UNIVERSIDADE ESTADUAL PAULISTA

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

JOÃO FERNANDO MONTANHER

INTRODUÇÃO DA CRIPTOGRAFIA NO ENSINO BÁSICO SOB A ÓPTICA DA ARITMÉTICA MODULAR

BAURU

2022

JOÃO FERNANDO MONTANHER

INTRODUÇÃO DA CRIPTOGRAFIA NO ENSINO BÁSICO SOB A ÓPTICA DA ARITMÉTICA MODULAR

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação – Mestrado Profissional em Matemática em Rede Nacional, da Faculdade de Ciências da Universidade Estadual Paulista “Julio de Mesquita Filho”, Campus de Bauru.

Orientador: Prof. Dr. Luis Antonio da Silva Vasconcellos

BAURU

2022

Montanher, João Fernando.
Introdução da criptografia no ensino básico sob a óptica da aritmética modular Montanher, 2022
Total de folhas. 63 : il.

Orientador: Dr. Luis Antonio da Silva Vasconcellos

Dissertação (mestrado profissional) - Universidade Estadual Paulista Faculdade de Ciências, Bauru, 2022.

1. Matemática (Ensino médio) - Estudo e ensino. 2. Criptografia. 3. Congruência. 4. RSA. 5. El Gamal. I. Universidade Estadual Paulista, Faculdade de Ciências. II. Título.

unesp

UNIVERSIDADE ESTADUAL PAULISTA

Câmpus de São José do Rio Preto

IBILCE

ATA DA DEFESA PÚBLICA DA DISSERTAÇÃO DE MESTRADO DE JOÃO FERNANDO MONTANHER, DISCENTE DO PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL, DO INSTITUTO DE BIOCIÊNCIAS, LETRAS E CIÊNCIAS EXATAS - CÂMPUS DE SÃO JOSÉ DO RIO PRETO.

Aos 22 dias do mês de junho do ano de 2022, às 09:00 horas, por meio de Videoconferência, realizou-se a defesa de DISSERTAÇÃO DE MESTRADO de JOÃO FERNANDO MONTANHER, intitulada **Introdução da Criptografia no Ensino Básico sob a Óptica da Aritmética Modular**. A Comissão Examinadora foi constituida pelos seguintes membros: Prof. Dr. LUIS ANTONIO DA SILVA VASCONCELLOS (Orientador(a) - Participação Virtual) do(a) Departamento de Matemática / UNESP/Câmpus de Bauru, Prof. Dr. WLADIMIR SEIXAS (Participação Virtual) do(a) CCET / UFSCar/São Carlos (SP), Prof. Dr. AGNALDO JOSÉ FERRARI (Participação Virtual) do(a) Departamento de Matemática / UNESP/Câmpus de Bauru. Após a exposição pelo mestrando e arguição pelos membros da Comissão Examinadora que participaram do ato, de forma presencial e/ou virtual, o discente recebeu o conceito final: Aprovado. Nada mais havendo, foi lavrada a presente ata, que após lida e aprovada, foi assinada pelo(a) Presidente(a) da Comissão Examinadora.

Prof. Dr. LUIS ANTONIO DA SILVA VASCONCELLOS

DEDICATÓRIA

Dedico este trabalho a todos os profissionais de educação que não se cansam de seu trabalho afim de promover a mudança necessária em nosso país, promovendo pequenas mudanças individuais e coletivas na vida de nossos alunos e aos meus alunos, responsáveis pelo meu contínuo aprendizado como docente.

AGRADECIMENTOS

Em primeiro lugar gostaria de agradecer minha mãe, por todo tempo gasto comigo, ter abdicado inúmeras ambições e aspirações próprias afim de manter dedicação exclusiva à educação de seus filhos, ensinando valores e a importância do estudo para o indivíduo. Mesmo sendo efusiva demonstra um amor e dedicação incondicional aos seus filhos.

A minha irmã por todo carinho, paciência e diligência empregada, atuando como uma tutora para a vida, sempre disposta a me ajudar a qualquer momento.

A minha melhor amiga e namorada Giovanna, por todo o apoio e incentivo nos piores momentos e também a toda distração e espairecimento com as melhores conversas proporcionadas pela sua companhia.

Daqueles que trilharam junto a mim durante todo esse percurso, todas as risadas, almoços, conversas, passeios, estudos e angústias que passamos juntos. Antônio Eduardo companheiro de viagem, grande amigo e uma das pessoas com um com coração enorme que conheço. Rafaela intimidadora, porém, com uma inteligência e sensatez enorme. Sílzia proporcionando ótimas conversas e histórias. A companhia de vocês facilitou muito este percurso.

Aos docentes que atuaram em nossa formação, possuindo grande dedicação e paciência em suas aulas e também longe delas através das respostas as nossas dúvidas sobre suas listas de exercício. Em especial agradeço ao Prof. Luís Antônio que atuou como meu orientador.

RESUMO

Este trabalho utilizará a aritmética modular com aplicações no ensino fundamental e médio, propondo aplicações como atividades em sala de aula. O trabalho se inicia com fundamentos teóricos servindo de base para as aplicações da aritmética modular em nosso cotidiano, como C.P.F., cartão de crédito, código de barras, calendários e criptografia. Por fim o trabalho se encerra promovendo atividades adaptadas da aritmética modular no ensino básico.

Palavras chave: aritmética modular, congruência, criptografia, RSA, El Gamal.

ABSTRACT

This work will use modular arithmetic with applications in elementary and medium education, proposing applications as activities in the classroom. The work begins with theoretical foundations serving as a basis for applications of modular arithmetic in our daily lives, such as C.P.F., credit card, barcode, calendars and cryptography. Finally, the work ends by promoting activities adapted from modular arithmetic in basic education.

Keywords: modular arithmetic, congruence, cryptography, RSA, El Gamal.

SUMÁRIO

INTRODUÇÃO 10
1- FUNDAMENTOS TEÓRICOS 11
2 - APLICAÇÕES DA MATEMÁTICA MODULAR EM NOSSO COTIDIANO 25
2.1 - Cadastros de Pessoas Físicas (C.P.F.) 25
2.2 - Cartão de Crédito 26
2.3 - Código de Barras 27
2.4 – Calendários 30
2.5 – Criptografia 32
2.5.1 – Modelo RSA 34
2.5.2 – Modelo El Gamal 39
3 - APLICAÇÕES EM PLANOS DE AULA PARA O ENSINO BÁSICO 42
3.1 – Cálculo dos dígitos verificadores do C.P.F. 42
3.1.1 – Plano de Aula 42
3.1.2 - Análise de resultados 44
3.2 – Cálculo dos dígitos verificadores do Cartão de crédito e código de barras 46
3.2.1 – Plano de Aula 46
3.2.2 - Análise de resultados 48
3.3 – Estudo de calendários e utilização do algoritmo de Zeller 50
3.3.1 – Plano de Aula 50
3.3.2 - Análise de resultados 52
3.4 – Um prelúdio a criptografia 55
3.4.1 – Plano de Aula 55
3.4.2 - Análise de resultados 57
CONSIDERAÇÕES FINAIS 60
REFERÊNCIAS 62

INTRODUÇÃO

Durante a história da humanidade a criptografia foi usada em diferentes contextos, inicialmente empregada em tempos de guerra e agora assumindo um papel essencial, como por exemplo em transações financeiras, troca de mensagens, contas pessoais, dentre outros, embora o objetivo sempre fosse proteger informações transmitidas em campos não seguros. Motivado por tal fato, a proposta deste trabalho é estudar a álgebra modular e teoria dos números aplicando-os no contexto do ensino básico, afim de entender a importância de sistemas que utilizam a criptografia em nosso cotidiano.

O objetivo principal é introduzir a aritmética modular a estudantes do ensino fundamental II (5º a 9º ano) e ensino médio (1ª a 3ª série), demostrando a sua utilidade e aplicação em sistemas que utilizamos de maneira corriqueira no cotidiano de nossa sociedade, além de fortalecer o estudo com números primos e introduzir a álgebra modular. Também, espera-se que seja utilizado por docentes como material complementar nos planos de aula.

Este trabalho está estruturado em três capítulos. O primeiro apresenta fundamentos teóricos da teoria dos números e aritmética modular. O segundo capítulo apresenta utilizações da aritmética modular em situações como Cadastro de Pessoas Físicas (C.P.F.), cartões de créditos, códigos de barras, calendário Gregoriano e métodos criptográficos, em especial os modelos RSA e El Gamal. O terceiro capítulo abordará aplicações na realidade escolar. Serão desenvolvidas atividades baseadas nas utilizações da aritmética modular citadas no capítulo anterior. Ao final de cada atividade apresenta-se uma breve discussão do desenvolvimento e resultados obtidos.

Por fim, apresentam-se as considerações finais e algumas sugestões de reestruturação para os planos de aula.

1- FUNDAMENTOS TEÓRICOS

Neste capítulo, serão apresentadas algumas definições, proposições e teoremas de aritmética fundamental e estruturas algébricas, com intuito de servir de ferramentas para facilitar a compreensão dos tópicos que serão abordados e estudados, culminando na adaptação em planos de aula para os alunos do ensino fundamental e médio.

Definição 1.1: Dados dois inteiros a, chamado de dividendo, e b > 0, chamado de divisor, definimos o quociente q e o resto r da divisão inteira de a por b como inteiros que satisfazem as seguintes condições: $a = b.q + r$ e $0 \leq r < b$. Considera-se que os divisores são positivos.

Teorema (Unicidade do Quociente e Resto) 1.2: Dados dois inteiros a e b > 0, existe um único par de inteiros q e r que satisfaz as condições da definição 1.1.

Demonstração: Suponha, por contradição, que para dado um par de inteiros a, b > 0, existem dois pares de inteiros diferentes (q, r) e (q_o, r_o) que satisfaçam as condições acima. Temos então que $a = b.q + r$ (i) e $a = b.q_o + r_o$ (ii), onde $0 \leq r \leq r_o < b$. Note que para fins de demonstração supomos que $r \leq r_o$, tal fato não perde a generalidade, pois para $r_o \leq r$ o processo é análogo. Se $0 \leq r \leq r_o < b$ então $0 \leq r_o - r < b$, subtraindo (i) de (ii), segue que $0 = b.(q - q_o) + (r - r_o)$, o que significa que $r_o - r = b.(q - q_o)$. Como $0 \leq r_o - r < b$, temos $0 \leq b.(q - q_o) < b$, mas $b \neq 0$ então $0 \leq q - q_o < 1$ sendo uma contradição pois $q, q_o \in \mathbb{Z}$, portanto, $q = q_o$ e $r = r_o$, mostrando a unicidade do teorema.

Definição 1.3: Sejam a, b > 0 números inteiros. Dizemos que a é múltiplo de b, ou que a é divisível por b (denotado por $b|a$), ou que b é divisor de a, ou que b é fator de a, se $a = b.x$, para algum $x \in \mathbb{Z}$, isto é, se a divisão de a por b produz resto 0.

Proposição (Euclides) 1.4: Sejam $a, b \neq 0$ naturais. Se p é primo e $p|a.b$ então $p|a$ ou $p|b$.

Demonstração: Suponha que p∤a, se p|a.b então existe um natural n, tal que n.p = a.b, logo n = $\frac{a.b}{p}$, como n é natural e p∤a então p|b. Analogamente p∤b ⇒ p|a. □

Corolário 1.5: Se p é primo e p|$a_1.a_2. \ldots .a_n$, então p | a_i para algum i.
Considerando os pares a_1 e $a_2.a_3. \ldots .a_n$, se p | a_1 então tem-se a prova do corolário. Caso p | $a_2.a_3. \ldots .a_n$, considere um novo par a_2 e $a_3.a_4. \ldots .a_n$ e utilize o mesmo raciocínio até encontrar p | a_i para algum i. □

Teorema 1.6 (Fundamental da Aritmética):
Todos os inteiros positivos maiores que 1 possuem uma decomposição única em fatores primos.

Demonstração: A demonstração será dividida em duas etapas. Inicialmente, provaremos que existe uma decomposição em fatores primos e, em seguida, provaremos que essa decomposição é única.
Provaremos a primeira parte utilizando o método de indução.

Para n = 2, é trivial pois o próprio número é primo, logo já se apresenta como uma decomposição em fator primo.

Supondo que o teorema seja válido para n, provaremos que a validade para n+1. Se n+1 é um número primo temos um caso idêntico ao n = 2, logo não há nada a demonstrar. Se n+1 não é primo, então, ele possui um divisor d, tal que n+1 = d.q, se d e q são primos o teorema está provado, caso não forem, pelo princípio da indução como n ≥ d e n ≥ q, eles podem ser escritos como fatores primos logo d = $p_1.p_2. \ldots .p_n$ e q = $q_1.q_2. \ldots .q_s$, então n+1 = d.q = $p_1.p_2. \ldots .p_n.q_1.q_2. \ldots .q_s$, com $p_1,p_2, \ldots .p_n,q_1,q_2,\ldots,q_s$ sendo primos. Portanto, pelo princípio de indução, fica demonstrado o teorema.
Na segunda parte, demonstra-se a unicidade do teorema, ou seja, que a decomposição é única. Vamos supor, por contradição, que a decomposição de n admita duas decomposições em números primos, n = $p_1.p_2. \ldots .p_n$, com $p_1 < p_2 < \ldots < p_n$ e n = $q_1.q_2. \ldots .q_s$, com $q_1 < q_2 < \ldots < q_s$. Então $p_1.p_2. \ldots .p_n = q_1.q_2. \ldots .q_s$. Logo p_1 divide $q_1.q_2. \ldots .q_s$ e pelo corolário 1.5, p_1 | q_j para algum j, $p_1 = q_j \geq q_1$. Analogamente q_1 divide $p_1.p_2. \ldots .p_n$, para algum i, $q_1 = p_i \geq p_1$. Portanto $p_1 = q_1$, pela minimalidade de

n. De $p_2.p_3. \ldots .p_n = q_2.q_3. \ldots .q_s$ e com o mesmo argumento, encontram-se as relações $p_2 = q_2$, $p_3 = q_3$, ..., $p_n = q_s$. Portanto, trata-se do mesmo produto de números primos, resultando em uma contradição. □

Definição 1.7: Função Totiente de Euler

A função totiente, representada por φ(x) é definida para um número natural x como sendo a quantidade de números menores ou igual a x co-primos com respeito a ele. Matematicamente a função é expressa por

$$\varphi(x) = \#\{n \in \mathbb{N} / n \leq x \wedge mdc(n, x) = 1\}.$$

Se $n = p1^{k1}. p2^{k2}. \ldots . pn^{kn}$, onde p_j são fatores primos distintos de n e k_j e sua respectiva multiplicidade, então pode-se determinar o valor de n como $n = (p1 - 1)^{k1-1}. (p2 - 1)^{k2-1}. \ldots . (pn - 1)^{kn-1}$. Em particular para a escolha de dois primos distintos p, q de multiplicidade 1 (um) que são fatores do número n, isto é, n = p.q, a função totiente é representada por φ(n) = (p - 1).(q – 1).

Definição 1.8: Seja n um número natural tal que n≥ 2. Dados a, b ∈ ℤ dizemos que a é congruente a b módulo n, denotado por $a \equiv b \pmod{n}$, se a – b é múltiplo de n. O número n é chamado de módulo da congruência.

Teorema 1.9: Seja n ≥ 2 um inteiro. A relação de congruência módulo n é uma relação de equivalência.

Demonstração: Para que a relação de congruência seja uma relação de equivalência deve-se mostrar que satisfaz as propriedades: reflexividade, simetria e transitividade.

Reflexividade: Seja a um inteiro. Tem-se que 0 é múltiplo de n, 0 = a – a, logo a – a é múltiplo de n. Portanto $a \equiv a \pmod{n}$.

Simetria: Sejam a e b inteiros tais que $a \equiv b \pmod{n}$, por definição segue que a – b é múltiplo de n, isto é, existe um número inteiro k, tal que a – b = n.k, multiplicando a equação por -1 implicando que (-1).(a – b) = -1.n.k. Por fim, (b – a) = n.(-k), como k ∈ ℤ, tem-se que (b – a) é múltiplo de n e portanto, $b \equiv a \pmod{n}$.

Transitividade: Sejam a, b e c inteiros tais que $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então por definição de congruência, segue que a – b e b – c são múltiplos de n, isto

é, existe $k_1, k_2 \in \mathbb{Z}$, tais que $a - b = n.k_1$ e $b - c = n.k_2$, somando as duas equações obtemos $a - c = n(k_1 + k_2)$, isto é, a – c também é múltiplo de n. Logo, pela definição de congruência $a \equiv c \pmod{n}$.

Teorema 1.10: Se $a \equiv a' \pmod{n}$ e se $b \equiv b' \pmod{n}$ então

(i) $a + b \equiv a' + b' \pmod{n}$

(ii) $a.b \equiv a'.b' \pmod{n}$.

Demonstração: (i) Usando a definição, podemos reescrever as congruências como

$a - a' = k.n$ e $b - b' = l.n$, com $k, l \in \mathbb{Z}$.

Somando as equações, segue que

$(a - a') + (b - b') = k.n + l.n$

$(a + b) - (a' + b') = (k + l).n$.

Como $k + l \in \mathbb{Z}$, temos, pela definição de congruência, que a igualdade corresponde a congruência

$a + b \equiv a' + b' \pmod{n}$.

(ii) Pela definição temos que

$a - a' = k.n$ e $b - b' = l.n$, com $k, l \in \mathbb{Z}$

$a = a' + k.n$ e $b = b' + l.n$.

Multiplicando -se as duas equações temos:

$a.b = (a' + k.n).(b' + l.n)$

$a.b = a'.b' + a'.l.n + b'.k.n + k.l.n^2$

$a.b = a'.b' + (a'.l + b'.k + k.l.n).n$

$a.b - a'.b' = (a'.l + b'.k + k.l.n).n$

Como $(a'.l + b'.k + k.l.n) \in \mathbb{Z}$, temos por definição de congruência que

$a.b \equiv a'.b' \pmod{n}$. □

Definição 1.11: Sejam $n \geq 2$ e $a \in \mathbb{Z}$. A classe de equivalência de a pela relação de congruência módulo n, denotada por $\bar{a}$, é definida como $\bar{a} = \{b \in \mathbb{Z} / a \equiv b \pmod{n}\}$.

Definição 1.12: Dado o conjunto $\mathbb{Z}$ dos números inteiros e a relação de congruência módulo n, que aqui denotaremos por $\equiv_n$, define-se o conjunto quociente de $\mathbb{Z}$ por $\equiv_n$, denotado por $\mathbb{Z}_n$, por:
$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1}\}$.

Definição 1.13: Seja $\bar{a} \in \mathbb{Z}_n$. Dizemos que $\bar{b}$ é o inverso multiplicativo de $\bar{a}$ em $\mathbb{Z}_n$ se $\bar{a}.\bar{b} = \bar{1}$ em $\mathbb{Z}_n$, isto é, se a.b ≡ 1 (mod n).

Teorema 1.14: Sejam a e n ≥ 2 números inteiros. As seguintes três afirmativas são equivalentes entre si:

1. $\bar{a}$ possui inverso multiplicativo em $\mathbb{Z}_n$;
2. mdc(a, n) = 1;
3. existe um inteiro positivo k tal que $a^k \equiv 1$ (mod n).

Demonstração: (1 ⇒ 2) Suponha que $\bar{a}$ possui um inverso multiplicativo em $\mathbb{Z}_n$. Então existe um $\bar{b} \in \mathbb{Z}_n$, tal que a.b ≡ 1 (mod n), logo a.b – 1 é múltiplo de n, isto é, existe k ∈ Z de modo que a.b = n.k (i). Suponha d = mdc (a,n) então d|a e d|n. Logo, existe k_1, $k_2 \in Z$ tal que a = d.k_1 e n = d.k_2. Substituindo esses valores em (i), segue que d.k_1.b – 1 = d.k_2.k. Rearranjando a equação temos que d.(k_1.b – k_2.k) = 1. Como k_1.b – k_2.k ∈ Z, implica que d|1, portanto d = 1.

(2 ⇒ 1) Seja mdc (a, n) = 1. Utilizando o Algoritmo Euclidiano Estendido, obtemos a igualdade k_1.a + k_2.n = 1, com k_1, $k_2 \in \mathbb{Z}$, manipulando a equação obtemos k_1.a – 1 = (-k_2).n, que por definição k_1.a ≡ 1 (mod n), portanto $\overline{k_1}$ é o inverso multiplicativo de $\bar{a}$ em $\mathbb{Z}_n$.

(1 ⇒ 3) Suponha que $\bar{a}$ possui um inverso multiplicativo em $\mathbb{Z}_n$. Considere a sequência de potências a, a², a³, ..., todas reduzidas módulo n. Suponha por contradição, que nenhuma delas é congruente a 1. Como a sequência de potências é infinita e o conjunto $\mathbb{Z}_n$ é finito, existem l, m ∈ $\mathbb{Z}$, onde l > m com $a^l \equiv a^m$ (mod n). Seja k o inverso multiplicativo de a. Multiplicando os dois lados da congruência por k^m, segue a^l. $k^m \equiv a^m$.k^m (mod n), obtendo $a^{l-m} \equiv 1$ (mod n), contradizendo a hipótese anterior. Portanto, existe um k = l – m tal que $a^k \equiv 1$ (mod n).

(3 ⇒ 1) Suponha que exista um inteiro positivo k tal que $a^k \equiv 1 \pmod{n}$. Então temos que $a.a^{k-1} \equiv 1 \pmod{n}$. Portanto, a^{k-1} é o inverso multiplicativo de a módulo n. □

Corolário 1.15: Sejam a, b números inteiros com b > a. Se a e b são co-primos então a é invertível módulo b.
Como mdc (a, b) = 1, ∃ k inteiro tal que $a^k \equiv 1 \pmod{b}$, onde $a^{k-1}.a \equiv 1 \pmod{b}$, sendo a^{k-1} o elemento inverso de a. □

Lema 1.16 (Euclides): Se x, y ≠ 0, mdc (x, y) = mdc (x, x + y).

Demonstração: Seja d um divisor comum de x e y. Então existem m, n ∈ ℤ, tais que, d.m = x e d.n = y. Somando as duas equações, segue que x + y = d.m + d.n = (m + n).d, então d|x +y. Portanto d é um divisor comum de x e x + y. Reciprocamente se f é um divisor comum de x e x + y então existem m, n ∈ ℤ, tais que x+y = f.m e x = f.n. Subtraindo as duas equações, segue que x + y – x = y = f.m – f.n = (m – n).f. Logo f é divisor comum de x e y. Como os conjuntos de divisores comuns dos dois pares dos números mencionados são os mesmos, o maior divisor comum também é o mesmo. □

Corolário 1.17: Mdc (n, n + 1) = 1.
Como mdc (n, 1) = 1 = mdc (n, n + 1). □

Teorema 1.18: Seja k um inteiro, então mdc (3, 6k – 2) = 1.

Demonstração: Suponha, por contradição, que exista um divisor d≠1, tal que, d | 3 e d | 6k – 2, como 3 é primo e d | 3 temos que d = 3 ou d = 1, mas por hipótese d = 3. Se d | 6k – 2, existe um inteiro m, tal que, 6k – 2 = 3d, implicando em 6k – 3d = 2. Mas 3(2k – d) = 2. Assim 3 | 2, levando a uma contradição. Portanto d = 1 = mdc (3, 6k – 2). □

Teorema 1.19: O inverso de 3 módulo 6k – 2, com k ∈ ℤ é 4.k -1.

Demonstração: Pelo teorema 1.18, o mdc (3, 6k – 2) = 1 e 3 admite inverso módulo 6k – 2. Seja n = 6.k – 2. Então

n = 6.k – 2

n – 1 = 6.k – 3

n – 1 = 3.(2.k – 1)

n = 3.(2.k – 1) + 1

Assim,

$3.(2.k – 1) + 1 \equiv 0 \pmod{n}$

$3.(2.k – 1) \equiv -1 \pmod{n}$

$3.(1 – 2.k) + 1 \equiv 1 \pmod{n}$

Logo 1 – 2.k é o inverso de 3 módulo n. Quando k > 0, o inverso é negativo. Utilizando o seu resíduo temos 1 – 2.k + n = 1 – 2.k + 6.k – 2 = 4.k – 1, sendo positivo para k > 0. Portanto o inverso de 3 módulo 6.k – 2 é 4.k – 1. □

Teorema 1.20 (Fermat): Se p é primo e a é um inteiro que não é divisível por p, então $a^{p-1} \equiv 1 \pmod{p}$.

Demonstração: Os possíveis resíduos de p são 1, 2, ..., p-1. Multiplicando cada resíduo por a temos a, 2.a, ..., (p – 1).a, denotando r_1 como resíduo de a, r_2 resíduo de 2.a, assim por diante até r_{p-1} resíduo de (p – 1).a. Então, temos

$r_1 \equiv a \pmod{p}$

$r_2 \equiv 2.a \pmod{p}$

⋮

$r_{p-1} \equiv (p – 1).a \pmod{p}$.

Multiplicando-se as congruências, segue que

$r_1.r_2. \ldots .r_{p-1} \equiv a.2.a. \ldots .(p – 1).a \pmod{p}$

$r_1.r_2. \ldots .r_{p-1} \equiv a^{p-1}.1.2. \ldots .(p – 1) \pmod{p}$. (i)

Mostraremos que os resíduos $r_1, r_2, \ldots, r_{p-1}$ não são iguais. Dados $k, l \in \{1, 2, \ldots, p – 1\}$, com $r_k = r_l$, por definição de resíduos, temos que

$a.r_k \equiv a.k \equiv a.l \equiv a.r_l \pmod{p}$

$a.k \equiv a.l \pmod{p}$

Como p não divide a, segue que mdc (a, p) =1. Pelo teorema 1.19, a é inversível módulo p, resultando em

$k \equiv l \pmod p$.

Como k e l são congruentes e $1 \leq k, l \leq p - 1$, concluímos que k = l, provando que os resíduos $r_1, r_2, ..., r_{p-1}$ não são iguais.

Logo $r_1.r_2. ... .r_{p-1} = 1.2. ... .(p - 1)$

Substituindo essa igualdade em (i), segue que

$r_1.r_2. ... .r_{p-1} \equiv a^{p-1}.1.2. ... .(p - 1) \pmod p$

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

Mas mdc (2, p) = 1, mdc (3, p) = 1, ..., mdc(p – 1, p) = 1, então 2, 3, ..., p – 1 são inversíveis módulo p, resultando em

$a^{p-1} \equiv 1 \pmod p$. □

Teorema 1.21 (Resto Chinês)

Sejam m e n inteiros positivos primos entre si. Se a e b são inteiros quaisquer, então o sistema

$x \equiv a \pmod m$

$x \equiv b \pmod n$

sempre tem solução e qualquer uma de suas soluções pode ser escrita da forma

$a + m.(m_o.(b - a) + n.t)$,

onde t é um inteiro qualquer e m_o é o inverso de m módulo n.

Definição 1.22: Um grupo é um par G = (G, ∗), onde G é um conjunto e ∗ é uma operação ∗: G x G → G, que satisfaz as seguintes propriedades:

1. Associatividade: para todo a, b, c ∈ G, (a ∗ b) ∗ c = a ∗ (b ∗ c);
2. Existência de elemento neutro: existe um elemento e ∈ G tal que, para todo a ∈ G, a ∗ e = e ∗ a = a;
3. Existência de inversos: para todo a ∈ G, existe um elemento a^{-1} ∈ G tal que $a ∗ a^{-1} = a^{-1} ∗ a = e$, onde e é o elemento neutro.

Definição 1.23: Um grupo G = (G, ∗) é chamado de grupo comutativo ou grupo abeliano se além das propriedades de grupo, ele satisfaz a

4. Comutatividade: para todo a, b ∈ G, a ∗ b = b ∗ a.

Definição 1.24: Definimos então o conjunto U(n), da seguinte forma: U(n) = {$\bar{a} \in \mathbb{Z}_n$ / mdc (a,n) = 1}, isto é, U(n) é o conjunto de todos os elementos de $\mathbb{Z}_n$ que possuem inverso multiplicativo.

Teorema 1.25: O par (U(n), .), onde "." representa o produto módulo n, é um grupo.

Demonstração: A prova da associatividade e da existência de inversos é imediata. Resta demonstrar apenas a existência de um elemento neutro. Para todo n ≥ 2, temos que mdc(1, n) = 1, logo, $\bar{1} \in U(n)$. Vamos mostrar se a, b ∈ U(n) então a.b ∈ U(n). Se a ∈ U(n) então existe $a^{-1} \in U(n)$ que é inverso de a. Analogamente, dado b ∈ U(n) então existe $b^{-1} \in U(n)$ que é inverso de b. Seja **u** o inverso de a.b, então

(a.b).u ≡ 1 (mod n)

a.(b.u) ≡ 1 (mod n)

a^{-1}. a.(b.u) ≡ a^{-1}.1 (mod n)

1.(b.u) ≡ a^{-1} (mod n)

b.u ≡ a^{-1} (mod n)

b^{-1}. (b.u) ≡ $b^{-1}.a^{-1}$ (mod n)

(b^{-1}.b).u ≡ $b^{-1}.a^{-1}$ (mod n)

1. u ≡ $b^{-1}.a^{-1}$ (mod n)

u ≡ $b^{-1}.a^{-1}$ (mod n),

logo $b^{-1}.a^{-1}$ é o inverso de a.b e portanto, ab ∈ U(n). □

Definição 1.26: A ordem de um grupo G = (G, ∗) é definida como sendo a cardinalidade do conjunto G.

Definição 1.27: Um grupo G = (G, ∗) é um grupo finito se a sua ordem é finita, isto é, se G é um conjunto finito.

Definição 1.28: Seja G = (G, ∗) um grupo finito e a ∈ G um de seus elementos. Definimos a ordem de a em G como menor inteiro positivo k tal que a^k = e em G.

Definição 1.29: Se G = (G, $*$) é um grupo, dizemos que H = (H, $*$) é um subgrupo de G se as seguintes propriedades são satisfeitas:

1. H $\subseteq$ G;
2. Para todo h, j $\in$ H, temos que h $*$ j $\in$ H;
3. e $\in$ H, onde e é o elemento neutro da operação;
4. Para todo h $\in$ H, existe um elemento $h^{-1} \in H$ tal que $h * h^{-1} = h^{-1} * h = e$.

Definição 1.30: Seja G = (G, $*$) um grupo finito e a $\in$ G um de seus elementos. Definimos a ordem de a em G como o menor inteiro positivo k tal que $a^k = e$, onde **e** é o elemento neutro.

Definição 1.31: Considere que (H, $*$) é um subgrupo cíclico de G gerado por a. Dizemos que a é uma raiz primitiva do grupo (H, $*$).

Definição 1.32: Um grupo diz-se cíclico se for gerado por um único elemento.

Lema 1.33 (Chave) Seja G = (G, $*$) um grupo finito e a $\in$ G. Temos que $a^t = e$ se e somente se t é divisível pela ordem de a em G.

Demonstração: ($\Leftarrow$) Seja k a ordem de a em G e suponha que t seja divisível por k. Logo t = k.t', para algum t' $\in Z$. Então

$a^t = a^{kt'} = (a^k)^{t'} = e^{t'} = e$.

($\Rightarrow$) Suponha que $a^t = e$. Vamos dividir t por k, obtendo t = kq + r, com $0 \leq r < k$. Temos então

$e = a^t = a^{kq+r} = (a^k)^q a^r = e^q a^r = a^r$.

Como k é a ordem de a, ele é o menor inteiro positivo tal que $a^k = e$. Por outro lado, pela igualdade acima, temos que $a^r = e$, com r < k. Desta forma, o único valor possível para r é r = 0, o que significa que t é divisível por k. □

Lema 1.34: Seja G = (G, $*$) um grupo abeliano finito. Sejam a, b $\in$ G tais que a ordem de a é **m** e a ordem de b é **n**, com mdc (m, n) = 1. Então, a ordem de ab é mn.

Demonstração: Como G é um grupo abeliano e temos que

$(a.b)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e^n e^m$ = e.

Logo pelo Lema Chave, a ordem de ab divide mn.

Suponha que exista k < mn, que seja a ordem de ab, segue que

e = $e^n = ((ab)^k)^n = a^{kn}b^{kn} = a^{kn}(b^n)^k = a^{kn}$e = a^{kn}.

Logo pelo Lema 1.33, a ordem de a, **m**, divide kn, mas mdc(m, n) = 1. Então m divide k.

Analogamente elevando a igualdade a m, n dividirá k.

Como m, n dividem k e mdc(m, n) = 1, então mn também divide k, concluindo k = mn. □

Lema 1.35: Sejam p primo e $f(x) = a_kx^k + a_{k-1}x^{k-1} + ... + a_1x + a_0$ um polinômio tal que os coeficientes a_i, $0 \leq i \leq k$, são inteiros, a variável x também assume valores inteiros e $a_k \not\equiv 0 \pmod p$. Então, a congruência $f(x) \equiv 0 \pmod p$ possui, no máximo k soluções distintas módulo p.

Demonstração: Provaremos por indução em k. Para k = 0 a congruência

$f(x) \equiv 0 \pmod p$

$a_0 \equiv 0 \pmod p$

Contradizendo a hipótese, logo $a_0 \equiv 0 \pmod p$ admite 0 soluções.

Vamos assumir a validade para k - 1 e demonstrar para k.

Se a congruência $f(x) \equiv 0 \pmod p$ possuir no máximo k - 1 soluções distintas módulo p, não há nada a provar. Suponha então que a congruência possui k soluções distintas módulo p, denotadas para $s_1, s_2, ..., s_k$. Demonstraremos que não existe outra solução módulo p, destas k soluções listadas para a congruência.

Seja

$g(x) = f(x) – a_k(x – s_1)(x – s_2)... (x – s_k)$

Note que o grau de g(x) é menor que que k, já que o termo a_kx^k de f(x) é cancelado pelo termo a_kx^k que aparece em $a_k(x – s_1)(x – s_2)... (x – s_k)$.

Pela hipótese de indução, se g(x) satisfaz as hipóteses do enunciado, a congruência $g(x) \equiv 0 \pmod p$ terá menos de k soluções distintas módulo p. Entretanto, temos que

$g(s_i) \equiv 0 \pmod p$ para todos os valores s_i, $1 \leq i \leq k$. Logo, a hipótese do enunciado de que o termo líder do polinômio não é congruente a zero módulo p, não pode ser satisfeita por g(x), implicando que g(x) é o polinômio identicamente nulo (módulo p). Assim, a partir da equação, temos

$f(x) \equiv a_k(x - s_1)(x - s_2)\ldots(x - s_k) \pmod p$.

Desta forma, $f(x) \equiv 0 \pmod p$ se, e somente se p divide o produto $a_k(x - s_1)(x - s_2)\ldots(x - s_k)$. Como p é primo e se p divide um produto, ele divide um dos termos deste produto.

Por hipótese, p não divide a_k, já que $a_k \not\equiv 0 \pmod p$. Desta forma, p divide $x - s_i$, para algum $1 \leq i \leq k$, o que significa que $x \equiv s_i \pmod p$.

Portanto, $f(x) \equiv 0 \pmod p$ se, e somente se $x \equiv s_i \pmod p$, para algum $1 \leq i \leq k$. Assim, todas as soluções da congruência $f(x) \equiv 0 \pmod p$ são congruentes a uma das k soluções listadas anteriormente. □

Teorema 1.36: Se p é primo, então U(p) é cíclico.

Demonstração: Como p é primo, $U(p) = \mathbb{Z}_p - \{\bar{0}\}$, de forma que a ordem de U(p) é p – 1. Vamos fatorar p – 1, obtendo

$$p - 1 = q_1^{e_1} q_2^{e_2} \ldots q_k^{e_k}$$

onde $1 < q_1 < q_2 < \ldots < q_k$ são primos distintos e $e_i \geq 1$ para todo $1 \leq i \leq k$.

Para cada potência $q_i^{e_i}$, $1 \leq i \leq k$, nesta fatoração, é possível encontrar um elemento de U(p) que tenha ordem $q_i^{e_i}$.

Para isso, buscamos um elemento $\bar{a}_i \in U(p)$ tal que

$$\bar{a}_i^{\frac{(p-1)}{q_i}} \not\equiv 1 (mod p).$$

Este elemento deve existir, já que os elementos $\bar{u} \in U(p)$ tais que

$$\bar{u}_i^{\frac{(p-1)}{q_i}} \equiv 1 (mod p),$$

são soluções da congruência

$$\bar{x}_i^{\frac{(p-1)}{q_i}} - 1 \equiv 0 (mod p),$$

que possui no máximo $\frac{(p-1)}{q_i} < p - 1$ soluções distintas módulo p, de acordo com o Lema 1.35.

Uma vez encontrado o valor a_i, calculamos

$h_i \equiv a^{\frac{(p-1)}{q_i^{e_i}}} (mod p)$.

Como

$h_i^{q_i^{e_i}} \equiv a_i^{(p-1)} (mod p)$,

então a ordem de $\bar{h}_i$ divide $q_i^{e_i}$, pelo Lema 1.33.

Suponha então que a ordem de $\bar{h}_i$ seja q_i^t, onde $t < e_i$. Temos então

$1 \equiv h_i^{q_i^t} \equiv (a^{\frac{(p-1)}{q_i^{e_i}}})^{q_i^t} \equiv a^{\frac{(p-1)}{q_i^{e_i - t}}} (mod p)$,

implicando que a ordem de $\bar{a}_i$ divide $\frac{(p-1)}{q_i^{e_i - t}}$ pelo Lema 1.33.

Mas como $e_i - t > 1$, $\frac{(p-1)}{q_i^{e_i - t}}$ divide $\frac{(p-1)}{q_i}$. Logo, a ordem de $\bar{a}_i$ divide $\frac{(p-1)}{q_i}$, o que implica que $a_i^{\frac{(p-1)}{q_i}} \equiv 1 \pmod p$, também pelo Lema 1.33.

Mas isto é uma contradição com a escolha de a_i. Desta forma a ordem de $\bar{h}_i$ é igual a $q_i^{e_i}$.

Realizado este cálculo para cada potência $q_i^{e_i}$ da fatoração, obtemos elementos

$\bar{h}_1, \bar{h}_2, ..., \bar{h}_k \in U(p)$,

tais que suas respectivas ordens são $q_1^{e_1}, q_2^{e_2}, \cdots, q_k^{e_k}$. Repare que, como estas ordens são potências de primos distintos e se **m** é a ordem de $\bar{h}_i$ e **n** a ordem de $\bar{h}_j$, com $i \neq j$, então mdc (m, n) = 1.

Temos que o elemento $\bar{g}$, onde

$g \equiv \prod_{1 \leq i \leq k} h_i \pmod p$

tem ordem

$\prod_{1 \leq i \leq k} q_i^{e_i} = p - 1$,

De acordo com o Lema 1.33, $\bar{g}$ é uma raiz primitiva de U(p), o que significa que U(p) é um grupo cíclico.

Problema do Logaritmo Discreto Genérico: Define-se o Problema do Logaritmo Discreto (PLD), da seguinte forma: dados um grupo finito cíclico G = (G, $*$) de ordem n, um gerador g de G e um elemento h ∈ G, determinar o valor de x no intervalo $0 \leq x < n$, tal que $g^x = h$ em G.

Problema do Logaritmo Discreto em U(p): No caso particular do grupo U(p), com p primo, o Problema do Logaritmo Discreto pode ser descrito da seguinte forma: dados um gerador g de U(p) e um elemento $h \in U(p)$, determinar o valor de x no intervalo $0 \leq x < p - 1$, tal que $g^x \equiv h \pmod{p}$.

2 - APLICAÇÕES DA MATEMÁTICA MODULAR EM NOSSO COTIDIANO

A aritmética modular cria a base de vários sistemas de identificação, mesmo não nos dando conta, ela faz parte da nossa vida, pois é utilizada em livros, cartões, produtos, mais especificamente, na criptografia atuando na codificação e decodificação de mensagens importantes. Neste capítulo abordaremos algumas das suas utilizações, de modo particular, em exemplos que serão adaptados em dinâmicas com aplicações no Ensino Básico e Médio.

2.1 - Cadastros de Pessoas Físicas (C.P.F.)

O C.P.F. é um documento que utiliza dígitos para identificar uma pessoa. Segundo Machado (2016), o uso de códigos numéricos se torna vantajoso, pois é universalmente entendido e possibilita registrar uma quantidade maior de informação do que um nome. Composto por onze dígitos onde os dois últimos são separados do restante por hífen (também chamados de dígitos de controle), têm por finalidade evitar fraudes ou erros de digitação e são calculados através dos noves primeiros dígitos. Tal método é calculado seguindo determinadas regras.

Sejam a n-úpla $(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9)$ os noves primeiros dígitos e (a_{10}, a_{11}) os dígitos de controle do C.P.F. multiplique a n-úpla respectivamente pelos números (1, 2, 3, 4, 5, 6, 7, 8, 9), depois some os noves produtos obtendo S_1, isto é, $S_1 = a_1.1 + a_2.2 + a_3.3 + a_4.4 + a_5.5 + a_6.6 + a_7.7 + a_8.8 + a_9.9$, a_{10} será o resto da divisão de S_1 por 11 (caso seja 10, adote $a_{10} = 0$). Calculando o último dígito, denotado por a_{11}, este dependerá dos noves dígitos anteriores, de maneira análoga, multiplique os termos $(a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10})$ respectivamente pelos números (1, 2, 3, 4, 5, 6, 7, 8, 9) e some todos produtos obtendo $S_2 = a_2.1 + a_3.2 + a_4.3 + a_5.4 + a_6.5 + a_7.6 + a_8.7 + a_9.8 + a_{10}.9$, a_{11} será o resto da divisão de S_2 por 11. Utilizando a aritmética modular podemos denotar os dígitos de controle como

$S_1 - a_{10} \equiv 0 \pmod{11}$

$S_2 - a_{11} \equiv 0 \pmod{11}$

Considerando o C.P.F. 134.806.752, calculemos os dígitos de controle.

$S_1 = 1.1 + 3.2 + 4.3 + 8.4 + 0.5 + 6.6 + 7.7 + 5.8 + 2.9$

$S_1 = 1 + 6 + 12 + 32 + 0 + 36 + 49 + 40 + 18$

$S_1 = 194.$

Utilizando a aritmética modular, segue que,

$194 - a_{10} \equiv 0 \pmod{11}$

$a_{10} \equiv 7 \pmod{11}$

$a_{10} = 7$

$S_2 = 3.1 + 4.2 + 8.3 + 0.4 + 6.5 + 7.6 + 5.7 + 2.8 + 7.9$

$S_2 = 3 + 8 + 24 + 0 + 30 + 42 + 35 + 16 + 63$

$S_2 = 221$

$221 - a_{11} \equiv 0 \pmod{11}$

$a_{11} \equiv 1 \pmod{11}$

$a_{11} = 1.$

2.2 - Cartão de Crédito

Os cartões de crédito possuem dezesseis dígitos onde o primeiro e o segundo dígitos têm a função de distinguir a função do cartão como uso para linhas aéreas, viagens, entretenimentos ou distinção entre bancos; do sétimo ao décimo quinto são os algarismos responsáveis pela identificação do cliente e por fim o último algarismo é calculado através dos anteriores, atuando de maneira análoga ao dígito de controle do C.P.F. .

Figura 2.1 – Ilustração do cartão de crédito

O método de cálculo é descrito da seguinte maneira:

Considere um cartão de crédito com dezesseis dígitos denotados por (a_1, a_2, ..., a_n, ..., a_{15}), onde $1 \leq n \leq 15$. Realiza-se duas somas, em que a primeira contém a

soma de todos os dígitos em posições ímpares multiplicados por 2, isto é, $S_1 = (a_1 + a_3 + ... + a_{15}).2$ e a segunda soma entre os elementos de posições pares, ou seja, $S_2 = a_2 + a_4 + ... + a_{14}$. Por fim realiza-se uma soma entre as duas somas anteriores e o último elemento, $S = S_1 + S_2 + a_{16}$, sendo que esta deve ser divisível por 10, em aritmética modular, isto é,

$S + a_{16} \equiv 0 \pmod{10}$.

Por exemplo, considerando um cartão de crédito com o número 4416 4321 8765 901X, calcula-se o último dígito da seguinte forma:

$S_1 = (4 + 1 + 4 + 2 + 8 + 6 + 9 + 1).2$

$S_1 = 35.2$

$S_1 = 70$

$S_2 = 4 + 6 + 3 + 1 + 7 + 5 + 0$

$S_2 = 26$

$S = S_1 + S_2 = 70 + 26 = 96$

$96 + a_{16} \equiv 0 \pmod{10}$

Portanto, o último dígito que validará o cartão será $a_{16} = 4$.

2.3 - Código de Barras

O código de barras é usado universalmente em diferentes áreas como comércio, indústrias, bibliotecas, bancos, etc. Foi criado por Joseph Woodland e Bernard Silver em 1952 e possuía doze dígitos recebendo o nome *Universal Product Code* (UPC).

Fonte: ESQUINCA, 2013

Figura 2.2 – Ilustração Código de Barras UPC

Posteriormente aprimorado por George J. Laurer, em meados da década de 1970, foi acrescido mais um dígito para identificar o país de origem e recebeu o nome *European Article Numbering system* (EAN-13), sendo adotado como o formato atual.

Fonte: ESQUINCA, 2013

Figura 2.3 – Ilustração Código de Barras EAN-13

"Em uma definição técnica, o código de barras é uma representação gráfica de dados que permite uma rápida captação de dados e proporciona velocidade nas transações, precisão nas informações e atualizações em tempo real. Tudo isso implica em maior controle, diminuição de erros, gerenciamento remoto, assegurando velocidade no atendimento de pedidos e clientes, além da significativa redução nos custos" (ESQUINCA, 2013).

Em um código de barras, os três primeiros dígitos representam o código do país, os próximos quatros algarismos referem-se ao código da empresa, os cinco números posteriores informam o código do produto e o último algarismo é o dígito verificador.

Fonte: ESQUINCA, 2013

Figura 2.4 – Significado dos números do código de barra

Para ler o código de barras, um leitor óptico afere a espessura e cor de uma sequência de quatro barras associando-as a uma sequência de sete dígitos binários. Existem três blocos de barras um pouco maior que não são lidos pelo aparelho óptico e possuem a finalidade de delimitar os campos do código de barras, podendo ser

denotados como lado esquerdo e lado direito. Cada dígito de 0 a 9 possui uma sequência referente aos sete dígitos binários. Especificamente o lado esquerdo possui duas representações diferentes dependendo da quantidade par ou ímpar de algarismos “uns”. Tal fato foi necessário para que um mesmo leitor óptico conseguisse realizar leituras nos sistemas UPC e EAN-13.

Tabela 2.1 – Sequência binária de dígitos no sistema EAN-13

Fonte: (ESQUINCA, 2013)

Dígito	Lado Esquerdo (Ímpar)	Lado Esquerdo (Par)	Lado Direito
0	0001101	0100111	1110010
1	0011001	0110011	1100110
2	0010011	0011011	1101100
3	0111101	0100001	1000010
4	0100011	0011101	1011100
5	0110001	0111001	1001110
6	0101111	0000101	1010000
7	0111011	0010001	1000100
8	0110111	0001001	1001000
9	0001011	0010111	1110100

Os números do lado esquerdo dependem da quantidade par ou ímpar de algarismos “uns” para serem identificados, e com essa classificação gera-se o primeiro algarismo do código de barras, seguindo a sequência.

Tabela 2.2 – Sequência geradora do primeiro dígito no sistema EAN-13

Fonte: (ESQUINCA, 2013)

Dígito Inicial	1º	2º	3º	4º	5º	6º
0	Ímpar	Ímpar	Ímpar	Ímpar	Ímpar	Ímpar
1	Ímpar	Ímpar	Par	Ímpar	Par	Par
2	Ímpar	Ímpar	Par	Par	Ímpar	Par
3	Ímpar	Ímpar	Par	Par	Par	Ímpar

4	Ímpar	Par	Ímpar	Ímpar	Par	Par
5	Ímpar	Par	Par	Ímpar	Ímpar	Par
6	Ímpar	Par	Par	Par	Ímpar	Ímpar
7	Ímpar	Par	Ímpar	Par	Ímpar	Par
8	Ímpar	Par	Ímpar	Par	Par	Ímpar
9	Ímpar	Par	Par	Ímpar	Par	Ímpar

Considerando o modelo EAN-13 e adotando a sequência dos treze dígitos e um vetor $\alpha = (a_1, a_2, ..., a_{12})$, para encontrar o valor do dígito verificador a_{13}, considera-se o vetor fixo $\omega = (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3)$ e o produto escalar $\alpha . \omega$, isto é, $\alpha . \omega = a_1.1 + a_2.3 + a_3.1 + a_4.3 + ... + a_{12}.3$. O dígito verificador será o valor da soma do produto escalar e a_{13} , além de ser múltiplo de 10. Da aritmética modular, temos:

$\alpha . \omega - a_{13} \equiv 0 \pmod{10}$.

Considerando por exemplo, um código de barras 600580965503X, calcularemos o seu dígito verificador. Considerando a sequência como vetor $\alpha = (6, 0, 0, 5, 8, 0, 9, 6, 5, 5, 0, 3)$ e o vetor fixo $\omega = (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3)$, segue que o produto escalar

$\alpha . \omega = 6.1 + 0.3 + 0.1 + 5.3 + 8.1 + 0.3 + 9.1 + 6.3 + 5.1 + 5.3 + 0.1 + 3.3$

$\alpha . \omega = 6 + 0 + 0 + 15 + 8 + 0 + 9 + 18 + 5 + 15 + 0 + 9$

$\alpha . \omega = 75$.

Por fim, utilizando a aritmética modular calculamos o a_{13}:

$\alpha . \omega - a_{13} \equiv 0 \pmod{10}$

$75 - a_{13} \equiv 0 \pmod{10}$

$75 - a_{13} = 10.q$, com $q \in \mathbb{Z}$

Logo $a_{13} = 5$

Portanto o dígito verificador é $a_{13} = 5$.

2.4 – Calendários

Durante o desenvolvimento de diferentes povos, foram criados calendários baseados em suas culturas, ritos e atividades.

"Estima-se que haja atualmente cerca de quarenta calendários em uso pelo mundo. Os mais conhecidos são: o gregoriano, o hebraico, o islâmico, o indiano, o chinês, o persa, o bahaí, o etíope e o recente calendário ISO. Também há alguns calendários antigos bastante conhecidos, porém não mais usados, como o juliano, o revolucionário francês, o maia, e o antigo calendário hindu" (RODRIGUES, 2012).

O calendário atualmente mais utilizado é o calendário gregoriano criado na Europa em 1582, por incentivo do papa Gregório XIII, para substituir o calendário juliano. Uma curiosidade ligada a ele seria prever em qual dia da semana, cairão determinadas datas tais como aniversário, natal, ano novo. De uma forma geral, um ano no calendário gregoriano possui 365 dias e como uma semana possui 7 dias, utilizando a aritmética modular, basta calcular o resto:

$365 \equiv 1 \pmod 7$.

Logo em um ano comum, a data atual será transferida para o dia posterior da semana, no próximo ano. No caso do ano bissexto, de acordo com o raciocínio anterior, calcula-se o resíduo, sendo neste caso $366 \equiv 2 \pmod 7$.

Poderíamos deduzir que em um ano bissexto, uma determinada data avançaria dois dias na semana. Embora tal pensamento pareça coerente, está incorreto pois, o dia adicional é acrescido no final do mês de fevereiro, posterior ao dia 28. O problema fica mais complexo quando pretende-se encontrar o dia de determinada data situada em um intervalo maior de anos. Pensando neste problema, o reverendo alemão Julius Christian Johannes Zeller desenvolveu um algoritmo, denominado Zeller, em que é possível calcular o dia da semana referente a uma data passada ou futura.

$$S(d, m, A) = d + 1 + \left[\frac{13m-1}{5}\right] + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \pmod 7.$$

Denotado por $\left[\frac{a}{b}\right]$, com a, b $\in \mathbb{N}$, como o quociente de a por b, com b $\neq$ 0, define-se o maior inteiro menor do que ou igual ao número racional $\frac{a}{b}$. O algoritmo é uma função com três variáveis, sendo:

d = dia do mês;

m = mês.

Como os meses tem nomes, para tal algoritmo associa-se números aos meses da seguinte forma: março = 1, abril = 2, ..., janeiro = 11 e fevereiro = 12.

A = ano

S(d, m, A) = dia da semana.

De maneira análoga ao mês, os dias da semana também serão denotados por números, isto é, domingo = 1, segunda = 2, ..., sexta = 6 e sábado = 7. Utilizando o algoritmo com a data 16 de julho de 1957, obtemos os valores d = 16, m = 5 e A = 1957. Aplicando no algoritmo, temos:

$$S(16, 5, 1957) = 16 + 1 + \left[\frac{13.5-1}{5}\right] + 1957 + \left[\frac{1957}{4}\right] - \left[\frac{1957}{100}\right] + \left[\frac{1957}{400}\right] \pmod 7$$

$$S(16, 5, 1957) = 16 + 1 + \left[\frac{64}{5}\right] + 1957 + \left[\frac{1957}{4}\right] - \left[\frac{1957}{100}\right] + \left[\frac{1957}{400}\right] \pmod 7$$

$$S(16, 5, 1957) = 16 + 1 + [12{,}8] + 1957 + [489{,}25] - [19{,}57] + [4{,}8925] \pmod 7$$

S(16, 5, 1957) = 16 + 1 + 12 + 1957 + 489 – 19 + 4 (mod 7)

S(16, 5, 1957) = 2460 (mod 7).

Utilizando a aritmética modular segue que

$2460 \equiv 3 \pmod 7$.

Logo, S(16, 5, 1957) = 3 e portanto o dia da semana que ocorreu a dará 16 de julho de 1957 foi uma terça-feira.

2.5 – Criptografia

A origem da criptografia (do grego *kryptós* = escondido e *gráphien* = escrita) vem dentre outras utilidades, da insegurança que havia no tráfego de mensagens entre o remetente e destinatário. Por exemplo, em um conflito militar, a execução de uma estratégia deve ser informada a um pelotão distante de seu general. Portanto a informação deve ser transmitida de forma segura ao responsável que executará tal estratégia. Como existe o risco da mensagem ser interceptada, este canal precisa da segurança para as transmissões de tais mensagens. Quando isto ocorre, métodos criptográficos se fazem necessários.

O código pode ser uma regra simples ou envolver o uso de ferramentas acessíveis.

“Os serviços básicos de segurança que um sistema criptográfico deve fornecer são, Confidencialidade, Integridade, Autenticação e Não Repudiação. A Confidencialidade consiste em manter a informação secreta para todos os que não estão autorizados ao contato com essa informação. Integridade garante que a

informação não foi alterada por entidades desconhecidas ou não autorizadas. Autenticação garante a identidade de uma entidade envolvida na comunicação. Por último, a Não Repudiação previne a negação de ações e compromissos previamente realizados.” (SILVEIRA, 2013)

Basicamente, a criptografia compreende práticas e técnicas para obter uma comunicação segura, isto é, um conjunto de técnicas pensadas para a proteção das informações de maneira que, apenas o emissor e receptor compreendam, dificultando a interceptação e entendimento por terceiros.

No período pós-guerra as empresas começaram a utilizar técnicas de criptografia com a finalidade de proteger seus dados, promovendo um grande desenvolvimento da criptografia além de fins militares. Com o advento da internet e a grande quantidade de dados que trafegam diariamente, se mostrou uma ferramenta essencial. Todos os métodos de criptografia desenvolvidos e utilizados desde a antiguidade até a década de 1970, pertenciam à categoria de métodos de *chave privada* ou de *chave simétrica*, pois a mesma chave é usada para criptografar e decodificar a mensagem. Esse sistema tem como característica que o emissor e receptor possuem uma única chave para manter conversas privadas. As características desse tipo de criptografia não favorecem algumas aplicações tais como operações realizadas na internet, pois, a criptografia exige uma chave diferente a cada par de indivíduos. Portanto as chaves devem ser distribuídas aos pares (emissor e receptor), e tal necessidade a torna vulnerável. Já no modelo de criptografia de chave pública, a chave usada pode ser de conhecimento público e apenas utilizada para decodificá-la e mantida de forma privada pelo destinatário da mensagem. Portanto, todos podem utilizar tal meio para encriptar uma mensagem, mas somente o destinatário legítimo possuirá a chave. Com a internet, o método da chave pública possibilitou o surgimento de um conceito complementar denominado *assinatura digital*, que tem como finalidade a garantia da autenticidade, isto é, confirmar que uma mensagem foi realmente criada pelo emissor. Assim, a chave da assinatura é mantida pelo remetente, enquanto a chave utilizada na verificação da autenticidade pode ser de conhecimento público, ou seja, apenas o emissor será capaz de gerar a assinatura digital e qualquer um poderá verificar se a assinatura foi produzida pelo suposto remetente.

A seguir, estudaremos os dois métodos criptográficos de chave pública mais conhecidos: modelos RSA e El Gamal, descrevendo cada um e comprovando matematicamente sua validade utilizando a aritmética modular.

2.5.1 – Modelo RSA

Descrito em (COUTINHO, 2015) como "o mais conhecido dos métodos de criptografia de chave pública", o RSA, cuja a sigla corresponde às iniciais dos inventores do código foi inventado em 1977 por R. L. **R**ivest; A. **S**hamir e L. **A**dleman, (M.I.T.), tem sua base na Teoria dos Números e suas chaves são geradas da seguinte forma:

1. Escolha dois números primos (na ordem de 10^{100}) p e q de forma aleatória;
2. Calcule o produto dos números primos, n = p.q;
3. Calcule a função de tontiente de Euler em n: ϕ(n) = (p - 1).(q – 1);
4. Escolha um inteiro e tal que 1 < e < ϕ(n), de forma que e e ϕ(n) sejam primos entre si;
5. Calcule d.e ≡ 1 mod ϕ(n), ou seja, d seja o inverso multiplicativo de e em mod ϕ(n).

Logo a chave pública é o par (n, e) e a chave privada é a tripla (p, q, d).

Para cifrar uma mensagem **m**, onde 1 < **m** < n – 1, numa outra **c** cifrada usando uma chave pública do destinatário **n** e **e,** basta realizar a operação $m^e \equiv$ c mod n. A mensagem pode ser transmitida para o receptor e para recuperar **m** da mensagem cifrada **c,** usando a respectiva chave privada do receptor **n** e **d**, basta resolver a equação modular: $c^d \equiv$ m mod n.

Definição 2.1: Chamamos de bloco b um trecho de uma sequência numérica em que seu primeiro algarismo deve ser diferente de zero e b < n, onde n = p.q, com p e q primos.

Definição 2.2: Dado um bloco b, chamamos de codificação de b, denotado por C(b), a seguinte expressão C(b) ≡ b^3 (mod n).

Definição 2.3: Dado um bloco codificado C(b), denomina-se de decodificação de C(b), a seguinte expressão

$$D(C(b)) \equiv (C(b))^d \pmod{n},$$

onde d é o inverso multiplicativo de um número inteiro $1 < e < \phi(n)$ em mod $\phi(n)$, isto é, $d.e \equiv 1 \bmod \phi(n)$.

2.5.1.2 - Demonstração do sistema RSA

Como dito anteriormente, um sistema RSA codifica com uma chave pública n, tal que n = p.q com p e q primos e decodifica com os parâmetros privados (p, q, d), onde, (p - 1).(q – 1) = 6.k – 2 e d = 4.k – 1. A congruência seguinte é suficiente para mostrar a validade do sistema RSA, pois, como b está no intervalo entre 1 e n – 1, uma vez que são congruentes módulo n, só podem ser iguais.

$D(C(b)) \equiv b \pmod{n}$.

Pela definição de **D** e **C,** segue que:

$C(b) \equiv b^3 \pmod{n}$

$D(a) \equiv a^d \pmod{n}$.

Substituindo temos que

$D(C(b)) \equiv D(b^3) \equiv b^{3d} \equiv b \pmod{n}$.

Por definição, $3d \equiv 1 \pmod{(p-1).(q-1)}$, onde $3d = 1 + k(p-1)(q-1)$ com $k \in \mathbb{Z}$, estamos calculando os resíduos de b^{3d} módulo p e módulo q, usando o teorema do resto chinês para calcular o resíduo módulo n. Como n = p.q, com p e q primos, calcularemos o resíduo de b^{3d} para p (para q o procedimento é análogo).

Se p não divide b, aplica-se o teorema de Fermat obtendo:

$b^{3d} \equiv b.(b^{p-1})^{k.(q-1)} \pmod{p}$.

Como p não divide b, temos que $b^{p-1} \equiv 1 \pmod{p}$. Substituindo na congruência acima, obtemos:

$b^{3d} \equiv b.(b^{p-1})^{k.(q-1)} \equiv b \pmod{p}$.

Se p divide b, logo $b^{3d} \equiv b \pmod{p}$.

Sendo análogo para q, obtemos o par de congruências

$b^{3d} \equiv b \pmod{p}$.

$b^{3d} \equiv b \pmod{q}$.

Logo b é uma solução de

$x \equiv b \pmod{p}$

$x \equiv b \pmod{q}$.

Pelo teorema do resto chinês, este sistema tem solução geral igual a b + p.q.t com $t \in Z$. Logo b^{3d} também é solução do mesmo sistema $b^{3d} = b + p.q.k$, para algum inteiro k. Mas isto é equivalente a $b^{3d} \equiv b \pmod{p.q = n}$, provando a congruência. □

2.5.1.3 – Exemplo

Para codificar uma mensagem no RSA, basta calcular sua potência módulo n, a um expoente arbitrário. Como a maioria das mensagens é um texto, é necessário converter a mensagem em uma sequência de números. Nesta etapa chamada de pré-codificação, pode-se usar uma variação da Cifra de César com a finalidade de transformar um texto em número. Para exemplificar, utiliza-se a tabela de conversão abaixo:

Tabela 2.3 – Código de decodificação adaptado para cifra de César

Fonte: O autor

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Logo a palavra MATEMÁTICA seria representada pelo código 2210291422102918 10.

Por fim, a última parte do processo de pré-codificação consiste em segmentar a sequência em blocos menores que n. Arbitrariamente, escolhe-se p e q, números com ordens muito menores que 10^{100} e com o objetivo de desenvolver os cálculos do

método RSA sem o auxílio de computadores, escolhe-se p = 17 e q = 23. Assim, n = p.q = 17.23 = 391, podendo o código ser dividido em 22-102-91-42-210-291-8-10.

Note que a maneira de dividir os blocos não é única, embora recomenda-se não começar um bloco com o algarismo 0 pois, pelo método RSA, não é possível distinguir no processo de decodificação, os blocos 029 e 29.

Na etapa seguinte denominada codificação, necessita-se do valor da chave pública n, obtida pelo produto de dois primos. Dizemos que n é a chave de codificação do sistema RSA e neste processo codificaremos cada bloco (obtido na pré-codificação) separadamente. Portanto a mensagem codificada será a sequência dos blocos codificados. Dada a chave de codificação **n** e um bloco **b**, calcularemos **C(b)** de todos os blocos abordados neste exemplo, segue que n = 391 e devemos encontrar os valores de C(22), C(102), C(91), C(42), C(210), C(291), C(8) e C(10). Para C(22) temos:

$22^3 \equiv 22^2 \times 22 \equiv 484 \times 22 \equiv 93 \times 22 \equiv 2046 \equiv 91 \pmod{391}$.

Logo C(22) = 91, analogamente para os demais blocos obtemos os valores C(102) = 34; C(91) = 70; C(42) = 200; C(210) = 165; C(291) = 178; C(8) = 64 e C(10) = 218.

Unindo os blocos, obtém-se a mensagem codificada:

91 – 34 – 70 – 200 – 165 – 178 – 68 – 218.

Seguimos para o processo de decodificação, isto é, decodificar cada bloco da mensagem. Para decodificar uma mensagem é necessária conhecer os dois números primos que compõe n (p e q) e o inverso d > 0 de 3 módulo (p -1).(q – 1). Pela definição de inverso, isto significa que se deve ter $3d \equiv 1 \pmod{(p-1).(q-1)}$. Logo a tripla (p, q, d) é chave privada de decodificação.

O próximo passo é realizar a decodificação de todos os blocos codificados. Portanto, calcule D(C(b)), mas é necessário encontrar o valor de d. Utilizando os dados do exemplo anterior, calculando $\phi(n) = (p-1).(q-1) = (17-1).(23-1) = 16 \times 22 = 352$ e tomando e = 3, temos que mdc(3,352) = 1. Logo eles são primos e pelo corolário, admite-se a existência de d. Então, temos $p \equiv 5 \pmod 6$ e $q \equiv 5 \pmod 6$, logo, $(p-1).(q-1) \equiv 4 \times 4 \equiv 16 \equiv 4 \equiv -2 \pmod 6$ onde, $(p-1).(q-1) = 6 \times k - 2$, para algum inteiro positivo k. Pelo teorema, o inverso de 3 módulo 6k – 2 é $4 \times k - 1$. Logo, podemos considerar $d = 4 \times k - 1$. Substituindo no exemplo acima, chega-se a p = 17 e q = 23, logo, $(p-1).(q-1) = 16 \times 22 = 352 = 6 \times 58 + 4 = 6 \times 59 - 2$, então para k = 59

temos d = 4.59 – 1 = 235. Portanto basta decodificar cada bloco, isto é, encontrar os valores de D(91), D(34), D(70), D(200), D(165), D(178), D(68) e D(218). D(91) é igual ao resto da divisão de 91^{235} por n = 391. Para determinar tal valor, necessita-se do algoritmo do resto chinês e o Teorema de Fermat. Calculando D(91), isto é, 91^{235} módulo 17 e módulo 23.

$91 \equiv 6 \pmod{17}$

$91 \equiv 22 \equiv -1 \pmod{23}$.

Assim, aplicando teorema de Fermat as congruências, segue que

$6^{235} \equiv (6^{16})^{14}.6^{11} \equiv 6^{11} \pmod{17}$

$(-1)^{235} \equiv ((-1)^{22})^{10}.(-1)^{15} \equiv (-1)^{15} \pmod{23}$;

logo,

$91^{235} \equiv 6^{235} \equiv 6^{11} \equiv 2^{11}.3^{11} \equiv 8.7 \equiv 56 \equiv 5 \pmod{17}$

$91^{235} \equiv (-1)^{235} \equiv (-1)^{15} \equiv -1 \equiv 22 \pmod{23}$

Portanto,

$91^{235} \equiv 5 \pmod{17}$

$91^{235} \equiv 22 \pmod{23}$

Isto corresponde ao sistema

$x \equiv 5 \pmod{17}$

$x \equiv 22 \pmod{23}$.

Utilizando o algoritmo chinês do resto, obtemos:

$x = 22 + 23y$.

Substituindo o valor na congruência, resulta

$22 + 23y \equiv 5 \pmod{17}$

$6y \equiv 0 \pmod{17}$

$6y.3 \equiv 0.3 \pmod{17}$

$18y \equiv 0 \pmod{17}$

$y \equiv 0 \pmod{17}$.

Substituindo, temos x = 22 + 23.0 = 22, portanto o valor de D(91) = 22. Analogamente encontramos D(34) = 102, D(70) = 91, D(200) = 42, D(165) = 210, D(178) = 291, D(68) = 8 e D(218) = 10. Evidentemente os valores correspondem as suas respectivas codificações.

2.5.1.4 – Segurança

Como já citado anteriormente, a criptografia consiste em codificar mensagens enviadas por um meio não seguro, utilizando a criptografia RSA. Se alguém consegue interceptar uma mensagem criptografada, não conseguirá ler tal mensagem apenas com a chave pública n. Conhecendo n, teoricamente seria fácil realizar o processo de decodificação (fatorando **n** em dois primos **p** e **q** afim de calcular **d** e aplicar a decodificação, descrita anteriormente). Apesar da evolução tecnológica, o processo de decodificação se torna inviável, devido ao grande processamento envolvido, corroborando com a segurança do processo.

No sistema RSA foram implementadas chaves públicas que variam de 200 a 2467 algarismos. A empresa que detêm os direitos deste sistema criptográfico lançava desafios que consistiam em realizar a decodificação, tendo como acesso apenas a chave pública. Umas das últimas chaves fatorada, possuía 193 primos na fatoração, foi finalizada em novembro de 2005 por F. Bahr, M. Boehm, J. Franke e T. Kleinjung, em que foram utilizados 80 computadores, demorando 5 meses para realizar o processo.

2.5.2 – Modelo El Gamal

Desenvolvida pelo egípcio Taher El Gamal (1985) este método é outra chave pública bastante empregada.

"O método El Gamal de criptografia é baseado em grupos abelianos finitos cíclicos. Originalmente, foi desenvolvido a partir da utilização dos grupos finitos U(p), onde **p** é primo, já que o Teorema da Raiz Primitiva garante que tais grupos são necessariamente cíclicos. No entanto, o método pode ser generalizado para utilizar quaisquer outros grupos abelianos finitos cíclicos"(SCHECHTER, 2014).

Para a chave, seleciona-se aleatoriamente um número inteiro **x** no intervalo (1,p-1) e por fim, calcula-se a chave pública de encriptação a $\equiv r^x \pmod p$, onde **r** é a raiz primitiva de U(p).

Os valores r, p e a são valores públicos e o valor x é o segredo da chave. Para codificar a mensagem, o remetente converte a mensagem em uma sequência de

dígitos, utilizando um procedimento de substituição semelhante ao descrito no tópico 2.5.1.3, exemplificado através da tabela 2.3, formando um bloco K, se K ≥ p. A mensagem deve ser dividida em blocos menores M, tal que M ≤ p – 1. Cada sub-bloco será encriptado separadamente, escolhendo-se um número natural 2 ≤ y ≤ p – 2 aleatoriamente. Calcula-se $r^y \equiv b \pmod p$ e o código será obtido por meio de $C \equiv M.\ a^y \pmod p$, resultando na dupla cifrada (b, C).

O procedimento para decifrar a mensagem, utilizará a chave privada x, para realizar os cálculos $P \equiv C.\ b^{p-1-x} \pmod p$.

2.5.2.2 - Demonstração do método El Gamal

A mensagem cifrada é o par (b, C), onde $C \equiv M.\ a^y \pmod p$ e $b \equiv r^y \pmod p$, então

$P \equiv C.\ b^{p-1-x} \pmod p$.

$P \equiv (M.a^y)(r^y)^{p-1-x} \pmod p$.

Mas, $a \equiv r^x \pmod p$, logo

$P \equiv M\ .\ (r^x)^y (r^{y(p-1)-xy}) \pmod p$.

$P \equiv M\ .\ (r^{p-1})^y \pmod p$.

Como r é raiz primitiva de p, então $r^{p-1} \equiv 1 \pmod p$, portanto

$P \equiv M \pmod p$ □.

2.5.2.3 – Exemplo

Escolhendo um número primo p = 29, uma raiz primitiva r = U(29) = 3 e a chave privada x = 8, calcula-se a chave pública $a \equiv 3^8 \pmod{29}$ e portanto $a \equiv 7 \pmod{29}$. Portanto, pelo método El Gamal, tem como chave pública a terna (29, 3, 7) e a chave secreta x = 8. Semelhante ao exemplo usando o sistema RSA, utiliza-se a tabela 2.3 e a substituição da palavra SOMA, obtendo a sequência 28242210, adotando blocos menores que o primo escolhido, resultando na sequência 28-24-22-10, sendo M_1 = 28, M_2 = 24, M_3 = 22 e M_4 = 10. Encriptando cada bloco adotando y = 5, obtém-se para C_i , i=1,...,4:

$C_1 \equiv M_1.\ a^y \pmod p$ $C_1 \equiv 28\ .\ 7^5 \pmod{29}$ $C_1 \equiv 470596 \pmod{29}$ $C_1 \equiv 13 \pmod{29}$

$C_2 \equiv M_2 . a^y$ (mod p) $C_2 \equiv 24.7^5$ (mod 29) $C_2 \equiv 403368$ (mod 29) $C_2 \equiv 7$ (mod 29)

$C_3 \equiv M_3 . a^y$ (mod p) $C_3 \equiv 22 . 7^5$ (mod 29) $C_3 \equiv 369754$ (mod 29) $C_3 \equiv 4$ (mod 29)

$C_4 \equiv M_4$.(mod p) $C_4 \equiv 10 . 7^5$ (mod 29) $C_4 \equiv 168070$ (mod 29) $C_4 \equiv 15$ (mod 29)

Portanto a mensagem criptografada será13-7-4-15, com $C_1 = 13$, $C_2 = 7$, $C_3 = 4$ e $C_4 = 10$.

Para decodificá-la, utilizaremos a chave privada x = 8. Calculemos b tal que $b \equiv 3^5$ (mod 29) b ≡ 11 (mod 29). Os P_i, i=1,...,4, resultantes serão:

$P_1 \equiv C_1 . b^{p-1-x}$ (mod p) $P_1 \equiv 13 . 11^{29-1-8}$ (mod 29) $P_1 \equiv 28$ (mod 29)

$P_2 \equiv C_2 . b^{p-1-x}$ (mod p) $P_2 \equiv 7 . 11^{29-1-8}$ (mod 29) $P_2 \equiv 24$ (mod 29)

$P_3 \equiv C_3 . b^{p-1-x}$ (mod p) $P_3 \equiv 4 . 11^{29-1-8}$ (mod 29) $P_3 \equiv 22$ (mod 29)

$P_4 \equiv C_1 . b^{p-1-x}$ (mod p) $P_4 \equiv 15 . 11^{29-1-8}$ (mod 29) $P_4 \equiv 10$ (mod 29).

2.5.1.4 – Segurança

Uma terceira pessoa que não conhece a chave secreta terá conhecimento das chaves públicas p, r, a, b e C. Para decodificar, é necessário calcular as duas congruências $a \equiv r^x$ (mod p) e $b \equiv r^y$ (mod p); o que significa resolver um problema do logaritmo discreto (definição 1.38), levando em conta que x e y são arbitrários e menores que p (primo muito grande). Como mencionado anteriormente, a resolução demanda muito tempo, o suficiente para torná-la inviável, resultando em um método seguro.

3 - APLICAÇÕES EM PLANOS DE AULA PARA O ENSINO BÁSICO

Apesar do currículo paulista não apresentar tópico sobre criptografia, consta no PCN que "a aquisição do conhecimento matemático deve estar vinculada ao domínio de um saber fazer matemática e de um saber pensar matemático" (MEC, 1998, p. 41). Portanto podemos introduzi-los dentro de conteúdos já existentes no currículo.

Utilizando a teoria apresentada, apresentaremos algumas aplicações através de trabalhos em grupo e discussões. Foram propostos cinco planos de aula para o ensino fundamental e médio.

3.1 – Cálculo dos dígitos verificadores do C.P.F.

3.1.1 – Plano de Aula

Público alvo: 2ª série do Ensino Médio
Tema: Matrizes
Objetivos: Desenvolver as habilidades em:

- Reconhecimento da condição de existência para a multiplicação entre matrizes.
- Operar multiplicação entre matrizes.
- Operar algoritmo da divisão de Euclides.

Conteúdo abordado: Multiplicação entre Matrizes.
Duração: 90 minutos (2 aulas).
Metodologia: (Aula 1) - Iniciamos a atividade realizando uma abordagem sobre os temas anteriores como caracterização de uma matriz, adição e subtração entre matrizes e multiplicação por um escalar, levantando as dúvidas em uma discussão com a sala e estruturando um resumo na lousa.

Após a recapitulação, a sala se reuniu em grupos de 5 ou 6 pessoas e foi proposto um problema inicial.

Atividade 1 - (VUNESP – 2009) Uma rede de comunicação tem cinco antenas que transmitem uma para outra, conforme mostrados na matriz A = (a_{ij}), onde a_{ij} = 1

significa que a antena i transmite diretamente para a antena j, e $a_{ij} = 0$ significa que a antena i não transmite para a antena j.

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Qual o significado do elemento b_{41} da matriz $B = A^2$?

(A) Como $b_{41} = 0$, isso significa que a antena 4 não transmite para a antena1.

(B) Como $b_{41} = 1$, isso significa que a antena 4 transmite para a antena 1.

(C) Como $b_{41} = 3$, isso significa que a antena 4 transmite para a antena 1.

(D) Como $b_{41} = 3$, isso significa que existem 3 maneiras diferentes de a antena 4 transmitir para a antena 1, usando apenas uma retransmissão entre elas.

(E) Como $b_{41} = 3$, isso nada significa, pois b_{ij} só pode valer 0 ou 1, conforme definido no enunciado da questão.

Nesta atividade, o professor fez questões norteadoras para os grupos explorarem o conceito de multiplicação entre matrizes, condição de existência, ordem da matriz resultante e o algoritmo.

(Aula – 2) Inicia-se essa aula expondo a importância do uso do C.P.F., sua composição e finalidade dos dígitos verificadores e a explicação do cálculo do esquema exibido no capítulo 2.1, adaptando a sequência de dígitos do C.P.F. como uma matriz linha e os números que seriam multiplicados para uma matriz coluna, obtendo uma matriz linha com elementos que variam com diferentes dígitos dos C.P.F. e uma matriz coluna fixa, responsável por calcular os dígitos verificadores. Foram propostas as seguintes atividades:

Atividade 2 - Calcule os dígitos verificadores do C.P.F. 123.456.789-XY.

Atividade 3 - (ENEM 2009) Para cada indivíduo, a inscrição no Cadastro de Pessoas Físicas (C.P.F.) é composto por um número de 9 algarismos mais outros 2, na forma d_1 d_2, denominados dígitos verificadores, calculados da seguinte forma:

- ✓ os 9 primeiros algarismos são multiplicados pela sequência 10, 9, 8, 7, 6, 5, 4, 3, 2 (o primeiro por 10, o segundo por 9, e assim sucessivamente);
- ✓ em seguida, calcula-se o resto r da divisão da soma dos resultados da multiplicação por 11, e se esse resto r for 0 ou 1, d_1 é zero, caso contrário $d_1 = (11 – r)$;
- ✓ O dígito d_2 é calculado pela mesma regra, na qual os números a serem multiplicados pela sequência são contados a partir do segundo algarismo, sendo d_1 o último algarismo, isto é, d_2 é zero se o resto **s** da divisão por 11 das somas das multiplicações for 0 ou 1, caso contrário, $d_2 = (11 – s)$.

Suponha que João tenha perdido seus documentos, inclusive o C.P.F. e, ao registrar a perda na delegacia, não conseguisse lembrar dos dígitos verificadores, recordando-se apenas dos nove primeiros algarismos, ou seja, 123.456.789. Neste caso, os dígitos verificadores d_1 e d_2 são respectivamente,
(A) 0 e 9. (B) 1 e 4. (C) 1 e 7. (D) 9 e 1. (E) 0 e 1.

Como este problema já foi resolvido e portanto, o resultado é conhecido, adotaremos um procedimento diferente. A partir deste fato, algumas questões são pertinentes:

● Podemos adaptar esse esquema em matrizes?
● Por que o processo de cálculo de dígito é diferente?
● Qual você preferiu?

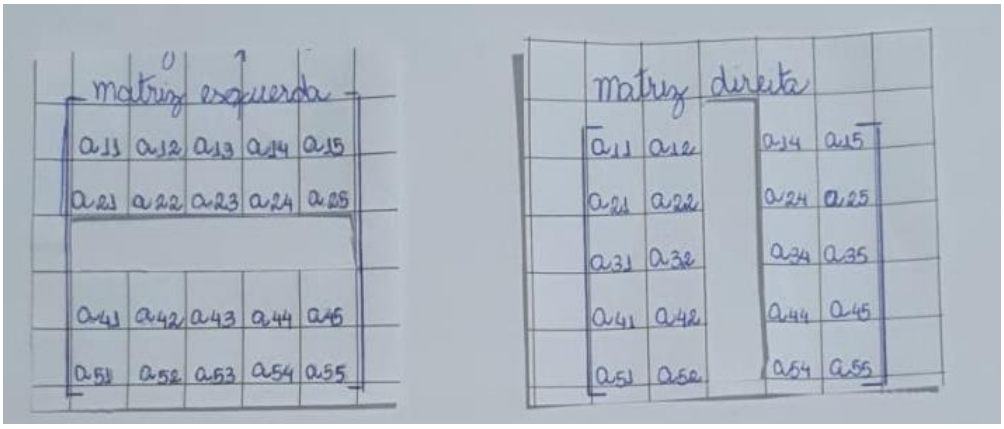
Ao final da atividade, foi proposto criar um C.P.F. aleatório sem os dígitos verificadores, tornando-se a tarefa de um outro grupo.

3.1.2 - Análise de resultados

Durante a multiplicação entre matrizes, um grupo desenvolveu um esquema que facilitava o processo que, com o auxílio do docente, foi posteriormente adaptado conforme Figura 3.1.

Figura - 3.1 – Esquema para algoritmo de multiplicação entre matrizes

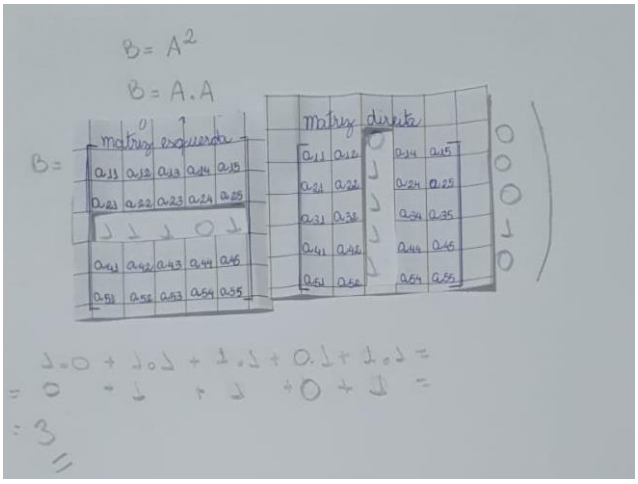
Fonte: O autor



Dado um produto C entre matrizes A e B, C = A.B, a imagem representa duas matrizes quadradas de ordem 5 com uma linha recortada na matriz esquerda e uma linha recortada na matriz direita. Foram escolhidas linhas e colunas arbitrárias. Esta estrutura têm a finalidade de servir como um esquema, para facilitar a resolução do problema proposto na Atividade 1.

Figura 3.2 – Molde desenvolvido sendo utilizado para resolver a Atividade 1

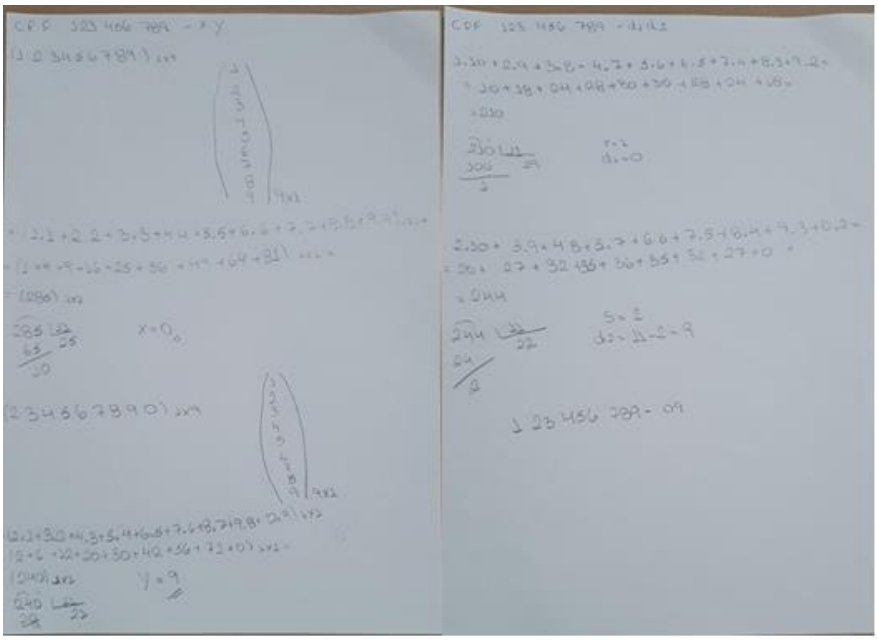
Fonte: O autor



A resolução do cálculo do C.P.F. não apresentou grandes problemas, embora não houvesse uma unanimidade na escolha do algoritmo para cálculo dos dígitos verificadores, tornando importante o desenvolvimento de outros algoritmos e raciocínios diferentes, de modo a conduzir o aluno à resposta correta.

Figura 3.3 – Emprego de algoritmos diferentes para o cálculo dos dígitos verificadores do C.P.F.

Fonte: O autor



3.2 – Cálculo dos dígitos verificadores do Cartão de crédito e código de barras.

3.2.1 – Plano de Aula

Público alvo: 7º ano do Ensino Fundamental.

Tema: Divisores de um número natural.

Objetivos: Desenvolver as habilidades dos alunos em:

● resolver e elaborar situações-problema com números naturais, envolvendo as noções de divisor e de múltiplo;

● resolver e elaborar situações-problema que envolvam operações com números inteiro;

● reconhecer que as resoluções de um grupo de problemas que têm a mesma estrutura, podem ser obtidas utilizando os mesmos procedimentos.

Conteúdo abordado: Critérios de Divisibilidade

Duração: 135 minutos (3 aulas)

Metodologia: (Aula 1) – Definir características de um divisor para construir junto aos alunos a definição de números primos.

Atividade 1 - Em grupo de 4 alunos, identifique os números primos no intervalo de 1 a 100, utilizando o crivo de Eratóstones.

Atividade 2 – A partir da definição de números primos, os grupos devem formular "regras" de divisibilidade para os primos 2, 3 e 5, e apresentá-los aos outros grupos, que, por sua vez, avaliarão a validade das "regras" elaboradas.

Atividade 3 – Definir números compostos através do algoritmo da decomposição e decompor o número 10. Propor aos grupos a definição de uma regra de divisibilidade por 10 e compará-la com as regras de divisibilidade por 2 e 5, analisando se existe alguma relação.

(Aula 2) – Explicar o processo de criação do número de um cartão de crédito, informando o significado dos números, conforme descrito no tópico 2.2.

Atividade 4 – Responder a seguinte questão "Qual a finalidade do dígito validador de um cartão de crédito?" E a situação problema: "José perdeu seu cartão de crédito e precisou cancelá-lo. Com não se lembrava do número, recorreu ao local onde guarda informações importantes e verificou que o último dígito do número de seu cartão estava ilegível. Sabendo que os demais números são 1234 5678 9123 456_, calcule o dígito verificador.

Atividade 5 – Os grupos devem gerar outros números de cartões de créditos aleatórios, propondo o cálculo de seu dígito verificador ao outro grupo.

(Aula 3) – Ainda em grupos, utilizar o processo de criação do código de barras modelo EAN-13, explicando cada agrupamento de números e o cálculo de seu dígito verificador conforme descrito no tópico 2.3.

Atividade 6 – Pesquisar sobre a função do código de barras e seus benefícios econômicos.

Atividade 7 – Ao passar um certo produto pelo sensor óptico, este não foi registrado pelo operador do caixa. Optou-se então pela digitação do número e reparou-se que o último número estava ilegível. Entretanto a caixa conhecia o processo de criação do código de barras, e conseguiu calcular o último dígito. Sabendo que o código era 567145604310X, determine o valor de X.

Atividade 8 – Desenvolva códigos de barras genéricos sem o dígito verificador, propondo a realização de seu cálculo aos outros grupos.

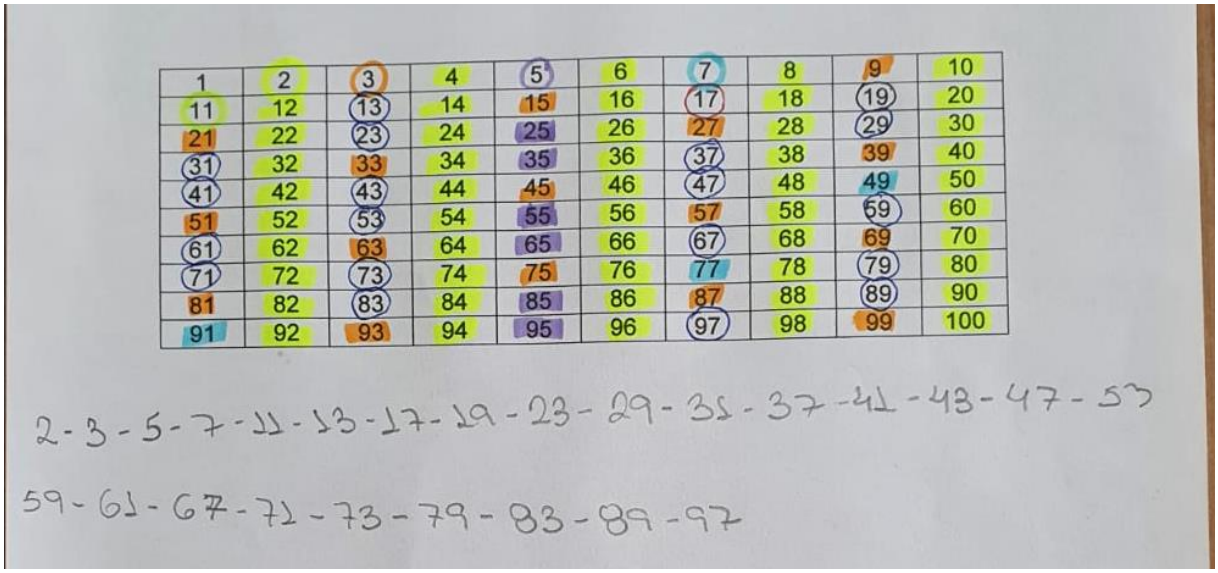
3.2.2 - Análise de resultados

Durante a aplicação do plano de aula em diferentes salas, os alunos de modo geral, se mostraram participativos nas primeiras atividades utilizando o crivo de Eratóstones e as regras de divisibilidade. Nessa última, embora fossem propostas regras incorretas ou incompletas, através de exemplos e contraexemplos dos outros grupos e orientações dadas pelo professor, foi possível a realização da atividade, mostrando o erro como um fator de aprendizagem quando compreendido.

"Se estabelecermos um laço entre o aluno, a época e o personagem relacionado com os conceitos estudados, se conhecerem as motivações e dúvidas que tiveram os sábios da época, então ele poderá compreender como foi descoberto e justificado um problema, um corpo de conceitos, etc.." (VALDÉS, 2002). Baseado nesse conceito e na contextualização dos alunos sobre o período histórico e uma biografia sintetizada de Eratóstones, antes da realização da atividade houve um aumento na participação da sala, ora com perguntas sobre o tema, ora com a resolução da atividade proposta.

Figura 3.4 – Realização da Atividade 1 - Crivo de Eratóstones.

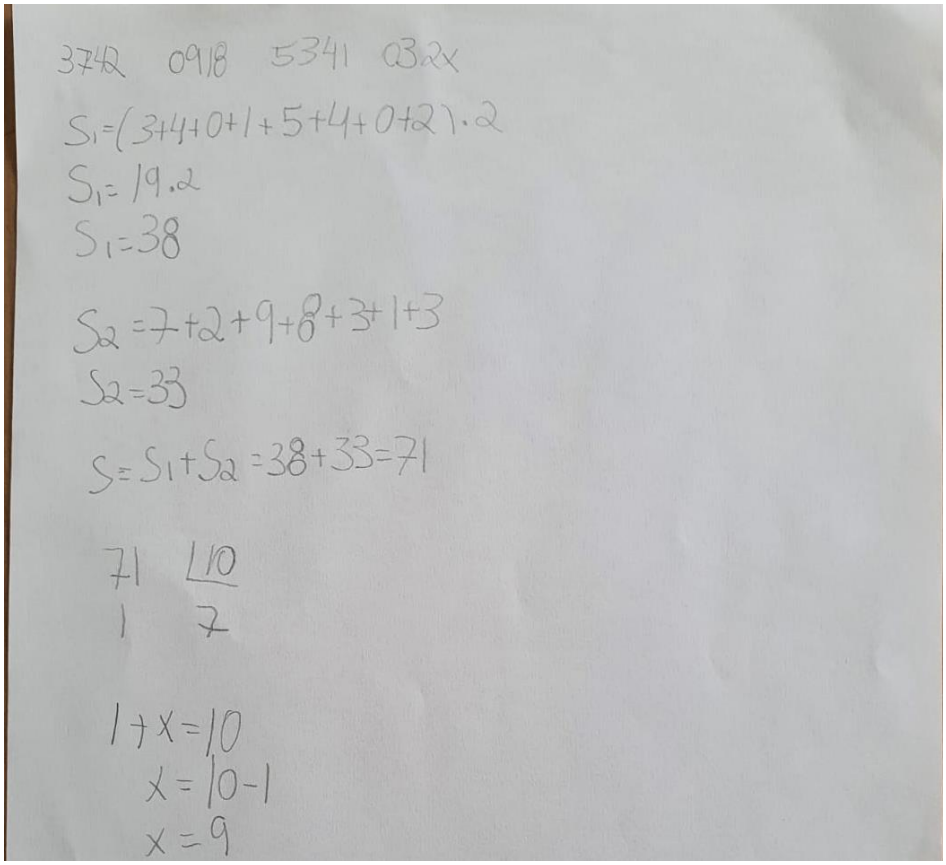
Fonte: O autor



Conforme seguiram as atividades nos tópicos envolvendo o cálculo de dígitos verificadores de cartão de crédito e código de barras, os alunos se depararam com um conteúdo com muitos cálculos aritméticos, se mostrando uma ferramenta de aprendizado contínuo onde, além das realizações de diferentes tipos de algoritmos para as quatro operações fundamentais, pode-se abordar alguns tópicos, como comutatividade, expressões, uso dos parênteses e propriedade distributiva da multiplicação em relação à adição. A organização da sala em grupos, tornou-se uma boa estratégia, uma vez que os próprios colegas auxiliavam os outros a compreender algumas dúvidas. Também foram desenvolvidas habilidades envolvendo a álgebra, introduzindo conceito de variáveis e equações.

Figura 3.5 – Cartão de Crédito criado e dígito verificador calculado como proposto na Atividade 5.

Fonte: O autor



Ao final da Atividade 7, foi passado um link: https://codigosdebarrasbrasil.com.br/calculadora-de-digito-verificador.html, onde os alunos puderam utilizar conferir o dígito verificador, conferindo com os seus códigos criados para a atividade específica.

3.3 – Estudo de calendários e utilização do algoritmo de Zeller

3.3.1 – Plano de Aula

Público alvo: 1ª série do Ensino Médio.

Tema: Números racionais na representação fracionária e na decimal.

Objetivos: Desenvolver as habilidades dos alunos em:

- Ler, interpretar e resolver um mesmo problema utilizando algoritmos;

● Reconhecer que os números racionais positivos podem ser expressos nas formas fracionária e decimal, estabelecer relações entre essas representações, passando de uma representação para outra;

Conteúdo abordado: Operações entre números racionais.

Duração: 135 minutos (3 aulas)

Metodologia: (Aula 1) – Iniciar a aula com a leitura compartilhada, situando os alunos no contexto.

"Um calendário é um sistema de medida de tempo que agrupa e faz a contagem dos dias, dividindo-os em meses e anos.

Quanto à etimologia, a palavra calendário vem do latim *calendarium*, que significa livro das calendas e era o livro usado para contar os dias das festividades religiosas marcadas no início de cada mês lunar na Roma Antiga, antes da introdução do calendário juliano. O calendário gregoriano é um calendário criado na Europa em 1582, por iniciativa do papa Gregório XIII."

Após a realização da leitura e formação dos grupos com 5 a 6 alunos, foram propostas as seguintes perguntas:

Atividade 1 - Quais as diferenças entre o calendário juliano e gregoriano?

Atividade 2 - Quais as fragilidades do calendário gregoriano?

Atividade 3 - Pesquise um tipo de calendário e cite suas principais características.

(Aula 2) – Propor a resolução da seguinte situação problema:

Atividade 4 - Em 2021, Ana comemorou seu aniversário com uma festa, que ocorreu no dia 19 de agosto, uma quinta-feira e está ansiosa para esta comemoração em 2022. É possível calcular em que dia da semana cairá? E em 2023? E em 2024?

Atividade 5 – Beatriz, amiga de Ana, nasceu no dia 19 de janeiro de 2021, uma terça feira. Que dia da semana ocorrerá o aniversário de Beatriz em 2022? E em 2023? E 2024? Foi possível utilizar o mesmo raciocínio para o caso de Ana? Por que?

(Aula 3) – A partir das conclusões tomadas na aula anterior com as duas situações, propor se é possível obter uma nova maneira de encontrar o dia da semana de acordo com uma data, e estabelecer o algoritmo de Zeller descrito no tópico 2.4. Apresentar um exemplo na lousa. Em seguida propor as seguintes atividades.

Atividade 6 - Calcule o dia da semana que você nasceu.

Atividade 7 - A independência do Brasil ocorreu no dia 7 de setembro de 1822. Calcule o dia da semana que ela ocorreu.

Atividade 8 - Calcule os possíveis dias do mês para uma certa data de maio de 2015, sabendo que tal data ocorreu em uma segunda.

3.3.2 - Análise de resultados

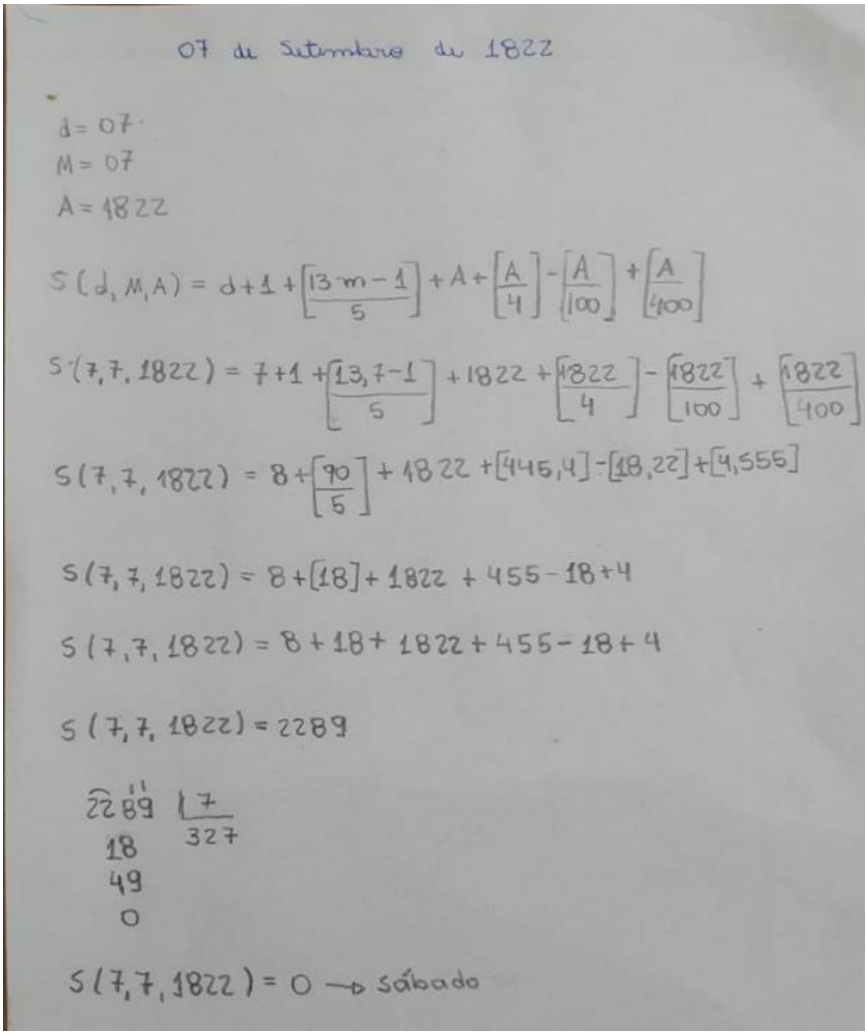
A leitura demonstrou ser uma estratégia efetiva, pois através dela muitos alunos participaram e levantaram questões sobre significado de palavras, como exemplo etimologia, calendas, equinócio e solstício, estes dois últimos exemplos demonstraram uma oportunidade de realizar uma atividade interdisciplinar, abordando o assunto de forma mais aprofundada através de experimentos, ao invés de uma simples explicação. Ao final da leitura, notava-se muitos alunos interessados e participativos em realizar a pesquisa e debater os itens propostos.

Para responder as questões da segunda aula, grande parte dos alunos utilizaram o calendário em seu celular para verificar a resposta do problema. O professor, por sua vez, interveio perguntando se existia uma outra forma de resolver a questão utilizando as operações básicas. Foi necessário retomar as características do calendário gregoriano levantadas pelos alunos na aula anterior, para começarem a formular as primeiras hipóteses de realização dos cálculos. Ao elaborarem um

processo que encontrava uma resposta correta, o professor atuou questionando o motivo do cálculo em cada parte do procedimento. Para verificar a validade, o professor solicitou que aplicassem o mesmo procedimento nos anos seguintes propostos na situação problema e conferissem a resposta no calendário para validar o raciocínio. Foram obtidas diferentes estratégias de solução, mas grande parte dos grupos apresentaram dificuldades no cálculo do dia referente ao ano de 2024, por se tratar de ano bissexto. No entanto, ao levar em consideração está informação, estes alcançaram a resposta correta. Através da apresentação de um método de resolução desenvolvido por um grupo, todos obtiveram um resultado satisfatório, demonstrando a compreensão do tema. Ao realizar a atividade 5, todos os grupos conseguiram replicar o mesmo raciocínio utilizado na atividade anterior. Ao conferirem as respostas verificou-se a mesma resposta incorreta para a data referente ao ano de 2024, levantando novas ideias para explicar a situação. Chegou-se à conclusão de que data do aniversário de Beatriz avança um dia da semana, pois ocorre antes do 29 de fevereiro, mesmo que 2024 seja bissexto e ainda $366 \equiv 2 \pmod 7$. Com isso, houve muitos questionamentos se existiria um método mais simples, pois existem muitas condições para resolver este problema, criando o ambiente perfeito para iniciar a terceira aula, apresentando um algoritmo (Zeller), onde não existiriam tais preocupações na resolução do problema. Embora inicialmente, alguns alunos demonstrassem dificuldades em realizar o algoritmo da divisão, através da recuperação contínua a atividade transcorreu de maneira satisfatória.

Figura 3.6 – Utilização do algoritmo de Zeller para realizar a Atividade 7, recuperação contínua sobre o algoritmo da divisão.

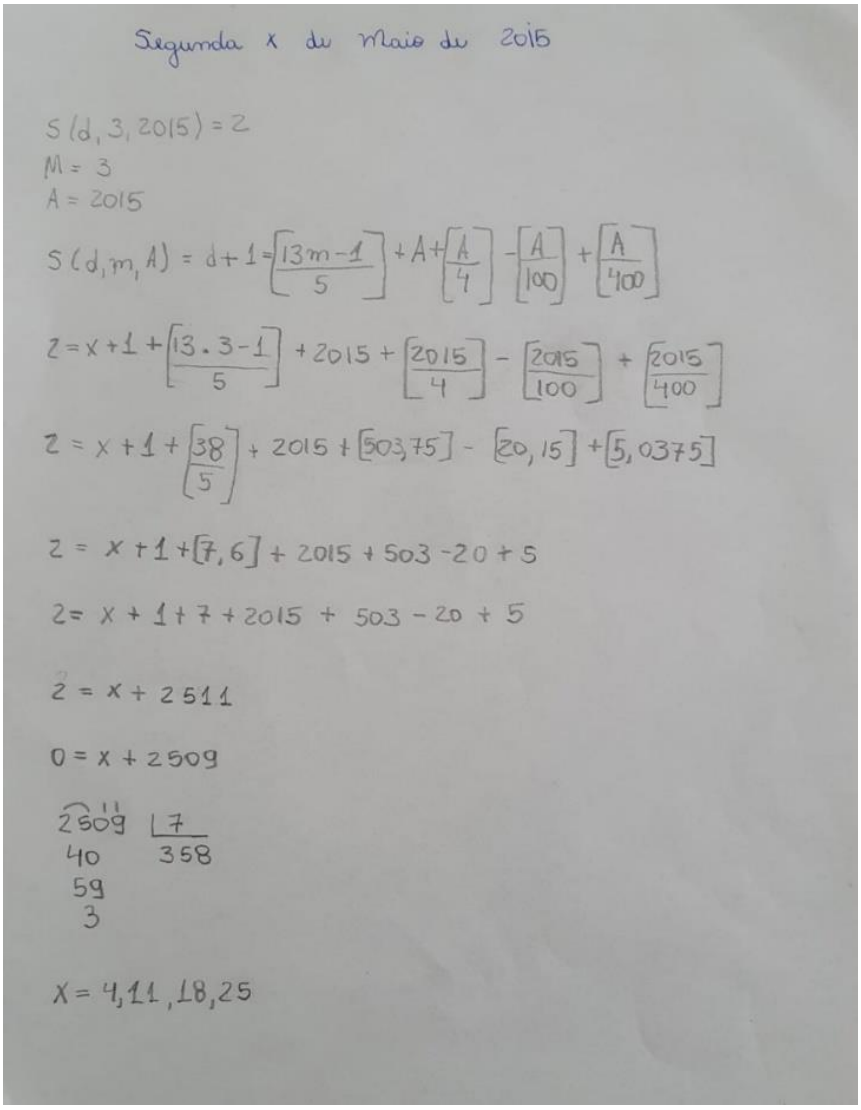
Fonte: O autor



A atividade 8, trouxe grandes problemas devido a resolução envolver o cálculo elemento simétrico e possuir mais de uma solução, evidenciando fragilidades, necessitando de mudanças em sua proposta ou até exclusão da atividade devido ao grau de dificuldade.

Figura 3.7 – Utilização do algoritmo de Zeller para realizar a Atividade 8.

Fonte: O autor



3.4 – Um prelúdio a criptografia

3.4.1 – Plano de Aula

Público alvo: 6º ano do Ensino Fundamental.

Tema: Operação entre números naturais.

Objetivos: Desenvolver as habilidades dos alunos em:

● Solucionar e propor problemas que envolvam cálculos (mentais ou escritos, exatos ou aproximados) com números naturais, por meio de estratégias pessoais, com compreensão dos processos neles envolvidos com e sem uso de calculadora;

● Reconhecer o sistema de numeração decimal como fruto de um processo histórico, percebendo semelhanças e diferenças com outros sistemas de numeração, de modo a sistematizar suas principais características (base, valor posicional e função do zero), utilizando, inclusive, a composição e decomposição de números naturais e números racionais em sua representação decimal.

Conteúdo abordado: Divisão Euclidiana.

Duração: 90 minutos (2 aulas)

Metodologia: (Aula 1) – Iniciar a aula propondo a leitura do pequeno trecho.

“Sem dvdúia, vcoê é cpaaz ler e etneednr etse ttexo com lreats tcaorads e plaarvas ftalndao.”

Após, realizar a leitura compartilhada do seguinte texto explicativo da mensagem.

...“É possível ler uma frase normalmente mesmo quando estão faltando letras nas palavras, palavras nas frases ou quando as letras estão embaralhadas. Isso acontece porque a mente humana consegue preencher as lacunas e corrigir a ordem das palavras de acordo com o contexto. Desde a nossa formação, o cérebro é uma máquina de aprender. Tem conhecimento de onde estão as letras. Ele já sabe que aquele desenho [da palavra] corresponde a algo que já conhece, então vai preenchendo as lacunas”, explica o psicólogo Alexandre Bortoletto, instrutor de Programação Neurolinguística (PNL), da Sociedade Brasileira de PNL.”

Após a leitura, organizou-se a sala em grupos de 5 alunos e foram propostas as seguintes atividades:

Atividade 1 - Podemos dizer que as palavras com letras trocadas estão criptografadas? Você já ouviu falar de criptografia? Pesquise sobre o tema e discuta com seus colegas.

Atividade 2 – Tente descobrir o “segredo” do código utilizado na frase abaixo.

Tf wpdf dpotfhvf mfs jttp, fou$\tilde{b}$p eftdpcsjv p tfhsfep

(Aula 2) – Iniciar com a seguinte atividade.

Atividade 3 – Com seu grupo, crie um modelo criptográfico e escreva uma palavra utilizando as suas regras.

Atividade 4 – Considere o sistema criptográfico, cujo segredo dependerá do resto de uma divisão por 26, substituindo-os pelos valores abaixo.

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

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

Por exemplo, para o número 452, tem-se:

$$\begin{array}{r|l} 452 & 26 \\ \cline{2-2} 10 & 17 \end{array}$$

Logo na divisão de 452 por 26 temos como resto 10, utilizando a tabela obtemos a letra K.
Utilizando este sistema escreva uma palavra de 5 a 8 letras.

3.4.2 - Análise de resultados

A frase encriptada da introdução não foi uma ferramenta eficaz em algumas salas, devido à grande defasagem na formação de alguns alunos. Para contornar tais obstáculos, realizou-se uma avaliação diagnóstica com a finalidade de identificar os alunos que apresentam dificuldades, pois (RABELO,2018) aponta para a necessidade de correção de rotas no planejamento do ensino de Matemática em nível médio e fundamental, onde tal prática é fundamental para a atividade docente. Adaptar a frase introdutória substituindo-a por uma palavra simples trouxe maior participação e aproveitamento na resolução da atividade. A leitura compartilhada sobre textos auxiliares sobre o tema também obteve maior interesse por parte dos alunos. Com

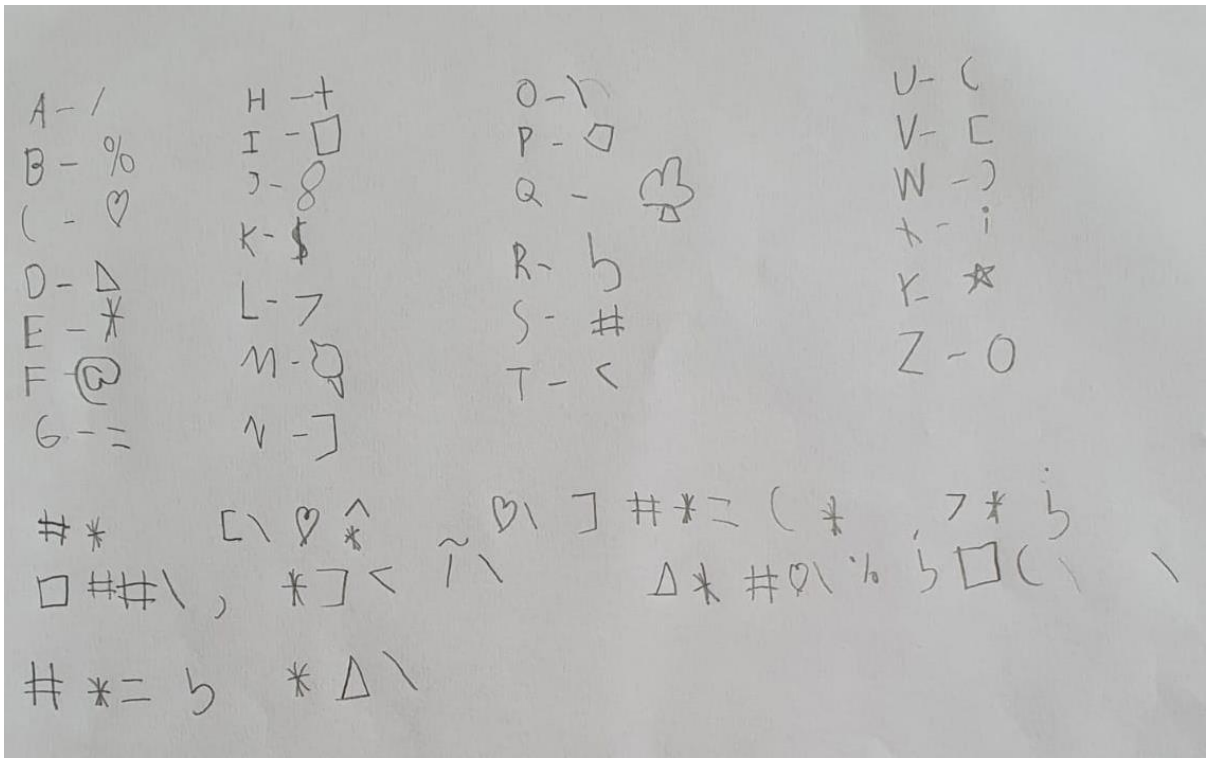
isso pode-se discutir as características da criptografia, avaliando sua função, quando foi empregada, onde é usada atualmente e até sobre o grau de dificuldade em decifrar o código, onde o segredo era praticamente inexistente.

Na segunda atividade houve mais dificuldade, embora alguns grupos conseguissem realizar, porém outros demoraram cerca de 15 minutos para desvendar. Quando questionados como descobriram o segredo, o símbolo "$\tilde{b}$" conduziu a uma linha de raciocínio correta, de que só poderia ser as vogais a ou o, pois são as únicas letras na língua portuguesa que recebem o til.

O entusiasmo gerado pelas atividades e a descoberta do código, despertou uma grande variedade de diferentes e criativos códigos criptográficos, elaborados pelos grupos na Atividade 3.

Figura 3.8 – Criação de um modelo criptográfico e criação de uma mensagem utilizando o código.

Fonte: O autor

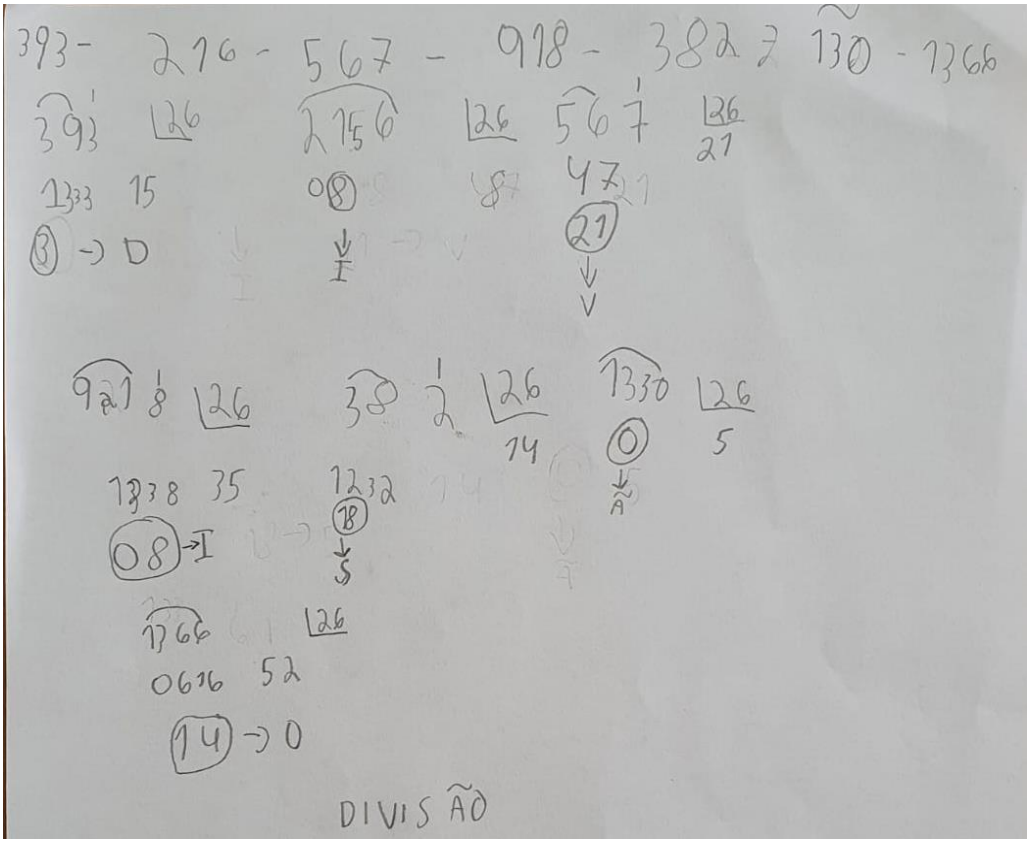


O objetivo da Atividade 4 era introduzir a aritmética dos restos. Para isso, foi utilizado o número 26 (quantidade de letras em nosso alfabeto). Esta atividade

também ajudaria a realizar a divisão Euclidiana, embora, o divisor 26 ocasionou muitas dúvidas e receio na realização da atividade, por se tratar de uma divisão, cujo divisor tem dois dígitos, necessitando da ajuda do professor e outros grupos. Por essa razão, uma possível melhoria seria utilizar poucas letras descartando as de menor incidência, resultando em um divisor menor, utilizando como divisores múltiplo de 5, como 15, 20 ou 25.

Figura 3.9 – Resolução da mensagem criptografada utilizando os códigos propostos na Atividade 4.

Fonte: O autor



Desta forma, o plano de aula resultou em grande participação, mas o alto grau de dificuldade de certas atividades e a falta de conhecimento, ocasionaram certas dificuldades exigindo a remodelação de algumas atividades.

CONSIDERAÇÕES FINAIS

Durante a elaboração dos planos de aula, tomou-se como prioridade atingir uma aprendizagem significativa, que segundo (BRUINI, 2015), é preciso desenvolver táticas que motivem educandos, para que o aprendizado deixe de ser passivo e se torne ativo. Visando isto, a estruturação de um plano de aula e planejamento de ações torna-se uma ferramenta indispensável para o docente. Neste trabalho foram utilizadas algumas abordagens de criptografia utilizando a aritmética modular, demostrando-se efetivas no âmbito de ensino aprendizagem e na formação contínua do professor.

Observou-se que os planos de aula que adotaram uma leitura inicial contextualizando os alunos sobre os temas, resultou em maior participação dos discentes. A utilização da história na matemática e realização de atividades interdisciplinares se mostrou uma boa estratégia para alcançarem melhores participações por parte dos discentes.

Apesar de abordar as habilidades específicas do ano de ensino, os planos mostram-se excelentes oportunidades de trabalhar habilidades defasadas, podendo atuar como ferramenta para a progressão contínua, revisitando habilidades defasadas vistas em anos anteriores, em que avaliações diagnósticas introdutórias mostram-se ferramentas de extremo valor na adaptação dos planos abordados, afim de alcançar melhores rendimentos, observando o nível de aprendizagem em linguagem matemática e habilidades dominadas pelo público alvo.

Por fim, através da realização deste trabalho pudemos contribuir na formação do aluno utilizando a educação interdimensional, afim de auxiliar no seu processo de descoberta, autoconhecimento, construção de um cidadão com senso-crítico e autonomia, pois essas atividades promovem o protagonismo por meio da leitura compartilhada, análise e compartilhamento da informação por meio das discussões em grupos, promovendo interações positivas divulgando os acertos e localizando os erros em um raciocínio incorreto ou incompleto, fomentando o pensamento científico, apresentando diversas formas de trabalho através da organização da sala de aula. Com isso, permitiu trabalhar e desenvolver as habilidades essenciais e objetos de

conhecimento da disciplina de matemática e também de outras voltadas ao social como empatia, comunicação, liderança, resiliência e respeito às diferenças.

REFERÊNCIAS

SILVEIRA, J. P. C. . Aplicações de Criptografia Baseada em Identidade com Cartões de Identificação Eletrônica. Universidade da Beira Interior. Outubro de 2013.

COUTINHO, S. C. . Criptografia. Instituto Nacional de Matemática Pura e Aplicada. 2015.

SCHECHTER, L. M. . Uma introdução à criptografia de chave pública através do método El Gamal. Universidade Federal do Rio de Janeiro. 2014.

ESQUINCA, J. C. P.. Aritmética: Códigos de barras e outras aplicações de congruências. Universidade Federal de Mato Grosso. 2013.

RODRIGUES, J. M. A.. Os calendários e a sua contribuição para o ensino da física. Universidade do Porto, Porto, Portugal, 2012.

MACHADO, D. A.. Uma abordagem de dígitos verificadores e códigos corretores no Ensino Fundamental. Universidade de São Paulo, São Carlos, 2016.

BRUINI, E. C. Aprendizagem Significativa. 2015. Brasil Escola. Acessado em 2020. Disponível em: https://educador.brasilescola.uol.com.br/trabalho-docente/aprendizagem-significativa.htm

VALDÉS, J. E. N. . La História como elemento unificador en lá Educación Matemática. Argentina, 2002.

RABELO, F. B. . Análise da Avaliação Diagnóstica da Aprendizagem do estado de Goiás: Um olhar sobre a área de Matemática. Universidade Federal de Goiás. Catalão, Goiás. 2018.

MEC. Parâmetros Curriculares Nacionais - Ensino Médio, Parte III - Ciências da Natureza, Matemática e suas Tecnologias: MEC/SEMT, 1999

SÃO PAULO (ESTADO). Secretaria da Educação. Currículo Paulista: Matemática e suas tecnologias / Secretaria da Educação; coordenação geral, Maria Inês Fini; coordenação de área, Paulo Miceli. – 1. ed. atual. – São Paulo, 2011.

BRASIL. Base Nacional Comum Curricular (BNCC). Educação é a Base. Brasília: MEC/CONSED/UNDIME, 2018. Disponível em: [http://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf].