEMÁTICA DAS CRIPTOGRAFIAS



Aline Márcia dos Santos
Instituto de Matemática e Estatística /Universidade Federal de Goiás

Mostra da Pós-Graduação Stricto Sensu e Lato Sensu

E-mail: alinemarcia@discente.ufg.br

INTRODUÇÃO

Ao longo da história a criptografia vem possibilitando a comunicação entre fontes autorizadas, e impendo fontes não autorizadas de terem acesso ao conteúdo dessas mensagens. Apesar da criptografia ser um método usado a milênios, somente a partir do século XX, durante a segunda guerra mundial e mais recentemente com o uso intensivo da internet, ganhou teoria própria e sua aplicação torna-se cada vez mais necessária no mundo atual, isso devido a segurança e a transmissão de informações nos sistemas digitais.

OBJETIVOS

Mostrar a professores e estudantes uma utilização prática da Teoria dos Números em codificações e descodificações de mensagens criptografadas, deixando claro a importância da matemática no processo de comunicação digital.

MÉTODOS

Revisão bibliográfica com elaboração de material específico numa proposta de ensino em Aritmética Modular para turmas do Ensino Médio da Educação Básica.

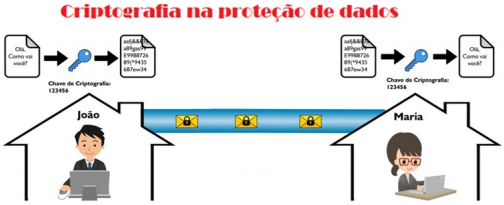
https://www.contabilidade-financeira.com/2015/02/cifra-de-cesar.html
https://radames.manosso.nom.br/bitabit/planilhas/criptografia-de-cesar-em-excel/

RESULTADOS

Foi desenvolvida uma sequência didática com 13 atividades, onde os estudantes retomaram conteúdos como divisões de números inteiros e multiplicação de matrizes. Durante a realização dessas atividades conseguimos resgatar conceitos e algoritmos que puderam facilitar nosso trabalho com a criptografia.

Algumas atividades tiveram o intuito de ampliar os conhecimentos em teoria dos números, como por exemplo, a introdução da aritmética modular, das operações módulo (m) e das equações diofantinas, tornando mais viável a verificação dos restos nas divisões euclidianas.

Os resultados foram satisfatórios, grande parte dos estudantes se envolveram no processo. Foi possível codificar mensagens e trocá-las com os colegas para que descobrissem como descodifica-las. Nem todos conseguiram no primeiro momento, mas ao final os estudantes compreenderam a lógica da teoria dos números no processo das comunicações digitais.



https://4future.com.br/index.php/2021/10/11/criptografia-chaves-simetricas-e-assimetricas/
https://tecnoblog.net/especiais/eniac-primeiro-computador-do-mundo-completa-65-anos/

CONCLUSÃO

Os tópicos de Aritmética Modular que foram abordados e usados em mensagens criptografadas, mostraram aos estudantes aplicações matemáticas que contribuíram para os avanços da comunicação ao longo do tempo. Sendo responsável pela criação da teoria dos códigos e por máquinas codificadoras que hoje chamamos de computadores.

Financiamento: Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) - Ministério da Educação (MEC).

Referências Bibliográficas

AUSUBEL, D. P. A aprendizagem significativa. *São Paulo*, 1982.

BARBOSA, R. M. *Descobrindo a Geometria Fractal-para a sala de aula*. [S.l.]: Autêntica, 2016.

BRASIL. *Base Nacional Comum Curricular*. 2018. <http://basenacionalcomum.mec.gov.br>. Acesso em: 28 abr. 2025.

BRASIL, T. S. E. *Criptografia*. 2024. Acesso em: 28 abr. 2025. Disponível em: <https://www.tse.jus.br/eleicoes/urna-eletronica/seguranca-da-urna/criptografia>.

COUTINHO, S. C. *Números Inteiros e Criptografia RSA*. 3. ed. Rio de Janeiro: IMPA, 2023. Acesso em: 28 abr. 2025. ISBN 978-85-244-0527-3. Disponível em: <https://www.dcc.ufrj.br/~collier/Books/RSA.html>.

FIARRESGA, V. M. C. *Criptografia e matemática*. 2010. Acesso em: 28 abr. 2025. Disponível em: <https://www.proquest.com/openview/c5ebf73531ef07ccf5d87ffc148a35a3/1?cbl=2026366&diss=y&pq-origsite=gscholar>.

FUSCO, C. A. da S.; COELHO, S. P. Um pouco da teoria dos números: da antiguidade até os dias atuais. *Ensino da Matemática em Debate*, v. 1, n. 2, 2014.

GIOVANNI, J. R.; CASTRUCCI, B. *A conquista da Matemática*. [S.l.]: Ftd, 2002.

GOIÁS. *Diretrizes Curriculares para o Componente Curricular de Geografia*. 2018. <https://www.seduce.go.gov.br/files/diretrizes/geografia.pdf>. Secretaria de Estado da Educação de Goiás. Acesso em: 28 abr. 2025.

HEFEZ, A. *Aritmética, Coleção PROFMAT, 1a edição*. [S.l.]: Sociedade Brasileira de Matemática, 2013.

KRISCHER, T. C. *Um estudo da máquina Enigma*. Dissertação (Mestrado) — Universidade Federal do Rio Grande do Sul, 2013. Acesso em: 28 abr. 2025. Disponível em: <https://lume.ufrgs.br/handle/10183/66106>.

MASINI, E. F. S.; MOREIRA, M. A. Aprendizagem significativa na escola. *Curitiba, PR: Crv*, 2017.

OLIVEIRA, V. M. d. Criptografia e a matemática. Mestrado Profissional em Matemática, 2021.

PAIS, L. C. *Didática da Matemática: uma análise da influência francesa*. [S.l.]: Autêntica, 2016.

POE, E. A. *Escaravelho de Ouro e outros Contos*. [S.l.]: L&PM Editores, 2011.

SANTOS, J. P. de O. *Introdução à teoria dos números*. [S.l.]: IMPA, 1998. v. 128.

SHOKRANIAN, S. *Criptografia para iniciantes*. [S.l.: s.n.], 2005.

SILVA, J. C.; GOMES, O. R. *Estruturas algébricas para licenciatura*. [S.l.: s.n.], 2020. v. 2.

SILVA, V. V. da. Números: Construção e propriedades. *Ed. UFG*, 2005.

SINGH, S. O livro dos códigos: A ciências do sigilo-do antigo egito à criptografia quântica. *Rio de Janeiro: Record*, 2003, p.13.

TECMUNDO. *Entenda o que é cripitografia*. 2024. Acesso em: 28 abr. 2025. Disponível em: <https://www.youtube.com/watch?v=u7HPHMxzMDk&t=5s>.