UNIVERSIDADE FEDERAL DE VIÇOSA

CRIPTOGRAFIA NO ENSINO BÁSICO

Alexandre Gonçalves Batista
Magister Scientiae

FLORESTAL - MINAS GERAIS
2024

ALEXANDRE GONÇALVES BATISTA

CRIPTOGRAFIA NO ENSINO BÁSICO

Dissertação Mestrado Profissional apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação em Matemática em Rede Nacional (Profissionalizante), para obtenção do título de *Magister Scientiae*.

Orientador: Luis F Goncalves Fonseca

FLORESTAL - MINAS GERAIS
2024

Ficha catalográfica elaborada pela Biblioteca da Universidade Federal de Viçosa - Campus Florestal

T
B333c
2024

Batista, Alexandre Gonçalves, 1983-
Criptografia no ensino básico / Alexandre Gonçalves Batista. – Florestal, MG, 2024.
1 dissertação eletrônica (119 f.): il. (algumas color.).

Inclui apêndices.
Orientador: Luís Felipe Gonçalves Fonseca.
Dissertação (mestrado) - Universidade Federal de Viçosa, Instituto de Ciências Exatas e Tecnológicas, 2024.
Referências bibliográficas: f. 119.
DOI: https://doi.org/10.47328/ufvcaf.2024.018
Modo de acesso: World Wide Web.

1. Aritmética . 2. Criptografia. 3. Planilhas eletrônicas. I. Fonseca, Luís Felipe Gonçalves, 1984-. II. Universidade Federal de Viçosa. Instituto de Ciências Exatas e Tecnológicas. Programa de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional. III. Título.

CDD 23. ed. 513

ALEXANDRE GONÇALVES BATISTA

CRIPTOGRAFIA NO ENSINO BÁSICO

Dissertação Mestrado Profissional apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação em Matemática em Rede Nacional (Profissionalizante), para

APROVADA: 23 de agosto de 2024.

Assentimento:

_____

Alexandre Gonçalves Batista
Autor

_____

Luis Felipe Goncalves Fonseca
Orientador

Essa dissertação mestrado profissional foi assinada digitalmente pelo autor em 28/10/2024 às 22:57:51 e pelo orientador em 29/10/2024 às 03:29:07. As assinaturas têm validade legal, conforme o disposto na Medida Provisória 2.200-2/2001 e na Resolução nº 37/2012 do CONARQ. Para conferir a autenticidade, acesse https://siadoc.ufv.br/validar-documento. No campo 'Código de registro', informe o código **BW9Y.85IA.TA97** e clique no botão 'Validar documento'.

Dedico este trabalho a minha esposa Fernanda, a amada filha Sofia, a minha mãe dona Ilda, meus irmãos, sobrinhos, tias e tios, primos e colegas que sempre torceram por mim.

AGRADECIMENTOS

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

Agradeço primeiramente a Deus, que sempre me conforta diante das adversidades e me capacita na busca dos meus objetivos. À Fernanda, minha esposa, pelo companheirismo e apoio que foi fundamental para realização do presente trabalho. À minha filha, Sofia, pela graça de sua presença que se transforma em combustível que me permite continuar em frente. À minha mãe pelo amor, cuidado e perseverança e meu irmão, Nando, por todo apoio. Aos meus tios e tias que sempre estiveram por perto, cuidando e me orientando. Aos amigos que sempre me incentivaram. Por fim, agradeço ao professor e orientador, Luis, pela confiança e ensinamentos, além de toda sua paciência e presteza no processo de orientação.

RESUMO

BATISTA, Alexandre Gonçalves, M.Sc., Universidade Federal de Viçosa, agosto de 2024. **Criptografia no Ensino Básico**. Orientador: Luis Felipe Goncalves Fonseca.

A criptografia, a cada dia que se passa, tem ficado mais em evidência na nossa sociedade. Muitas atividades humanas necessitam da transmissão segura e sigilosa de dados. Grande parte das pessoas desconhecem que, ao realizarem transações bancárias online, ou ao trocarem mensagens através de aplicativos em smartphone, utilizam pelo menos um método de criptografia como recurso de segurança.

Alguns modelos criptográficos têm interseção com conteúdos matemáticos trabalhados na educação básica. Nesse sentido, o estudo da criptografia tem se apresentado como uma estratégia promissora, uma vez que trabalha com modelagem de conteúdos matemáticos, aliados a uma base teórica desses conteúdos.

Nesta dissertação, apresentaremos a Criptografia de César, a Criptografia de funções afins e a Criptografia RSA. Com o objetivo de facilitar o processo de aprendizagem, trabalhamos com os programas Google Planilhas e Wolfram Alpha no processamento dos cálculos.

Destacamos que esses recursos foram utilizados com o objetivo de consolidar os conteúdos vistos em sala de aula. Acreditamos que o trabalho com o Google Planilhas possa, mesmo que de maneira rudimentar, ser um primeiro contato do aluno com uma linguagem de programação.

Palavras-chave: aritmética; criptografia; planilhas eletrônicas

ABSTRACT

BATISTA, Alexandre Gonçalves, M.Sc., Universidade Federal de Viçosa, August, 2024. **Cryptography in Elementary Education**. Adviser: Luis Felipe Goncalves Fonseca.

Cryptography, with each passing day, has become more evident in our society. Many human activities require secure and confidential transmission of data. Most people are unaware that, when carrying out transactions online banking, or when exchanging messages through smartphone applications, use at least one encryption method as a security feature.
Some cryptographic models intersect with worked mathematical content lated in basic education. In this sense, the study of cryptography has presented itself as a promising strategy, as it works with content modeling mathematical, combined with a theoretical basis of these contents.

In this dissertation, we will present Caesar's Cryptography, related functions and RSA Cryptography. With the aim of facilitating the process of learning, we work with Google Sheets and Wolfram Alpha programs in processing calculations.

We highlight that these resources were used with the objective of consolidating the content seen in the classroom. We believe that the Working with Google Sheets can, even in a rudimentary way, be a student's first contact with a programming language.

Keywords: arithmetic; cryptography; electronic spreadsheets

Lista de Figuras

Lista de Tabelas

Lista de Comandos para o Google Planilhas e Excel

Comando	Função
*	Inserir símbolo da multiplicação
/	Inserir o símbolo da divisão
CIRCUNFLEXO (^)	Inserir símbolo da potenciação
=MMC(A3:A6)	Calcular o mmc dos números inseridos nas células A3 até A6
=MMC(A3;A6) ou =LCM(A3;A6)	Calcular o mmc dos números inseridos nas células A3 e A6
=MDC(A3;A6) ou GCD(A3;A6)	Calcular o mdc dos números inseridos nas células A3 e A6
=PROCV(C2;A$2:B$27;2;0) ou =VLOOKUP(C2;A$2:B$27;2;0)	Procurar o valor C2 na tabela (A2 até B27) e retornar o número da coluna B que está na mesma linha do valor C2, porém na coluna A. O último parâmetro 0 é padrão.
=SOMA(C3:C7)	Calcular a soma dos números inseridos nas células C3, C4, C5, C6 e C7.
=MOD(A3;A6)	Calcular o resto da divisão euclidiana em que o dividendo está inserido na célula A3 e o divisor na célula A6.

Sumário

1

Introdução

Em diferentes épocas da humanidade, é possível perceber a utilização de um ou mais tipos de comunicações secretas relacionadas à criptografia. Geralmente, essa comunicação deveria ser sigilosa, pois nela estavam presentes táticas militares ou segredos de estados. Apesar de estar em evidência nos tempos atuais, a criptografia acompanha a história da humanidade há bastante tempo.

Um dos exemplos mais conhecidos do uso da criptografia foi a cifra de César, utilizada durante o Império Romano. Nos dias atuais, a criptografia desenvolve um papel importante na segurança de dados e informações. Encontra-se presente em aplicativos de mensagens como o WhatsApp.

As grandes transformações sofridas pelo mundo, principalmente na segunda metade do século XX, nos convidam a repensar acerca das metodologias de ensino e aprendizagem do conteúdo de matemática. A forma com que os seres humanos se relacionam entre si, com a natureza, com o trabalho e com o ensino vem sofrendo profundas transformações. Muitas dessas mudanças foram, e ainda são, provocadas pelo desenvolvimento da tecnologia da informação. Nesse sentido, repensar nossa prática pedagógica na busca do desenvolvimento de habilidades e capacidades dos estudantes que convirjam para a formação de indivíduos adaptados às tais transformações é fundamental. A BNCC [1] traz orientações nesse sentido.

> *No novo cenário mundial, reconhecer-se em seu contexto histórico e cultural, comunicar-se, ser criativo, analítico-crítico, participativo, aberto ao novo, colaborativo, resiliente, produtivo e responsável requer muito mais do que o acúmulo de informações. Requer o desenvolvimento de competências para aprender a aprender, saber lidar com a informação cada vez mais disponível, atuar com discernimento e responsabilidade nos contextos das culturas digitais, aplicar conhecimentos para resolver problemas, ter autonomia para tomar decisões, ser proativo para identificar os dados de uma situação e buscar soluções, conviver e aprender com as diferenças e as diversidades. (BRASIL, 2018a, p. 14).*

O estudo de alguns métodos de criptografia exige do estudante o desenvolvimento de algumas dessas características. Nesse sentido, esse trabalho foi construído. Ao

término do trabalho, esperamos que o leitor professor esteja apto para investigar tanto outros modelos de criptografia quanto utilizar softwares computacionais a favor da educação.

O presente trabalho inicia com uma revisão do conteúdo de aritmética. Neste tópico, iniciamos com a apresentação de alguns axiomas acerca do conjunto dos números inteiros. Seguimos com a apresentação das principais definições e teoremas, até chegarmos ao contéudo da aritmética modular. Esse último contéudo é a base do modelo de criptografia RSA. Para otimizar o tempo, apresentamos as demonstrações das proposições que estão diretamente ligadas à teoria apresentada nos métodos criptográficos utilizados aqui. As demais, deixamos a referência para o leitor.

Os testes de primalidade ganharam um capítulo a parte. Na criptografia RSA, o conhecimento acerca da primalidade de um determinado número é relevante. Sendo assim, apresentamos alguns testes de primalidade e os números de Fermat e Mersenne.

Num terceiro momento do trabalho, trazemos um contexto histórico da criptografia. Para além, apresentamos também como funcionam, teoricamente, os métodos de codificação, a saber: cifras de substituição, cifra de transposição, cifra afim e a cifra RSA com e sem assinatura.

Logo após, dedicamos um capítulo mostrando como realizar a codifição e decodificação de uma mensagem, utilizando cada um dos métodos apresentados. Para facilitar o procedimento e trazer uma visão mais tecnológica ao nosso estudo, apresentamos funcionalidades do Google Planilhas, que realizaram todo o trabalho repetitivo. Em alguns casos, conseguimos realizar programações no software, de modo que, ao mudarmos a mensagem ou os parâmetros do método de criptografia adotado, não é necessário nenhum grande esforço para realização da codificação ou decodificação. As planilhas ficaram automatizadas. O programa Wolfram Alpha nos auxiliou com os cálculos de congruências modulares com números grandes. Esse programa possui menor limitação do que o Google Planilhas, que por sua vez apresentou erros ao realizar alguns desses cálculos.

Para finalizar, disponibilizamos, nos apêndices, um plano de aula para cada método de cifra, utilizando os recursos computacionais citados. Para além, seguem atividades de aritmética do ensino básico.

O diferencial deste trabalho está na utilização do Google Planilhas como processador de cálculos. Desejamos evidenciar, para os estudantes, a necessidade de conhecer as propriedades matemáticas na programação. Portanto, antes de utilizar o Planilhas e o Wolfram, é importante que o professor tenha apresentado a teoria, explicado os algoritmos e prosposto alguns exercícios. A tecnologia deve ser utilizada como estratégia de consolidação do contéudo aprendido, bem como servirá ao propósito de familiarização dos estudantes com a interpretação de dados em planilhas e fórmulas (funções) utilizadas em ambientes de programação. Assim, desejamos uma leitura agradavél e proveitosa.

1.1 Objetivos

O objetivo geral deste trabalho é desenvolver estudos para professores e alunos do Ensino Fundamental II e Médio da criptografia, utilizando as cifras de substituição, cifras afins, e o método RSA com e sem assinatura; com o auxílio de programas computacionais. Aliado a isso, como objetivos específicos, apresentamos planos de estudos desses modelos criptográficos. Tais estudos buscam a consolidação do conhecimento e habilidades matemáticas, principalmente no campo da aritmética, presentes na grade curricular da BNCC. A modelagem matemática dos conteúdos, bem como a experiência com o uso de recursos computacionais, tanto pelo aluno quanto pelo professor, constituem-se como metas. Dessa forma, trazemos para o leitor professor, um produto educacional que contém a descrição de várias atividades realizadas no Google Planilhas, presentes no Capítulo 5, planos de aulas e atividades propostas que podem ser conferidos nos Apêndices.

1.2 Metodologia de Trabalho

A metodologia de pesquisa utilizada foi a leitura de trabalhos especializados em métodos criptográficos, pesquisa de funcionamento e comandos do Google Planilhas e do Wolfram Alpha, bem como uma revisão bibliográfica do conteúdo de aritmética. Foram realizados encontros semanais com o orientador, via Google Meet, para discussão e organização deste trabalho.

O tema dessa dissertação foi dividido em itens aplicados ou adaptados na educação básica. O objetivo é que o leitor professor tenha a sua disposição um material para complementar suas aulas.

2

Noções de Aritmética

A maioria dos métodos criptográficos tratados aqui tem a aritmética como alicerce. Sendo assim, torna-se necessário apresentar um resumo com definições, teoremas, proposições e demonstrações que são mais utilizadas nos estudos dessas criptografias.

É importante salientar que o objetivo deste capítulo não é trabalhar a disciplina de aritmética do Profmat na íntegra, Buscamos assim, disponibilizar uma fonte de consulta para o leitor que possui pouco contato com a disciplina. Contemplamos neste capítulo as operações de adição, multiplicação, divisão, divisibilidade, potenciação e operações módulo n .

Grande parte dos resultados apresentados neste capítulo advém da interpretação e consulta da obra "Aritmética", usada no curso de Mestrado profissional em Matemática (PROFMAT), escrita por Abramo Hefez, 3^a edição de 2022.

2.1 Números Naturais

A ideia de número está diretamente ligada às necessidades do ser humano. A princípio, essa ideia se relacionava com a atividade de contagem de elementos de um determinado conjunto, ganhando maior rigor no início do século XX com o trabalho do matemático italiano Giuseppe Peano. Com o conhecimento acerca do sistema de numeração decimal, Peano nos permite descrever precisamente o conjunto dos números naturais, baseando-se no conceito primitivo de "sucessor" e cinco axiomas, contando também com noções de conjuntos e funções. O conjunto dos números naturais é representado pelo seguinte conjunto de números:

$$\mathrm{N} = \{1, 2, 3, 4, ...\}.$$

A seguir, apresentamos os axiomas de Peano e algumas propriedades dos números naturais. As demonstrações bem como outras observações podem ser consultadas em Lima [4].

Axioma 2.1.1: Peano

i. Todo número natural tem um único sucessor.

ii. Números naturais diferentes têm sucessores diferentes.

iii. Existe um único número natural, chamado de *um* cuja representação é 1, que não é sucessor de nenhum outro número natural.

iv. Seja X um conjunto de números naturais, ou seja, $X \subset \mathbb{N}$. Se $1 \in X$ e se, além disso, o sucessor de todo elemento de X ainda pertence a X, então o conjunto X é o próprio conjunto $\mathbb{N}$.

O último item do Axioma de Peano, é também conhecido como *Axioma da Indução*, sendo frequentemente utilizado para demonstrar proposições referentes aos números naturais.

O conjunto dos números naturais possui duas operações fundamentais: a *adição* e a *multiplicação*. Dessa forma, sejam os números naturais n e p. Denotaremos o sucessor de n por $S(n) = n + 1$.

i. **Adição**: A *soma* $n + p$ é o número natural $S^p(n)$.

ii. **Multiplicação**: O *produto* np é o número natural obtido pela soma de p parcelas iguais a n.

Com as definições dessas operações, podemos demonstrar a validade das seguintes propriedades pelo axioma da indução:

a) *Transitividade*: se $m < n$ e $n < p$, então $m < p$.

b) *Tricotomia*: dados m e $n \in \mathbb{N}$, vale uma, e somente uma, das alternativas: $m = n$, $m < n$ ou $n < m$. Essa última alternativa pode ser substituída por $m > n$.

c) *Monotonicidade*: se $m < n$, para qualquer $p \in \mathbb{N}$, tem-se $m + p < n + p$ e $mp < np$.

d) *Boa-ordenação*: Todo subconjunto não-vazio $X \subset \mathbb{N}$ possui um menor elemento. Isso significa que existe um elemento n_0 em X que é menor do que qualquer outro elemento de X.

As demonstrações dessas propriedades fogem ao objetivo deste trabalho. No entanto o leitor pode consultá-las em Lima [4].

2.2 Números Inteiros

Admitimos a coleção de números expressa por $\mathbb{Z} = \{... - 3, -2, -1, 0, 1, 2, 3, ...\}$ como o conjunto dos Números Inteiros. Uma característica muito importante desse conjunto é ser fechado para as operações adição e multiplicação. Isso quer dizer que, quando realizamos qualquer uma dessas operações, com dois números inteiros, o resultado é, sempre, um número inteiro. No presente texto, é comum indicarmos a operação de multiplicação escrevendo ab, $a.b$ ou ainda $a \times b$. Segue lista de propriedades e operações dos números inteiros que são apresentadas de forma axiomática, como podemos encontrar em Hefez [3]. Em todos os itens abaixo, os números a, b, c, a' e b' são inteiros.

Axioma 2.2.1: i. Boa definição;

Se $a = a'$ e $b = b'$, então $a + b = a' + b'$ e $a.b = a'.b'$.

ii. Comutatividade;

$a + b = b + a$ e $a.b = b.a$.

iii. Associatividade;

$(a + b) + c = a + (b + c)$ e $(a.b).c = a.(b.c)$.

iv. Possuem elementos neutros;

$a + 0 = a$ e $a.1 = a$.

Além das propriedades acima, temos também que todo inteiro possui um simétrico aditivo ;

v. Para todo a , existe $b = (-a)$ tal que $a + b = 0$.

E a multiplicação é distributiva com relação à adição.

vi. $a.(b + c) = a.b + a.c$.

Para a e b números inteiros, dizemos que a é menor ou igual do que b ou b é maior ou igual do que a quando $b - a \in \mathbb{N} \cup \{0\}$. Representamos pela relação $a \leq b$.

2.3 Divisão nos Inteiros

Iniciamos este tópico, apresentando, por meio de uma definição, uma propriedade envolvendo números inteiros.

Definição 1: *Divisibilidade*
Sejam a e b dois números inteiros com $b \neq 0$. Dizemos que a divide b (escrevemos $a \mid b$) quando existe um número inteiro c tal que $b = a.c$.

Nessa situação, dizemos que a é um divisor inteiro de b, ou de modo equivalente, b é um múltiplo inteiro de a. Por outro lado, quando não existir esse número inteiro c, dizemos que a não divide b e representamos por $a \nmid b$.

Vejamos alguns exemplos que ilustram bem essas situações.

Exemplo 2.3.1: $(-3) \mid 12$, pois (-3) . (-4) =12.

Exemplo 2.3.2: $3 \nmid 5$, significa que 3 não divide 5. Sendo assim, nenhum inteiro c satisfaz a equação $5 = 3c$.

Antes de apresentamos algumas proposições acerca da divisibilidade dos inteiros, veremos uma definição.

Definição 2: $Valor Absoluto$

O valor absoluto (ou *módulo*) de um número inteiro a, indicado por $|a|$, é definido como:

$$|a| = \begin{cases} a, & \text{se } a \in \mathbb{N} \cup \{0\} \\ -a, & \text{caso contrário.} \end{cases}$$

Proposição 1: Sejam a, b e $c \in \mathbb{Z}$. Tem-se que:

i - $1 \mid a$, $a \mid a$ e $0 \mid a$.

ii - $0 \mid a \iff a = 0$.

iii - a divide b se, e somente se, $|a|$ divide $|b|$.

iv - Se $a \mid b$ e $b \mid c$, então $a \mid c$.

Segue demonstração do quarto item. Escolha feita por tratar-se da propriedade transitiva na divisibilidade. Os demais itens ficam como exercício para o leitor. Tanto essa demonstração quanto as provas das demais podem ser encontradas em Hefez ([3],p.32).

Demonstração. Sejam a, b, c, m e n números inteiros tais que: $b = a.n$ e $c = b.m$. Temos que $c = (a.n)m = a(n.m)$. Logo $a \mid c$. □

A seguir, veremos uma proposição que trata da divisibilidade relacionada com as duas operações desse conjunto: a soma e a multiplicação. Essas propriedades são importantes para o estudo de congruência modular. Suprimimos algumas demonstrações, no entanto, o leitor pode encontrar sua prova na íntegra em Shokranian ([7],p.6).

Teorema 2.3.1: Sejam a, b e c números inteiros. Se $c \mid a$ e $c \mid b$, então:

I - $c \mid (a + b)$, $c \mid (a - b)$ e $c \mid (b - a)$.

II - $c \mid (a.b)$.

III - Se $b \mid a$, então $b \mid a.t$ qualquer que seja o número t inteiro.

Demonstração. No item I - temos por hipótese, que exitem n e m inteiros tais que $a = c.n$ e $b = c.m$. Daí $a + b = c.n + c.m = c(n + m)$. Então $c \mid (a + b)$. As demais afirmações seguem de modo análogo.

No item II - considere $a = c.n$ e $b = c.m$, então temos $a.b = c.n.c.m = c(c.n.m)$. Daí segue o resultado.

O item III - é provado de maneira análoga ao anterior. □

O seguinte corolário pode ser entendido como a generalização dos resultados anteriores.

Corolário 1: Sejam a, b e c números inteiros. Se $c \mid a$ e $c \mid b$, então

$$c \mid (ax + by).$$

Demonstração. Do teorema anterior decorre que para todos $x, y \in \mathbb{Z}$,

$$(ax + by) = c.n.x + c.m.y = c(nx + my),$$

o que finaliza a demonstração. □

Vejamos alguns exemplos.

Exemplo 2.3.3: Se $5 \mid 10$ e $5 \mid 15$, então $5 \mid (10.2 + 15.3) = 65$.

Exemplo 2.3.4: Se $3 \mid -6$ e $3 \mid 9$, então $3 \mid [(-6).4 + 9.5]) = 21$.

Até o presente momento, trabalhamos, na maior parte das vezes, com a condição de que existe a relação de divisibilidade entre dois números inteiros quaisquer. Trataremos também das situações em que um número não é divisível por outro, exploraremos a aritmética dos restos, uma poderosa ferramenta para a realização de alguns métodos de criptografia.

Iniciamos essa discussão com um teorema conhecido como Divisão Euclidiana. Porém, antes devemos apresentar um axioma. Para além, devemos lembrar que dizemos que o conjunto X é *limitado inferiormente* quando existe a inteiro tal que $a \leq b$ para todo $b \in X$.

Axioma 2.3.1: *Princípio da Boa Ordenação em* $\mathbb{Z}$:
Se S é um subconjunto não vazio de $\mathbb{Z}$ que é limitado inferiormente, então S possui um menor elemento. Em particular, consideramos o número 1 como o menor elemento do conjunto $\mathbb{N}$.

Esse axioma pode ser visto como a generalização do axioma da Boa Ordenação, apresentado para os números naturais.

Proposição 2: *Propriedade Arquimediana.*
Sejam a,b pertencentes a $\mathbb{Z}$, com $b \neq 0$. Então existe $n \in \mathbb{Z}$ tal que $nb > a$.

Encontramos a demonstração completa dessa proposição em Hefez ([3],p.9), apresentada pelo autor como um corolário.

Teorema 2.3.2: (*Divisão Euclidiana*).
Sejam a e b dois números inteiros com $b \neq 0$. Existem dois unicos números inteiros q e r tais que

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

Demonstração. A seguinte demonstração é estruturada de acordo com Hefez ([3],p.37), no entanto justificamos, propositadamente, algumas relações, isso é o que diferencia o nosso trabalho da fonte pesquisada. É necessário demonstrar tanto a existência de q e r, quanto a unicidade desses números. Primeiramente, consideremos o conjunto

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

Começamos pela existência. Com base na propriedade arquimediana, podemos tomar um número $n \in \mathbb{Z}$ tal que $n(-b) > -a$. Logo $a - nb > 0$. Assim, temos que S é não vazio. Além disso, S é limitado inferiormente por zero. Então o Axioma da Boa Ordenação garante que existe $r \in S$ tal que, $r \leq s$ para todo $s \in S$. Percebemos que r é maior ou igual a 0. Agora basta mostrar que $r < |b|$. Suponhamos por absurdo que $r \geq |b|$. Isso implica que existe um número $s \in \mathbb{N} \cup \{0\}$ tal que $r = s + |b|$. Dessa forma, $0 \leq s < r$. Mas isso contradiz o fato de que r ser o menor elemento de S.

Suponha que (q,r), $(q',r') \in \mathbb{Z}^2$ são tais que

$$a = bq + r = bq' + r'$$

com $0 \leq r < |b|$ (*) e $0 \leq r' < |b|$ (**). Multiplicando (*) por -1 chegamos em $-|b| < -r \leq 0$ (***). Ao analisarmos as inequações (**) e (***), levando em conta que r e r' são inteiros não negativos, verificamos que $-|b| < -r \leq r' - r \leq r' < |b|$. Disso tudo, temos $|r' - r| < |b|$. Como

$$a = bq + r = bq' + r',$$

o que inplica $|b||q - q'| = |r' - r| < |b|$. Então $|b||q - q'| < |b|$ Ora, essa desigualdade só é possível caso $|q - q'| = 0$, fazendo com que q e q' sejam iguais. Consequentemente temos $r' = r$. □

Na divisão euclidiana, os termos da expressão $a = bq + r$ recebem cada um nome. O a é chamado *dividendo*, o *divisor* é b, o q é designado por *quociente* enquanto r é o *resto*. Além disso, quando o resto da divisão de a por b for igual a zero, dizemos que b divide a e que a divisão é exata.

Exemplo 2.3.5: $15 = 6 \times 2 + 3$.

Em que 15 é nosso dividendo, 6 é o divisor, 2 é o quociente e 3 o resto. De fato, podemos verificar que $0 \leq 3 < 6$.

Exemplo 2.3.6: - $11 = 5 \times (-3) + 4$.

Em que -11 é nosso dividendo, 5 é o divisor, - 3 é o quociente e 4 o resto. De fato, podemos verificar que $0 \leq 4 < 5$

2.4 Máximo Divisor Comum (MDC)

Sejam a,b,c inteiros tais que $a|b$ e $a|c$. Denominamos a como um *divisor comum* de b e c. A definição apresentada, está de acordo com Hefez ([3],p.58).

Definição 3: Máximo Divisor Comum.

Um número inteiro $a > 0$ é dito *máximo divisor comum* de b e c, o qual indicamos por $mdc(b, c)$, se esse número atende às seguintes condições:

i. a é um divisor comum de b e c;

ii. a é *divisível* por todo divisor comum de b e c.

Não é comum encontrarmos essa definição em livros didáticos do ensino fundamental. Na maioria das vezes, a segunda parte dessa definição é suprimida e o mdc de dois números inteiros não nulos é apresentado como o maior elemento dentre os divisores comuns a esses números. Chamamos a atenção para a importância desse trecho da definição, pois ele subsidia muitas demonstrações na Aritmética, como, por exemplo, a prova da existência do próprio Máximo Divisor Comum. A seguinte proposição traz algumas importantes propriedades do mdc para o nosso estudo.

Proposição 3: Propriedades do MDC
Sejam a e b dois inteiros não nulos. Suponhamos que $mdc(a,b)$ exista. Então:

i. $mdc(a,b) = mdc(b,a)$.

ii. $mdc(a,1) = 1$ e $mdc(a,a) = |a|$.

iii. $mdc(a,b) = mdc(-a,b) = mdc(a,-b) = mdc(-a,-b)$.

Demonstração. i. Notamos que a ordem em que se calcula o mdc não altera seu valor.

ii. Sabemos que o único divisor positivo de 1 é o próprio 1. Na segunda parte, o mdc está em módulo devido à definição.

iii. Podemos comprovar o resultado usando as propriedades de divisibilidade. Por exemplo, suponhamos que, $mdc(a,b) = c$. Então, $c|a$ e $c|b$. Pelo Item III - do Teorema 2.3.1, temos que $c|a(-1)$. Dessa forma, $mdc(a,b) = mdc(-a,b) = c$. □

A demonstração do próximo resultado pode ser encontrada na íntegra em Hefez ([3],p.59). Vejamos:

Lema 2.1: Sejam a, b e n números inteiros. Se $mdc(a, b-na)$ existe, então $mdc(a,b)$ existe e,

$$mdc(a,b) = mdc(a, b-na).$$

Demonstração. Iniciamos supondo que se existe $d = mdc(a, b-na)$, então d divide tanto a quanto $b-na$. Portanto $d \mid b-na+na = b$. Logo d é um divisor comum de a e b. Agora devemos mostrar que ele é múltiplo de qualquer divisor comum de a e b. Sendo assim, vamos supor que exista um inteiro c, tal que $c \mid a$ e $c \mid b$. Assim, temos que $c \mid b-na$. Dessa forma, $c \mid d$. Logo d é o máximo divisor comum de a e b □

Esse lema não prova a existência do mdc. No entanto, ele é, praticamente, a base do *algoritmo de Euclides* que demonstra a existência do mdc para quaisquer dois números inteiros positivos. Para mais esclarecimentos, o leitor pode encontrar o algoritmo, bem como sua demonstração em Hefez ([3],p.60-61).

Exemplo 2.4.1: 8 é o *mdc* de 16 e 40. De fato, os divisores comuns positivos desses dois números são {1, 2, 4 e 8}, e podemos notar que 8 é divisível por todos divisores comuns aos números dados.

Vamos calcular esse mdc usando o Lema 2.1.

Pelo lema temos que $mdc(a,b) = mdc(a, b - na)$, logo

$$mdc(16,40) = mdc(16, 40 - n.16).$$

Pondo $n = 2$, temos $mdc(16,40) = mdc(16, 40 - 32) = mdc(16, 8)$. Repetindo o processo, encontramos

$$mdc(8, 16) = mdc(8, 16 - 8) = mdc(8, 8) = 8.$$

Exemplo 2.4.2: 7 é o máximo divisor comum de 14 e 21. De fato, pois seus divisores positivos comuns são 1 e 7. Temos que $1|7$ e $7|7$.

Pelo Lema 2.1 temos que

$$mdc(a,b) = mdc(a, b - na),$$
$$\text{logo}$$
$$mdc(14,21) = mdc(14, 21 - 1.14) = mdc(7,14) = mdc(7, 14 - 7) = mdc(7, 7) = 7.$$

Veremos na prática, através de exemplos, como funciona o algoritmo de Euclides para determinar o mdc de dois números inteiros positivos.

Exemplo 2.4.3: Vamos calcular o *mdc* de 18 e 24 pelo algoritmo de Euclides. Agora utilizaremos um diagrama.

	1	
24	18	
6		

	1	3
24	18	6
6	0	

Posicionamos na segunda linha, os dois números na ordem decrescente. Logo após realizamos a divisão euclidiana do primeiro número pelo segundo. O quociente dessa divisão deve ser colocado acima do divisor (do número 18) e o resto, abaixo do 24(dividendo). Como a divisão não é exata, colocamos o resto (6) a direita do 18 e repetimos o procedimento. Como essa divisão é exata, significa que 6 é o maior divisor de 18 e 24.

Exemplo 2.4.4: Determine $mdc(60,25)$ pelo algoritmo de Euclides e o diagrama.

Resolução:

$60 = 2.\mathbf{25} + \mathbf{10}$ (dividimos o maior pelo menor número).

$25 = 2.\mathbf{10} + \mathbf{5}$ (dividimos o divisor anterior pelo resto anterior)

$10 = 2.\mathbf{5} + \mathbf{0}$ (dividimos o divisor anterior pelo resto anterior).

	2	2	2	
60	25	10	5	
10	5	0		

Como o resto da última divisão é igual a zero, paramos o procedimento. Voltamos à penúltima equação e o resto representa o mdc. Logo $mdc(60, 25) = 5$.

Esse algoritmo não só calcula o mdc, mas nos permite escrever o mdc como uma combinação dos números dados. Acompanhe.

$$\mathbf{5} = 25 - 2.10 = 25 - 2(60 - 2.25) = (-2).\mathbf{60} + 5.\mathbf{25}.$$

Exemplo 2.4.5: Escreva o mdc(18,24) como combinação dos números dados.

Resolução: Vimos que

$$24 = 18.1 + 6.$$

Além do mais, $6 = mdc$(18,24). Logo

$$6 = 24 + (-1) \times 18.$$

2.5 Números primos

Seja a um número natural maior do que 1. Dizemos que esse número é **primo** se possuir apenas dois divisores positivos, sendo um deles o número 1 e o outro o próprio a.

Segue, imediatamente da definição, duas consequências importantes. Comecemos admitindo dois números a e b primos.

i) Se $a \mid b$, então $a = 1$ ou $a = b$.

ii) Se $a \nmid b$, implica que o $mdc(a,b) = 1$.

Definição 4: Sejam a e b dois inteiros positivos. Dizemos que esses números são *primos entre si* ou *coprimos* se $mdc(a,b) = 1$.

Vejamos alguns exemplos.

Exemplo 2.5.1: Verifique que mdc(4,9) = 1 pelo algoritmo de Euclides.

Pelo algoritmo de Euclides, temos:
$9 = 2.\mathbf{4} + \mathbf{1}$ (dividimos o maior pelo menor número).
$4 = 4.\mathbf{1} + \mathbf{0}$ (dividimos o divisor anterior pelo resto anterior).
Ao voltarmos na penúltima equação, percebemos que o resto é 1. Logo ele é o mdc.

Exemplo 2.5.2: Calcule o mdc(7,55).

Pelo algoritmo de Euclides, temos:
$55 = 7.\mathbf{7} + \mathbf{6}$ (dividimos o maior pelo menor número).
$7 = 1.\mathbf{6} + \mathbf{1}$ (dividimos o divisor anterior pelo resto anterior).
$6 = 6.\mathbf{1} + \mathbf{0}$ (dividimos o divisor anterior pelo resto anterior).

Ao voltarmos na penúltima equação, percebemos que o resto é 1. Logo ele é o mdc.

Da mesma forma que fizemos antes, podemos escrever o mdc como uma expressão dos números dados. No primeiro exemplo, temos $mdc(4,9) = 1 = 1.\mathbf{9} + (-2)\mathbf{4}$.

No segundo,

$$mdc(7,55) = 1 = 1.\mathbf{7} - 1.6 = 1.\mathbf{7} - 1.(\mathbf{55} - 7.\mathbf{7}) = 8.\mathbf{7} + (-1).\mathbf{55}.$$

A proposição a seguir generaliza os resultados apresentados.

Proposição 4: Dados a e b inteiros positivos, existem x e y inteiros tais que,

$$mdc(a,b) = a.x + b.y.$$

A prova dessa proposição foge aos objetivos do trabalho, no entanto, o leitor, pode ler sua demonstração em Hefez ([3],p.63).

Como consequência dessa proposição, apresentaremos dois resultados. O primeiro deles o Colorário 2 . Já o segundo nos traz uma condição que amplia o entendimento da Proposição 4.

Corolário 2: Dois números a e b inteiros são *primos entre si* se, e somente se, existem dois inteiros x e y tais que $ax + by = 1$.

Demonstração. Supondo que a e b são primos entre si, pela definição, temos que $mdc(a,b) = 1$. Daí, pela Proposição 4, vem $a.x + b.y = mdc(a,b) = 1$. A primeira parte está concluída.

Reciprocamente, se $ax + by = 1$, e d é um divisor positivo comum de a e b, então $d|1$. Logo $mdc(a,b) = 1$. □

Teorema 2.5.1: Sejam a, b e c números inteiros. Então existem dois inteiros x e y tais que,

$$ax + by = c \text{ se, e somente se, } mdc(a,b) \mid c.$$

Demonstração. Na primeira parte da prova, vamos supor que $ax + by = c$ e mostrar que $mdc(a,b) \mid c$.

Todos os números dessa equação são inteiros, logo

$$\frac{a}{mdc(a,b)} = a_1, \text{ em que } a_1 \in \mathbb{Z} \text{ e } \frac{b}{mdc(a,b)} = b_1, \text{ com } b_1 \in \mathbb{Z}.$$

Pela Proposição 4, temos que $a_1x + b_1y = mdc(a_1, b_1)$. Nessa última equação, substituimos a_1 e b_1 pelas frações acima, logo depois multiplicamos ambos os membros por $mdc(a,b)$. Teremos como resultado:

$$ax + by = mdc(a,b).mdc(a_1,b_1) = c.$$

Mostramos que $mdc(a,b) \mid c$.

Para mostrarmos que a recíproca é verdadeira, inicialmente, consideremos que $mdc(a,b) \mid c$ e as mesmas relações envolvendo a_1 e b_1. Pela Proposição 4, segue que $a_1x + b_1y = mdc(a_1, b_1)$. Multiplicando ambos os membros por $mdc(a,b)$, teremos:

$$mdc(a,b)(a_1x) + mdc(a,b)(b_1y) = mdc(a_1, b_1).mdc(a,b).$$

Mas vimos que $mdc(a,b).a_1 = a$, o mesmo ocorre com b. Logo podemos escrever a última equação como,

$$ax + by = mdc(a_1, b_1).mdc(a,b) = c.$$

De fato, por hipótese, temos que c é o produto do $mdc(a,b)$ por um número inteiro. □

Após esses resultados, temos teoria suficiente para demonstrar um teorema conhecido como "Lema de Gauss". De acordo com Hefez ([3],64-65).

Lema 2.2: Lema de Gauss

Sejam a, b e c números inteiros.

$$\text{Se } a \mid b.c \text{ e } mdc(a,b) = 1, \text{ então } a \mid c.$$

Demonstração. A primeira parte da nossa hipótese indica que existe um inteiro d tal que $a.d = b.c$. A segunda parte nos revela que a e b são coprimos, logo o Corolário 2 garante a existência de inteiros x e y tais que $ax + by = 1$. Multiplicando essa última equação pelo inteiro c, teremos que $(a.c)x + (b.c)y = c$. Substituindo $b.c$ por $a.d$, chegamos a

$$c = (a.c)x + (a.d)y = a(cx + dy).$$

Sendo assim $a \mid c$. □

De posse desse último resultado, enunciaremos mais uma propriedade semelhante a que acabamos de mostrar. Essa propriedade foi publicada por Euclides em sua obra "Os Elementos".

Corolário 3: Corolário do Lema de Euclides

Sejam p um número primo e a e b dois inteiros quaisquer. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$

Demonstração. Começamos supondo que $p \mid ab$ e $p \nmid a$. Desse modo temos que $mdc(a,p) = 1$. Assim, pelo Lema 2.2, concluímos que $p \mid b$. De modo análogo, poderíamos supor que $p \nmid b$ e mostrar que $p \mid a$. □

Exemplo 2.5.3: $4 \mid 5 \times 12$, pois $4 \mid 12$.

Exemplo 2.5.4: Se $7 \mid 5 \times 14$, então $7 \mid 5$ ou $7 \mid 14$.

Voltando à análise de *primalidade*. Quando um número natural, maior do que 1, não é *primo*, dizemos então que ele é *composto*. Para mais, todo número n composto possui pelo menos um divisor natural n_k que será maior do que 1 e menor do que o próprio n.

Exemplo 2.5.5: Discuta a primalidade de 33.

O número 33 é composto, pois possui mais de dois divisores. Além disso, pode ser escrito como $33 = 3.11$, em que $1 < 3 < 11 < 33$

Em seguida, veremos um teorema essencial na discussão sobre os inteiros. Sua demonstração, bem como outros comentários, estão disponíveis em Hefez ([3],p.95).

Teorema 2.5.2: *Teorema Fundamental da Aritmética*

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

Demonstração. Ver prova de Hefez em ([3],p.95). □

Antes de encerrarmos esta seção, voltamos ao estudo de divisibilidade, agora envolvendo números primos. Os chineses, por volta de 500 anos antes de Cristo, já sabiam que $2 \mid a^2 - a$, em que a é um número inteiro qualquer. No entanto, a generalização desse resultado para um número p primo qualquer, é fruto do trabalho do francês Pierre de Fermat, publicado no século XVII. A demonstração do teorema que generaliza esse resultado pode ser encontrado em Hefez ([3],p.105) e inicia-se com a proposição do seguinte lema.

Lema 2.3: Seja p um número primo. Os números $\binom{p}{i}$, onde $0 < i < p$, são todos divisíveis por p.

Demonstração. O resultado desse lema é, facilmente, verificado para $i = 1$. Vamos supor então que $1 < i < p$. Dessa condição para i, tem-se, como podemos observar em Hefez ([3],p.22), que $i!\binom{p}{i} = p(p-1)...(p-i+1)$. Como $mdc(i!.p) = 1$, decorre que, pelo Lema 2.2, $i!\binom{p}{i} = p(p-1)...(p-i+1)$. Consequentemente:

$$\binom{p}{i} = p\frac{(p-1)...(p-i+1)}{i!}$$

O resultado está provado. □

Apresentaremos agora o enunciado e a prova do Pequeno Teorema de Fermat, cuja demonstração é realizada utilizando indução.

Para aprofundamento no assunto recomendamos Hefez ([3],p.10-13) como leitura.

Teorema 2.5.3: Pequeno Teorema de Fermat (PTF)

Dado um número primo p, tem-se que p divide o número $a^p - a$, para todo $a \in \mathbb{Z}$.

Demonstração. Como 2 é o único par que é primo, verifica-se que, $2 \mid (a^2 - a) = a(a-1)$, uma vez que algum desses dois fatores é par.

Verificamos o Teorema para os demais números primos. Mesmo que $a \in \mathbb{Z}$, basta verificar os resultados para $a \geq 0$, isto porque $p \mid (a^p - a)$ se, e só se, $p \mid (-a^p) - a$ ou $p \mid -(a^p - a)$. Verifica-se claramente que a proposição é verdadeira para $a = 0$, pois $p \mid 0$. Suponhamos então, que o resultado é válido para a, ou seja, $p \mid a^p - a$. Agora verificaremos que o resultado é válido para $a+1$, isto é, $p \mid (a+1)^p - (a+1)$. Pela identidade do binômio de Newton, temos: $(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + ... + \binom{p}{p-1}a + 1$. Então:

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

Pelo Lema 2.3 e pela hipótese de indução, temos que p divide o segundo membro da equação acima. Daí segue o resultado. □

Vejamos alguns exemplos para clarear as ideias.

Exemplo 2.5.6: Mostre que $14 \mid a^7 - a$, para todo $a \in \mathbb{Z}$

Solução:

Lembramos que todo número divisível por 14 é divisível por 2 e por 7 simultaneamente.

Tem-se que $2 \mid (a^7 - a) = a(a^6 - a)$. De fato, para a par, $2 \mid a$. Se a for ímpar, $(a^6 - a)$ é par.

Por outro lado, pelo PTF tem-se que $7 \mid a^7 - a$, concluindo a prova.

Do Pequeno Teorema de Fermat, surge um corolário que, frequentemente, é enunciado com o mesmo nome do teorema.

Corolário 4: Se p é um número primo e se a é um número natural não divisível por p, então $p \mid a^{p-1} - 1$.

Demonstração. Pelo Teorema 2.2, temos que $p \mid (a^p - a) = a(a^{p-1} - 1)$. Como $mdc(a,p) = 1$, pelo Lema 2.2 (Lema de Gauss), temos $p \mid a^{p-1} - 1$. □

2.6 Mínimo Múltiplo Comum. (MMC)

Voltaremos ao estudo de divisões exatas. Na Definição 1, vimos que b é um *múltiplo comum* de a e de c se $a|b$ e $c|b$. Um múltiplo comum que merece destaque é o *mmc*.

Definição 5: Mínimo Múltiplo Comum (MMC)

Um inteiro m, maior do que zero, é o *mínimo múltiplo comum* de dois números inteiros a e b se m possuir as seguintes propriedades:

I. m é um *múltiplo comum* de a e b e;

II. se c é um múltiplo comum de a e b, então $m \mid c$.

Por exemplo, 8 é múltiplo comum de 2 e 4, porém não é o mínimo múltiplo comum desses números. Temos que 4 também é múltiplo de 2 e 4, além disso $4 \mid 8$. Então $mmc(2,4) = 4$.

Percebemos que o item II da Definição 5 nos garante a unicidadde do mmc quando ele existe. Sejam m e m' dois mínimos múltiplos comuns de a e b. Temos que $m \mid m'$ e $m' \mid m$. Como esses números são inteiros não negativos, segue que $m = m'$.

Agora, suponha que m é o mmc de a e b, e que esses números possuem também um número c como múltiplo comum. Verifica-se que $m \mid c$. Se c for positivo, decorre que $m \leq c$. Logo m é o menor múltiplo comum de a e b.

Por meio das propriedades de divisibilidades estudadas até aqui. Pode-se verificar que

$$mmc(-a,b) = mmc(-a,-b) = mmc(a,-b) = mmc(a,b).$$

Desse modo, consideraremos sempre a e b inteiros não negativos.

Proposição 5: Dados dois números inteiros a e b, temos que $mmc(a,b)$ existe e, além disso, $mdc(a,b).mmc(a,b) = |ab|$.

Demonstração. Veja Hefez ([3],p.70) □

Ao observamos a Proposição 5, percebemos que podemos encontrar o mmc de dois números se conhecermos o seu mdc. Para isso, basta dividir o módulo do seu produto pelo mdc. Além disso, temos o corolário.

Corolário 5: Se a e b são números inteiros primos entre si, então $mmc(a,b) = |ab|$.

Demonstração. Sejam a e b números inteiros primos entre si. Temos $mdc(a,b) = 1$. Logo, pela Proposição 5, $mmc(a,b) = |ab|$. □

Podemos estender o cálculo de mmc para três ou mais números inteiros não nulos. Neste sentido, seja m o $mmc(a_1, a_2)$. Para três elementos, definimos

$$mmc(a_1, a_2, a_3) = mmc(a_1, (a_2, a_3)).$$

Para $n \geq 4$ elementos, definimos

$$mmc(a_1,a_2...a_n) = mmc(a_1,(mmc(a_2...a_n))) \ .$$

Vejamos alguns exemplos para ilustrar a teoria.

Exemplo 2.6.1: Encontraremos o $mmc(8, 10, 15)$.

Primeiramente, devemos notar que 8 e 15 são primos entre si, Então, $mmc(8, 10, 15) = mmc(10, 8.15) = mmc(10,120) = 120$.

Exemplo 2.6.2: Sabendo que o $mdc(45,75) = 15$, calcularemos o $mmc(45,75)$.

Visto que $mdc(45,75).mmc(45,75) = |45.75|$, temos

$$mmc(45,75) = \frac{|45 \times 75|}{15} = 3 \times 75 = 225.$$

2.7 Números inteiros módulo m

Nesta seção, apresentaremos a aritmética dos restos. Dessa noção aritmética, considerada como uma das mais importantes, inicia-se por volta do início do século XIX, sendo introduzida por Carl Friedrich Gauss. Esse registro bem como os resultados que apresentamos a seguir podem ser encontrados em Hefez ([3],p.130-210).

Definição 6: Sejam a e b inteiros e m um número natural maior que 1. Dizemos que a e b são **congruentes módulo** m, ou simplesmente *congruentes*, quando os restos da divisão euclidiana de cada um por m são iguais. Escrevemos

$$a \equiv b \pmod{m}.$$

O caso em que $m = 1$ é trivial, por isso consideramos $m > 1$.

Exemplo 2.7.1: $12 \equiv 7 \pmod{5}$, pois 12 deixa resto 2 na divisão por 5. O mesmo acontece na divisão de 7 por 5.

Exemplo 2.7.2: $-3 \equiv 7 \pmod{5}$, pois -3 deixa resto 2 na divisão por 5 e o mesmo ocorre com 7.

Nem sempre, conseguimos estabelecer essa relação entre dois inteiros a e b. Quando isso ocorre, dizemos que os números são incongruentes módulo m e representamos por $a \not\equiv b \pmod{m}$. Nesse caso, dizemos que a é incongruente a b módulo m. Vejamos um exemplo.

Exemplo 2.7.3: Verifique que 9 e 13 são incongruentes módulo 7. Na divisão euclidiana de 9 por 7 o resto é 2. O mesmo não ocorre na divisão euclidiana de 13 por 7, cujo resto é 6. Essa situação é expressa como $9 \not\equiv 13 \pmod{7}$.

Percebemos por um dos exemplos anteriores que $12 \equiv 7 \pmod{5}$. Além disso, temos que $5 \mid 12 - 7$. Outrora, $9 \not\equiv 13 \pmod{7}$. E de modo análogo, $7 \nmid 13 - 9$. Com a próxima proposição, veremos que esse processo, que acabamos de mostrar, pode ser usado para verificar relações de congruência entre dois números inteiros.

Proposição 6: Seja m um número natural e sejam a e b dois inteiros. Temos

$$a \equiv b \pmod{m} \text{ se, e só se, } m \mid (b - a).$$

Demonstração. Sejam $a = mq + r$, com $0 \leq r < m$; $b = mq' + r'$, com $0 \leq r' < m$. Temos que

$$b - a = m(q' - q) + (r' - r).$$

Primeiramente, suponhamos $a \equiv b \pmod{m}$. Sendo assim, $r = r'$. Daí,

$$b - a = m(q' - q). \text{ Logo } m|b - a.$$

Por outro lado, suponha que $m|b-a$. Temos $m|[m(q'-q)+(r'-r)]$. Ora, então $m|(r'-r)$, pois $m|m(q'-q)$. Logo $r'=r$ e, consequentemente, $a \equiv b \pmod{m}$. □

A Proposição 6 tem como consequência direta o seguinte resultado.

Corolário 6: Se $a \equiv b \pmod{m}$, então $m \mid (a-b)$.

Demonstração. De acordo com a Proposição 6 e pela Definição 1, temos que $m \mid (b-a) = -1.(a-b)$. Daí, segue o resultado. □

Para verificar se dois números inteiros são congruentes módulo m, basta observar se satisfazem uma das condições, estar de acordo com a Proposição 6 ou atender ao Corolário 6. Acompanhe os exemplos.

Exemplo 2.7.4: $2 \equiv 7 \pmod{5}$, pois $5 \mid (2-7)$.

Exemplo 2.7.5: $2 \not\equiv 7 \pmod{3}$, pois $3 \nmid (2-7)$.

Exemplo 2.7.6: $-3 \equiv 9 \pmod{12}$, pois $12 \mid (9-(-3))$.

Por meio da proposição a seguir, poderemos garantir que a congruência é uma relação de equivalência, visto que é uma relação contemplada pela reflexividade, simetria e transitividade. A prova a seguir foi baseada em Hefez ([3],p.130).

Proposição 7: Seja m um número natural e sejam a, b e c inteiros. Temos,

i. $a \equiv a \pmod{m}$,

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

iii. se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

Demonstração. Para verificar o item i, basta notar que $m|a-a$, pois $m|0$. Já em ii, temos $m|b-a$ se, e só se, $m|-(b-a)$. A conclusão segue da Proposição 6. No terceiro item, temos $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$ como hipóteses. Disso, pelo Teorema 2.3.1 (I), implica que se $m|(b-a)$ e $m|(c-b)$, então

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

Logo $m|(c-a)$. □

Exemplo 2.7.7: Encontre 5 valores que satisfaçam a congruência $a \equiv 3 \pmod{5}$.

Solução: Escolhemos os valores de k no conjunto {-2, -1, 0, 1, 2}. Analisaremos os valores possíveis de $a = 5.k + 3$,

$$\begin{gathered} a = 5.(-2)+3 = -7, \\ a = 5.(-1)+3 = -2, \\ a = 5.0+3 = 3, \\ a = 5.1+3 = 8, \\ a = 5.2+3 = 13. \end{gathered}$$

Exemplo 2.7.8: Encontre o menor valor positivo para x, com $x \neq 7$, que satisfaça a congruência $x \equiv 7 \pmod 8$.

Solução: Estamos procurando o menor número positivo, diferente de 7, que deixa resto 7 quando divido por 8. Pela definição temos que $8 \mid (x-7)$, então $x - 7 = 8.q$. Daí, $x = 8.q + 7$. Tomando $q = 1$, temos que $x = 15$.

O leitor já deve ter observado que quando trabalhamos com módulo 8, estamos trabalhando com os possíveis restos da divisão de um número por 8, que são 0, 1, 2, 3, 4, 5, 6, 7. O mesmo acontece quando estamos trabalhando com módulo m, os restos são 0, 1, 2, ..., $m-1$. Nesse sentido, a próxima proposição nos revela resultados acerca da adição e multiplicação, envolvendo os números módulo m.

Proposição 8: Sejam a, b, c e d inteiros. Dado m um natural maior do que 1, temos:

i. se $a \equiv b \pmod m$ e $c \equiv d \pmod m$, então $a + c \equiv b + d \pmod m$.

ii. se $a \equiv b \pmod m$ e $c \equiv d \pmod m$, então $a.c \equiv b.d \pmod m$.

Demonstração. Em ambos os itens, vamos supor que $a \equiv b \pmod m$ e $c \equiv d \pmod m$. Consequentemente temos que $m \mid (b-a)$ e $m \mid (d-c)$.

i. Neste item, há pouco a se fazer, bastando apenas observar que

$$m \mid (b-a) + (d-c).$$

Portanto, $m \mid (b+d) - (a+c)$. Pela Proposição 6, temos que

$$a + c \equiv b + d \pmod m.$$

ii. Como $m \mid b - a$ e $m \mid d - c$, temos que $m \mid [d(b-a) + a(d-c)]$, ou seja, $m \mid (d.b - a.c)$. Novamente, pela Proposição 6 temos que

$$a.c \equiv b.d \pmod m.$$

□

Após as Proposições 7 e 8, concluímos que a congruência módulo m é uma relação de *equivalência* compatível com a adição e multiplicação dos inteiros.

Exemplo 2.7.9: Visto que $15 \equiv 7 \pmod 8$ e $35 \equiv 3 \pmod 8$, temos algumas observações.

i. Na adição, temos: $(15 + 35) \equiv (7 + 3) \equiv 10 \equiv 2 \pmod 8$.

ii. Na multiplicação, percebemos que: $(15.35) = 525$ e $(7.3) = 21$. Logo $525 \equiv 21 \equiv 5 \pmod 8$.

Exemplo 2.7.10: Seja $4 \equiv 10 \pmod 6$. Mostraremos que $4^2 \equiv 10^2 \pmod 6$.

Solução:

Temos que $6 \mid (100 - 16)$, pois $6.18 = 84$. Assim $4^2 \equiv 16 \equiv 100 \equiv 10^2 \pmod 6$.

Nesse exemplo, podemos perceber que a congruência módulo m preservou a potenciação. Mostraremos que esse fato ocorre sempre, na verdade, é mais uma propriedade das congruências.

Proposição 9: Para todo $m \in \mathbb{N}$, se $a \equiv b \pmod{m}$, então tem-se que $a^m \equiv b^m \pmod{m}$.

Demonstração. A prova será realizada usando indução sobre m. Sendo assim, devemos mostrar que a proposição é verdadeira para $m = 1$ inicialmente. Depois vamos supor que seja verdadeira para um m qualquer. A demonstração se efetiva se conseguirmos mostrar que a proposição é válida para $m + 1$.

Primeiramente, observamos que a proposição é obviamente válida para $m = 1$. Daí vamos supor que é válida para m, ou seja, $a^m \equiv b^m \pmod{m}$. Desse modo, tem-se que $m \mid b^m - a^m$.

Por outro lado,

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

Como $m \mid b - a$ e, pela hipótese de indução, $m \mid b^m - a^m$, segue que,

$$m \mid b^{m+1} - a^{m+1}.$$

Daí, temos que

$$a^{m+1} \equiv b^{m+1} \pmod{m}.$$

□

Teorema 2.7.1: Pequeno Teorema de Fermat (PTF - versão congruências)
Se p é um número primo e $a \in \mathbb{Z}$, então

$$a^p \equiv a \pmod{p}.$$

Além disso, se $mdc(p, a) = 1$, então

$$a^{p-1} \equiv 1 \pmod{p}.$$

Demonstração. O resultado segue do Teorema 2.5.3 e o Corolário 4. □

Vejamos alguns exemplos.

Exemplo 2.7.11: Vamos encontrar o resto de 13^{130} por 7.
Solução:
Usaremos dois fatos, no primeiro, temos que $13 \equiv 6 \pmod{7}$, logo $13^2 \equiv 6^2 \equiv 1 \pmod{7}$. Ocorre que $7 \nmid 13$, pelo PTF segue que $13^6 \equiv 1 \pmod{7}$.
Assim, $13^{130} \equiv [(13^6)^{21}.13^4] \equiv [(1)^{21}.(13^2)^2] \equiv 1 \pmod{7}$.
Logo o resto procurado é 1.

Exemplo 2.7.12: Determinar o menor inteiro, não negativo, que somado com 10^{18} resulta em um número múltiplo de 19.

Solução:

Note que 10^{18} não é múltiplo de 19. Pelo PTF decorre $10^{18} \equiv 1 \pmod{19}$; o resto é 1. Pela Proposição 8 (i), temos que

$$x + 10^{18} \equiv x + 1 \equiv 19 \pmod{19}.$$

Daí, observamos que $x = 18$.

Até o presente momento, no estudo das congruências do tipo $a \equiv b \pmod{m}$, só foram apresentadas e discutidas propriedades que envolviam os números a ou b. Ampliaremos o estudo das congruências em situações que envolvam o número m.

Proposição 10: Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$. Temos que

$$ac \equiv bc \pmod{m} \iff a \equiv b \pmod{\frac{m}{mdc(c,m)}}.$$

Demonstração. Veja Hefez ([3],p.133). □

De imediato, segue dessa proposição um corolário.

Corolário 7: Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$ e $mdc(c,m) = 1$. Temos que

$$ac \equiv bc \pmod{m} \iff a \equiv b \pmod{m}.$$

Demonstração. A prova seque imediatamente da Proposição 10. □

Exemplo 2.7.13: Repare que, $21 \equiv 9 \pmod{4}$. Como os dois números são múltiplos de 3 e $mdc(3,4) = 1$, temos que

$$3.7 = 21 \equiv 9 = 3.3 \pmod{\frac{4}{mdc(3,4)}}.$$

Logo $7 \equiv 3 \pmod{4}$.

Devemos observar que o procedimento acima, pode ser interpretado como cancelamento multiplicativo.

Proposição 11: Sejam, $a, b \in \mathbb{Z}$ e $m, n, m_1, ..., m_r$ inteiros maiores do que 1. Temos que:

i. Se $a \equiv b \pmod{m}$ e $n \mid m$, então $a \equiv b \pmod{n}$.

ii. $a \equiv b \pmod{m_i}$, para qualquer $i = 1, 2, ...r \iff$ a $\equiv b \pmod{mmc(m_i, ..., m_r)}$.

iii. se $a \equiv b \pmod{m}$, então $mdc(a,m) = mdc(b, m)$.

Demonstração. i. Se $a \equiv b \pmod{m}$, então $m \mid b-a$. Logo $n \mid b-a$, pois $n|m$.

ii. Se $a \equiv b \pmod{m_i}$, com $i = 1, 2, ...r$, então $m_i \mid b-a$. Por outro lado, sabemos que $mmc(m_i, ..., m_r)$ divide o produto de todos m_i com $i = 1, 2, ...r$. Pelo item 1,verfica - se a recíproca.

iii. Como $m \mid b-a$ e $m \mid a-b$, existem $q, q' \in \mathbb{Z}$ tais que, $b = mq + a$ e $a = mq' + b$. Pela Proposição 2.1,

$$mdc(a,m) = mdc(m,a) = mdc(m, a+mq') = mdc(m,b) = mdc(b,m).$$

□

A proposição anterior traz algumas implicações. Vejamos, por exemplo, que $4 \equiv 37 \pmod{33}$. Temos $4 \equiv 37 \pmod{3}$ e $4 \equiv 37 \pmod{11}$. Isso se deve ao fato de $3 \mid 33$, bem como $11 \mid 33$.

Note que a divisão de um número inteiro por 6 pode ter como resto os seguintes números: 0, 1, 2, 3, 4 e 5. Já os restos da divisão por m, são: $0, 1, 2, ..., m-1$. Percebemos que, esses números formam um subconjunto de números inteiros não negativos que inicia-se em 0 e termina em $m-1$. Sendo assim, apresenta exatamente m elementos. Nesse sentido, apresentamos o seguinte conjunto.

Definição 7: Definimos como *sistema completo de resíduos módulo m* (SCRMm) todo conjunto de m números inteiros cujos restos pela divisão euclidiana por m são os números da lista

$$0,\ 1,\ 2,\ ...,\ m-1.$$

Observamos que o sistema completo de resíduos módulo m possui exatamente m elementos, sendo estes, dois a dois incongruentes módulo m. Dessa forma, qualquer conjunto que possui m números inteiros consecutivos forma um sistema completo de resíduos módulo m. Vejamos alguns exemplos.

Exemplo 2.7.14: A sequência 0, 1, 2, 3, 4, 5, 6, representa um sistema completo de resíduos módulo 7.

Exemplo 2.7.15: Verifique que sequência 11, 12, 13, ..., 16 representa um sistema completo de resíduos módulo 6.

De fato, temos que os restos da divisão euclidiana de cada número dessa sequência por 6 são, nessa ordem, 5, 0, 1, 2, 3 e 4.

Um subconjunto do sistema completo de resíduos módulo m merece destaque.

Definição 8: Um sistema *reduzido* de resíduos módulo m (SRRMm) é um conjunto de números inteiros $r_1, r_2, ..., r_s$ tais que:

a) O $mdc(r_i,m) = 1$, para todo $i = 1, 2, ..., s$;

b) $r_i \not\equiv r_j \pmod{m}$, se $i \neq j$;

c) Para cada $n \in \mathbb{Z}$ tal que $mdc(n,m) = 1$, existe $i \in \mathbb{Z} \cap [1,s]$ tal que $n \equiv r_i \pmod{m}$.

Um fato bem conhecido é que dois SRRMm têm sempre a mesma quantidade de elementos. Esta quantidade é dada pelo número de elementos do conjunto $\{x \in \mathbb{Z} | mdc(x,m) = 1,\ 1 \leq x \leq m\ \}$. Os dois últimos exemplos nos permitem explorar bem esse novo conceito, diferenciando os dois tipos de sitemas de resíduos estudados.

Exemplo 2.7.16: Um sistema reduzido de resíduos módulo 6 é formado pelos números 1 e 5. Basta verificar que esses dois números são coprimos com 6. Exibiremos outro conjunto com essa propriedade, pondo $n = 7$, decorre que $mdc(7,6) = 1$ e $7 \equiv 1 \pmod{6}$.

Para além, se $n = 11$, tem-se $mdc(11,6) = 1$ e $11 \equiv 5 \pmod{6}$. Assim, as três condições exigidas na Definição 8 são satisfeitas para 7 e 11.

Neste caso, foram apresentados dois sistemas de resíduos módulo 6. O primeiro é formado pelos números 1 e 5 e o segundo tem 7 e 11 como elementos.

O exemplo anterior exibe dois sistemas reduzidos de resíduos módulo 6 com a mesma quantidade de elementos. Além disso, percebemos também, a existência de uma bijeção entre esses dois conjuntos.

Em algumas situações, não precisaremos explicitar todos os elementos de um sistema reduzido de resíduos, nestes casos, o conhecimento do quantidade de elementos desse sistema já será suficiente. Nesse sentido, apresentaremos mais uma definição.

Esclarecemos que o símbolo φ representa a letra grega fi e a notação "card(A)", sendo A um conjunto finito, refere - se a cardinalidade (número de elementos) do conjunto A.

Definição 9: *Função φ de Euler.*

Seja $\varphi(m)$ uma função definida dos naturais para os naturais com a seguinte regra de formação:

$$\varphi(m) = \text{card}\ \{\ x \in \mathbb{Z} | mdc(x,m) = 1,\ 1 \leq x \leq m\}.$$

Observe que, $\varphi(m) \leq m - 1$, para todo $m \geq 2$. Além disso, $\varphi(m) = m - 1$ para todo m primo. Note que, todos os elementos de 1,2,....$m - 1$ são coprimos com um número m primo. Vejamos o cálculo de $\varphi(m)$ no exemplo abaixo.

Exemplo 2.7.17: Vamos calcular a $\varphi(m)$ para os seguintes m:

a) Para $m = 7$. Os coprimos com 7, positivos e menores ou iguais a 7 pertencem ao seguinte conjunto: {1, 2, 3, 4, 5, 6}. Temos $\varphi(7) = 6$.

b) Se $m = 8$. Os coprimos com 8, positivos e menores ou iguais a 8 pertencem ao seguinte conjunto: {1, 3, 5, 7}. Logo $\varphi(8) = 4$.

c) Tomando $m = 11$. Os coprimos com 11, positivos e menores ou iguais a 11 pertencem ao seguinte conjunto: {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}. Portanto $\varphi(11) = 10$.

d) Com $m = 15$. Os coprimos com 15, positivos e menores ou iguais a 15 pertencem ao seguinte conjunto: {1, 2, 4, 7, 8, 11, 13, 14}. Temos $\varphi(15) = 8$.

Notamos um padrão no cálculo da $\varphi(m)$ para números primos. Nesse sentido apresentamos mais um resultado.

Proposição 12: Se $m \geq 2$, então $\varphi(m) = m - 1$ se, e somente se, m é um *número primo*.

Demonstração. Admitindo m primo, temos que todos os números 1,2,...,$m - 1$ atendem às condições da Definição 8, logo essa lista forma um sistema reduzido de resíduos módulo m. Por outro lado, se $\varphi(m) = m - 1$, todos os elementos do conjunto {1,2,...,$m - 1$} são coprimos com m. Logo m é primo, pois os únicos divisores positivos são 1 e m. □

No caso em que $m = 8$, retiramos do sistema completo de resíduos, os números não coprimos com 8,ou seja: 0, 2, 4 e 6. Logo $\varphi(8) = 8$ - 4 = 4.

Para determinar $\varphi(15)$, o procedimento adotado para $m = 8$, revela-se mais trabalhoso. Segue um resultado que otimiza esse cálculo.

Proposição 13: Sejam m e m' dois números naturais primos entre si. Então

$$\varphi(m.m') = \varphi(m).\varphi(m).$$

Demonstração. Ver Hefez ([3],p.159). □

Nesse sentido, temos $\varphi(15) = \varphi(3.5) = 2.4 = 8$.

Exemplo 2.7.18: Calculando $\varphi(26)$.

Primeiramente, 26 = 2.13. Além disso, mdc(2,13) = 1. Então

$$\varphi(26) = \varphi(2).\varphi(13) = 1.12 = 12.$$

Perceba que, a Proposição 13 não se aplica para $m = 8$. O problema pode ser solucionado com a aplicação da próxima proposição.

Proposição 14: Sejam p é um número primo e r um número natural. Temos

$$\varphi(p^r) = p^r - p^{r-1} = p^r(1 - \frac{1}{p}).$$

Demonstração. Para p primo, observa-se que a sequência de números inteiros de 1 até p^r possui exatamente p^r números. Pela definição 9, para calcular $\varphi(p^r)$ devemos excluir, desses, todo número não coprimo com p^r, ou seja, os múltiplos de p, que são os números p, $2p$, $3p$, ..., p^r. O último múltiplo de p pode ser escrito como $p^{r-1}p$, revelando que essa sequência possui p^{r-1} números. Então $\varphi(p^r) = p^r - p^{r-1}$, provando o resultado. □

O próximo teorema possibilita uma maneira mais direta para calcular a função φ *de Euler* para qualquer m.

Teorema 2.7.2: Sejam $m > 1$ e $m = {p_1}^{\alpha_1}...{p_n}^{\alpha_n}$ a sua decomposição em fatores primos p_1,p_2,...,p_n, com $(\alpha_1, ...,\alpha_n) \in \mathbb{N}^n$. Então

$$\varphi(m) = {p_1}^{\alpha_1}...{p_n}^{\alpha_n}\left(1 - \frac{1}{p_1}\right)...\left(1 - \frac{1}{p_n}\right).$$

Demonstração. Aplicando as Proposições 13 e 14, o resultado é imediato. □

A expressão acima pode ser reescrita de forma mais simples:

$$\varphi({p_1}^{\alpha_1}...{p_n}^{\alpha_n}) = {p_1}^{\alpha_1-1}...{p_n}^{\alpha_n-1}(p_1 - 1)...(p_n - 1).$$

Exemplo 2.7.19: Calculando $\varphi(m)$

a) $\varphi(210) = 2^{1-1}.3^{1-1}.5^{1-1}.7^{1-1}.(2-1).(3-1).(5-1).(7-1) = 1.2.4.6 = 48.$

b) $\varphi(36) = 2^{2-1}.3^{2-1}.(2-1).(3-1) = 2.3.1.2 = 12.$

Tendo em vista que um sistema reduzido de resíduos módulo 6 é formado pelos números 1 e 5, percebemos que os pares de números 5 e 25, bem como 7 e 35 também formam um sistema reduzido de resíduos módulo 6. Esse fato pode ser generalizado como uma propriedade desses conjuntos, como observamos em Hefez ([3],p.156-157).

Proposição 15: Seja $r_1, r_2, ..., r_{\varphi(m)}$ um sistema reduzido de resíduos módulo m e seja $a \in \mathbb{Z}$ tal que $mdc(a,m) = 1$. Então $ar_1, ar_2, ..., ar_{\varphi(m)}$ é um sistema reduzido de resíduos módulo m.

Demonstração. Seja $a_1, a_2, ..., a_m$, um sistema completo de resíduos módulo m, do qual retiramos o sistema reduzido de sistemas módulo m: $r_1, r_2, ..., r_{\varphi(m)}$. Escolhendo a inteiro tal que, $mdc(a,m) = 1$, pelo fato de $r_i \not\equiv r_j \pmod m$ para $i \neq j$, decorre que $ar_i \not\equiv ar_j \pmod m$ para $i \neq j$. Então $mdc(aa_i,m) = 1$ e consequentemente, $ar_1, ar_2, ..., ar_{\varphi(m)}$, é um SRRMm. □

Teorema 2.7.3: *Teorema de Euler*

Sejam a e m dois inteiros coprimos, sendo $m > 1$, Então:

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

Demonstração. Seja $r_1, r_2, ..., r_{\varphi(m)}$ um SRRMm. De acordo com a Proposição 15, temos que os conjuntos $r_1, r_2, ..., r_{\varphi(m)}$ e $ar_1, ar_2, ..., ar_{\varphi(m)}$ são dois sistemas reduzidos de resíduos módulo m,. Daí, ao fazermos o produtos de cada conjunto, entre si, temos:

$$ar_1.ar_2.....ar_{\varphi(m)} \equiv r_1.r_2.....r_{\varphi(m)} \pmod m.$$

Observamos que, no primeiro membro, temos a $\varphi(m)$ vezes. Logo podemos reescrever essa congruência como:

$$a^{\varphi(m)}.(r_1.r_2.....r_{\varphi(m)}) \equiv (r_1.r_2.....r_{\varphi(m)}) \pmod{m}.$$

De sorte, temos que $mdc((r_1.r_2.....r_{\varphi(m)}),m) = 1$, então segue do Corolário 7 que

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

□

Exemplo 2.7.20: Vamos calcular o resto de 5^{42} por 16.

Resolução:

Temos que $mdc(5,16) = 1$. Daí, $5^{\varphi(16)} \equiv 1 \pmod{16}$. Por outro lado, $\varphi(16) = 2^{4-1}(2-1) = 8$.

Então $5^{42} \equiv (5^8)^5.5^2 \equiv 1^5.25 \equiv 9 \pmod{16}$.

Veremos que, nem sempre, uma congruência do tipo $aX \equiv b \pmod{m}$ com a e b inteiros, possui alguma solução em x. Essas congruências merecem um destaque em nossa investigação sobre a criptografia.

Definição 10: Sejam, $a, b, m \in \mathbb{Z}$, com $m > 1$. A *congruência linear* $aX \equiv b \pmod{m}$ tem solução quando existe $x_0 \in \mathbb{Z}$ tal que $ax_0 \equiv b \pmod{m}$.

Proposição 16: Sejam, $a, b, m \in \mathbb{Z}$, com $m > 1$. A congruência,

$$aX \equiv b \pmod{m}$$

possui soluções se, e somente se, $mdc(a,m) \mid b$.

Demonstração. Suponhamos que, $aX \equiv b \pmod{m}$ possui uma solução em $\mathbb{Z}$. Então existe $y \in \mathbb{Z}$ tal que, $aX - my = b$ se, e somente se, $mdc(a,m) \mid b$, garantido pelo Teorema 2.5.1. Reciprocamente, suponha que $mdc(a,m) \mid b$. Pelo Teorema 2.5.1, temos que existem x e y inteiros tais que $ax - my = b$. Logo $ax - b = my$. Consequentemente, $aX \equiv b \pmod{m}$ tem solução. □

Uma observação acerca do resultado que acabamos de encontrar se faz necessária. Seja x_0 uma solução para $aX \equiv b \pmod{m}$, então todo x tal que $x \equiv x_0 \pmod{m}$ é também uma solução para $aX \equiv b \pmod{m}$, visto que

$$ax \equiv ax_0 \equiv c \pmod{m}.$$

Nesse sentido, percebe-se que ao encontrar uma solução para a congruência linear, uma solução dita particular, determinamos infinitas soluções para a congruência.

Exemplo 2.7.21: Resolva a congruência $2x \equiv 4 \pmod 6$

Solução:

Primeiramente, verificamos que $mdc(2,6) = 2$ que divide 4. Então a congruência possui solução. De modo equivalente, isso significa dizer que $2x - 4$ é um múltiplo de 6. Para terminar, igualamos essa expressão a alguns múltiplo de 6.

$2x - 4 = 0 \Rightarrow x = 2$.
$2x - 4 = 6 \Rightarrow x = 5$.
$2x - 4 = 12 \Rightarrow x = 8$.
$2x - 4 = 18 \Rightarrow x = 11$.
$2x - 4 = 24 \Rightarrow x = 14$.
$2x - 4 = 30 \Rightarrow x = 17$.

Não é dificil perceber que os dois primeiros valores de x são incongruentes. E por outro lado, $2 \equiv 8 \equiv 14 \pmod 6$, assim como $5 \equiv 11 \equiv 17 \pmod 6$. Logo, essa congruência possui 2 soluções módulo 6. Uma é 2 e a outra 5, ambas módulo 6.

A proposição a seguir indica o número de soluções de uma congruência.Porém, antes de estudá-la, vamos definir o conjunto de soluções de uma congruência linear como **sistema completo de soluções incongruentes módulo m**.

Teorema 2.7.4: Sejam, $a, b, m \in \mathbb{Z}$, com $m > 1$ e $mdc(a,m) \mid b$. Se x_0 é uma solução da congruência $aX \equiv b \pmod m$, então

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, ..., x_0 + (d-1)\frac{m}{d},$$

em que $d = (a,m)$, formam um sistema completo de soluções da congruência, duas a duas incongruentes módulo m.

Demonstração. Veja Hefez ([3],p.171). □

A partit desse teorema, vamos resolver, de maneira mais direta, o próximo problema.

Exemplo 2.7.22: Determine o sistema completo de soluções da congruência $4x \equiv 8 \pmod{12}$

Solução: Primeiramente, note que $mdc(4,12) = 4$ que divide 8. Então a congruência possui 4 soluções. Essas 4 soluções formam um sistema completo de soluções incongruentes módulo m. Decorre que $12 \mid 4x - 8$, então $x = 2$ é uma solução. Pelo Teorema 2.7.4 temos, $2, 2 + \frac{12}{4}, 2 + 2\frac{12}{4}, 2 + 3\frac{12}{4}$ são soluções. Um sistema completo de soluções da congruência é 2, 5, 8, 11.

Do Teorema 2.7.4, surge um colorário importante que vem ao encontro da Proposição 16.

Corolário 8: Se $mdc(a,m) = 1$, então a congruência $aX \equiv b \pmod m$ possui única solução módulo m.

É importante observarmos, diante desses resultados, que $d = mdc(a,m)$ representa *o número de soluções módulo m* de uma congruência linear.

As congruências lineares contribuíram com o desenvolvimemto de alguns sistemas criptográficos, como por exemplo o método RSA. As congruências do tipo $aX \equiv 1 \pmod{m}$ serão uma ferremanta importante nesse método criptográfico, como veremos mais adiante. Sendo assim, nos limitaremos a esse tipo de congruência.

Proposição 17: Sejam a e $m \in \mathbb{Z}$, com $m > 1$. A congruência $aX \equiv 1 \pmod{m}$ possui solução se, e somente se, $mdc(a,m) = 1$. Além disso, se $x_0 \in \mathbb{Z}$ é uma solução, então x é uma solução da congruência se, e somente se, $x \equiv x_0 \pmod{m}$.

Demonstração. Suponhamos que $ax \equiv 1 \pmod{m}$. Pela Proposição 6, $m \mid ax-1$. Decorre que $ax - mq = 1$ tem solução nos inteiros, de acordo com a Proposição 4, se, e somente se, $mdc(a,m) = 1$. A primeira parte da prova está completa.

Reciprocamente, vamos supor $mdc(a,m) = 1$. Temos, pela Proposição 4, que existem x e y, números inteiros tais que, $ax - mq = 1$. Logo $m \mid ax - 1$. Pela Proposição 6, temos que $ax \equiv 1 \pmod{m}$.

Por outro lado, se $ax \equiv ax_0 \pmod{m}$, como $mdc(a,m) = 1$, decorre do Corolário 7 que $x \equiv x_0 \pmod{m}$. □

A proposição acima tem valor no processo de criptografia do modelo RSA.

Definição 11: Sejam a,b e m inteiros, com $m > 1$. Suponha que mdc$(a,m) =$ mdc(b,m)=1. Dizemos que b é um **inverso multiplicativo de** a **módulo** m quando $a.b = 1 \bmod m$.

Continuando, traremos um teorema que, no nosso trabalho, servirá como ferramenta na discussão da primalidade de um número. Embora o teorema receba o nome e atribuído ao matemático inglês, John Wilson, ele foi demonstrado pela primeira vez pelo matemático J.L Lagrange.

Teorema 2.7.5: Se p é um número primo, então,

$$(p-1)! \equiv -1 \pmod{p}$$

Demonstração. Para $p = 2$, tem-se $(2-1)! \equiv 1 \equiv -1 \pmod{2}$. Analogamente, verifica-se a validade para $p = 3$. Suponhamos $p \geq 5$, com p primo. A congruência $iX \equiv 1 \pmod{p}$, em que $i \in \{1,2,3,...,p-1\}$ (SRRMm), possui solução módulo p de acordo com a Proposição 17, visto que $mdc(i,m) = 1$. Além disso, pelo Corolário 8, essa solução é única módulo p, ou seja, dado $i \in \{1,2,3,...,p-1\}$ existe um único $j \in \{1,2,3,...,p-1\}$ tal que $i.j \equiv 1 \pmod{p}$. Por outro lado, quando $i = j$, temos $i^2 \equiv 1 \pmod{p}$. Daí $p \mid i^2 - 1$, o que equivale a $p \mid (i-1)$ ou $p \mid (i+1)$. No entanto, isso só ocorre se $i = 1$ ou $i = p-1$. Com base nestes fatos, temos:

$$1.2...(p-2) \equiv 1 \pmod{p}.$$

Multiplicando a congruência por $(p-1)$,

$$1.2...(p-2)(p-1) \equiv 1(p-1) \equiv -1 \pmod{p}.$$

□

A importância desse resultado, nos testes de primalidade, justifica-se pela validade de sua recíproca.

Proposição 18: Seja $p \geq 2$ um número inteiro. Se $(p-1)! \equiv -1 \pmod{p}$, então p é primo.

Demonstração. Veja Hefez ([3],p.165) □

Vejamos um exemplo para fixar as ideias.

Exemplo 2.7.23: Verifique que $11 \mid 10! + 1$
Pelo Teorema 2.7.5, temos $(11-1)! \equiv -1 \pmod{11}$. Então $11 \mid (11-1)! + 1$.

2.8 Classes Residuais

As congruências módulo $m > 1$ nos permitiram avançar ainda mais nos estudos da aritmética.

Voltando a discutir sobre os sistemas completos de resíduos módulo m, vimos que existem infinitos conjuntos de m números inteiros que podem representar esse mesmo sistema. Em outras palavras, existe, por exemplo, uma quantidade infinita de números que deixam resto zero na divisão euclidiana por m. Do mesmo jeito, uma infinidade de números que deixam resto 1 nessa mesma divisão, e assim por diante. Nesse sentido, temos a seguinte partição do conjunto $\mathbb{Z}$.

$$\begin{aligned}
[0] &= \{\, x \in \mathbb{Z}; x \equiv 0 \pmod{m}\}. \\
[1] &= \{x \in \mathbb{Z}; x \equiv 1 \pmod{m}\}. \\
&\vdots \\
[\text{m - 1}] &= \{\, x \in \mathbb{Z}; x \equiv m-1 \pmod{m}\}.
\end{aligned}$$

Cada conjunto numérico acima é denominado *classe residual módulo m.* Seja a um inteiro. A classe de a módulo m é definida por:

$$[a] = \{\, x \in \mathbb{Z}; x \equiv a \pmod{m}\}.$$

Proposição 19: Sejam $[a]$ e $[b]$ duas classes módulo m. Então

$$[a] = [b] \text{ se, e somente se, } a \equiv b \pmod{m}.$$

Demonstração. Suponhamos $[a] = [b]$. Então temos que os restos de a e b por m são iguais. Sem perda de generalidade, suponhamos $a < m < b$. Temos que $a = m.0 + a$ e $b = m.q + a$. Daí $b - a = m.q$. Logo $(b-a) \equiv 0 \pmod{m}$.

A recíproca é feita de maneira análoga. □

O resultado acima tem como consequência o próximo corolário.

Corolário 9: Para cada $a \in \mathbb{Z}$ existe um, e somente um, $r \in \mathbb{Z}$, com $0 \leq r < m$, tal que $[a] = [r]$.

Demonstração. Seja $a \in \mathbb{Z}$. Pela divisão euclidiana, existem únicos q e r tais que, $a = mq + r$ com $0 \leq r < m$. Daí, $(a - r) \equiv 0 \pmod{m}$. Pela Proposição 19, temos $[a] = [r]$.

□

Definição 12: Conjunto $\mathbb{Z}_m$

Conjunto formado por todas as classes residuais módulo m, denominado $\mathbb{Z}_m$.

$$\mathbb{Z}_m = \{[0], [1], [2], .., [m-1]\}.$$

Exemplo 2.8.1: Vamos explicitar cada conjunto $\mathbb{Z}_m$ para:

a) $m = 2$. Neste caso, $\mathbb{Z}_2$. Temos $\mathbb{Z}_2 = \{[0], [1]\}$. Note que $[0] = [a]$ para todo a par inteiro e $[1] = [a]$ se a for ímpar.

b) $m = 6$. De maneira análoga, temos que $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$.

Note que, se escolhermos a classe $[2]$ em $\mathbb{Z}_6$, então

$$[2] = \{6t + 2; t \in \mathbb{Z}\} = (... \text{ -10, -4, 2, 8, 14, ...}).$$

Esse conjunto é formado pelos **representantes de [2]**. Desse fato, se a é um inteiro, a classe de a módulo m pode ser representada por:

$$[a] = \{6m + a; m \in \mathbb{Z}\}.$$

Vamos definir as operações de soma e multiplicação em $\mathbb{Z}_m$.

Definição 13: Sejam $[a]$ e $[b]$ duas classes residuais pertencentes a $\mathbb{Z}_m$. Temos:

i. $[a] + [b] = [a + b]$,

ii. $[a].[b] = [a.b]$.

Devemos perceber que se alterarmos os representantes das classe residuais, não alteraremos os valores da soma e nem do produto em $\mathbb{Z}_m$.

Se $a \equiv a' \pmod{m}$ e $b \equiv b' \pmod{m}$, pelas Proposições 19 e 8(i), temos:

$$a + b \equiv a' + b' \pmod{m} \text{ se, e só se, } [a' + b'] = [a + b].$$

Por outro lado, tomando $a \equiv a' \pmod{m}$ e $b \equiv b' \pmod{m}$, pelas Proposições 19 e 8(ii), temos:

$$a.b \equiv a'.b' \pmod{m} \text{ se, e só se, } [a'.b'] = [a.b].$$

Podemos verificar em Hefez ([3],p.183), que para todos $[a], [b]$ e $[c] \in \mathbb{Z}_m$, valem as seguintes propriedades:

Proposição 20: Propriedades
Adição

a) **Comutatividade**, $[a] + [b] = [b] + [a]$.
$[a] + [b] = [a + b] = [b + a] = [b] + [a]$.

b) **Associatividade**,$([a] + [b]) + [c] = [a] + ([b] + [c])$.
$([a] + [b]) + [c] = [a + b] + [c] = [a] + [b + c] = [a] + ([b] + [c])$.

c) **Existência do elemento neutro, (zero)**, $[a] + [0] = [a]$.
$[a] + [0] = [a + 0] = [a]$.

d) **Existência do elemento simétrico**, $[a] + [-a] = [0]$.
$[a] + [-a] = [a + (-a)] = [0]$.

Multiplicação

e) **Comutatividade**, $[a].[b] = [b].[a]$.
$[a].[b] = [a.b] = [b.a] = [b].[a]$.

f) **Associatividade**,$([a].[b]).[c] = [a].([b].[c])$.
$([a].[b]).[c] = [a.b].[c] = [a].[b.c] = [a].([b].[c])$.

g) **Existência do elemento unitário**, $[a].[1] = [a]$.
$[a].[1] = [a.1] = [a]$.

h) **Distributiva**, $[a].([b] + [c]) = [a].[b] + [a].[c]$.
Temos que, $[a].([b] + [c]) = [a].[b + c] = [a.(b + c)] = [a.b + a.c] = [a.b] + [a.c] = [a].[b] + [a].[c]$.

Vejamos alguns exemplos envolvendo as operações em Z_m.

Exemplo 2.8.2: Utilizando [4] e [5] em $\mathbb{Z}_6$ e as operações acima.

a) $[4] + [5] = [4 + 5] = [9] = [3]$.
Pois $4 + 5 \equiv 9 \equiv 3 \pmod 6$.

b) $[4].[5] = [4.5] = [20] = [2]$. De modo análogo ao realizado anteriormente, $4.5 \equiv 20 \equiv 2 \pmod 6$.

Exemplo 2.8.3: Observe as tabelas de soma e produto em $\mathbb{Z}_3$.

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

(a) Adição

×	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

(b) Multiplicação

Tabela 2.1: Adição e Multiplicação em Z_3

Diante das propriedades das classes residuais e da observação da Tabela 2.1(a) do Exemplo 2.8.3, percebemos que o [0] é elemento neutro para todas as classes na operação de adição.

Exemplo 2.8.4: Observe as tabelas com operações definidas em $\mathbb{Z}_6$

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

(a) Adição

.	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

(b) Multiplicação

Tabela 2.2: Adição e Multiplicação em Z_6

Definição 14: Dizemos que duas classes em $\mathbb{Z}_m$ $[a]$ e $[b]$ são **inversas** se

$$[a].[b] = [1].$$

Na multiplicação em $\mathbb{Z}_3$, percebemos que somente as classes [1] e [2] possuem inversa, enquanto em $\mathbb{Z}_6$, somente duas classes residuais possuem inversas. Vejamos a condição para determinarmos a inversa de uma classe residual em $\mathbb{Z}_m$.

Proposição 21: Seja m um número inteiro e seja x um inteiro tal que $x \not\equiv 0 \pmod{m}$. Então a classe $[x]$ em $\mathbb{Z}_m$ tem inversa (é inversível) se, e somente se, $mdc(x, m) = 1$.

Demonstração. Suponhamos que, em $\mathbb{Z}_m$, $[x]$ é invertível. Assim existe y tal que $[x].[y] = [1]$. Escolhendo x como representante de $[x]$, temos $x.y - 1 \equiv 0 \pmod{m}$. Logo existe q inteiro tal que $x.y - 1 = m.q$ e $x.y + mq = 1$. Pelo Teorema 2.5.1, decorre que $mdc(x,m) = 1$.

Por outro lado, consideremos $mdc(x,m) = 1$. Pelo Corolário 2, existem y e q inteiros tais que $x.y + m(q) = 1$. Logo temos $x.y - 1 = mq$. Isso implica que $x.y - 1 \equiv 0 \pmod{m}$. Então $x.y \equiv 1 \pmod{m}$, ou seja, $[x].[y] = 1$. □

A Proposição 21 tem como consequência o seguinte resultado.

Corolário 10: Seja p um número *primo* e seja x um número inteiro que não é múltiplo de p . Então toda classe $[x]$ tem inversa em $\mathbb{Z}_p$.

Demonstração. Basta notar que todo número, não nulo, menor do que p é coprimo com p. □

Exemplo 2.8.5: Em $\mathbb{Z}_6$:

a) Observamos que [1] . [1] = [1]. Perceba que $mdc(1,6) = 1$. Vejamos por exemplo, 7 e 13 são representantes de [1], logo $7.13 = 91 \equiv 1 \pmod 6$.

b) Vimos que [5] . [5] = [1] e $mdc(5,6) = 1$. Escolhendo agora 5 e 11 como representantes da classe [5] em $\mathbb{Z}_6$, temos que $5.11 = 55 \equiv 1 \pmod 6$.

Exemplo 2.8.6: Vimos que [2] não apresentou nenhuma classe inversa em $\mathbb{Z}_6$. De fato, o $mdc(2,6) = 2$.

Exemplo 2.8.7: Determine as classes módulo 9 que possuem inversas.

Resolução. O conjunto $Z_9 = \{[0], [1], [2], [3], [4], [5], [6], [7], [8]\}$.

As classes [0], [3] e [6] não possuem inversas. Note que $1.1 = 1 \equiv 1 \pmod 9$. Logo, [1] e [1] são inversas uma da outra.

Observe que $2.5 = 10 \equiv 1 \pmod 9$. Daí, [2] e [5] são inversas uma da outra.

Continuando, $4.7 = 28 \equiv 1 \pmod 9$. Assim, [4] e [7] são classes inversas uma da outra.

Para terminar, $8.8 = 64 \equiv 1 \pmod 9$. Assim, [8] e [8] também são inversas uma da outra.

As classes que possuem inversas em $\mathbb{Z}_9$ são [1], [2], [4], [5], [7] e [8].

Encontrar a inversa de uma classe módulo m, ou identificar quando não é possível encontra-lá, é uma habilidade fundamental para o entendimento de dois modelos de criptografia que veremos. Pensando nisso, apresentaremos três exemplos relacionados à busca de classe inversas módulo 26. O conjunto $\mathbb{Z}_{26}$ será um muito utilizado no nosso trabalho, uma vez que contempla as 26 letras do nosso alfabeto. Vamos aos exemplos em $\mathbb{Z}_{26}$.

Exemplo 2.8.8: Quais são os inversos de 5 módulo 26?

Solução:

Primeiramente, $mdc(5,26) = 1$, logo 5 possui inverso.

Comecemos com $26 = 5.5 + 1$, logo $(-5)5 + 1.26 = 1$. Decorre que [-5] é inversa de [5]. Para encontrar os representantes de [-5] devemos lembrar que:

$$[-5] = \{26t - 5, \text{ sendo que } t \in \mathbb{Z}\}.$$

Logo [-5] = {..., -31, -5, 21,...}.

Tomando [21] como exemplo, temos $5.21 = 105 = 4.26 + 1$, ou seja,

$$5.21 = 105 = 1(\text{mod } 26).$$

Exemplo 2.8.9: Qual é a classe inversa de [13] em $\mathbb{Z}_{26}$?

Solução:

Primeiramente, mdc(13,26) = 13 $\neq$ 1. Logo [13] **não** possui inversa em $\mathbb{Z}_{26}$.

Exemplo 2.8.10: Qual é o inverso de [19] módulo 26?

Solução:

Primeiramente, mdc(19,26) = 1. Logo [19] possui inversa em $\mathbb{Z}_{26}$. Começamos dividindo 26 por 19 e seguimos com divisões do divisor pelo resto subsequente até que o resto seja um.

26 = 19.1 + 7 (resto $\neq$ 0). Agora dividi-se 19 por 7.

19 = 7.2 + 5 (resto $\neq$ 0)). Agora dividi-se 7 por 5.

7 = 5.1 + 2 (resto $\neq$ 0). Agora dividi-se 5 por 2.

5 = 2.2 + 1 (resto $\neq$ 0).

Começando da pela última equação e terminando com a primeira, temos:

1= 5 - 2.2 = 5 - 2(7 - 5.1) = 3.5 -2.7 = 3(19 -2.7) -2.7 = 3.19 - 8.7 = 3.19 - 8(26 - 19.1) = 26(-8) + 19(11). Segue que [11] é a inversa de [19] em $\mathbb{Z}_{26}$.

As classes que possuem inverso módulo m formam um conjunto númerico Nessa linha de pensamento, abordaremos esse conjunto de acordo com Hefez(Hefez,p.186).

Definição 15: Seja $m > 1$ um inteiro. A classe dos invertíveis em $\mathbb{Z}_m$ é denotada por U(m), em que:

$$U(m) = \{[a_1],[a_2],...[a_{\varphi(m)}]\}.$$

Além disso, o conjunto $\{a_1, a_2, ...a_{(m)}\}$ é um sistema reduzido de resíduos módulo m.

O Exemplo 2.8.8 revelou que [5] e [21] são inversos em $\mathbb{Z}_{26}$. Para além disso, sabemos que ambas as classes pertencem ao conjunto $U(m)$. Daí, [5] + [21] = [0]. No entanto, [0] $\notin U$(m), que por sua vez, mostra não ser fechado para adição. Por outro lado, [5] . [21] = [1]. E [1] $\in U(m)$. Mostraremos que esse fato é válido para qualquer classe de $U(m)$.

Sejam [a] e [b] $\in U$(m). Considere [a'] e [b'] suas respectivas inversas. Então:

$$[1] = [a].[a'].[b].[b'] = [a.b].[a'.b'] \in U(m).$$

Assim, mostramos que $U(m)$ é um conjunto multiplicativamente fechado.

A seguir, vamos expor alguns conjuntos $U(m)$.

Exemplo 2.8.11: Determine o conjunto $U(m)$ para cada cada $\mathbb{Z}_m$:

a) $\mathbb{Z}_3$. Temos que $U(3) = \{[1],[2]\}$.

b) $\mathbb{Z}_6$. Temos que $U(6) = \{[1],[5]\}$.

c) $\mathbb{Z}_9$. Temos que $U(9) = \{[1],[2],[4],[5],[7],[8]\}$.

d) $\mathbb{Z}_{26}$. Temos que $U(6) = \{[1],[3],[5],[7],[9],[11],[15],[17],[19],[21],[23],[25]\}$.

Podemos verificar, em todos os conjuntos do Exemplo 2.8.11, o fechamento para a operação de multiplicação.

Com a base teórica apresentada, acreditamos estar preparados para estudar, mesmo que de maneira elementar, alguns modelos de criptografia.

Para finalizar, trazemos demonstrações de dois critérios de divisibilidades, trabalhados no ensino básico, utilizando a aritmética modular.

2.9 Critérios de Divisibilidades

Teorema 2.9.1: Divisibilidade por 3

n é divisível por 3, se e somente se, a soma de seus algarismos é divisível por 3.

Demonstração. Temos que, $10 \equiv 1 \pmod 3$. Desse resultado, decorre que:

$$\begin{gathered} n_1.10^{k-1} \equiv n_1 \pmod 3 \\ n_2.10^{k-2} \equiv n_2 \pmod 3 \\ . \\ . \\ . \\ n_k \equiv n_k \pmod 3 \end{gathered}$$

Somando as congruências, segue que

$n = n_1.10^{k-1} + n_2.10^{k-2} + ... + n_k \equiv (n_1 + n_2 + ... + n_k) \pmod 3$. Assim, $m \equiv 0 \pmod 3$ se, e só se, $n_1 + n_2 + ... + n_k \equiv 0 \pmod 3$. □

Teorema 2.9.2: Divisibilidade por 11

m é divisível por 11, se e somente se, a soma de seus algarismos de ordens pares subtraída pela soma dos algarismos de ordens ímpares é divisível por 11.

Demonstração. Temos que: $10 \equiv -1 \pmod{11}$, $10^2 \equiv 1 \pmod{11}$, $10^3 \equiv -1 \pmod{11}$, e assim por diante. Desse resultado, decorre que $10^n \equiv 1 \pmod{11}$, se n for par e $10^n \equiv -1 \pmod{11}$ quando n é ímpar. Supondo que o número $m = a_n a_{n-1}...a_1 a_0$ seja divisível por 11, temos

$$m = a_n a_{n-1}...a_1 a_0 = a_n.10^n + a_{n-1}.10^{n-1}...a_1.10 + a_0 \equiv 0 \pmod{11}.$$

Dessa forma,

$$a_n 10^n + a_{n-1}10^{n-1} + ... + a_1 10 + a_0 \equiv 0 \pmod{11}$$

o que mostra que $11|n$.

Para demonstrar a recíproca, considere $m = a_n a_{n-1}...a_1 a_0$. Iremos supor, sem perda de generalidade, que n é impar. Assim, por hipótese, temos:

$$a_n.(-1) + a_{n-1}.(1)...a_1.(-1) + a_0 \equiv -a_n + a_{n-1}... - a_1. + a_0 \equiv 0 \pmod{11}.$$

□

3

Testes de Primalidade

Determinar se um número inteiro é primo ou não é uma tarefa que intriga estudiosos há muito tempo. Neste sentido, um teste de primalidade deve ser interpretado como uma tarefa para tal empreitada

Atualmente, a verificação de primalidade de um número pode ser feita em tempo polinomial. O algoritmo AKS, por exemplo, nos possibilita uma resposta em tempo polinomial. Já a decomposição em fatores primos é um problema mais custoso do ponto de vista computacional. Ele é dito um problema NP-Hard.

Por volta do ano 300 AEC (Antes da Era Comum), Euclides demonstrou, em seu Livro IX da obra Elementos, a infinitude dos números primos. Mais tarde, no século XVIII, o matemático Leonhard Euler publicou a fórmula $f(n) = n^2 + n + 41$, com $n = 1,2,3,..,39$, a qual gera uma sequência finita de números primos. A prova do teorema proposto por Euclides é considerada uma beleza da matemática, sendo utilizada a técnica lógica de redução ao absurdo como ferramenta para o feito. A base do material apresentado nesta seção é resultado do estudo de Shokranian ([7],p.61-72).

Teorema 3.0.1: Existem infinitos números primos.

Demonstração. Suponhamos que exista uma quantidade finita de números primos, denotados por $p_1, p_2,..., p_r$ em que $r \in \mathbb{N}$. Consideramos o natural $n = p_1.p_2.....p_r + 1$. Pelo Teorema 2.5.2 decorre que um fator primo p de $\{p_1, p_2,..., p_r\}$ divide o produto $p_1.p_2.....p_r + 1$. Logo p divide 1, o que é um absurdo. Então o conjunto tem cardinalidade infinita. □

Em regra geral, todo estudante tem a primeira experiência com a primalidade de um número no fim da educação infantil ou nos anos iniciais do ensino fundamental. Já no sexto ano dessa mesma etapa de ensino, a análise de primalidade se baseia nos critérios de divisibilidade. Como os números estudados são relativamente pequenos, a decisão se um número é primo ou não, geralmente é realizada verficando se ele é divisível por algum dos primeiros números primos. Vejamos alguns métodos para tais verificações.

3.0.1 Metódo da Divisão

Esse teste de verificação de primalidade de um número é baseado na definição de número primo. Para certificar que n é um número primo, devemos verificar se n é divisível por todos números primos menores do que ele. Esse procedimento aumenta, substancialmente, o grau de dificuldade à medida que n se torna um número grande.

Por outro lado, basta observar se n é divisível por algum primo menor ou igual a $\lfloor\sqrt{n}\rfloor$. De fato, se a é divisor de n, temos que $n = a.b$ para algum b natural. A medida que a se aproxima de $\sqrt{n}$, o mesmo acontece com b. Reforçando essa ideia, trazemos o seguinte lema de acordo com Hefez ([3],p.102).

Lema 3.1: Se um número natural n maior do que 1 não é divisível por nenhum número primo p tal que $p^2 \leq n$, então esse número é primo.

Demonstração. Suponhamos, por absurdo, que o número n não seja primo.Assim sendo, n é composto. Tomando q como o menor divisor primo de n, pelo Teorema 2.5.2, temos $n = q.n_1$ com $2 \leq n_1 < n$. Como $q \leq n_1$, decorre que $q^2 \leq q.n_1 = n$, indicando que n é divisível por q e $q^2 \leq n$. Isso contradiz a nossa hipótese, absurdo. □

Vejamos na prática.

Exemplo 3.0.1: Vejamos, pelo método da divisão, que 101 é primo.

Solução: Por cálculos rotineiros, verificamos que $10 < \sqrt{101} < 11$. Então devemos procurar algum divisor primo de 101 que seja menor ou igual a 10. Como os números primos 2, 3, 5, 7 não são divisores de 101, temos que o número em questão é primo.

Exemplo 3.0.2: Pelo método da divisão, mostraremos que 143 não é primo.

Solução: Não é difícil constatar que $11 < \sqrt{143} < 12$. Então devemos procurar algum divisor primo de 143 que seja menor ou igual a 11.Os números primos 2, 3, 5, 7 não são divisores de 143, mas $11.13 = 143$, logo o número é composto.

3.0.2 Crivo de Eratóstenes

Este é um dos métodos para encontrar números primos mais antigos. Seu desenvolvimento é atribuido ao matemático grego Eratóstenes, que viveu por volta dos séculos III e II AEC. O crivo é bastante difundido atualmente em livros didáticos utilizados no ensino fundamental. Devemos perceber que além de verificar a primalidade de um número, o crivo permite encontrar primos menores do que número que estamos testando.

Exemplo 3.0.3: Verifique a primalidade de 101 pelo Crivo de Eratóstenes.

Primeiramente, façamos uma lista de 2 até 101. Depois de feito isso,marcarmos o número 2, primeiro número primo, e riscamos todos os seus múltiplos. Em seguida, marcamos o número 3 (primo), e riscamos os seus múltiplos na nossa lista. Sigamos

com o procedimento até o número 7, como vimos no método da divisão. Concluímos que o número 101 é primo, uma vez que não foi marcado.

Adicionalmente, se quisermos encontrar uma lista de primos menores que 101, só precisamos observar os números que não foram riscados no procedimento feito até os múltiplos de 7.

2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21
22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41
42	43	44	45	46	47	48	49	50	51
52	53	54	55	56	57	58	59	60	61
62	63	64	65	66	67	68	69	70	71
72	73	74	75	76	77	78	79	80	81
82	83	84	85	86	87	88	89	90	91
92	93	94	95	96	97	98	99	100	101

Figura 3.1: Crivo de Eratóstenes

Com isso, segue lista dos números primos menores ou igual a 101

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97,101\}.$$

Na busca de teste de primalidade mais eficientes, para grandes números, apresentamos um importante conceito.

3.1 Pseudoprimalidade

O Teorema 2.5.3 e o Corolário 4, ambos conhecidos como o Pequeno Teorema de Fermat, não garantem a validade da reciprocidade, ou seja, se a congruência mencionada for verdadeira, não significa que o número m é primo.

No entanto, podemos usar esses dois resultados para afirmar que um número é composto.

Proposição 22: Se existir um número a com $m \nmid a$ tal que

$$a^{m-1} \not\equiv 1 \pmod{m},$$

então m é um número composto.

Demonstração. O Corolário 4 (Pequeno Teorema de Fermat) nos fornece um teste de não primalidade. De fato, a congruência $a^{m-1} \equiv 1 \pmod{m}$ é válida para m primo e para qualquer a não divisível por m. Como $m \nmid a$ e $m \nmid a^{m-1} - 1$ segue que m não é primo. □

Exemplo 3.1.1: Verificamos que 51 é um número composto com auxílio da Proposição 22. De fato, $2^8 = 256 \equiv 1 \pmod{51}$. Decorre que $2^{50} = (2^8)^6.2^2 \equiv 4 \pmod{51}$.

Veremos que a recíproca do Pequeno Teorema de Fermat não é válida. Nesse sentido, apresentaremos um exemplo que confirma esse fato, a fim de introduzirmos nosso próximo estudo.

Exemplo 3.1.2: O número 91 satisfaz o Pequeno Teorema de Fermat para $a = 3$, mesmo não sendo primo.

De fato, temos que $3^6 \equiv 1 \pmod{91}$. Logo $3^{90} \equiv (3^6)^{15} \equiv 1^{15} \equiv 1 \pmod{91}$.

Definição 16: Dizemos que um número inteiro positivo composto m é *a-pseudoprimo* ou *pseudoprimo na base* $a \in \{2, 3, ..., m-1\}$ quando

$$a^{m-1} \equiv 1 \pmod{m}.$$

Caso $a = 2$, dizemos simplesmente que m é **pseudoprimo**. Ou seja, esse número satisfaz a congruência $2^{m-1} \equiv 1 \pmod{m}$.

De acordo com o Exemplo 3.1.2, **91 é pseudoprimo na base 3**. Continuaremos, apresentando alguns números pseudoprimos especiais.

De acordo com Shokranian ([7],p.65), os quatros primeiros números pseudoprimos com suas respectivas fatorações, são:

$341 = 11 \cdot 31$.

$561 = 3 \cdot 11 \cdot 17$.

$645 = 3 \cdot 5 \cdot 43$.

$1105 = 5 \cdot 13 \cdot 17$.

Obviamente, nenhum dos números listados são primos. Para além disso, vamos a mais uma definição.

Definição 17: Números de Carmichael

Se um número m é pseudoprimo para toda classe $a \in \{2, 3, ..., m-1\}$ dizemos que esse número é um *número de Carmichael*.

Os primeiros cinco números de Carmichael são: 561, 1105, 1725, 2465 e 2821. Suas respectivas fatorações, de acordo com Shokranian ([7],p.65),são:

$561 = 3 \cdot 11 \cdot 17$.

$1105 = 5 \cdot 13 \cdot 17$.

$1725 = 7 \cdot 13 \cdot 19$.

$2465 = 5 \cdot 17 \cdot 29$.

$2821 = 7 \cdot 13 \cdot 31$.

Note que esses números, quando fatorados, apresentam apenas três fatores. No entanto, tal fato não é válido para todos os números de Carmichael. Na sequência, traremos o primeiro número de Carmichael que possui 4 fatores. Posteriormente, o primeiro número com 5, fatores como podemos observar em Shokranian ([7],p.66):

$41041 = 7 \cdot 11 \cdot 13 \cdot 41$ e $825265 = 5 \cdot 7 \cdot 17 \cdot 19 \cdot 73$.

Apesar dos números de Carmichael serem raros, eles formam um conjunto infinito.A prova da infinitude dos números de Carmichael veio em 1994, por meio de um artigo de Alford, Granville e Pomerence, como podemos observar em Shokranian ([7],p.66). A raridade dos números de Carmichael pode ser atribuída ao fato de que

esses números devem satisfazer a uma série de condições. Os seguintes teoremas mostram essas condições e outras propriedades desses números.

Teorema 3.1.1: (Korselt 1899)
Um inteiro positivo $n = p_1p_2...p_k$, representado pelo produto de seus divisores primos p_i, é um número de Carmichael se, e somente se, os divisores p_i para todo $i = 1, 2,..., k$ são distintos e o mínimo múltiplo comum de $(p_1 - 1, p_2 - 1, ..., p_k - 1)$ divide $n - 1$.

Demonstração. Veja Shokranian ([7],p.67-67). □

Do Teorema 3.1.1, temos dois importantes resultados.

Corolário 11: n é um número de Carmichael se, e somente se, ele é livre de quadrados e $p - 1|n - 1$ para todo p divisor primo de n.

Demonstração. Veja em Shokranian ([7],p.67). □

Corolário 12: Números de Carmichael são ímpares e tem pelo menos três divisores primos.

Demonstração. Veja Shokranian ([7],p.67). □

Exemplo 3.1.3: Verificaremos que 561 é um número de Carmichael.
Solução:
Primeiramente, devemos notar que $561 = 3.11.17$ é ímpar e tem pelo menos três divisores primos, satisfazendo o Corolário 12. Para além, o número é livre de quadrados e também satisfaz as condições do Corolário 11: $p - 1|n - 1$ para todo $p \in \{3, 11, 17\}$. De fato,

a) $3 - 1|561 - 1$.

b) $11 - 1|561 - 1$.

c) $17 - 1|561 - 1$.

Por último, temos $mmc(p_1 - 1, p_2 - 1, ..., p_k - 1) = mmc(2,10,16) = 80$ que divide $561 - 1$.

Em seguida, apresentaremos mais um teste de primalidade, conhecido como Teorema de Lucas. A demonstração é baseada em Shokranian ([7],p.67).

3.2 Teorema de Lucas

Teorema 3.2.1: Seja $m \geq 3$ um número inteiro e seja $a \in \mathbb{Z}$ tal que $a^{m-1} \equiv 1 \pmod{m}$ e $a^x \not\equiv 1 \pmod{m}$ para todo x com $1 \leq x < m-1$. Então m é primo.

Demonstração. Pela primeira parte da nossa hipótese, a congruência $a^{m-1} \equiv 1 \pmod{m}$, temos que $mdc(a^{m-1},m)$ é 1. Portanto $mdc(a,m) = 1$. Por outro lado, a segunda parte da hipótese garante que os inteiros a^i e a^j, para $1 \leq i < j < m-1$, são incongruentes módulo m. De fato, caso contrário, teríamos $a^i \equiv a^j \pmod{m}$ e

$$a^i(a^{j-i} - 1) \equiv 0 \pmod{m}.$$

No entanto, $mdc(a,m) = 1$, o que implica que $mdc(a^i,m) = 1$ e, consequentemente, a^i é invertível módulo m. Daí $a^{j-i} \equiv 1 \pmod{m}$. Isso seria impossível, pois consideramos $a^x \not\equiv 1 \pmod{m}$ para todo x com $1 \leq x < m-1$ como hipótese. Sendo assim, os números $a, a^2,...,a^{m-1}$ são congruentes aos números 1,2,3,...,$m-1$ módulo m, não necessariamente nessa ordem. Pelo Teorema 2.5.2, tomaremos p, o menor divisor primo de m; então existe um inteiro positivo r, em que, $1 \leq r \leq m-1$, tal que $a^r \equiv p \pmod{m}$. Mas isso é impossível, pois $mdc(a,m) = 1$. Com efeito, se existisse um primo p com essa propriedade, teríamos $m|a^r - p$ e $p|m$. Logo $p|a^r - p$. Dessa forma $p|a^r$. Isso implica que $mdc(a,m) \geq p$. Logo não existem primos que dividem m, concluindo se tratar de um número primo. □

Ressaltamos que o teste de primalidade que utiliza o Teorema de Lucas como ferramenta é mais eficiente com o uso de recursos computacionais. Sendo assim, omitiremos exemplos com a utilização deste teste.

3.3 Teorema de Pocklington

Teorema 3.3.1: Teorema de Pocklingtom (1914)

Seja $m > 1$ um número inteiro e seja $s > 0$ um divisor de $m - 1$. Suponha que existe um inteiro a satisfazendo $a^{m-1} \equiv 1 \pmod{m}$ e $mdc(a^{(m-1)/(q)} - 1,m) = 1$ para todo divisor primo q de s. Então todo divisor primo p de m satisfaz a congruência

$$p \equiv 1 \pmod{s}, \text{ e se, } s > \sqrt{m} - 1,$$

m é primo.

Demonstração. Ver Shokranian ([7],p.68-69) □

Na sequência, apresentaremos alguns números especiais. Os primeiros são chamados de números de Fermat, em homenagem a Pierre Fermat.

Proposição 23: Sejam a e n números naturais maiores do que 1. Se $a^n + 1$ é primo, então a é par e $n = 2^m$.

Demonstração. Ver Hefez ([3],p.112). □

3.4 Números de Fermat

Definição 18: Os números da forma

$$F_n = 2^{2^n} + 1, \text{ em que } n = 0, 1, 2, ...,$$

são chamados de *números de Fermat*.

De acordo com Hefez ([3],p.112), Fermat achava que todo número escrito nessa forma fosse primo. Em 1640, ele teria escrito essa crença em uma de suas cartas enviadas para Mersenne, outro matemático . Vejamos os primeiros números de Fermat.

$$n = 0 \text{ temos, } F_0 = 2^{2^0} + 1. \text{ Logo, } F_0 = 3.$$
$$n = 1 \text{ implica que } F_0 = 2^{2^1} + 1 \text{ e } F_1 = 5.$$
$$n = 2 \text{ temos, } F_2 = 2^{2^2} + 1. \text{ Logo, } F_2 = 17.$$
$$n = 3 \text{ implica que, } F_3 = 2^{2^3} + 1. \text{ Logo, } F_3 = 257.$$
$$n = 4 \text{ temos, } F_4 = 2^{2^4} + 1. \text{ Logo, } F_4 = 65537.$$

Esses primeiros 5 números, pelo fato de serem primos, são chamados de **primos de Fermat**.

Fato é que, em 1732 o matemático Leohnard Euler mostrou que, para $n = 5$ temos um número de Fermat que não é primo. Até hoje, não sabemos se existem mais números primos de Fermat.

$$\text{Para } n = 5, \text{ decorre que } F_5 = 4294967297 = 641.6700417.$$

O número $F_6 = 18446744073709551617 = 2741177.67280421310721$ também não é primo.

Os seguintes teoremas indicam algumas propriedades bem conhecidas dos números de Fermat.

Teorema 3.4.1: Quaisquer dois números distintos de Fermat são primos entre si. Ou seja, se $n \neq m$ são números de Fermat, então $mdc(F_n, F_m) = 1$.

Demonstração. Ver Hefez ([3],p.112). □

Para finalizar o estudo dos números de Fermat, apresentamos um teorema que caracteriza esse tipo de número, como podemos obesrvar em Shokranian ([8],p.54).

Teorema 3.4.2: Um número de Fermat é primo ou é pseudoprimo.

Demonstração. Suponha que o número $F_n = 2^{2^n} + 1$ não seja primo. Repare que $F_n - 1 = 2^{2^n}$. Como todo número é divisível por si, temos que $2^{2^n} \equiv -1 \pmod{F_n}$. Elevando ambos os membros da igualdade a $2^{(2^n - n)}$, que notadamente é par, teremos

$$(2^{2^n})^{2^{(2^n - n)}} = 2^{2^{2^n}} = 2^{F_n - 1} \equiv 1 \pmod{F_n}.$$

Mostrando que F_n possui requisitos de um pseudoprimo. □

3.5 Números de Mersenne

Antes de apresentarmos outro conjunto de números especiais, os **números de Mersenne**, traremos um resultado.

Proposição 24: Sejam a e n números naturais maiores do que 1. Se $a^n - 1$ é primo, então $a = 2$ e n é primo.

Demonstração. Ver Hefez ([3],p.113) □

Um outro conjunto de números notáveis nos problemas de primalidade é o conjunto dos números de Mersenne. Esse conjunto recebe esse nome em homenagem ao monge e matemático francês, Marin Mersenne.

Definição 19: O número de Mersenne é da forma

$$M_n = 2^n - 1,$$

em que n é um número natural.

Seguem os 7 primeiros números de Mersenne.
$M_1 = 1$, $M_2 = 3$, $M_3 = 7$, $M_4 = 15$, $M_5 = 31$, $M_6 = 63$ e $M_7 = 127$.
De forma análoga aos números de Fermat, verificaremos que nem todo número de Mersenne é primo. Aqueles que possuem tal propriedade são chamados de **primos de Mersenne**.
Segue um exemplo com números primos.

Exemplo 3.5.1: Os primeiros primos de Mersenne são:

$n = 2$, temos $M_2 = 2^2 - 1$. Logo, $M_2 = 3$;
$n = 3$ implica que $M_3 = 2^3 - 1$ e $M_3 = 7$;
$n = 5$, temos $M_5 = 2^5 - 1$. Logo, $M_5 = 31$.
$n = 7$ implica que $M_7 = 2^7 - 1$ e $M_7 = 127$;
$n = 13$ implica que $M_{13} = 2^{13} - 1$ e $M_{13} = 8191$.

Não é difícil de perceber que no Exemplo 3.5.1, usamos somente números primos para encontrar os primos de Mersenne. No entanto, excluímos o número $M_{11} = 2047$, pois ele não é primo. Pode ser escrito como 23.89.

Nesse sentido, os números de Mersenne podem indicar a não primalidade de um número escrito nessa forma, uma vez que, se n não é primo, ocorre que M_n também não será primo. Como observsamos em Shokranian ([8],p.42).

Exemplo 3.5.2: De acordo com o Instituto de Matemática Pura e Aplicada (IMPA [5]), o maior número primo calculado é um número de Mersenne.

O maior número primo conhecido atualmente é o $2^{82.589.933} - 1$. Esse número foi descoberto em 7 de dezembro de 2018 por Patrick Laroche, um voluntário do projeto GIMPS (Great Internet Mersenne Prime Search). Ele é um número de Mersenne com 24.862.048 dígitos.

4

Contexto Histórico da Criptografia

Traremos, neste capítulo, um breve resumo de como surgiu e se desenvolveu a criptografia. O objetivo aqui proposto é mostrar para o leitor que poucas vezes, ou nunca, ouviu falar nesse termo e o seu papel importante desempenhado junto ao desenvolvimento da sociedade. Iniciamos com a definição apresentada por Menezes Neto ([6],p.7),

> *Criptografia é a arte de cifrar, codificar mensagens de modo que o texto fique incompreensível para leitores não autorizados.*

O termo criptografia se originou de duas palavras gregas, *Kryptos* que significa segredo ou oculto, e *graphein* que designa as palavras escrita ou escrever. Seu surgimento pode ser tão antigo quanto à própria escrita. Em muitos momentos, civilizações antigas precisavam manter informações importantes ocultas a fontes não autorizadas. Mensagens com essas características são encontradas no sistema de escrita Hieroglífica dos egípcios, veja Carneiro ([2],p.3). Atualmente, ainda vivemos essa realidade, informações de segredos de Estado são exemplo de comunicação sigilosa.

Notamos também, uma mudança criada ao longo da história.Nesse sentido, apresentaremos alguns modelos criptográficos, começando com um método de codificação de mensagens utilizado durante o Império Romano.

4.0.1 Cifra de substituição

Esse modelo de criptografia consiste na troca de cada letra da mensagem original por um caractere do alfabeto de cifras (alfabeto). A cifra de substituição mais conhecida é também chamada de "**Cifra de César**", por ter sido constantemente usada pelo imperador romano Júlio César. Era seu meio de comunicação sigilosa.

Segundo Carneiro (p.6, [2]), o método de codificação de Júlio César era realizado por meio da substituição de cada letra de sua mensagem original por outra letra do alfabeto, que ficava a três posições adiante, ou seja, substituía a letra "A" pelo "D", por exemplo, a letra "B" pelo "E", e assim por diante.

Na tabela da Figura 4.1, as linhas 1 e 3 representam o texto original, já as linhas 2 e 4 referem-se as cifras de César.

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

Figura 4.1: Cifra de César (autoria própria)

Exemplo 4.0.1: Vamos codificar a mensagem "a matemática é bela", utilizando a Cifra de César.

Mensagem	A	M	A	T	E	M	A	T	I	C	A	E	B	E	L	A
Cifra	D	P	D	W	H	P	D	W	L	F	D	H	E	H	O	D

Tabela 4.1: Codificação pela Cifra de César (autoria própria)

A mensagem cifrada parece sem sentido, obviamente esse é o objetivo. No entanto, não teríamos muito esforço para descobrir o seu significado por se tratar de uma mensagem codificada pela Cifra de César. De fato, teríamos somente mais 25 valores possíveis para as chaves, revelando assim o conteúdo da mensagem. Esse é o primeiro ponto de vulnerabilidade desse método de criptografia.

A Cifra de César é um tipo de **Cifras de Substituição Monoalfabética**, uma vez que realiza a substituição de letra por letra. A chave de segurança, nesse caso, representa quantas posições devemos avançar no alfabeto para encontrar a cifra correspondente ao texto original. Analisando a frequência com que os códigos aparecem, podemos associá-los às letras que apresentam maior ocorrência nas palavras de um determinado idioma. Segue tabela [1],com a frequência de cada letra, no alfabeto da língua portuguesa.

A	14.63%	N	5.05%
B	1.04%	O	10.73%
C	3.88%	P	2.52%
D	4.99%	Q	1.20%
E	12.57%	R	6.53%
F	1.02%	S	7.81%
G	1.30%	T	4.34%
H	1.28%	U	4.63%
I	6.18%	V	1.67%
J	0.40%	W	0.01%
K	0.02%	X	0.21%
L	2.78%	Y	0.01%
M	4.74%	Z	0.47%

Figura 4.2: Frequência de cada letra

A letra "A" apresenta a maior frequência. Outras características da escrita na língua portuguesa são que a letra "Q" sempre é seguida pela letra "U", bem como o fato da letra "N" nunca preceder a letra "B" e "P". Isso nos dá dicas para a revelação das cifras, diminuindo a inviolabilidade do sistema de encifração.

[1]Tabela encontrada em https://www.gta.ufrj.br/grad/06_2/alexandre/criptoanalise.html, acesso em 29/03/2024

Segundo Singh [9], durante a "era de ouro" da civilização islâmica, por volta do século VII, os árabes manipulavam e possuíam conhecimentos relacionados à Cifra por substituição monoalfabética. Manuais administrativos, datados do século X, possuem um seção específica sobre criptografia. Documentos com segredos de estado codificados evidenciam o uso rotineiro desse conhecimento pelo povo árabe. Além disso, eles não só eram capazes de codificar mensagens, mas também de decifrá-las. Assim, é atribuído a esses povos a criação da *criptoanálise*, que em resumo é o entendimento do texto original a partir do texto cifrado, mesmo sem conhecer a chave de segurança. Os *criptoanalistas* são os responsáveis pela quebra da segurança de um sistema criptográfico. O cientista árabe conhecido por al-Kindi, ainda no século IX, publicou um trabalho no qual descreve uma técnica para decifrar textos, é o que conhecemos como *análise de frequência*. No entanto, ainda de acordo com o autor, não existem registros que mostrem a relevância do conhecimento desenvolvido pelos árabes na história da criptografia.

Ainda de acordo com Singh [9], a reintrodução da criptografia, na cultura ocidental, ocorre em grande parte por meio dos monges medievais. Somente no século XIII, surge a primeira produção que descreve o uso da criptografia escrito pelo monge franciscano inglês, Roger Bacon. Daí em diante, o estudo da criptografia ganha força na Europa. Mudanças nas organizações sociais e movimentos históricos como a Renascença favoreceram a utilização e estudo da criptografia.

Se por um lado, os criptoanalistas vão se desenvolvendo cada vez mais, os "criptográficos", responsáveis pela criação e desenvolvimento de métodos seguros de escritas secretas, precisavam não só acompanhar esse desenvolvimento, mas estar um passo à frente dos criptoanalistas que por sua vez, estavam, cada vez mais, atualizados acerca da análise de frequência das letras. Esse fato vai enfraquecendo a segurança do modelo de criptografia monoalfabética. Surge assim, a necessidade, por parte dos criptógrafos, de se criar métodos mais seguros e difíceis de terem sua segurança quebrada. Um modelo de cifra de substituição que promete atender a essa demanda é a **cifra polialfabética**.

No fim do século XVI, mais especificamente em 1586, um tratado sobre escrita secreta é publicado pelo diplomata francês Blaise de Vigenère. Esse trabalho, com o título "Traicté des Chiffres", é a consolidação de ideias e conhecimentos de outros estudiosos do tema. Dentre eles, Leon Battista Alberti merece destaque especial. Apesar do italiano ser conhecido por suas contribuição à arquitetura renascentista, suas ideias em utilizar dois ou mais alfabetos, no processo de cifragem, com o propósito de evitar a análise da frequência das letras, é o início para que outros estudiosos desenvolvessem esse procedimento até chegamos à teoria publicada por Vigenère.

É necessário ressaltar uma importante invenção, a primeira "máquina criptográfica" de que se tem registro. Estamos falando do **Disco de Cifra** de Leon Alberti. O arquiteto italiano, além de iniciado os estudos das cifras polialfabéticas, introduz a primeira ideia de "automação" na criptografia com a confecção dessa "ferramenta". Em resumo, como observamos em Hefez ([3],p.213), a invenção era composta por dois discos concêntricos com uma agulha no centro. O disco maior, era fixo, ficava

embaixo e possuía em sua borda um alfabeto com 20 letras e os números de 1 a 4, para a escrita da mensagem original. Na borda do disco menor, que girava, encontrava-se um alfabeto, com exceção das letras *j*, *u*, *w*, além da palavra em latim *et*, todas minúsculas e em uma ordem pré-estabelecida, alinhadas com as letras do disco maior. Para codificar uma mensagem, tanto o destinatário quanto o remetente possuíam discos idênticos, além de ter combinado previamente, uma posição inicial para o disco menor ao iniciar o procedimento de cifragem. Assim, cada letra da mensagem original era substituída pela letra do disco menor, originando a mensagem codificada.

Alberti vai mais além e introduz a cifra polialfabética em sua máquina utilizando o seguinte procedimento. A cada grupo de palavras, pré-determinadas entre as fontes envolvidas na comunicação, o disco era girado e a cifragem iniciava-se novamente, tomando a letra A do disco maior como referência para as novos grupos de cifras do disco menor. Dessa forma, um código poderia ter valores diferentes de referência na mensagem original. Segue imagem do artefato.

Figura 4.3: Disco de Cifras Fonte:https://cgreinhold.dev/2020/03/18/crypto2 acesso em 02/04/2024.

Outra contribuição importante, segundo Hefez ([3],p.214), é atribuída ao intelectual alemão Johannes Trithemius, que em uma publicação em 1518, propõe um sistema de criptografia em forma de uma tabela com 26 alfabetos alternados, denominada tabela recta. Nessa tabela, escrevemos na primeira linha o alfabeto em sua ordem original, na segunda linha inserimos o alfabeto iniciado pela segunda letra original. Procedemos assim, até a vigésima sexta linha que iniciará com a última letra do alfabeto original. Logo, os alfabetos são inseridos na sequência de uma permutação circular.

A consolidação do processo de substituição polialfabética ocorre por meio ideias do italiano Giovanni Battista Bellaso, que introduz a utilização de uma chave no processo que utilizava a tábua recta de Trithemius. Mais tarde, esses trabalhos são descritos, com a alteração de poder utilizar o próprio texto original como chave, vindo a ser publicado por Blaise de Vigenère. A partir desse momento, a tabela recta fica conhecida pelo sobrenome de Blaise.

Para codificar uma mensagem usando a cifra polialfabética e utilizando a tabela de Vigenère, é necessário criar uma chave, que deve ser conhecida somente pelos remetente da mensagem e pelo seu destinatário. Essa chave pode ser um número,

uma palavra ou até mesmo uma frase. Logo após, a palavra-chave era escrita sobre a mensagem original repetidas vezes, de modo que cada letra da mensagem original ficasse associada a uma letra da palavra-chave. A cada par de letras da palavra chave, a mensagem original será correlacionada com a primeira letra da linha (que contém a letra da mensagem original, no interior da tabela). Vejamos um exemplo.

Exemplo 4.0.2: Codificação da frase "A MATEMÁTICA É BELA", usando a chave "FERMAT".

Para encontrar cada cifra da mensagem, na coluna da letra da palavra chave, procuramos a letra da mensagem original. Feito isso, termos a letra da mensagem original será a interseção entre a coluna (chave) e linha (texto original). Logo a primeira letra dessa linha será a cifra procurada. Prosseguimos assim, até a última letra da mensagem que desejamos cifrar. Acompanhe na tabela.

Palavra-chave	F	ERMATFERMA	T	FERMA
Mensagem original	A	MATEMÁTICA	É	BELA
Mensagem cifrada	V	IJHETVPRQH	Z	XNZA

Tabela 4.2: autoria própria

Para melhor entendimento, o leitor pode consultar a Tabela 9.1 do Apêndice B, na qual retiramos as cifras.

Ao observarmos atentamente a mensagem codificada: "V I J H E T V P R Q H Z X N Z A", encontraremos dificuldades em ralizar a análise de frequência das letras. Por exemplo, a cifra "V" aparece duas vezes, "ocupando" o lugar da letra "A", no entanto, a cifra "Z", ora ocupa o lugar da letra "E", ora substituiu "L" na mensagem original. Isso demonstra que, nesse método, à análise de frequência de letras não funciona muito bem.

Para decodificar a mensagem, procedemos de maneira análoga. Vejamos como deve ser feito, com uma cifra, para ampliarmos o entendimento. Como temos a chave para decodificar a cifra "V", por exemplo. Por se relacionar com a primeira letra da chave ("F"), devemos procurar a letra que está, simultaneamente, na coluna F e na linha "V". Nesse caso, temos que a letra "A" da Tabela de Vigenère é a interseção procurada. Assim, essa será a letra da mensagem original. O procedimento deve seguir até a última cifra.

4.0.2 Cifra de Transposição

Este método de codifição tem como característica fundamental o embaralhamento das letras da mensagem original. Logo a mensagem original é transportada para um ou vários anagramas. Existem variações de codificações dentro desse modelo, no entanto, esses procedimentos seguem a premissa de transpor a mensagem. Iniciamos as apresetações dessas variações, por uma técnica considerada por Carneiro ([2],p.4) como a forma mais simples de utilização desse método. Carneiro chama este método de transposição por **Cerca de Ferrovia**. Consiste em escrever a mensagem original em uma sequência de diagonais de duas linhas. Na primeira linha, colocamos a

primeira letra da mensagem original e saltamos a segunda, escrevendo a terceira e saltando a quarta letra. Continuamos com esse procedimento até a última letra. Em seguida, dessa última letra, começamos a escrever as letras que saltamos, uma após a outra. Vejamos um exemplo.

Exemplo 4.0.3: Criptografando a mensagem "A MATEMÁTICA É BELA", utilizando a Cerca de Ferrovia.

Solução: Vamos escrever a mensagem em duas linhas, na primeira linha colocamos a primeira letra e saltamos a segunda, colocamos a terceira letra e saltamos a quarta e prosseguimos assim até o final da frase. Já a segunda linha, contém as letras que saltamos ao realizar o passo anterior.

A - A - E - A - I - A - B - L
M - T - M - T - C - E - E - A

Mensagem criptografada: AAEAIABLMTMTCEEA.

Observando a mensagem codificada, temos a impressão que não foi utilizado o método de substituição, uma vez que tem muitos códigos iguais em sequência. Logo, analisar a frequência das letras não ajuda muito na revelação da mensagem.

Para decodificar a mensagem, devemos realizar o caminho inverso, ou seja, escrever as letras que aparecem em ordem ímpares na primeira linha, saltando um espaço entre elas, e as demais letras na segunda. Para finalizar, basta transpor as letras da segunda linha para os espaços que deixamos na primeira linha.

Outro procedimento, denominado **método retangular**, compõe-se pela escrita da mensagem em uma tabela retangular e pelo uso de uma chave de segurança. Nesse sentido, o procedimento se apresenta mais robusto do que o anterior. Para realizarmos a codificação da mensagem, devemos, primeiramente, definir uma chave que deve ser conhecida pelas fontes envolvidas na comunicação. Logo após, colocamos essa palavra em uma tabela, cada letra em uma coluna, assim teremos que o número de colunas da tabela é igual ao número de letras da palavra chave. Na linha debaixo, escrevemos a mensagem, cada letra numa coluna, criando várias linhas nessa tabela. Os espaços vazios tabela podem ser preenchidos por caracteres aleatórios. Para terminar, escrevemos cada coluna de letras (que serão anagramas), seguindo a ordem crescente de posição das letras da palavra chave. Vejamos na prática a operacionalização do método.

Exemplo 4.0.4: Criptografando a mensagem "UM ALUNO DEDICADO", utilizando a chave EULER.

A mensagem criptografada é UNI LED ADA UDO MOC.

Como a chave escolhida possui cinco letras, a mensagem final será composta por cinco anagramas.

Para o destinatário realizar a decodificação da mensagem, ele deve proceder de maneira análoga, ou seja, construir uma tabela, colocando a chave na primeira linha e posteriormente inserir os anagramas em cada coluna, seguindo a ordem de posição de cada letra da palavra chave.

Palavra-chave	E	U	L	E	R
Ordem	1	5	3	2	4
Mensagem original	U N I	M O C	A D A	L E D	U D O

Tabela 4.3: Método retangular (autoria própria)

É perceptível a dificuldade de se quebrar a segurança desse método. Contudo, o problema maior surge na distribuição da chave. É difícil distribuir, com segurança, uma chave entre um grupo maior de destinatários da mensagem. Mais além, criar várias chaves, para distribuí-las tambem não parece uma tarefa simples. Então, esse método se inviabiliza por esses motivos.

Percebemos em Singh [9] que apesar da pouca segurança, as cifras monoalfabéticas ofereciam comodidade e praticidade tanto momento da encifração como na decifração. Foi o método que chegou até a população comum. Assim uma pessoa com pouca instrução em criptografia podia guardar, por exemplo, segredos íntimos em suas agendas.

O próximo método de criptografia é baseado na substituição de letras, mas impõe uma maneira matemática de criar chaves de segurança, que determinam como devem ser feitas as substituições das letras pelas cifras. Veremos que este sistema de criptografia diferencia-se de todos os sistemas descritos até o momento por não utilizar *chaves de segurança simétricas*. Até agora, utilizamos processos que dispõem de *chaves simétricas*, ou seja, a chave que é utilizada para fazer a codifiacão da mensagem é **a mesma** usada para a decodificação.

4.0.3 Cifra Afim

Nesse processo, utilizaremos a função polinomial de primeiro grau e suas propriedades para criptografar mensagens. Assim, utilizaremos *chaves assimétricas de segurança*. Neste caso, a chave construída para o processo de codificação da mensagem é diferente da chave utilizada para decodificar a mensagem. A inversa de uma função afim, na maioria das vezes, é diferente.

$$\text{Mensagem Original} \rightarrow \text{Mensagem Codificada}$$

$$\text{Mensagem Codificada} \rightarrow \text{Mensagem Original}$$

Nesse sentido, traremos um breve estudo acerca desse método, sob orientações de Menezes Neto ([6],11-17), objetivando uma aplicação matemática.

O processo de codificação, inicia-se com a construção de um dicionário de caracteres que deve ser conhecido entre as partes envolvidas na comunicação. Definimos aqui que o nosso dicionário será construído pela substituição da letra A pelo número 0 (zero), a letra B pelo 1 e assim por diante, até termos a letra Z substituída pelo número 25.

O próximo passo deve ser: definir entre as fontes uma chave de codificação. Nesse caso, devemos definir uma função polinomial do primeiro grau.

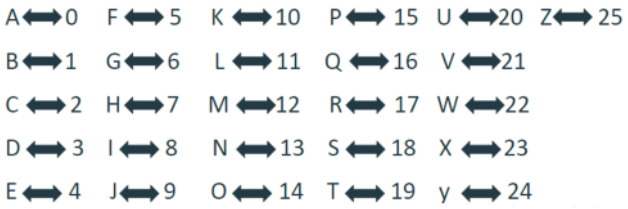


Figura 4.4: Alfabeto de caracteres

Seja $f : \mathbb{R} \to \mathbb{R}$ tal que $f(x) = ax + b$, em que a,$b \in \mathbb{R}$, com $a \neq 0$. Sua função inversa é dada por

$$f^{-1}(x) = cx + d,$$

em que $c = \frac{1}{a}$ e $d = -\frac{b}{a}$.

Agora, devemos substiuir x pelo valor de cada letra, de acordo com o alfabeto de cifras, na função afim e calcular $f(x)$. Assim, a mensagem vai sendo codificada, letra por letra.

Exemplo 4.0.5: Vamos criptografar a palavra "ARITMÉTICA" usando a chave $f(x) = 11x + 5$.

Solução:

Seja $f : \mathbb{R} \to \mathbb{R}$ tal que $f(x) = 11x + 5$.

Primeiro vamos substituir cada letra da mensagem original pelo número correspondente no dicionário de cifras. Neste caso, utilizaremos o dicionário apresentado na Figura 4.4.

Logo em seguida, vamos encontrar cada uma das imagens da função em cada número (pré-código) dado.

Para A $= 0$, temos $f(0) = 11.0 + 5 = 5$. Além disso, temos:
R $= 17$, logo $f(17) = 11.17 + 5 = 192$.
I $= 8$, então $f(8) = 11.8 + 5 = 93$.
T $= 19$, segue que $f(19) = 11.19 + 5 = 214$.
M $= 12$, assim $f(12) = 11.12 + 5 = 137$.
E $= 4$, logo $f(4) = 11.4 + 5 = 49$.
T $= 19$, segue que $f(19) = 11.19 + 5 = 214$.
I $= 8$, então $f(8) = 11.8 + 5 = 93$.
C $= 2$, então $f(2) = 11.2 + 5 = 27$.
A $= 0$, assim $f(0) = 11.0 + 5 = 5$.
A mensagem criptografada é 5 192 93 214 137 49 214 93 27 5.

Para decodificar a mensagem, basta encontrarmos a chave para a decodificação, que é a inversa da função dada. Logo usaremos a função $f^{-1}(x) = \frac{x}{11} - \frac{5}{11}$. Substituindo cada valor de $f^{-1}(x)$, revelando o conteúdo secreto da mensagem através da consulta ao alfabeto de caracteres.

4.0.4 Máquinas criptográficas

Entre os séculos XVI e XIX, o estudo da criptografia ficou adormecido, restrito a teóricos da área que, por 300 anos, consideraram inquebrável a cifragem polialfabética. Em meados do século XIX, o inglês Charles Babbage e o polonês Friedrich Kasiski, em estudos independentes, conseguiram quebrar a segurança desse sistema, veja Hefez ([3],p.215).

Ainda assim, as cifras polialfabéticas (ou suas variações misturadas com as cifras monoalfabéticas) voltaram a ser utilizadas com a criação de maquinas cifradoras. Como observamos em Singh ([9]), duas dessas máquinas são mais conhecidas devido ao importante papel desempenhado durante a Segunda Guerra Mundial. Uma é a máquina eletromecânica *Enigma*, criada pelo alemão Arthur Scherbius, ainda no início do século XX, sendo inspirada no disco de Alberti. A outra a japonesa *Purple*, uma adaptação da primeira. De maneira resumida, essas máquinas faziam o trabalho mecânico que antes era realizado pelos criptógrafos, contudo, as transmissões das mensagens eram realizadas por meios de télegrafos ou via rádio.

Voltando ao período da Segunda Guerra Mundial, ainda de acordo com Singh ([9]), devemos salientar o papel fundamental dos britânicos e aliados que conseguiram, com muito esforço, quebrar a seguranças das cifras produzidas pela máquina alemã, Enigma. A quebra da comunicação secreta dos alemães ocasionou grande impacto na guerra, uma vez que os países europeus do bloco dos Aliados sofriam consideravelmente com avanços cada vez mais frequentes das forças militares alemãs. Dessa forma, as forças armadas dos Aliados começam a ganhar vantagem sobre os alemães por estarem sempre adquirindo informações sobre suas estratégias de combantes, acabavam assim com o fator da imprevisibilidade dos ataques nazistas, considerada como um dos principais fatores de vantagem até o momento. A partir desse momento, a guerra tem sua duração encurtada, levando os Aliados a vitória. A quebra do código se deu por vários trabalhos do matemático inglês Alan Turing, uma das mentes mais brilhantes do século XX e considerado como um dos pais da computação, segundo Hefez ([3],p.215-216).

As invenções do rádio, telégrafos e, finalmente os computadores, revolucionaram, cada um a seu tempo e modo, a Teoria da Informação. Assim que os computadores se tornam mais acessíveis, a uniformização dos processos de criptografia se torna realidade.

Como os computadores utilizam códigos binários, toda a informação deve ser inserida através desse código, ou seja, utilizando apenas os caracteres 0 e 1. A partir dos anos 1960, nasce o Americam Standard Code for Information Interchang ou ASCII. Esse não era um sistema de cifragem, na verdade tratava-se de uma tradução dos símbolos mais utilizados na comunicação para a linguagem binária . Ela transformou os símbolos que utilizamos para nos comunicar, como letras, algarismos, sinais de pontuação, em números de sete algarismos formados apenas por 1 e 0.

Várias empresas buscavam implementar agora a tão desejada padronização dos processos criptográficos, quando em 1973, a empresa norte america IBM desenvolveu um complexo sistema de criptografia. A esse sistema deran o nome de Data Encrytion

Standard (DES), que foi adotado pelo governo americano e utilizado até o ano de 1999. Esse programa funcionava com a utilização de chaves simétricas de segurança. Isso criou um enorme problema logístico na distribuição dessas chaves, uma vez que a segurança de todo sistema estava na preservação da segurança das chaves. Nesse contexto, surge a necessidade de distribuir essas chaves de maneira mais racional.

Os norte americanos Whitfield Driffie, Martin Hellman e Ralph Merkle quebraram o paradigma da transferência de chaves entre duas fontes sem a interferência de um portador dessas chaves. É assim que a Teoria dos Números entra em cena na criptografia, fazendo-se valer das congruências e mudando o rumo desses processos, como podemos observar em Hefez (p.216,[3]). Driffie considerou a ideia de usar duas chaves, uma para criptografar, sendo esse processo realizado sem grandes dificuldades, e outra chave para descriptograr. Nesta etapa, ele conjecturou que devesse ser impossível de se realizar o processo de decifragem sem a chave. No entanto, ele não conseguiu por em prática suas ideias, mas ainda sim publicou na esperança de que outros conseguissem resolver. A partir daí, inicia-se uma nova revolução nos sistemas de cripitografia.

4.0.5 Sistema RSA de Criptografia

Primeiramente, devemos relembrar que Diffie e Hellman convenceram o mundo que havia solução para o problema para distribuição das chaves. Eles acreditavam que um sistema de codificação com uso de chaves assimétricas, no qual a chave para codificar é diferente da chave para decifrar, era o caminho que mudaria os rumos da criptografia. Uma *função de mão única* é aquela na qual o "caminho" utilizado na *encriptação* da mensagem **não** é o mesmo do "caminho" usado na *desencriptação*. Apesar de não conseguirem encontrar uma função com essas características, os dois americanos mostraram ao mundo que isso poderia se tornar realidade. Eles abriram caminho para três pesquisadores do Instituto de Tecnologia de Massachussets (MIT), **Ron Rivest** e **Adi Shamir**, cientistas da computação e **Leonard Adleman**, um matemático. Segundo Carneiro (p.21, [2]), no ano de 1977, Rivest escreveu, em uma única noite, toda teoria que os três já vinham investigando há mais de um ano. Adleman ficou responsável pela revisão e tinha por objetivo apontar falhas e inconsistências na teoria. Porém, nesse material, não encontrou qualquer erro ou equívoco que impedisse a validade da teoria ali aplicada. Assim, o trabalho desses três pesquisadores recebeu o nome de **RSA** em alusão a Rivest, Shamir e Adleman, tornando-se um sistema de cifras influente da Criptografia moderna.

Vejamos os detalhes matemáticos que possibilitam a efetivação de um sistema com duas chaves assimétricas. O passo a passo seguinte é uma adaptação do que foi apresentado por Shokranian ([7],p.47) em forma de um teorema.

Criptografando e Descriptografando

Imaginemos que Fernanda deseja enviar uma mensagem secreta para sua filha Sofia. Nesse sentido, a filha produz duas chaves assimétricas, uma denominada por **chave pública**, usada para codificar a mensagem e a outra **chave privada**, essencial para a decodificação. A chave pública é formada pelo par de números (n,e), em que n

é o produto de dois números primos p e q, muito grandes e distintos, que devem ficar sob sigilo. A filha define também o número e, de modo que seja um número natural tal que $mdc(e, \varphi(n)) = 1$. Essa chave é enviada para Fernanda que irá codificar a mensagem seguindo os passos abaixo, logo depois a mensagem estará pronta para o envio.

a) Realizar a pré-codificação da mensagem, ou seja, substituir cada letra do texto original por um código do alfabeto de caracteres numéricos pré-estabelecido com o destinatário da mensagem.

b) Em seguida, ela enfileira todos os códigos, transformando-os em um único número com muitos dígitos. Logo após, separa-os em blocos $T_1, T_2, ...T_r$ de forma que todos sejam menores do que n e não inicie com o algarismo zero. Além disso, Fernanda deve escolher blocos que não sejam múltiplos de p e nem de q.

c) Para codificar sua mensagem, Fernanda define cada número

$$C_i \equiv T_i^e \pmod{n},$$

para todo i = 1,2,3,..,r. Então a mensagem recebida por Sofia será:

$$C_1C_2C_3...C_r.$$

A condição de que os blocos não ultrapassem o número n é para evitar sua alteração quando for reduzido módulo n. Além do mais, se não iniciar com zero, podemos recuperar a sequência em que os blocos foram separados depois da pré-codificação. Assim recuperaremos também a mensagem original.

Para decodificar a mensagem, Sofia utiliza sua chave privada formada pelo par (n,d), no qual d é um número natural definido pelas duas condições:

$$ed \equiv 1 \pmod{\varphi(n)} \text{ e } 1 \leq d < \varphi(n).$$

Então basta que ela aplique a sua chave privada nas cifras por meio da relação

$$T_i \equiv C_i^d \pmod{n}$$

para cada i = 1,2,3,..,r. Assim, ela recupera a mensagem original $T_1, T_2, ...T_r$. Usando o alfabeto de cifras revela seu significado.

Apontamos os detalhes aritméticos que mostram como esse procedimento é o inverso da codificação.

Ao iniciarmos o processo matemático, definimos

$$C_i \equiv T_i^e \pmod{n} \text{ para cada } i = 1,2,3,..,r.$$

Decorre que

$$C_i^d \equiv (T_i^e)^d \equiv T_i^{ed} \pmod{n}.$$

Como $ed \equiv 1 \pmod{\varphi(n)}$, existe um $k \in \mathbb{N}$ tal que $ed = k\varphi(n) + 1$. Dessa forma, temos:

$$C_i^d \equiv T_i^{ed} \equiv T_i^{k\varphi(n)+1} \equiv T^{k\varphi(n)}.T_i \equiv T_i \pmod{n}.$$

Para finalizar nossa justificativa, vale relembrar que, pelo Teorema 2.7.3 (Teorema de Euler) e a Proposição 9, vale a seguinte congruência:

$$T^{k\varphi(n)} \equiv 1 \pmod{n}.$$

Mesmo que uma fonte conheça a chave pública, ela precisará encontrar os números p e q para determinar a chave privada. No entanto, a decomposição de números muito grandes em fatores primos é extremamente trabalhosa e demorada, até mesmo para os sistemas computacionais mais avançados.

Observamos que a chave pública pode ser conhecida por todos. Ao mesmo tempo, ela está ligada a uma chave privada, muito difícil de ser encontrada para aqueles que não conhecem esses números primos que determinaram a chave pública. Essa é uma das grandes vantagens que o sistema de criptografia RSA tem sobre os outros modelos estudados.

Mas ainda falta resposta para um último questionamento: como ter certeza que a mensagem codificada, enviada por Fernanada, foi preservada durante o envio? Essa mensagem, dificilmente pode ser decifrada, no entanto, o procedimento até aqui feito, não garante sua veracidade, ou seja, alguma fonte poderia interceptar e corromper essa mensagem. Vejamos agora, como garantir a verificação de veracidade de uma mensagem criptografada.

Assinaturas

A utilização de assinaturas em mensagens criptografadas poderia ter salvado a vida de Maria, ex-rainha da Escócia, em meados do século XVI, e de seus fiéis seguidores. A história do trágico fim da rainha Maria, decaptada no ano de 1587, a mando de sua prima a rainha da Inglaterra Elizabeth I, é um fato histórico bem conhecido. No entanto, detalhes dessa história, encontrados na leitura de Singh [9], nos chamam a atenção. Segundo o autor, quando ainda estava em uma prisão inglesa, Maria comunicava-se com alguns aliados por meios de cartas criptografadas. O intuito era fugir da prisão, matar a rainha Elizabeth I e tomar novamente o seu trono na Escócia. Esse plano foi descoberto, uma vez que a guarda real da rainha inglesa possuía conhecimentos para quebrar a segurança de cifras por substituição monoalfabética. A guarda de Elizabeth I não só teve acesso aos conteúdos das mensagens. Modificaram algumas mensagens trocadas entre Maria e seus alidos, que não desconfiaram do que estava ocorrendo. Assim, acabaram revelando quem estava ajudando a princesa escocesa em seu plano. Maria recebe a pena de morte.

Para termos confiança que a mensagem recebida é realmente autêntica, devemos verificar sua assinatura. Nos dias atuais, usamos a assinatura a próprio punho, e mais recentemente, contamos com o certificado digital para validar assinatura em

documentos. Um resultado apresentado por Shokranian ([7],p.54-58) revela como ocorre a assinatura de uma mensagem sigilosa codificada pelo sistema RSA.

Lembramos que Sofia havia definido suas chaves, a pública (n,e) e a privada (n,d). Por outro lado, Fernanda também precisa definir duas chaves, a pública (n',e') e a privada (n',d'). O processo de assinatura é dividido em dois casos:

1) Primeiro caso: $n' \leq n$ (O n' de quem envia é menor ou igual do que n de quem recebe).

   Fernanda deve seguir os passos:

   a) Pré-codifica a mensagem no dicionário digital e escreve a mensagem digital T. No entanto, ela deve verificar que ao quebrar a mensagem T em blocos $T_1, T_2, ...T_r$, cada um desses blocos não deve iniciar com 0 (zero). Terá que ser menor do que n' (este caso, será menor do que n também). Além disso, cada bloco deve ser coprimo com tanto com n' quanto com n.

   b) Fernanda assina a mensagem, utilizando os parâmetros da sua chave privada, para isso, ela determina números $c_1, c_2, ...c_r$, de modo que

   $$c_i \equiv T_i^{d'} \pmod{n'},$$

   para todo $i = 1, 2, ...r$.

   c) Agora ela determina as cifras $C_1, C_2, ...C_r$, sendo que

   $$C_i \equiv c_i^{e} \pmod{n},$$

   para todo $i = 1, 2, ...r$. Percebe-se que os números C_i são menores dos que n.

   Assim termina o processo de transmissão de uma mensagem com assinatura.

   Para que Sofia tenha certeza da autenticidade da mensagem e consiga decifrá-la, ela deve realizar o seguinte procedimento:

   d) Decifra os números $C_1, C_2, ...C_r$, usando sua chave privada, ou seja, ela deve determinar os números

   $$u_i \equiv C_i^{d} \pmod{n},$$

   para todo $i = 1, 2, ...r$.

   Nessa etapa, temos que $u_i < n$. Na verdade, pode-se verificar que u_i é o próprio c_i. Com efeito, observamos que

   $$u_i \equiv C_i^{d} \equiv (c_i^{e})^{d} \pmod{n},$$

   para todo $i = 1, 2, ...r$. Para além,

   $$u_i \equiv c_i^{ed} \equiv c_i^{k\varphi(n)+1} \equiv {c_i}^{k\varphi(n)} \cdot c_i \equiv c_i \pmod{n}.$$

e) Sofia, nesse momento, usa a chave pública de Fernanda para revelar o conteúdo da mensagem. Nesse sentido, determina os números

$$y_i \equiv u_i^{e'} \pmod{n'},$$

para todo $i = 1, 2, ...r$. Verificamos que $y_i < n'$. Temos que y_i é o próprio T_i escrito por Fernanda, pois:

$$y_i \equiv u_i^{e'} \equiv c_i^{e'} \equiv (T^{d'})^{e'} \equiv T_i \pmod{n'}.$$

Uma vez que,

$$T_i^{e'd'} \equiv T_i^{k'\varphi(n')+1} \equiv T_i \pmod{n'}.$$

Desse modo, ela realiza o processo inverso de pré codificação e revela o conteúdo original da mensagem recebida.

2) Segundo caso: Se $n \leq n'$, o procedimento deve ser realizado do seguinte modo:

a) Como feito, no primeiro caso, Fernanda pré-codifica a mensagem no dicionário digital, e escreve a mensagem digital T, verifica que os blocos $T_1, T_2, ...T_r$, são menores do que n (neste caso, serão menores do que n' também). Ela deve garantir também que cada bloco deve ser coprimo tanto com n' quanto com n, além de não iniciar com 0 (zero).

b) Fernanda determina as cifras abaixo, utilizando a chave pública de Sofia.

$$c_i \equiv T_i^{e} \pmod{n},$$

para todo $i = 1, 2, ...r$.

c) Agora, ela deve assinar as cifras usando a sua chave privada, para isso determina C_i de modo que

$$C_i \equiv c_i^{d'} \pmod{n'},$$

para todo $i = 1, 2, ...r$. Sendo assim, a mensagem assinada e enviada por ela é $C_1, C_2, ...C_r$.

Ao receber a mensagem, Sofia deve:

d) Decifrar os números $C_1, C_2, ...C_r$, usando sua chave pública de Fernanda, ou seja, determina os números

$$u_i \equiv C_i^{e'} \pmod{n'},$$

para todo $i = 1, 2, ...r$.

Temos que $u_i < n'$. Para além, u_i é o próprio c_i.

De fato, nota-se que

$$u_i \equiv C_i^{e'} \equiv (c_i^{d\prime})^{e'} \equiv c_i \pmod{n'},$$

para todo $i = 1, 2, ...r$. Isto porque,

$$u_i \equiv c_i^{e'd'} \equiv c_i^{k'\varphi(n')+1} \equiv c_i \pmod{n'}.$$

e) Por fim, o destinatário da mensagem determina $y_i \leq n$, tal que

$$y_i \equiv u_i^d \pmod{n},$$

para todo $i = 1, 2, ...r$. Veja que, y_i é o próprio T_i escrito por Fernanda. Assim a mensagem recebida é $T_1, T_2, ..., T_r$.

De fato, para justificar essa última congruência, basta notar que

$$y_i \equiv u_i^d \equiv c_i^d \equiv (T^e)^d \equiv T_i \pmod{n}.$$

Haja vista que

$$T_i^{ed} \equiv T_i^{k\varphi(n)+1} \equiv T_i \pmod{n}.$$

Novamente, o processo de envio e leitura de mensagem criptografada e assinada é concluído.

Dessa forma, encerramos mais uma seção e os exemplos do sistema RSA serão apresentados mais à frente.

5

Google Planilhas e Wolfram Alpha no Ensino de Matemática na Educação Básica

A cada avanço tecnológico, nossa sociedade é transformada. Desse modo, faz-se necessário pensar em processos de ensino e aprendizagem que acompanhem essas transformações.

Conhecer e manipular tecnologias digitais que possam contribuir para o ensino de matemática, tornou-se um dos objetivos do presente trabalho. Sendo assim, buscamos a produção de materiais que sirvam como suporte para docentes que desejam assegurar aos alunos o desenvolvimento de algumas competências relacionadas com o ensino e aprendizagem de matemática, conforme estabelece a BNCC (Base Nacional Comum Curricular) ([1],p.267).

> *Utilizar processos e ferramentas matemáticas, inclusive tecnologias digitais disponíveis, para modelar e resolver problemas cotidianos, sociais e de outras áreas de conhecimento, validando estratégias e resultados.*

Inicialmente, apresentaremos algumas funcionalidades do editor **Google Planilhas** enquanto recurso educacional. Este será utilizado para o processamento de cálculos mecânicos. Assim, buscamos que o estudante desenvolva a habilidade de analisar criticamente e aplicar conceitos matemáticos, deixando em segundo plano o papel de mero executor cálculos.

O Google Planilhas é um editor de planilhas eletrônicas online, oferecido pela plataforma Google Workspace. Sua interface e funcionalidades se assemelham com o programa Excel, mostrando-se uma poderosa ferramenta de automação de cálculos, criação e leituras de gráficos e tabelas, além de um ótimo organizador de dados. Para completar, três vantagens do editor Google Planilhas foram determinantes para a escolha da ferramenta. A primeira, foi a gratuidade de editor. Em seguida, sua função de trabalho colaborativo em tempo real. Por fim, sua maior compatibilidade com smartphones e tablets.

Esses editores de planilhas, devido a suas funcionalidades, são bem conhecidos em rotinas administrativas e empresariais. No entanto, buscamos maior utilização no ensino da educação básica.

Seguem descrições de atividades que podem ser utilizadas em sala de aula. Nesse momento, apresentamos com uma maior riqueza de detalhes como o editor pode ser usado no ensino. Para além, o leitor poderá conferir planos de aula na sessão *Aplicação de tecnologias em aulas de matemática* e lista de exercícios propostos no Apêndice A.

5.1 Descrição de atividades no Google Planilhas

Antes de iniciar as atividades, é importante reservar um tempo e fazer algumas orientações que favoreçam a interação do aluno com o editor. Informações como, acesso ao editor de Planilhas, renomear, salvar e abrir algum trabalho são importantes. O conhecimento da sua interface, bem como a percepção de que cada célula funciona como uma "calculadora"; para isso basta iniciar a inserção dos dados com o sinal de "=", são requisitos fundamentais para as atividades aqui propostas. Essas experiências podem aumentar o interesse do estudante, fazendo com que ele tenha uma noção inicial da ferramenta que utilizará.

O editor pode ser uma ferramenta de aprendizagem para vários conteúdos matemáticos, inclusive para criptografia.

Todas as atividades abaixo podem ser acessadas no link https://l1nk.dev/mEcsY. Isso permitirá ao professor leitor a verificação dos resultados.

5.1.1 Cálculo de MDC e MMC no Google Planilhas

Para realizar o cálculo do MDC ou do MMC de dois ou mais números, o Google Planilhas possui uma fórmula própria. Trazemos um exemplo de utilização do cálculo de MMC, somente com o objetivo de ambientação com o editor, uma vez que não usaremos esse conteúdo nos processos criptográficos.

Exemplo 5.1.1: Atividade 1.

Propor o cálculo do MMC de quatro números. Para a realização dessa atividade, vamos construir uma tabela.

1) Na célula A1, inserimos o enunciado do exercício: "ENCONTRE O MMC DOS NÚMEROS". Essa célula pode ser mesclada com B1 por motivo estético.

2) Na célula A2, vamos inserir nome da coluna, escolhemos a descrição "Números".

3) Na célula B2, entramos com a descrição "Resultado".

4) Nas células A3 até A6, inserimos os números 7, 12, 15 e 18. Um em cada célula.

5) Na célula A7, inserimos a descrição "MMC". Na célula defronte, B7, inserimos a formula

$$=\text{MMC(A3:A6)}.$$

O resultado, do mmc dos números inseridos nas células A1 até A6, será calculado na célula B7, e os alunos poderão fazer novos testes trocando os números da coluna A. Com isso, a programação realizada possibilitará novos resultados. O professor pode ensinar como formatar a tabela, além de explorar propriedades do MMC e do seu cálculo.

	A	B	C	D	E	F	G	H
1	ENCONTRE O MMC DOS NÚMEROS			ENCONTRE O MMC DOS NÚMEROS			ENCONTRE O MMC DOS NÚMEROS	
2	Números	resultado		Números	resultado		Números	resultado
3	7			7			7	
4	12			9			14	
5	15			16			28	
6	18			25			56	
7	mmc	1260		mmc	25200		mmc	56
8	Produto	22680		Produto	25200		Produto	153664
9	Tabela I			Tabela II			Tabela III	

Figura 5.1: MMC (Autoria própria)

Atividade disponível na página "Atividade 1" em https://l1nk.dev/mEcsY.

Exemplo 5.1.2: Atividade 2.

Encontrar os possíveis restos da divisão de um número inteiro, coprimo com 26, por 26. Nessa atividade, será explorada a propriedade do MDC de dois números coprimos. Trabalharemos também com a construção de uma tabela composta por 15 linhas e 2 colunas. Para a realização da atividade, siga os passos a seguir:

1) Inserir a descrição da atividade nas células A1, que receberá o texto "NÚMEROS COPRIMOS COM". Na célula B1, insira o número a ser analisado. Neste exemplo, será o "26". Agora a tabela deve ser rotulada, começamos pela coluna A. A célula A2 receberá a inscrição: "NÚMERO A". Logo após, a célula B2 deve receber o texto "MDC(A,26)=1".

2) Na coluna A, vamos inserir os números que podem ser coprimos com 26. Inserimos o número 1 na célula A3 e, 2 na célula A4. Na célula A5 inserimos o número 3, e da célula A6 em diante, vamos inserir uma sequência de números ímpares. Para isso, basta entrar com o número 5 na célula A6. Depois, deve-se selecionar as duas últimas células, posicionar o cursor no canto inferior direito da última célula selecionada, e arrastar o cursor para baixo com o botão de clique pressionado, até chegar ao número 25.

3) Na célula B3, insera a fórmula

$$\text{MDC(A3;B\$1)}$$

e conclua teclando em "Enter". Essa função calcula, inicialmente, o MDC do número inserido em A3 e o número inserido em B1. Logo após, use a função arrastar o cursor para baixo, até a linha que tenha um número correspondente na coluna A. Assim, o editor calcula o MDC de cada célula abaixo de A3 e

o número inserido em B1 (o símbolo "$" fixa a célula na fórmula, impedindo que a cada linha que descemos seja usada, na fórmula, o valor de cada célula abaixo de B1).

4) Por fim, deve ser feita a análise de quais células, da coluna B, possuem o número 1 como resultado.

A quantidade de números com essa propriedade é, neste caso, igual a 12. São os números da coluna "A" nos quais tem correspondentes iguais a 1 na coluna "B".

	A	B
1	NÚMEROS COPRIMOS COM	26
2	NÚMERO A	MDC (A,26)=1
3	1	1
4	2	2
5	3	1
6	5	1
7	7	1
8	9	1
9	11	1
10	13	13
11	15	1
12	17	1
13	19	1
14	21	1
15	23	1
16	25	1

Figura 5.2: Coprimos com 26 (autoria própria)

Nesta atividade, o que de fato estamos calculando é a função φ de Euler para o número 26. No ensino básico, não é comum realizar atividades com essa denominação. Fica a cargo do professor mencionar ou não essa aplicação. Ainda neste sentido, torna se interessante escolher números primos aleatórios para realizar os testes dessa atividade. Feito isso, será possível verificar o cálculo da função $\varphi(m)$ para m primo, como vimos na Definição 9.

Atividade disponível na página "Atividade 2" em https://l1nk.dev/mEcsY.

5.1.2 Teste de primalidade no Google Planilhas

Testaremos a primalidade de alguns números usando o Google Planilhas. Este material de estudos foi pensado para o Ensino Fundamental Anos finais (6° ano até 9° ano), podendo ser trabalhado em qualquer Ano (Série) dessa etapa de ensino. Nesse sentido, vamos explorar o **Método da Divisão**, visto na seção Testes de Primalidade, aplicado no Google Planilhas.

Exemplo 5.1.3: Atividade 3.

Testar a primalidade de 1117 .

1) Abra o Google Planilhas.

2) Estabeleça o número que deseja investigar a primalidade. Por exemplo, ao investigar o número 1117, devemos inseri-lo na célula B2.

3) Vamos construir uma tabela. As linhas 1, 2 e 3 foram destinadas às informações da tabela. Nessa parte, será exibido os rótulos das colunas, o número a ser investigado, bem como o valor aproximado de sua raiz quadrada.

4) Na coluna A, a partir da 4ª linha, inserimos uma lista de números. Vamos iniciar essa lista pelo número 2, e depois vamos inserir todos os números ímpares menores ou iguais do que a parte inteira da raiz quadrada do número avaliado. O programa tem uma fórmula que calcula a raiz quadrada, que será inserida na célula D2

   $$=\text{RAIZ(B2)}.$$

   Essa fórmula devolve a raiz quadrada do número inserido na célula B2. Porém vamos considerar somente a parte inteira do resultado obtido. É importante mostrar para o estudante que, ao inserirmos uma fórmula referente à célula (B2), ao invés do número nela inserido, tem-se procedimento que facilita o cálculo da raiz quadrada de qualquer outro número. Nesse caso, basta trocar o inserido na célula B2 pelo novo número e o editor calcula o valor.

5) Na construção da lista de números, vamos observar a raiz quadrada que encontramos no item anterior. No nosso caso, encontramos um número menor do que 33. Assim, vamos listar os números 2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31 e 33. Com essa listagem, vamos utilizar a função autocompletar. O programa facilitou esse processo. Para isso, fizemos o seguinte: inserimos o número 2 na célula A4, nas células A5 e A6 entramos com os números 3 e 5, respectivamente. Logo após, selecionamos as células A5 e A6, em seguida posicionamos o cursor no canto inferior direito da segunda célula selecionada e arrastamos para as células abaixo. Com isso, o programa vai completando a sequência de números ímpares até o número desejado.

6) Na célula B4, devemos inserir a fómula: o quociente da célula B2 (1117) pela célula A4, célula da coluna A na mesma linha de B4. Por exemplo, na célula B4, vamos inserir a fórmula:

   $$=\text{B\$2/A4}.$$

   O símbolo "/" é o comando para a operação de divisão, já o símbolo "$" serve para fixar a célula B2. Desse modo, quando arrastarmos o cursor da célula B4 para uma posição para baixo, o programa vai inserir, automaticamente, na célula B5, a fórmula "=B$2/A5". Para encontrarmos todos os valores dessa coluna, basta selecionar a célula B4 e arrastar até a linha desejada.

Verificamos que o número 1117 é primo, uma vez que nenhum dos quocientes encontrados até o número 33 é inteiro.

Feito isso, o professor pode explicar a teoria presente no procedimento, uma vez que as contas foram todas feitas pela máquina. Apesar de não termos feitos nenhum cálculo, nosso conhecimento foi utilizado para programar a plataforma.

	A	B	C	D
1	VERIFICAÇÃO DE PRIMALIDADE			RESULTADO
2	Número	1117	Raiz quadrada	33,42154993
3	N	Quociente de B2 por A(N)		
4	2	558,5		
5	3	372,3333333		
6	5	223,4		
7	7	159,5714286		
8	9	124,1111111		
9	11	101,5454545		
10	13	85,92307692		
11	15	74,46666667		
12	17	65,70588235		
13	19	58,78947368		
14	21	53,19047619		
15	23	48,56521739		
16	25	44,68		
17	27	41,37037037		
18	29	38,51724138		
19	31	36,03225806		
20	33	33,84848485		
21	ANÁLISE:	NÃO ENCONTRADO QUOCIENTE INTEIRO.		
22	CONCLUSÃO:	1117	É PRIMO	

Figura 5.3: Primalidade de 1117 (autoria própria)

Exemplo 5.1.4: Atividade 4.

Outra alternativa pode ser a função "MOD" do Google Planilhas que informa o resto de uma divisão. Para isso, podemos seguir os passos 1 até 5 do Exemplo 5.1.3. Já no item 6, basta modificar a fórmula da célula B4 por

$$=\text{MOD}(\text{B\$2};\text{A4}),$$

e fazer a análise dos restos.

Neste caso, devemos observar que nenhum dos quocientes é igual a 0 (zero).

Atividade disponível na página "Atividade 4" em https://l1nk.dev/mEcsY.

5.1.3 Cifras de Substituição no Google Planilhas

Exemplo 5.1.5: Atividade 5

Cifrar a frase "A MATEMÁTICA É BELA", usando cifras de César, com a chave "E".

1) Abra o Google Planilhas.

2) Construir uma tabela com quatro colunas. A célula A1 indicará que se trata da coluna do "Texto Original". É nela que estará o alfabeto original. Para isso, a célula A2 deve conter a seguinte fórmula:

   =ARRAYFORMULA(CARACT(SEQUENCE(26;1;65))).

   Essa fórmula "gera" uma sequência de 26 letras do alfabeto, uma em cada linha. O programa insere os caracteres por meio de linguagem de programação, utilizando a tabela ASCII (tabela de códigos binários), apresentada na Subseção 4.0.4 e na Figura 9.2 do Apêndice B. Assim, essa lista de caracteres tem início no símbolo 65 da tabela ASCII, que corresponde à letra "A" (maiúsculo) e termina no código 90 (65 + 26 - 1), que tem como corresponde a letra "Z"(maiúscula).

3) A célula B1 receberá a descrição: "Cifra". Nessa coluna, estarão presentes os códigos representantes de cada letra do alfabeto original. Dessa forma, vamos inserir na célula B2 a seguinte fórmula:

   =ARRAYFORMULA(CARACT(SEQUENCE(22;1;69))).

   Repare que mudamos o primeiro parâmetro da fórmula para 22. Assim, as quatro últimas células dessa coluna devem ser preenchidas manualmente. O terceiro parâmetro também foi modificado de 65 para 69. Pois desejamos iniciar o alfabeto pela letra "E", quatro letras à frente, logo devemos aumentar quatro unidades nessa fórmula.

4) Na terceira coluna, inserimos a mensagem para ser codificada. Nesse caso, C1 terá "Mensagem Original" como descrição. Cada letra da mensagem deve ser digitada em uma única célula dessa coluna.

5) Por fim, a última coluna nos retornará a "Mensagem Cifrada", texto que colocaremos na célula D1. Já em D2, deve ser inserida a fórmula:

   =PROCV(C2;A$2:B$27;2;1).

   Após a inserção dessa fórmula, basta arrastar para baixo a célula onde está a função, a partir da célula D2, até a linha desejada. Feito isso, a mensagem aparecerá na coluna D.

   Na fórmula "PROCV", procura-se o valor inserido em C2 na tabela formada pelos valores de A2 até B27 (o "$" mantém a tabela fixa nesses valores). No entanto, ela retorna como resultado o valor da coluna B que está na mesma linha do valor inserido em C2. Por isso, o terceiro parâmetro da fórmula é o número 2. O último parâmetro é padrão, neste caso.

A mensagem "A MATEMÁTICA É BELA" é transformada em

E Q E X I Q E X M G E I F I P E.

O leitor pode conferir na página "Atividade 5" em https://l1nk.dev/mEcsY.

	A	B	C	D
1	TEXTO ORIGINAL	CIFRA	MENSAGEM ORIGINAL	MENSAGEM CRIPTOGRAFADA
2	A	E	A	E
3	B	F	M	Q
4	C	G	A	E
5	D	H	T	X
6	E	I	E	I
7	F	J	M	Q
8	G	K	A	E
9	H	L	T	X
10	I	M	I	M
11	J	N	C	G
12	K	O	A	E
13	L	P	E	I
14	M	Q	B	F
15	N	R	E	I
16	O	S	L	P
17	P	T	A	E
18	Q	U		
19	R	V		
20	S	W		
21	T	X		
22	U	Y		
23	V	Z		
24	W	A		
25	X	B		
26	Y	C		
27	Z	D		

Figura 5.4: Cifra de César chave "E" (autoria própria)

Exemplo 5.1.6: Atividade 6
Decifrar a mensagem

S P I K E H S H I I V E X S W X I R I W

usando a cifra de César com a chave E.

1) Abra o Google Planilhas.

2) Na coluna A, deve ser colocado o dicionário de cifras. Contudo, o primeiro código é a letra "E", logo devemos inserir o alfabeto começando por essa letra:

=ARRAYFORMULA(CARACT(SEQUENCE(22;1;69))).

Note que a lista começa na letra E e termina na letra Z, com isso devemos completar mais quatro letras iniciando pela letra A.

3) Na coluna B, deve ser colocado o texto original.

4) Na coluna C, vamos digitar a mensagem codificada inserindo cada letra em uma célula desta coluna.

5) Na coluna D, vamos recuperar cada letra da mensagem original. Para isso, insira, na célula D2, a fórmula:

$$=\text{PROCV}(\text{C2};\ A\$2:\text{B}\$27;\ 2;\ 1).$$

A mensagem original encontrada será

O LEGADO DE ERATÓSTENES.

	A	B	C	D
1	CIFRA	TEXTO ORIGINAL	MENSAGEM CRIPTOGRAFADA	MENSAGEM ORIGINAL
2	E	A	S	O
3	F	B	P	L
4	G	C	I	E
5	H	D	K	G
6	I	E	E	A
7	J	F	H	D
8	K	G	S	O
9	L	H	H	D
10	M	I	I	E
11	N	J	I	E
12	O	K	V	R
13	P	L	E	A
14	Q	M	X	T
15	R	N	S	O
16	S	O	W	S
17	T	P	X	T
18	U	Q	I	E
19	V	R	R	N
20	W	S	I	E
21	X	T	W	S
22	Y	U		
23	Z	V		
24	A	W		
25	B	X		
26	C	Y		
27	D	Z		

Figura 5.5: Decodificação pela cifra de César (autoria própria)

Disponível em “Atividade 6” no link https://l1nk.dev/mEcsY.

5.1.4 Cifra Afim no Google Planilhas

Exemplo 5.1.7: Atividade 7

Criptografar a mensagem "O ALUNO FOI BEM NA PROVA", utilizando a função $f(x) = 7x + 6$.

1) Abra o Google Planilhas.

2) Vamos estabelecer o dicionário de caracteres com 26 letras (na ordem alfabética) que serão substituídas por números inteiros de 10 até 35.

3) O texto original deve estar na coluna A. Na célula A2, digite:

$$=\text{ARRAYFORMULA(CARACT(SEQUENCE(26;1;65))).}$$

4) Na coluna B, adicione o dicionário de cifras, iniciando no número 10 e terminando em 35. Basta digitar os dois primeiros números da sequência e usar a função arrastar o cursor para baixo.

5) Na coluna C, digite a mensagem original, com cada letra em uma célula.

6) Na coluna D, busque cada correspondente das letras, no dicionário de Cifras (estamos usando a cifra de substituição). Para isso, basta inserir, em D2 a fórmula:

$$=\text{PROCV(C2;A\$2:B\$27;2;0).}$$

   Depois complete a coluna com a função arrastar, para baixo, o cursor.

7) A coluna E será destinada para encontrar os valores de cada cifra aplicada à função escolhida. Na célula E2, vamos inserir a função:

$$=7*\text{D2}+6.$$

   Em seguida, complete a coluna com a função arrastar. A mensagem criptografada será calculada automaticamente. O símbolo "*" representa o sinal de multiplicação.

A mensagem codificada é

174 76 153 216 167 174 111 174 132 83 104 160 167 76 181 195 174 223 76.

A atividade pode ser acessada em "Atividade 7", https://l1nk.dev/mEcsY.

	A	B	C	D	E
1	TEXTO ORIGINAL	CIFRA	MENSAGEM	PRÉ CODIFICAÇÃO	CIFRA POR f(x)= 7x + 6
2	A	10	O	24	174
3	B	11	A	10	76
4	C	12	L	21	153
5	D	13	U	30	216
6	E	14	N	23	167
7	F	15	O	24	174
8	G	16	F	15	111
9	H	17	O	24	174
10	I	18	I	18	132
11	J	19	B	11	83
12	K	20	E	14	104
13	L	21	M	22	160
14	M	22	N	23	167
15	N	23	A	10	76
16	O	24	P	25	181
17	P	25	R	27	195
18	Q	26	O	24	174
19	R	27	V	31	223
20	S	28	A	10	76
21	T	29			
22	U	30			
23	V	31			
24	W	32			
25	X	33			
26	Y	34			
27	Z	35			

Figura 5.6: Cifra Afim $f(x) = 7x + 6$ (autoria própria)

Exemplo 5.1.8: Atividade 8

Decifrar o código

22 73 46 79 58 34 79 46 28 22 61 22 28 73 46 67 79 64 40 73 22 37 46 22,

criptografado pela cifras de substituição de chave 10 (alfabeto na sua ordem original) e pela função afim $f(x) = 3x - 8$.

Para resolver essa atividade, o caminho é construir uma tabela com quatro colunas e 27 linhas.

1) Determinar a função inversa de $f(x) = 3x - 8$. Sugerimos que esse cálculo seja feito manualmente pelos alunos.

2) Abrir o Google Planilhas.

3) Inicialmente, vamos rotular a coluna A, inserindo o texto "CIFRA" na célula A1. Da célula A2 até A27, insira a sequência de números inteiros começando pelo número 10. Como o procedimento é o inverso da codificação, devemos inserir primeiro a coluna de Cifras. O procedimento deve ser realizado desse modo para que a função "PROCV" funcione corretamente.

4) Rotular a coluna B, inserindo o texto "TEXTO ORIGINAL" na célula B1 e expandir o alfabeto nessa coluna. Para isso, basta digitar em B2 o comando

$$=\text{ARRAYFORMULA(CARACT(SEQUENCE(26;1;65))}.$$

5) Na coluna C, insira as cifras da mensagem secreta, uma em cada célula, iniciando em C2. Rotule essa coluna inserindo o texto "MSG CODIFICADA" em C1.

6) Na coluna D, aplique cada número da coluna C na inversa da função que é expressa por $f^{-1}(x) = \frac{x}{3} + \frac{8}{3}$. Fazemos isso, inserindo em D2 a fórmula

$$=\text{(C2/3)+(8/3)}.$$

Logo após, arraste o curso para completar todos os dados dessa coluna. Rotule essa coluna com a expressão da função inversa determinada.

7) Na coluna E, que recebe em E1 o rótulo "MSG ORIGINAL", faça o processo inverso da pré-codificação. Para isso, vamos procurar (função PROCV) o item da coluna D, na tabela formada pelas colunas A e B, verificando qual é seu correspondente na coluna B. Insira em E2 a seguinte função:

$$=\text{PROCV(D2;A2} : B27;\ 2;\ 0).$$

Logo após, use a funcionalidade arrastar o curso, pra baixo, para completar a tabela.

A mensagem original é revelada:

A R I T M E T I C A N A C R I P T O G R A F I A.

O leitor pode visualizar o resultado final dessa atividade em Figura 5.7 e a planilha produzida pode ser acessada na página "Atividade 8" em https://l1nk.dev/mEcsY.

	A	B	C	D	E
1	CIFRA	TEXTO ORIGINAL	MSG CODIFICADA	f⁻¹(x)=(x/3)+(8/3)	MSG ORIGINAL
2	10	A	22	10	A
3	11	B	73	27	R
4	12	C	46	18	I
5	13	D	79	29	T
6	14	E	58	22	M
7	15	F	34	14	E
8	16	G	79	29	T
9	17	H	46	18	I
10	18	I	28	12	C
11	19	J	22	10	A
12	20	K	61	23	N
13	21	L	22	10	A
14	22	M	28	12	C
15	23	N	73	27	R
16	24	O	46	18	I
17	25	P	67	25	P
18	26	Q	79	29	T
19	27	R	64	24	O
20	28	S	40	16	G
21	29	T	73	27	R
22	30	U	22	10	A
23	31	V	37	15	F
24	32	W	46	18	I
25	33	X	22	10	A
26	34	Y			
27	35	Z			

Figura 5.7: Decodificação por Cifra Afim (Autoria própria)

5.1.5 Cifra RSA no Google Planilhas e Wolfram Alpha

Exemplo 5.1.9: Atividade 9

Criptografar a mensagem "SOMA OU TOTAL", utilizando a chave pública (91,5), com alfabeto de pré-codificação começando na cifra 10 e terminando em 35.

Antes de iniciarmos o trabalho no editor de planilhas, vamos reelembrar a construção de alguns elementos essenciais no processo de encriptação RSA. O estudo completo pode ser conferido na Subseção 4.0.5. Primeiramente, o remetente deve conhecer a chave pública do destinatário. Essa chave é composta por dois números (n,e), que são chamados de parâmetros da chave. Para além, n é o produto de números primos e distintos p e q. Já o parâmetro e pode ser escolhido livremente, com a condição de ser coprimo com $\varphi(n)$, em que $\varphi(n) = (p-1)(q-1)$.

1) Abra o Google Planilhas.

2) Na célula A1, insira o texto "**p**". A célula B1 deve ser nomeada por "**q**". Já C1, deve ser rotulada com "**n=p.q**" e D1 deve receber o texto "**e**".

3) Nas células E1, F1 e G1, insira os respectivos textos:

"**(p-1)(q-1)**", "**mdc(e,(p-1)(q-1)** " e "**d**".

4) Na linha 2, vamos inserir os valores equivalentes a cada célula rotulada na linha 1. Comece pela célula A2 que recebe o valor 7. B2 recebe o valor 13. Em C2, insira a fórmula "**=A2 * B2**". Dessa forma, estamos programando essa célula que será modificada, automaticamente, caso modifiquemos os números p e q. Em seguida, insira em D2 o valor 5, como indicado na chave pública.

5) Agora, vamos programar a célula E2 com a fórmula "**=(A2 - 1)*(B2 - 1)**". F2 receberá a fórmula "**=MDC(D2;E2)**", e G2 será preenchida com o número 29, que representa o valor de "**d**", parâmetro da chave privada $(n,d) = (91,29)$.

6) O cálculo do valor de "**d**" geralmente é realizado por meio de resolução de equações diofantinas. No entanto, esse cálculo pode ser adaptado para o ensino médio, como veremos a seguir.

   "**d**" é um número inteiro definido pelas duas condições,

$$ed \equiv 1(\ (\text{mod } (p-1)(q-1)) \text{ e } 1 \leq d < (p-1)(q-1).$$

   Dessa forma, as condições podem ser reescritas como:

$$5d \equiv 1\ (\text{mod } 72) \text{ e } 1 \leq d < 72.$$

   Nesse sentido, resolver a primeira condição equivale a solucionar a equação:

$$5d - 1 = 72x, \text{ em que } x \text{ é inteiro.}$$

   Logo

$$d = \frac{72x+1}{5} = \frac{2x+1}{5} + 14x.$$

   Interessa-nos encontrar um valor para x, de modo que a primeira parcela da equação acima, represente um número inteiro. Ao testar a expressão $2x + 1$, para $x \in \{0, 1, 2, 3, 4\}$, verifica-se que $2x + 1$ é divisível por 5 quando $x = 2$ (apenas ele). Temos:

$$d = \frac{2.2+1}{5} + 14.2 = 29.$$

   Devemos observar que esse número atende à condição

$$1 \leq d < 72.$$

7) Voltando para a planilha, vamos estabelecer o dicionário de caracteres com 26 letras (na sua ordem natural) que serão substituídas por números inteiros de 10 até 35. Sendo assim, na célula A4, inserimos "**TEXTO ORIGINAL**" e em A5 digitamos a fórmula:

$$=\text{ARRAYFORMULA(CARACT(SEQUENCE(26;1;65))).}$$

8) Na coluna B, adicione o dicionário de cifras, iniciando no número 10 e terminando em 35. Basta digitar os dois primeiros números da sequência e usar a função arrastar o cursor para baixo. Com isso, a célula B4 será rotulada com o texto "**CIFRA**" e da célula B5 em diante, colocaremos a sequência de números.

9) Na célula C4, insira o rótulo "**MENSAGEM ORIGINAL**". Nas células abaixo, vamos digitar a mensagem original, lembrando de inserir uma letra em cada célula.

10) Na coluna D, vamos "buscar" cada correspondente das letras, no dicionário de Cifras (estamos usando a cifra de substituição). Estamos pré-codificando a mensagem original. O rótulo de D4 será "**PRÉ-CODIFICAÇÃO**" e em D5 inserimos a fórmula:

$$=\text{PROCV(C5; } A\$5 \text{ :B\$30; 2; 0).}$$

Em seguida, devemos completar a coluna com a função arrastar o cursor baixo.

11) A coluna E será destinada para a inserção dos "Blocos". São eles que serão codificados. Como vimos na Subseção 4.0.5, os blocos são números formados a partir da mensagem pré-codificada. Para formar os blocos, devemos primeiramente, visualizar a mensagem pré-codificada como um único número. Dessa forma, visualizaremos um número com muitos algarismos. Logo após, devemos "quebrar" os algarismos, desse número, em numerais menores B_1,B_2...B_r, com $1, 2, ..., r$ números naturais, de modo que cada numeral atenda às condições:

- $B_r < pq$;
- $B_r \not\equiv 0 \pmod{p}$ e $B_r \not\equiv 0 \pmod{q}$;
- Nenhum bloco pode iniciar com o algarismo zero.

Dessa maneira, vamos rotular a coluna E, inserindo na célula E5 o texto "**BLOCOS B ($<$ pq)**", em seguida apenas copiamos os pré-códigos da coluna D para serem colados na célula E5. Precisaremos avaliar essa coluna, no entanto, faremos isso com auxílio do editor de planilhas. Nesse sentido, caminhamos ao passo seguinte para facilitar a avaliação.

12) Na coluna F, vamos verificar quais Blocos são incongruentes a zero módulo p. A célula F4 terá a inscrição: "$\mathbf{B} \not\equiv \mathbf{0} \pmod{p}$". Na célula F5, inserimos a fórmula:

$$=\text{MOD(E5;A\$2)}.$$

Em seguida, usamos a função autocompletar. Para isso, selecionamos essa célula e posicionamos o cursor no canto direito inferior dessa célula. Ao aparecer uma cruz, arrastamos para baixo. Não analisaremos os resultados ainda, sigamos para o próximo passo.

13) Repetimos o passo anterior com algumas adaptações. A primeira é rotular a coluna G, inserindo em G4 o texto "$\mathbf{B} \not\equiv \mathbf{0} \pmod{q}$". Em seguida, na célula G5 inserimos a fórmula:

$$=\text{MOD(E5;B\$2)}.$$

14) Nesse passo, analisaremos simultaneamente as colunas F e G para que atendam às três condições do Item 11). Começaremos pela segunda condição, verificando que nenhum valor dessas colunas seja 0 (zero). Se isso ocorrer, passamos para a próxima análise. Caso contrário, voltamos à coluna dos blocos (Coluna E) e modificamos os valores que não atendem às condições das colunas F e G. A modificação de um bloco será realizada por meio da separação de seus algarismos, criando dois novos blocos que serão vizinhos na coluna. Da mesma forma, dois blocos vizinhos podem ser unidos formando um único bloco. No entanto, o valor do bloco deve ser menor do que n, isso satisfaz a primeira condição. Para finalizar, devemos observar que um bloco não pode ter o algarismo inicial igual a zero, como estabelece a terceira condição.

Esse procedimento é realizado por meio de tentativa e erro. Como já programamos as colunas F e G para apresentarem os resultados que nos interessam, cada modificação feita nas colunas de blocos reflete nas colunas F e G.

15) Sigamos para o passo final. Rotulamos a coluna H, inserindo em H4 a inscrição "$C = B\hat{}e \pmod{pq}$". Na célula H5, devemos inserir a fórmula:

$$=\text{MOD(E5 \^{}D\$2;C\$2)}.$$

Essa fórmula devolve o resto da divisão por "n" (na célula C2) de cada bloco, da coluna E, elevado (símbolo circunflexo) ao valor de "e" (presente na célula D2). Após isso, basta usar a função autocompletar, arrastando o cursor da célula selecionada para baixo.

Dessa forma, a mensagem "SOMA OU TOTAL" é transformada na mensagem criptografada

	A	B	C	D	E	F	G	H
1	p	q	p x q	e	(p -1)(q-1)	mdc(e, (p -1)(q-1	d	
2	7	13	91	5	72	1	29	
3								
4	TEXTO ORIGINAL	CIFRA	MENSAGEM ORIGINAL	PRÉ-CODIFICAÇÃO	BLOCOS B (< pxq)	B ≡/0 (mod p)	B ≡/0 (mod 13)	C=B ^e (mod pq)
5	A	10	S	28	2	2	2	32
6	B	11	O	24	8	1	8	8
7	C	12	M	22	24	3	11	33
8	D	13	A	10	22	1	9	29
9	E	14	O	24	10	3	10	82
10	F	15	U	30	24	3	11	33
11	G	16	T	29	30	2	4	88
12	H	17	O	24	29	1	3	22
13	I	18	T	29	24	3	11	33
14	J	19	A	10	29	1	3	22
15	K	20	L	21	10	3	10	82
16	L	21			2	2	2	32
17	M	22			1	1	1	1
18	N	23						
19	O	24						
20	P	25						
21	Q	26						
22	R	27						
23	S	28						
24	T	29						
25	U	30						
26	V	31						
27	W	32						
28	X	33						
29	Y	34						
30	Z	35						
31								

Figura 5.8: RSA chave (91,5) (autoria própria)

32 8 33 29 82 33 88 22 33 22 82 32 1,

utilizando a chave pública (91,5).

A planilha produzida pode ser acessada na página "Atividade 9" em https://l1nk.dev/mEcsY.

Exemplo 5.1.10: Atividade 10

Decifrar a mensagem

32 8 33 29 82 33 88 22 33 22 82 32 1,

criptografada com a chave pública (91,5) e o alfabeto de substituição com cifras de 10 a 35.

Como o receptor da mensagem codificada foi o responsável por construir a chave pública usada na codificação, somente ele conhece a chave privada. É nesse momento que o sistema de criptografia RSA mostra sua segurança, uma vez que, para encontrarmos o parâmetro d (da chave privada), necessitamos conhecer os números primos p e q que formam o parâmetro n da chave pública.

Atualmente, procedimentos que envolvem a criptografia RSA utilizam dois números primos com mais de uma centena de algarismos. Consequentemente, o número n se torna um número muito grande, tornando sua decomposição em fatores primos trabalhosa e demorada até para as máquinas e/ou programas mais tecnológicos.

Nesse sentido, o receptor autorizado a ler a mensagem é aquele que definiu ou tem conhecimento das duas chaves.

1) Abra o Google Planilhas.

2) Na célula A1, insirimos o texto "**n**". A célula B1 será rotulada com "**d**".

3) Na linha 2, vamos inserir os valores equivalentes a cada célula rotulada na linha 1. Começamos por A2 que receberá o valor 91. Já B2, será preenchida com 29. Esses valores foram determinados no Exemplo 5.1.9.

4) Vamos construir uma tabela para melhor visualização do processo. Como iremos descriptografar uma mensagem, realizaremos o caminho inverso da codificação. Começando pela inserção do dicionário de cifras na coluna A.

   Nesse sentido, a célula A4 será rotulada com o texto "**CIFRA**". Da célula A5 em diante, colocaremos a sequência de cifras, que inicia no número 10 e termina em 35. A automatização desse procedimento pode ser realizada da seguinte maneira: digite os dois primeiros números da sequência e use a função arrastar o cursor para baixo.

5) Criaremos o dicionário de caracteres com 26 letras, posicionadas na sua ordem alfabética. Dessa forma, a célula B4 será rotulada por "**TEXTO ORIGINAL**" e em B5 digitaremos a fórmula:

   $$=\text{ARRAYFORMULA(CARACT(SEQUENCE(26;1;65))).}$$

6) A célula C4 receberá a inscrição "**MENSAGEM CRIPTOGRAFADA (C)**". Nas células de baixo, digitaremos a mensagem codificada, lembrando de inserir um código em cada célula.

7) Na coluna D, rotularemos D4 com o texto "$C = B \,\hat{}\, d \,(mod\, n)$". Na célula D5, devemos inserir a fórmula:

   $$=\text{MOD(C5 ⌃ B\$2;A\$2).}$$

   Essa fórmula devolve o resto da divisão por "n" (na célula A2) de cada cifra, da coluna C elevado ao valor de "d" (presente na célula B2). Após isso, basta usar a função autocompletar, arrastanto o cursor da célula selecionada para baixo.

   Ao executarmos os passos acima, esperávamos encontrar como resultados, nas células da coluna D, números inteiros. No entanto, o editor de planilhas devolveu, nessas células, a indicação de erros com a descrição **#NUM!**. Isso ocorreu devido à limitação do Google Planilhas ao trabalhar com números grandes.

	A	B	C	D	E	F	G	H
1	n	d						
2	91	29						
3								
4	CIFRA	MSG ORIGINAL	MSG CODIFICADA (C)	RESTO DE (C elev 29) : 91				
5	10	A	32	#NUM!				
6	11	B	8	#NUM!				
7	12	C	33	#NUM!				
8	13	D	29	#NUM!				
9	14	E	82	#NUM!				
10	15	F	33	#NUM!				
11	16	G	88	#NUM!				
12	17	H	22	#NUM!				
13	18	I	33	#NUM!				
14	19	J	22	#NUM!				
15	20	K	82	#NUM!				
16	21	L	32	#NUM!				
17	22	M	1	1				
18	23	N						
19	24	O						
20	25	P						
21	26	Q						
22	27	R						
23	28	S						
24	29	T						
25	30	U						
26	31	V						
27	32	W						
28	33	X						
29	34	Y						
30	35	Z						

Erro

Os parâmetros em MOD causaram um erro de valor fora do intervalo. O erro ocorre quando o seguinte é verdadeiro: (o divisor * 1125900000000) é menor ou igual ao dividendo.

Figura 5.9: RSA com chave privada (91,29). Autoria própria

8) Utilizaremos o programa **Wolfram alpha** para fazer esses cálculos. Ele pode ser acessado no site: https://www.wolframalpha.com. Esse programa possui um amplo conjunto de funcionalidades matemáticas envolvendo números e menor limitação que o Google Planilhas ao trabalhar com números grandes. Sendo assim, mostra-se como uma ferramenta apta para trabalhos acadêmicos e também para uso profissional. Apresenta características que viabilizam seu uso, dentre elas destacamos: sua interface intuitiva e de fácil utilização, além de ser muito rápido no processamento dos cálculos e apresentação das respostas.

9) O programa possui uma caixa de entrada para os cálculos que desejamos realizar. Como exemplo, apresentaremos o cálculo de decifragem da primeira cifra. Os demais cálculos devem ser feito de maneira análoga. Nesse sentido, basta digitarmos, na caixa de entrada do site, a seguinte expressão:

$$32 \hat{} \ 29 \ (\text{mod } 91).$$

Dentro de poucos instantes, a ferramenta nos apresenta na caixa "*Result*" o valor 2. Assim, o primeiro bloco foi encontrado.

Importante apontar que o Wolfram Alpha disponibiliza para seus usuários duas versões. Uma delas é paga, apresentando funcionalidades adicionais, com

explicações acerca das resoluções. De forma mais limitada, porém efeciente, temos a versão gratuita. Foi por meio dela que este trabalho foi elaborado.

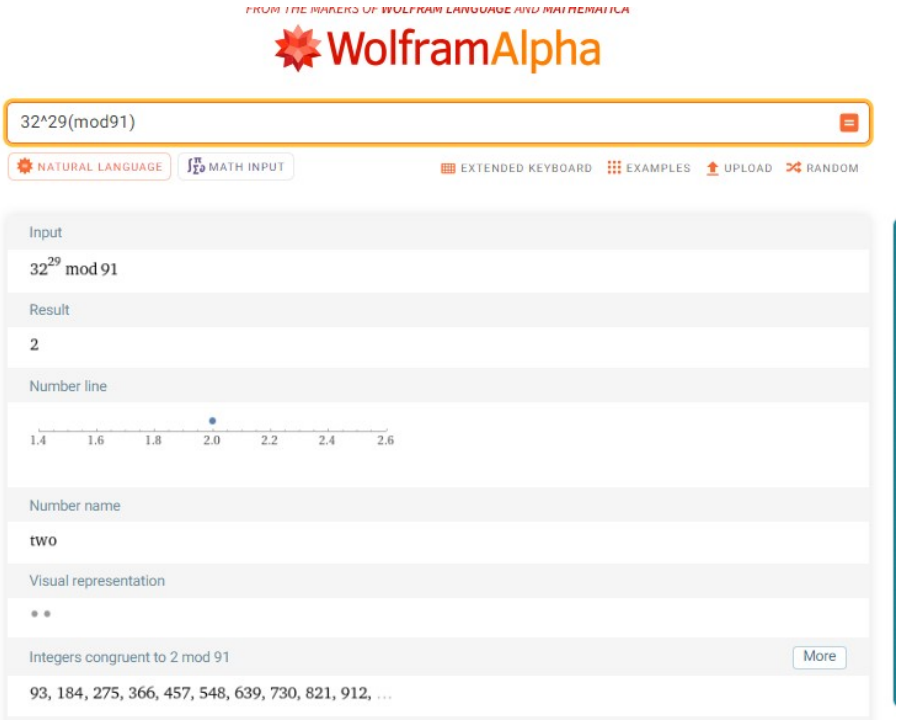


Figura 5.10: Interface do Wolfram Alpha

Os valores calculados através do Wolfram Alpha são:

2 8 24 22 10 24 30 29 24 29 10 2 1

10) À medida que vamos realizando os cálculos no Wolfram Alpha, devemos inserir esses resultados na nossa planilha. Apesar de sua limitação, com a resolução dos cálculos de congruências, o Google Planilhas ainda tem um papel importante na finalização desse trabalho. Nesse sentido, rotulamos a célula E4 com o texto: **BLOCOS B (< pxq) WOLFRAM**. Logo após, inserimos, nessa coluna, os dados obitos no programa. Iniciamos a lista pela célula E5.

11) No item anterior, os números encontrados representam os blocos relativos às cifras pré-codificadas. Sendo assim, necessitamos encontrar as cifras, nas quais a mensagem foi pré-codificada. Para isso, rotulamos a célula F5 com **CIFRA DIGITAL**. Em seguida, juntamos os números da coluna E, menores do que 10, por justaposição, sem exceder o número 35. Temos que digitar todos esses números na coluna F, começando pela célula F5.

12) Para recuperarmos a mensagem original, usaremos a funcionalidade do editor de planilhas. Iniciamos rotulando a célula G4 com: **MENSAGEM ORIGINAL**. Feito isso, na célula G5, inserimos a fórmula:

$$=\text{PROCV}(\text{F5};\text{A5} : B30;2;0).$$

A mensagem **SOMA OU TOTAL** foi recuperada.

A planilha produzida pode ser acessada em "Atividade 10", https://l1nk.dev/mEcsY.

5.1.6 RSA (Assinado) no Google Planilhas e Wolfram Alpha

Exemplo 5.1.11: Atividade 11

Criptografar a mensagem "UM BOM ALUNO", em que o remetente utiliza as chaves pública e privada iguais a (187,7) e (187,23), respectivamente. Já o destinatário possui as chave pública e privada iguais a (299,5) e (299,53), respectivamente. Admitamos que o alfabeto de cifras usado na comunicação esteja pré-codificado com números naturais de 10 a 35.

Para a assinar a mensagem, será utilizado o caso 1, apresentado em 4.0.5. Nesse sentido, o parâmetro n' (do remetente) é menor do que o parâmetro n (do destinatário). Importante salientar que: **nenhuma das partes envolvidas na troca da mensagem conhece a chave privada da outra**.

1) Abra o Google Planilhas.

2) Defina o remetente e o destinatário da mensagem. Logo após, vamos inserir os parâmetros das chaves dos envolvidos na troca de mensagem. Começaremos pelo destinatário. Na célula A1, insira o texto "**p**". A célula B1 deve ser renomeada por "**q**". Já C1 deve ser rotulada com "**n=p.q**" e D1 deve receber o texto "**e**".

   Nas células E1, F1 e G1, insira os respectivos textos:

   "**(p-1)(q-1)**", "**mdc(e,(p-1)(q-1)** " e "**d**".

3) Na linha 2, vamos inserir os valores equivalentes a cada célula rotulada na linha 1. Comece pela célula A2 que recebe o valor 23. B2 recebe o valor 13. Em C2, insira a fórmula "**=A2 * B2**". Dessa forma, estamos programando essa célula que será modificada, automaticamente, caso modifiquemos os números p e q. Em seguida, insira em D2 o valor 5, como indicado na chave pública.

4) Agora, vamos programar a célula E2. Para isso, inserimos a fórmula:

   "**=(A2 - 1)*(B2 - 1)**".

   F2 receberá a fórmula "**=MDC(D2;E2)**", e G2 será preenchida com o número 53 que representa o valor de "**d**", parâmetro da chave privada $(n,d) = (299,53)$.

5) O cálculo do valor de "**d**" geralmente é realizado por meio de resolução de equações diofantinas. No entanto, esse cálculo pode ser adaptado para o ensino médio, como veremos a seguir. "**d**" é um número inteiro definido pelas duas condições:

$$ed \equiv 1(\ (\text{mod}\ (p-1)(q-1)) \text{ e } 1 \leq d < (p-1)(q-1).$$

Dessa forma, as condições podem ser reescritas como:

$$5d \equiv 1\ (\text{mod}\ 264) \text{ e } 1 \leq d < 264.$$

Nesse sentido, resolver a congruência equivale solucionar a equação:

$$5d = 264x + 1, \text{ em que } x \text{ é inteiro.}$$

Daí

$$d = \frac{264x+1}{5} = \frac{4x+1}{5} + 52x.$$

O interessante é encontrar um valor para x, de modo que a primeira parcela da equação acima represente um número inteiro. Ao testar a expressão $4x + 1$, para $x \in \{0, 1, 2, 3, 4\}$, verifica-se que $4x + 1$ é divisível por 5 quando $x = 1$ (apenas ele). Temos:

$$d = \frac{4.1+1}{5} + 52.1 = 53.$$

Devemos observar que esse número satisfaz a condição

$$1 \leq d < 264.$$

Agora devemos inserir os dados do remetente, cujas chaves pública e privada são (187,7) e (187,23), respectivamente.

Na célula H1, insira o texto "**p'**" e em I1 a inscrição: "**q'**". A célula J1 será rotulada com "**e'**", enquanto K1 receberá "**n'=p'.q'**".

Nas células L1, M1 e N1, insira os respectivos textos:

"**(p'-1)(q'-1)**", "**mdc(e',(p'-1)(q'-1)** " e "**d'**".

6) Na linha 2, vamos inserir os valores equivalentes a cada célula rotulada anteriormente. Começamos por H2 que recebe o valor 17. I2 será preenchida com 11. Em J2, entramos com o valor 7. K2 receberá a fórmula "**=H2*I2**". Dessa forma, estamos programando essa célula que será modificada, automaticamente, caso modifiquemos os números p' e q'.

7) Agora programaremos a célula L2 com a fórmula "**=(H2-1)*(I2-1)**". M2 receberá a fórmula "**=MDC(J2;L2)**", e N2 será preenchida com o número 53, que representa o valor de "**d'**", parâmetro da chave privada.

8) O cálculo do valor de d', geralmente, é realizado por meio de resolução de equações diofantinas. No entanto, esse cálculo pode ser adaptado para o ensino médio, como veremos a seguir. d' é um número inteiro definido pelas duas condições,

$$e'd' \equiv 1(\ (\text{mod } (p'-1)(q'-1)) \text{ e } 1 \leq d' < (p'-1)(q'-1).$$

Dessa forma, as condições podem ser reescritas como,

$$7d' \equiv 1\ (\text{mod } 160) \text{ e } 1 \leq d' < 160.$$

Nesse sentido, resolver a primeira condição equivale solucionar a equação:

$$7d' = 160x' + 1, \text{ em que } x' \text{ é inteiro.}$$

Segue que

$$d' = \frac{160x+1}{7} = \frac{6x+1}{7} + 22x.$$

A meta é encontrar um valor para x', de modo que a primeira parcela da equação acima represente um número inteiro. Ao testar a expressão $6x'+1$, para $x' \in \{0,1,2,3,4,5,6\}$, verifica-se que $6x'+1$ é divisível por 7 quando $x'=1$ (apenas ele). Temos:

$$d' = \frac{6.1+1}{7} + 22.1 = 23.$$

Devemos observar que esse número atende à condição

$$1 \leq d' < 160.$$

9) Voltando para a planilha, vamos estabelecer o dicionário de caracteres com 26 letras (na ordem alfabética) que serão substituídas por números inteiros de 10 até 35. Sendo assim, na célula A4, inserimos "**TEXTO ORIGINAL**" e em A5 digitamos a fórmula

$$=\text{ARRAYFORMULA(CARACT(SEQUENCE(26;1;65))).}$$

10) Na coluna B, adicione o dicionário de cifras, iniciando no número 10 e terminando em 35. Basta digitar os dois primeiros números da sequência e usar a função arrastar o cursor para baixo. Com isso, a célula B4 será rotulada com o texto "**CIFRA**" e da célula B5 em diante, colocaremos a sequência de números.

11) Na célula C4, insira o rótulo "**MENSAGEM ORIGINAL**". Nas células abaixo, vamos digitar a mensagem original, lembrando de inserir uma letra em cada célula.

12) Na coluna D, vamos "buscar" cada correspondente das letras no dicionário de cifras (estamos usando a cifra de substituição). Estamos pré-codificando a mensagem original, o rótulo de D4 será "**PRÉ-CODIFICAÇÃO**" e em D5 inserimos a fórmula:

$$=\text{PROCV(C5; } A\$5 :\text{B\$41; 2; 0).}$$

Em seguida, devemos completar a coluna com a função arrastar o cursor para baixo.

13) A coluna E será destinada para a inserção dos "Blocos". São eles que serão codificados. Como vimos na Subseção 4.0.5, os blocos são números formados a partir da mensagem pré-codificada. Para formar os blocos, devemos primeiramente, visualizar a mensagem pré-codificada como um único número. Dessa forma, visualizaremos um número com muitos algarismos. Logo após, devemos "quebrar" os algarismos, desse número, em números menores B_1,B_2...B_r, com $1, 2, ..., r$ números naturais, de modo que cada numeral atenda às condições:

(a) $B_r < n'$;

(b) B_r deve ser coprimo tanto com n' quanto com n;

(c) Nenhum bloco pode inciar com o algarismo zero.

Dessa maneira, vamos rotular a coluna E, inserindo na célula E5 o texto "**BLOCOS B (< n')**", em seguida, apenas copiaremos os pré-códigos da coluna D para serem colados na célula E5. Precisaremos avaliar essa coluna, no entanto, faremos isso com auxilio do editor de planilhas. Nesse sentido, passamos ao passo seguinte para facilitar a avaliação.

14) Na coluna F, vamos verificar quais blocos são coprimos com n. A célula F4 terá a inscrição: "**mdc(B,n)=1**". Na célula F5, inserimos a fórmula:

$$=\text{MDC(E5;C\$2).}$$

Em seguida, usamos a função autocompletar.

15) Repetimos o passo anterior com algumas adaptações. A primeira é rotular a coluna G, inserindo em G4 o texto "**mdc(B,n')=1**". Em seguida, na célula G5, inserimos a fórmula:

$$=\text{MDC(E5;K\$2).}$$

16) Nesse passo, analisaremos simultaneamente as colunas F e G para que atendam às três condições do item 13). Começaremos pela segunda condição, verificando todos os valores dessas colunas que são iguais a 1. Se isso ocorrer, passamos para a próxima análise. Caso contrário, voltamos à coluna dos blocos (Coluna E) e modificamos os valores que não atendem às condições das colunas F e G. A modificação de um bloco será realizada por meio da separação de seus algarismos, criando dois novos blocos que serão vizinhos na coluna. De mesma forma, dois blocos vizinhos podem ser unidos formando um único bloco. No entanto, o valor do bloco deve ser menor do que n', isso satisfaz a primeira condição. Para finalizar, devemos observar que um bloco não pode ter o algarismo inicial igual a zero, como estabelece a terceira condição.

    Esse procedimento é realizado por meio de tentativa e erro. Como já progamamos as colunas F e G para apresentarem os resultados que nos interessam, cada modificação feita na colunas de blocos reflete nas colunas F e G.

    Nesse exemplo, copiamos os pré-códigos:

    $$30\ 22\ 46\ 11\ 24\ 22\ 46\ 10\ 21\ 30\ 23\ 24,$$

    para a coluna de blocos (coluna E). Imediatamente, algumas células das colunas F e G apresentaram valores diferentes de 1. Assim, os blocos dessas linhas devem ser modificados.

17) Neste momento, vamos mostrar a assinatura da mensagem, em que o remetente usa a sua chave privada para tal procedimento. Rotulamos a coluna H, inserindo em H4 a inscrição "**C = B ^d' (mod n')**". Na célula H5, devemos inserir a fórmula:

    $$=\text{MOD(E5 ^N\$2;K\$2)}.$$

    Essa fórmula devolve o resto da divisão por "n'" (na célula K2) de cada bloco, da coluna E, elevado (símbolo circunflexo) ao valor de "d'" (presente na célula N2). Após isso, basta usar a função autocompletar, arrastanto o cursor da célula selecionada para baixo.

    Ao executarmos os passos acima, esperávamos encontrar como resultados, nas células da coluna H, números inteiros. No entanto, o editor de planilhas devolveu, na maioria das dessas células, a indicação de erros com a descrição **#NUM!**. Isso ocorreu devido à limitação do Google Planilhas ao trabalhar com números grandes.

18) Utilizaremos o programa **Wolfram alpha** para fazer esses cálculos.

19) Basta digitarmos, na caixa de entrada do site, a seguinte expressão:

    $$30\ \hat{}\ 23 \bmod 187.$$

Dentro de poucos instantes, a ferramenta nos apresenta na caixa "*Result*" o valor 72. Assim, o primeiro bloco foi encontrado. Os valores calculados através do Wolfram Alpha são:

72 162 63 73 177 168 63 150 175 98 72 162 76 64.

20) Vamos inserir esses resultados na nossa planilha, a partir de I5 e rotulamos a célula I4 com o texto: "**C WOLFRAM**".

21) Até esse momento, a mensagem já foi assinada e agora só resta ao remetente criptografar. Para isso, ele usará a chave pública do destinatário. Sendo assim, criamos a coluna de códigos "T". Na célula J4, digitamos o texto "**T = C ^ e (mod n)**". Na célula J5, inserimos a fórmula:

=MOD(I5 ^ D$2;C$2).

Para finalizar, basta usar a função autocompletar do editor de planilhas. Logo a mensagem criptografada será:

128 93 228 242 190 155 228 271 15 232 128 93 293 233.

Em resumo, o remetente usou o parâmetro de sua chave privada para assinar e a chave pública do destinatário para codificar. De maneira análoga, o destinatário usará a sua chave privada para decodificar, inicialmente a mensagem, logo após, usa a chave pública do remetente para ter acesso à mensagem original.

A planilha produzida pode ser acessada na página "Atividade 11" em https://l1nk.dev/mEcsY.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	p	q	n = p x q	e	(p -1)(q-1)	mdc(e, (p -1)(q-1))	d	p'	q'	e'	n' = p' x q'	(p '-1)(q'-1)	mdc(e', (p'-1)(q'-1))	d'
2	23	13	299	5	264	1	53	17	11	7	187	160	1	23
3														
4	TEXTO ORIGINAL	CIFRA	MENSAGEM ORIGINAL	PRÉ-CODIFICAÇÃO	BLOCOS B (< n')	mdc(B, n)=1	mdc(B,n')=1	C=B ^d' (mod n')	C (Wolfram)	T=C ^e (mod n)				
5	A	10	U	30	30	1	1	#NUM!	72	128				
6	B	11	M	22	2	1	1	162	162	93				
7	C	12	_	46	24	1	1	#NUM!	63	228				
8	D	13	B	11	61	1	1	#NUM!	73	242				
9	E	14	O	24	12	1	1	#NUM!	177	190				
10	F	15	M	22	42	1	1	#NUM!	168	155				
11	G	16	_	46	24	1	1	#NUM!	63	228				
12	H	17	A	10	6	1	1	#NUM!	150	271				
13	I	18	L	21	10	1	1	#NUM!	175	15				
14	J	19	U	30	21	1	1	#NUM!	98	232				
15	K	20	N	23	30	1	1	#NUM!	72	128				
16	L	21	O	24	2	1	1	162	162	93				
17	M	22			32	1	1	#NUM!	76	293				
18	N	23			4	1	1	64	64	233				
19	O	24												
20	P	25												
21	Q	26												
22	R	27												
23	S	28												
24	T	29												
25	U	30												
26	V	31												
27	W	32												
28	X	33												

Figura 5.11: Autoria própria

6

Considerações finais

No presente trabalho, com auxílio do Google Planilhas, desenvolvemos esquemas didáticos de criptografia e aritmética da educação básica.

Destacamos que a experiência adquirida através do trabalho com planilhas corrobora com o aprendizado da informática profissional, servindo também como primeiro contato com linguagens de programação. Para além, pode proporcionar a consolidação da aprendizagem dos alunos.

Perceber a matemática como ciência não acabada e aplicável pode despertar o interesse dos nossos estudantes.

Esperamos que esse trabalho sirva de referência e inspiração para futuras pesquisas educacionais em matemática.

7

Aplicações de tecnologias em aulas de matemática

Para acessar as planilhas com as aulas propostas clique em:

https://l1nk.dev/4pQI1.

7.0.1 Aula 1

1) **Tema**: Cálculo do MMC e MDC.

2) **Problematização**: No primeiro momento, encontre o MMC dos seguintes números:

   (a) 11, 14, 21 e 36.

   (b) 11, 14, 25 e 27.

   (c) 11, 22, 44 e 88.

   Logo após, encontre todos os números menores do que 36 que são coprimos com 36.

3) **Público Alvo**: Turmas dos Anos finais do Ensino Fundamental e Ensino Médio.

4) **Pré-requisitos**:

   - Multiplicação e divisão de números naturais.

5) **Objetivo**: Trabalhar conceitos básicos acerca dos números inteiros (múltiplos e divisores, divisão euclidiana, definição de números primos). Esse roteiro foi construído pela compilação das ideias apresentadas nos Exemplos 5.1.1 e 5.1.2.

6) **Recursos didáticos**: Lousa, pincel, aparelho de Data Show (se possível), computador, ou *tablet* ou *smartphone* com acesso à internet.

7) **Duração**: Cinquenta minutos.

8) **Desenvolvimento**:

- O professor deve explicar a dinâmica da aula, orientando que a aula terá dois momentos. No primeiro, será explorado conteúdos relacionados ao cálculo de MMC. No segundo momento, será investigado uma aplicação para o MDC.
- Definir o conceito de múltiplo e divisor de um número natural.
- Apresentar o conceito de mínimo múltiplo comum e máximo divisor comum.
- Definir número primo e mostrar a importância desses números e suas várias aplicações como visto ao longo deste trabalho. Além disso, definir os números coprimos.
- Apresentar o Google Planilhas, mostrar sua localização, interface e funcionalidades.
- Orientar na construção de uma tabela, como fizemos no Exemplo 5.1.1. O professor preenche sua tabela com os 4 números, aplica a fórmula de cálculo do mmc deles. Paralelamente, em outra célula, entrar com fórmula para o produto desses números.
- Analisar os resultados da tabela. Explorar propriedades do cálculo do MMC.
- Iniciar o segundo momento. Agora devemos encontrar números inteiros positivos menores do que 36 que são coprimos com o próprio 36. Ver referência no Exemplo 5.1.2.
- Analisar os resultados da tabela. Explorar propriedades do cálculo do MDC.
- Investigar a percepção de que a lista de resultados fornece também todos os divisores do número 36. Lembramos que para isso, basta observar que o MDC, apresetando na segunda coluna, deve ser igual ao número da primeira coluna. Deve ser observado que, o número 1 e o próprio 36 não aparecerão nessa lista, ainda assim, eles são, respectivamente, o menor e o maior divisor de 36. Com isso, é possível determinar a quantidade de divisores desse número.
- Sugerir que os alunos testem outros números e analisem os cálculos quando os números envolvidos são coprimos e no caso em que não são coprimos.
- Para além, investigar a relação da tabela com a escrita do número 36 como o produto de seus fatores primos. Essa relação fica mais evidente com decomposição, em fatores primos, dos dois divisores de 36 cuja a diferença entre eles seja a menor possível.

9) **Conclusão**:

- Pedir para que os alunos produzam uma análise de resultados. Nessa análise, é importante que seja apresentada explicação acerca do algoritmo utilizado e análise do uso da tecnologia, comparando-a com o trabalho manual.
- Solicitar "feedback" da aula, com apontamentos de pontos positivos e negativos.

7.0.2 Aula 2

1) **Tema**: Números primos.

2) **Problematização**: Teste primalidade dos números 1129 e 1141. Caso encontre um número composto, determine seus divisores.

3) **Público Alvo**: Turmas dos Anos Finais do Ensino Fundamental e Ensino Médio.

4) **Pré-requisitos**:

   - Multiplicação e divisão de números naturais.

5) **Objetivos**: Trabalhar conceitos básicos acerca dos números inteiros (múltiplos e divisores, definição de números primos). O objetivo principal é testar a primalidade de números inteiros com a utilização de método da divisão.

6) **Recursos didáticos**: Lousa, pincel, aparelho de Data Show (se possível), computador, ou *tablet* ou *smartphone* com acesso à internet.

7) **Duração**: Trinta minutos.

8) **Desenvolvimento**:

   - Definir o conceito de número primo. Explicar a necessidade de encontrar, no mínimo, um divisor do número que seja diferente dele mesmo e do número 1.
   - Explicar o método da divisão utilizado no teste de primalidade, destacando a importância da operação de radiciação para eficiência do método.
   - Apresentação do Google Planilhas. Mostrar funcionalidades do editor que poupam o trabalho manual.
   - Orientar na construção de uma tabela, como fizemos no Exemplo 5.1.3.
   - Analisar os resultados da tabela e concluir de acordo com os números obtidos com as divisões.
   - Sugerir que os alunos testem outros números (observar o aumento de dados da tabela à medida que o número a ser analisado fica maior).

9) **Conclusão**:

- Solicitar aos alunos a análise do processo, por meio de explicação do algoritmo e opinião acerca do uso da tecnologia, comparando-a com o trabalho manual.
- Solicitar "feedback" da aula com indicação de pontos positivos e negativos.

7.0.3 Aula 3

1) **Tema**: Criptografia pelo método da Substituição.

2) **Problematização**: Criptografar e descriptografar a mensagem "TUDO É NÚMERO", utilizando a Cifra de César com chave "D".

3) **Público Alvo**: Turmas dos Anos finais do Ensino Fundamental e Ensino Médio.

4) **Objetivos**: Trabalhar a relação biunívoca e o contexto histórico da Cifra de César. Interpretação de tabelas. Noções de programação.

5) **Recursos didáticos**: Lousa, pincel, aparelho de Data Show (se possível), computador, ou *tablet* ou *smartphone* com acesso à internet.

6) **Duração**: Cinquenta minutos.

7) **Desenvolvimento**:

   - Apresentação da Cifra de César, mostrando contexto histórico.
   - Na primeira parte da aula, o trabalho é voltado para a codificação da mensagem. Comece com a apresentação do Google Planilhas. Enfatize as funcionalidades do editor que poupam o trabalho manual. Nesse sentido, oriente na criação de uma coluna com o alfabeto e outra com as cifras. Ver Exemplo 5.1.5 fazendo adaptações das fórmulas, quando necessário.
   - Crie uma coluna para ser a entrada da mensagem original.
   - Determine a coluna, na qual aparecerá a mensagem criptografada, inserindo a função "PROCV" como feito no Exemplo 5.1.5
   - Analisar, mesmo que superficialmente, o resultado da codificação.
   - Inicar o segundo momento da aula, ou seja, o processo de decodificação da mensagem.
   - Criar uma tabela com quatro colunas, como feito no Exemplo 5.1.6. Inicie inserindo o dicionário de cifras (adaptar fórmula) na primeira coluna. Na segunda coluna, deve ser preenchida com o texto original (alfabeto original).
   - Crie a coluna para ser a entrada da mensagem codificada, inserindo cada cifra em uma única célula.
   - Determine a coluna na qual aparecerá a mensagem criptografada, inserindo a função "PROCV" como feito no Exemplo 5.1.6

- Verificar se a mensagem decodificada confere com a mensagem do primeiro momento.

8) **Conclusão**:

- Solicitar aos alunos a análise do processo, apresentando explicação do algoritmo, opinião acerca do uso da tecnologia em comparação com o trabalho manual.
- Solicitar "feedback" da aula com indicação de pontos positivos e negativos.

7.0.4 Aula 4

1) **Tema**: Criptografia por Cifra Afim.

2) **Problematização**: Criptografar e descriptografar a mensagem "ESTUDAR VALE A PENA", utilizando a Cifra Afim com chave $f(x) = 2x + 6$.

3) **Público Alvo**: Nono Ano do Ensino Fundamental e Ensino Médio.

4) **Pré-requisitos**:

- Multiplicação e divisão de números naturais.
- Noção de resolução de uma equação polinomial do primeiro grau com uma variável.
- Noções do estudo de função polinomial do primeiro grau.

5) **Objetivos**: Trabalhar com o estudo de funções polinomiais do primeiro grau. Criptografia por substituição. Noções de programação de planilhas eletrônicas. Construção e interpretação de tabelas.

6) **Recursos didáticos**: Lousa, pincel, aparelho de Data Show (se possível), computador, ou *tablet* ou *smartphone* com acesso à internet.

7) **Duração**: Cinquenta minutos.

8) **Desenvolvimento**:

- Breve revisão do conteúdo de função polinomial do primeiro grau, com maior ênfase no cálculo da imangem de um elemento da função com a determinação da sua função inversa. Contextualização com funções do 1º grau.
- Na primeira parte da aula, o trabalho é voltado para a codificação da mensagem. Comece com a apresentação do Google Planilhas. Enfatize as funcionalidades do editor que poupam o trabalho manual. Nesse sentido, oriente na criação de uma coluna com o alfabeto e outra com a sequência de números inteiros. Ver Exemplo 5.1.7, fazendo adaptações das fórmulas, quando necessário.

- Crie na coluna A uma lista para o texto original (alfabeto original), usando a fórmula de inserir alfabeto.
- Na coluna B, insira o dicionário de caracteres, ou seja, as cifras. Lista de números de 10 a 35.
- Na coluna C, digite a mensagem original, com cada letra em uma célula.
- Na coluna D, busque cada correspondente das letras no dicionário de Cifras (estamos usando a cifra de substituição). Use a função "PROCV". Terminado esse procedimento, a mensagem estará pré-codificada.
- A coluna E será destinada para encontrar os valores das imagens dos pré-codigos aplicados à função. É nessa coluna que está o resultado de todo processo.
- Iniciar o segundo momento da aula, ou seja, o processo de decodificação da mensagem.
- Determinar a função inversa, manualmente.
- Criar uma tabela com quatro colunas, como feito no Exemplo 5.1.8. Inicie inserindo o dicionário de cifras na primeira coluna. Na segunda coluna, deve ser preenchida com o texto original (alfabeto original).
- A terceira coluna será a entrada da mensagem codificada, inserindo cada cifra em uma única célula.
- Na quarta coluna, devemos aplicar o valor de cada código da coluna anterior na inversa da função. Assim, chegamos até a mensagem pré-codificada.
- Na última coluna, inserimos a função "PROCV" como feito no Exemplo 5.1.8 chegando ao texto original.
- Verificar se a mensagem decodificada confere com a mensagem do primeiro momento.
- Solicitar que os alunos façam testes, trocando a mensagem original e verifiquem a codificação e pré-codificação.

9) **Conclusão**:

- Solicitar aos alunos uma análise do processo, apresentando explicação do algoritmo, opinião acerca do uso da tecnologia em comparação com o trabalho manual.
- Solicitar "feedback" da aula com indicação de pontos positivos e negativos.

7.0.5 Aula 5

1) **Tema**: Criptografia RSA.

2) **Problematização**: Criptografar e descriptografar a mensagem

"PROFMAT_2024",

utilizando o RSA com chave pública (187,7) e chave privada (187,23).

3) **Público Alvo**: Alunos do Ensino Médio.

4) **Pré-requisitos**:

- Multiplicação e divisão no conjunto dos números inteiros.
- Noção de resolução de uma equação polinomial do primeiro grau com duas variáveis.

5) **Objetivos**: Trabalhar com criptografia RSA. Noções de programação de planilhas eletrônicas. Segurança da informação. Construção e interpretação de tabelas.

6) **Recursos didáticos**: Lousa, pincel, aparelho de Data Show (se possível), computador, ou *tablet* ou *smartphone* com acesso à internet.

7) **Duração**: Cem minutos.

8) **Desenvolvimento**:

- Na primeira parte da aula, o trabalho é voltado para a codificação da mensagem. Comece com a apresentação do Google Planilhas. Enfatize as funcionalidades do editor que poupam o trabalho manual. Inicie inserindo os parâmetros das chaves. Nesse sentido, rotule as células da primeira linha (A1,...,G1) com os respectivos rótulos p, q, $p.q$, e, $(p-1)(q-1)$, $mdc(e,(p-1)(q-1))$ e d. Na linha 2, vamos inserir os respectivos valores das células rotuladas, são eles: 11, 17, 187, 7, 160, 1 e 23. Nessa segunda linha, pode ser feita a programação dos cálculos nas células C2 (=A2*B2), E2 (=(A2-1)*(B2-1)) e F2 (=MDC(D2;E2)). Ver Exemplo 5.1.9.
- Crie na coluna A uma lista para o texto original, usando a fórmula de inserir alfabeto, ver Exemplo 5.1.9. Nessa mesma coluna, logo após o alfabeto, insira os algarismos de 0 até 9. Na célula abaixo do algarismo 9, entre com o símbolo _ (underline). Ele representará o espaço entre as palavras na mensagem original.
- Na coluna B, insira o dicionário de caracteres, ou seja, as cifras. Lista de números de 10 a 46.
- Na coluna C, digite a mensagem original, com cada letra em uma célula. Lembre-se que o espaço deve ser preenchido pelo símbolo *underline*.
- Na coluna D, busque cada correspondente das letras no dicionário de Cifras (estamos usando a cifra de substituição). Use a função "PROCV", inserindo em D5 a fórmula:

$$=\text{PROCV}(\text{C5};\ \text{A5} : B41;\ 2;\ 0).$$

Terminado esse procedimento, a mensagem estará pré-codificada.

- A coluna E será destinada para encontrar os blocos dos pré-codigos. São eles que serão codificados no final do processo.
- A célula F4 será rotulada com "B $\not\equiv 0 \pmod{p}$". Na célula abaixo, insira a fórmula:

  $$=\text{MOD(E5;A\$2)}$$

  e use a funcionalidade autocompletar.
- Faça o procedimento análago ao item anterior. As modificações são que a célula G4 recebe "B $\not\equiv 0 \pmod{q}$" e em G5 insira:

  $$=\text{MOD(E5;B\$2).}$$

  Use a funcionalidade autocompletar.
- Na coluna H, vamos encontrar o resultado do procedimento. A célula H4 será rotulada com

  "C=B ^ e (mod pq)".

  O símbolo circunflexo (^) realiza a exponencial. Na célula H5 insira a fórmula:

  $$=\text{MOD(E5 ^ D2;}C2).$$

  Logo após use a função autocompletar, nas células dessa coluna, aparecerá as cifras codificadas:

  $$185\ 124\ 29\ 93\ 128\ 128\ 175\ 160\ 7\ 47\ 9\ 47\ 116.$$

- Iniciar o segundo momento da aula, ou seja, o processo de decodificação da mensagem.
- Rotule a célula J4 com "CIFRA". Na célula abaixo, insira o dicionário de cifras. Copie da coluna B.
- Rotule a célula K4 com "TEXTO ORIGINAL", na célula abaixo insira o alfabeto. Copie da coluna A.
- Na coluna L, vamos inserir a mensagem criptografada. Para isso, rotule L4 com o texto "MENSAGEM CRIPTOGRAFADA" e na célula abaixo, cole a mensagem obitida na coluna H. Cole somente os valores.
- Na coluna M, vamos fazer o processo inverso da codificação. Para isso, rotulamos a célula M4 com o texto "RESTO DE (C ^ 29) : 187". Na célula abaixo, digite a expressão responsável pela codificação;

  $$=\text{MOD(L5 ^ G\$2;C\$2).}$$

  Use a função autocompletar.

  O programa Google Planilhas não é capaz de realizar esses cálculos. Sendo assim, devemos usar o programa Wolfram Alpha para realizá-los.

- Abra o site no navegador de internet. Para isso, basta digitar ou clicar no endereço:

  https://www.wolframalpha.com.

- Na caixa de entrada da tela principal do site, digite o comando que necessitamos, ou seja,

  $$185 \widehat{} \ 23 \ (\text{mod } 187).$$

  Na tela, um pouco mais abaixo, será possível visualizar o resultado, 25.

- Prossiga realizando o passo anterior para cada cifra da coluna L. Cada valor encontrado deve ser digitado na planilha, na coluna N, a partir da célula N5. Para melhor entendimente e estética, rotule a célula N4 com o texto "BLOCOS B ($< p.q$) WOLFRAM". A coluna será composta pelos números:

  $$25\ 27\ 24\ 15\ 2\ 2\ 10\ 29\ 46\ 38\ 36\ 38\ 40.$$

- Perceba que dois elementos não fazem parte do dicionário de cifras. Sendo assim, escrevemos essa sequência de números, tomando cuidado para que nenhum deles seja menor do que 10 e ou maior do que 46. As modificação devem ser feitas por união de números por justaposição.

- Na coluna O, vamos escrever as cifras que foram encontradas com os blocos da etapa anterior. Rotulamos a célula O4 com "CIFRA DIGITAL", e a partir de O5, encontraremos a sequência

  $$25\ 27\ 24\ 15\ 22\ 10\ 29\ 46\ 38\ 36\ 38\ 40.$$

- O processo final se dará pela substituição dessas cifras. Nesse sentido, rotule a célula P4 com o texto "MENSAGEM ORIGINAL" e, na célula P5, insira a fórmula:

  $$=\text{PROCV(O5;J\$5:K\$41;2;0)}.$$

  Ao usar a função autocompletar, deve aparecer a mensagem:

  $$\text{PROFMAT\_2024}.$$

9) **Conclusão**:

- Solicitar aos alunos uma análise do processo, apresentando explicação do algoritmo, opinião acerca do uso da tecnologia em comparação com o trabalho manual.
- Solicitar "feedback" da aula com indicação de pontos positivos e negativos.

7.0.6 Aula 6

1) **Tema**: Criptografia RSA com assinatura.

2) **Problematização**: Descriptografar a mensagem

$$128\ 93\ 228\ 242\ 190\ 155\ 228\ 271\ 15\ 232\ 128\ 93\ 293\ 233,$$

utilizando o RSA com assinatura do remetente que possui a chave pública (187,7) e (187,23) como chave privada, e o destinatário da mensagem tem em mãos as chaves pública e privada, respectivamente, iguais a (299,5) e (299,53).

3) **Público Alvo**: Alunos do Ensino Médio.

4) **Pré-requisitos**:

- Possuir noção de criptografia RSA.

5) **Objetivos**: Trabalhar com criptografia RSA com assinatura de mensagem. Noções de programação de planilhas eletrônicas. Construção e interpretação de tabelas.

6) **Recursos didáticos**: Lousa, pincel, aparelho de Data Show (se possível), computador, ou *tablet* ou *smartphone* com acesso à internet.

7) **Duração**: Cinquenta minutos.

8) **Desenvolvimento**:

- Inicie inserindo os parâmetros das chaves. Nesse sentido, rotule as células A1 até E1, da primeira linha, com os respectivos rótulos $n = pq$, e, d, $n' = p'q'$ e e'. Na linha 2, vamos inserir os respectivos valores das células rotuladas, são eles: $n = 299$, $e = 5$, $d = 53$, $n' = 187$ e $e' = 7$.
- A célula A4 será rotulada com o texto "**CIFRA**". Da célula A5 em diante, colocaremos a sequência de cifras que inicia no número 10 e termina em 46. Para isso, digite os dois primeiros números da sequência e use a função arrastar o cursor para baixo.
- Criaremos o dicionário de caracteres com 26 letras, posicionadas na sua ordem alfabética. Dessa forma, na célula A4, será rotulada por "**TEXTO ORIGINAL**" e em A5 digitaremos a fórmula:

  $$=\text{ARRAYFORMULA(CARACT(SEQUENCE(26;1;65))).}$$

  Na célula A31, inicie a sequência dos algarismos (de 0 até 9). Por fim, insira o símbolo "*underline*" na célula A41. Esse símbolo representará os espaços que podem haver entre as palavras na mensagem recebida.

- A célula C4 receberá a inscrição "**MENSAGEM CRIPTOGRAFADA**". Nas células de baixo, digitaremos a mensagem codificada, lembrando de inserir um código em cada célula.
- Na coluna D, rotularemos D4 com o texto "$C = B \hat{} d\,(mod\, n)$". Na célula D5, devemos inserir a fórmula:

  $$=\text{MOD(C5 ⌃ C\$2;A\$2)}.$$

  Na sequência, use a função autocompletar do editor de planilhas. O programa retornará o erro **#NUM!** na fórmula. Dessa forma, esses cálculos podem ser feitos pelo programa Wolfram Alpha, no endereço eletrônico:

  https://www.wolframalpha.com.

- Na coluna E, insira os resultados dos cálculos realizados pelo Wolfram Alpha. Na célula E4, rotule com a inscrição "**U (wolfram)**". Os dados serão inseridos da célula E5 em diante.

  Até esse momento, o destinatário fez a primeira parte da decodificação da mensagem. Ele usou a chave privada.

- Agora vamos verificar a assinatura do remetente. Sendo assim utilizaremos a fórmula:

  $$=\text{MOD(E5 ⌃ E\$2;D\$2)},$$

  que deve ser insirida em F5. Essa coluna receberá o rótulo de "**B=U ⌃ e' (mod n')**" em F4. Após a inserção da fórmula, use a função autocompletar do editor de planilhas. Essa coluna apresentará erros. Isso novamente ocorrerá devido à limitação desse programa. Use novamente o programa Wolfram Alpha para realizar os cálculos que não foram realizados até o momento.
- Na coluna G, insira em G4 a descrição "**B (Wolfram)**". Insira todos os cálculos da coluna anterior. Com essa coluna completa, o destinatário possui os blocos que foram codificados.
- Rotule a célula H4 com "**CIFRA**". Da célula H5 em diante, insira, manualmente, os blocos originais formados a partir da coluna anterior. Logo devemos ter números que variam de 10 até 46. Na ordem que aparecem e utilizando união por justaposição.
- Para finalizar, vamos procurar cada cifra encontrada na coluna anterior no nosso dicionáio de cifras. Iniciamos, rotulando a célula I4 com "**TEXTO ORIGINAL**". Em I5, insira a fórmula:

  $$=\text{PROCV(H5;A\$5:B\$41;2;0)}.$$

  Ao utilizar a função autocompletar, a mensagem irá sendo revelada.

UM_BOM_ALUNO.

9) **Conclusão**:

- Solicitar aos alunos uma análise do processo, apresentando explicação do algoritmo.
- Solicitar "feedback" da aula com indicação de pontos positivos e negativos.

8

Apêndice A

8.0.1 Atividades propostas

Neste apêndice, apresentaremos alguns exercícios contextualizados envolvendo o mdc e o mmc. Para facilitar o planejamento das aulas disponibilizamos planilhas com as resoluções dos exercícios. Para acessar clique em https://acesse.one/uZniz .

Exercício 8.0.1: Em uma empresa, os cinco gerentes de produção precisam definir o número de funcionários a serem contratados para iniciar a sua operação. Eles poderão distribuir o número total de os funcionários em setores iguais, todos com 608 funcionáios, ou todos com 416, ou todos com 247 funcionários, sem que haja sobra de funcionários. Desse modo, qual é o número mínimo de funcionários que essa empresa precisa ter para entrar em operação, incluindo os gerentes?

Solução:

Para resolver esse problema, devemos primeiramente encontrar o mmc dos números de funcionários que os setores podem conter. Para isso, vamos construir uma tabela no Google Planilhas.

- Mescle as células A1 e B2 e coloque o título da sua tabela.
- Na célula A2, inclua a descrição *FUNCIONÁRIOS*. Já em B2, inclua: *RESULTADO*
- Entre com os valores de funcionários que os setores podem ter nas células A3, A4 e A5.
- Na célula A7, introduza o texto: *mmc*.
- Na célula B7, insira uma das fórmulas:

$$=\text{MMC(A3;A4;A5) ou } =\text{MMC(A3:A5).}$$

O programa nos retorna como valor o número 7904. Com mais os cincos gerentes, concluímos que o total de funcionários é 7909. Esse passo pode ser automatizado, para isso, em qualquer célula vazia do editor, por exemplo em B8, insira:

=B6+5.

Nota: A construção e formatação de tabelas no Google Planilhas são habilidades que podem ser trabalhadas a critério do professor.

Exercício 8.0.2: Uma árvore de natal possui luzes que acendiam e imediatamente apagavam nas seguintes frequências: as luzes amarelas piscavam de 15 em 15 segundos. Já as vermelhas faziam o mesmo procedimento de 19 em 19 segundos. As luzes azuis piscavam de 21 e 21 segundos. Por último, as verdes piscavam de 27 em 27 segundos. Ao ligar a árvore, todas as luzes piscam juntas. Depois de quanto tempo elas tornarão a piscar todas ao mesmo tempo?

Solução:

Esse problema é resolvido, diretamente, pelo cálculo do mmc dos números 15, 19, 21 e 27, que representam o intervalo que cada lâmpada demora para piscar. Sendo assim, entramos com esses valores nas células da coluna A. No final dessa coluna, inserimos uma das fórmulas:

=MMC(A1:A4) ou =MMC(A1;A2;A3;A4).

O programa nos retorna como valor o número 17 955 segundos.

Exercício 8.0.3: Ilda está estudando o resultado com testes dos medicamentos A, B e C em cobaias. O medicamento A está sendo ministrado a 162 cobaias. Outro grupo formado por 270 cobaias é testado com o medicamento B. Por fim, um terceiro grupo com 306 animais recebem o medicamento C. Para uma análise, ela precisa que as cobaias sejam divididas em grupos com o mesmo número de indivíduos, sendo que o número de indivíduos por grupo seja o maior possível e que os grupos possuam somente cobaias que receberam o mesmo medicamento. Após essa separação, cada grupo é enviado para uma gaiola que deve ser identificada. Quantas gaiolas serão necessárias para acolher todos os novos grupos?

Solução:

Esse problema é resolvido pelo cálculo do mdc dos números 162, 270 e 306. Sendo assim, construíremos uma tabela com seis linhas e três colunas. Na primeira, vamos inserir cada medicamento (A, B e C). Na segunda coluna, será inserido os números de cobais que receberam cada um dos medicamentos (162, 270, 306). Na terceira, vamos encontrar o número de grupos após as divisões das cobaias. Todos os dados devem ser inseridos a partir da 3ª célula de cada coluna. Dessa forma, basta inserir na coluna B, de frente para o texto "mdc", a fórmula:

=MDC(B3:B5).

Na célula C3, vamos inserir a fórmula:

=B3/B$7.

Logo após, usamos a função autocompletar, arrastando o cursor, da célula selecionada, para baixo. O programa retornará, nessa coluna, as quantidades relativas de cada um dos grupos. Para finalizar, basta aplicar a função soma nos resultados encontrados. Na célula C8, insira a fórmula:

$$=\text{SOMA(C3:C7)}.$$

O número de gaiolas necessárias para acolher todos os grupos é 41.

Exercício 8.0.4: Uma máquina produz peças de ferragem de dois comprimentos diferentes, uma com 156 metros e outra com 180 metros. Para atender a uma obra na construção de uma ponte, essa empresa precisa partir essas ferragens em pedaços iguais, de maior tamanho possível, sem que haja desperdício nas peças que a máquina produz.

Nesse sentido, qual deve ser o tamanho de cada pedaço vendido pela empresa?

Solução:

Esse problema é resolvido pelo cálculo direto do mdc dos números 156 e 180. Sendo assim, construa uma tabela e inserira os dois números nas duas primeiras células da coluna B. Na terceira célula dessa coluna, insira a fórmula:

$$=\text{MDC(B3;B4)}.$$

O programa nos retornará 12 metros.

Exercício 8.0.5: Considere dois intervalos de números inteiros. O primeiro é formado pelos números de 1 a 100, o segundo de 101 a 200. Encontre a quantidade de números primos contidos em cada intervalo. Logo após, encontre a diferença das quantidades de números primos encontrados em cada intervalo.

Solução:

Sugererimos a construção de uma tabela no Google Planilhas. Na coluna A, vamos inserir o número 2 e todos os números ímpares menores do que 100. Siga os passos:

i. Na linha 1, vamos mesclar as três primeiras células dessa linha (A1, B2,C3) e inserir o título da tabela,

   "VERIFICAÇÃO DE PRIMALIDADE de 1 a 100".

ii. Na célula A2, insira o texto:

   "NÚMERO".

iii. Na célula A4, insira o número 2. Nas células A5 e A6, insira, respectivamente, 3 e 5. Logo após, selecione os dois números e arraste o curso para baixo até chegar ao número 99.

iv. A célula B2 será destinada aos números que vamos testar. Observe que só precisamos testar números ímpares. Se o aluno conhecer todos os produtos da tábua de múltiplicação de 2 até 9 mais os critérios de divisibilidade por 3 e 5, o trabalho será reduzido significativamente. Além disso, podemos informar os 5 primeiros números primos (2, 3, 5, 7 e 11) que não precisarão ser testados. Começaremos testando o número 13 que deve ser digitado em B2.

v. Na célula B3, entre com o título:

"Resto de B2 por A(N)".

vi. Na célula B4, inicie a programação. Nessa célula, será calculado o resto da divisão do número inserido em B2 pelo número inserido em A4, que na fórmula acima é representado por A(N). Para isso, insira na célula a seguinte fórmula:

=MOD(B$2;A4).

vii. Agora use a função "arrastar", na célula B4 até o final da tabela.

viii. Verifique se algum número da coluna B é igual a zero. Se apareçer apenas um número zero, o número é divisível somente por ele mesmo, logo é primo. Caso contrário, ele é não primo.

ix. Agora é só testar os outros números, inserindo-os na célula B2 e analisando essa coluna.

x. Crie uma coluna, fora da tabela, na coluna E, por exemplo, para inserir os números primos encontrados.

Nota: Para facilitar a análise do item anterior, podemos colocar um destaque em todos os números zeros que por ventura aprareçam nessa coluna. Para isso, use a formatação condicional:

- Selecione as células B4 até B53.
- Acesse na barra superior do menu, do Google Planilhas a função **Formatar**. Logo após, clique em **Formatação condicional**.
- Verifique se o intervalo esta correto. Logo após, no subitem **Regras de formatação**, escolha a opção: "*O texto é exatamente*".
- Na caixa de dialógo, logo abaixo, digite "0".
- No subitem **Estilo de formatação**, escolha a cor vermelha, por exemplo, clicando no balde de tinta. Clique em **Concluído**. Pronto, todos os números zeros, no intervalo selecionado ficarão com o fundo da célula vermelho. Veja ilustração.

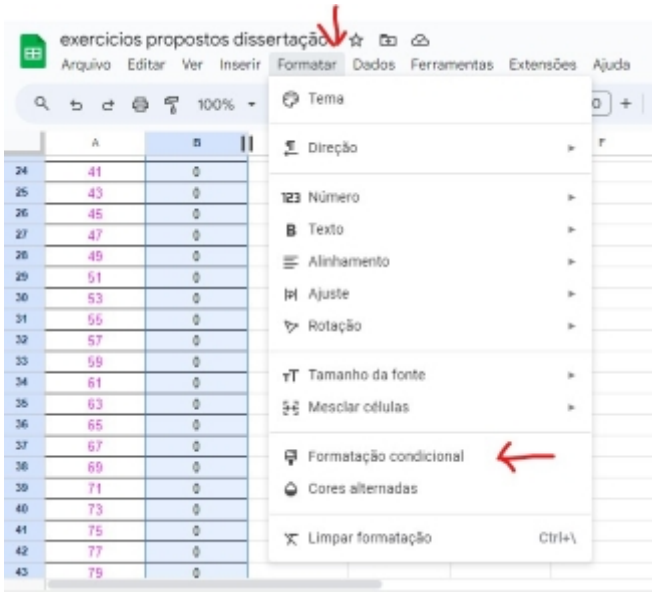


Figura 8.1: Formatação 1, Autoria própria

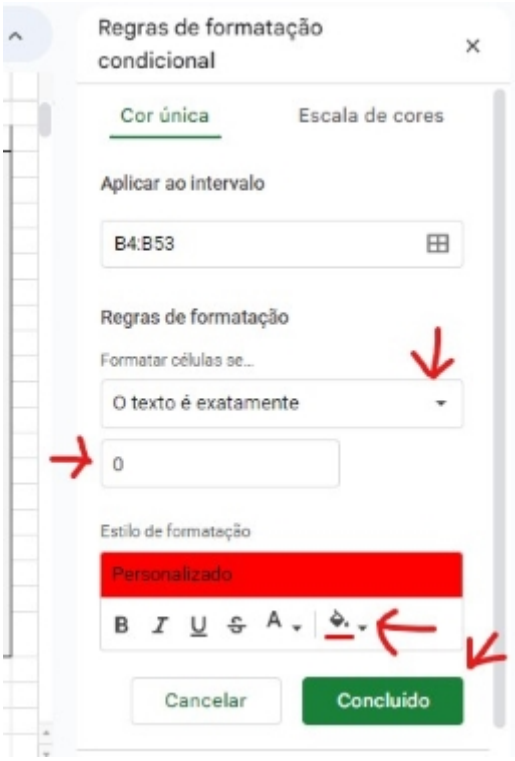


Figura 8.2: Formatação 2, Autoria própria

Para obter a quantidade de números que inserimos nas colunas dos números primos, contaremos com ajuda do programa. Para isso, selecione todos os números dessa coluna. Observe que, no canto direito da barra inferior da planilha, aparece a expressão "soma:" seguida de um número. Ao lado direito desse número, há uma seta preta, apontada para baixo. Ao clicar na seta, surgirá uma mini guia com várias opções, uma delas será a opção: "contagem", que nesse caso estará representado pela expressão: "contagem:25". Dessa forma,

indicará 25 números inseridos na coluna selecionada. Segue ilustração.

Figura 8.3: Contagem, Autoria própria

Para concluir o exercício, repita o procedimento para os números de 101 a 200. Nesse passo, crie uma coluna de primos ao lado da coluna anterior (coluna F). Serão, 21 números primos neste intervalo. A diferença entre as quantidades será de 4 números.

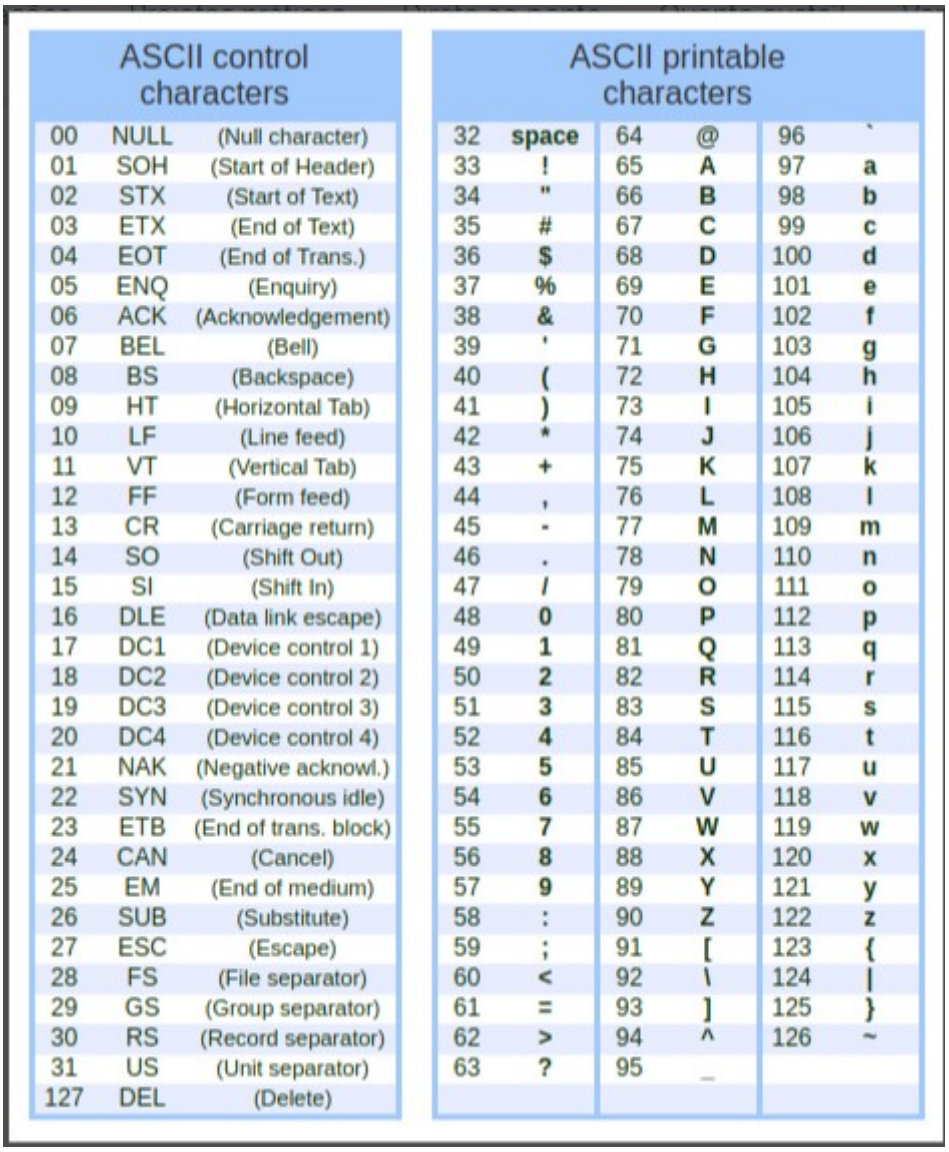
9

Apêndice B

9.0.1 Figuras

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figura 9.1: Tabela de Vigenère



ASCII control characters

00	NULL	(Null character)
01	SOH	(Start of Header)
02	STX	(Start of Text)
03	ETX	(End of Text)
04	EOT	(End of Trans.)
05	ENQ	(Enquiry)
06	ACK	(Acknowledgement)
07	BEL	(Bell)
08	BS	(Backspace)
09	HT	(Horizontal Tab)
10	LF	(Line feed)
11	VT	(Vertical Tab)
12	FF	(Form feed)
13	CR	(Carriage return)
14	SO	(Shift Out)
15	SI	(Shift In)
16	DLE	(Data link escape)
17	DC1	(Device control 1)
18	DC2	(Device control 2)
19	DC3	(Device control 3)
20	DC4	(Device control 4)
21	NAK	(Negative acknowl.)
22	SYN	(Synchronous idle)
23	ETB	(End of trans. block)
24	CAN	(Cancel)
25	EM	(End of medium)
26	SUB	(Substitute)
27	ESC	(Escape)
28	FS	(File separator)
29	GS	(Group separator)
30	RS	(Record separator)
31	US	(Unit separator)
127	DEL	(Delete)

ASCII printable characters

32	space	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		

Figura 9.2: Fonte: //www.treinaweb.com.br/blog/uma-introducao-a-ascii-e-unicode acesso 26/04/24.

Bibliografia

[1] Brasil. “Base Nacional Comum Curricular”. Ministério da Educação (20 de dez. de 2017). Portaria 1570. Estabelece as diretrizes e bases da educação nacional. URL: http://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf (acesso em 25 de jul. de 2023).

[2] Carneiro, F. J. F. Criptografia e Teoria dos Números. Editora Ciência Moderna Ltda, 2017.

[3] Hefez, A. Aritmética. 3ª edição. Rio de Janeiro: SBM: Sociedade Brasileira de Matemática, 2022.

[4] Lima, E. L. Números e funções Reais. 1ª edição. Rio de Janeiro: SBM, 2013.

[5] Matemática Pura e Aplicada, I. de. Descoberto número primo com quase 25 milhões de dígitos. 2024. URL: https://impa.br/noticias/descoberto-numero-primo-com-quase-25-milhoes-de-digitos/ (acesso em 14 de jul. de 2024).

[6] Menezes Neto, J. L. de. Primeiros passos em criptografia [recursos eletrônicos]. João Pessoa: Editora UFPB, 2021.

[7] Shokranian, S. Criptografia para Iniciantes. 2ª edição. Editora Ciência Moderna Ltda, 2012.

[8] Shokranian, S. Números Notáveis. 2ª edição. Editora UnB, 2002.

[9] Singh, S. O livro dos Códigos. Editora Record, 2001.