Revista Eletrônica Paulista de Matemática

ISSN 2316-9664
v. 22, n. 3, dez. 2022

Introdução da Criptografia no Ensino Médio e Fundamental utilizando Aritmética Modular

Introduction of Cryptography in Middle and Elementary School using Modular Arithmetic

Luis Antonio da Silva Vasconcellos
Faculdade de Ciências
UNESP - Universidade Estadual Paulista "Julio de Mesquita Filho"
luis.a.vasconcellos@unesp.br

João Fernando Montanher
SEE/SP
jf.montanher@unesp.br

Resumo

Este trabalho utiliza a aritmética modular em aplicações no ensino fundamental e médio, através de atividades desenvolvidas em sala de aula. Inicialmente, são apresentados os fundamentos teóricos que serão a base para as aplicações como cpf, cartão de crédito, código de barras, calendários e criptografia. Finaliza-se, analisando estas aplicações e as consequências para este público.

Palavras-chave: Aritmética modular. Congruência. Criptografia. RSA. El Gamal.

Abstract

This work uses modular arithmetic in applications in elementary and high school, through activities developed in the classroom. Initially, the theoretical foundations that will be a basis for applications such as cpf, credit card, bar code, calendars and cryptography are presented. It ends by analyzing these applications and the consequences for this public.

Keywords: Modular arithmetic. Congruence. Cryptography. RSA. El Gamal

Artigo recebido em ago. 2022 e aceito em dez. 2022

1 Introdução

Durante a história da humanidade, a criptografia foi utilizada em diferentes contextos, inicialmente em tempos de guerra e atualmente assumindo um papel fundamental em transações financeiras, mensagens, contas pessoais, dentre outros. Motivado por este fato, a proposta deste trabalho é apresentar a álgebra modular e teoria dos números como aplicações para o ensino fundamental e médio, demonstrando a importância de sistemas que utilizam a criptografia atualmente.Assim, será introduzida a aritmética modular, mostrando a sua utilidade e aplicação em situações mais aplicadas, além do estudo com números primos. Este trabalho está estruturado da seguinte forma. Inicialmente apresenta-se fundamentos da teoria dos números e aritmética modular.Após, serão apresentadas algumas aplicações da aritmética modular em situações conhecidas tais 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. Por fim, as aplicações que foram desenvolvidas em sala de aula e uma breve discussão do desenvolvimento. Ao final, apresentam-se as considerações finais e algumas sugestões para planos de aula.

2 Fundamentação teórica

Definição 1.1 Dados dois inteiros **a**, chamado de dividendo e $b > 0$, 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 $0 \leq r \leq b$.

Teorema 1.2 (Unicidade do Quociente e Resto) - De acordo com [1], dados dois inteiros a e b ambos positivos, existe um único par de inteiros q e r que satisfaz as condições da definição 1.1.

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 $b \mid a$, ou que b é divisor de a, ou que b é fator de a, se $a = b.x$, para algum $x \in Z$, isto é, se a divisão de a por b produz resto 0.

Proposição 1.4 (Euclides): Sejam a, b $\neq 0$, $a, b \in N$ naturais. Se p é primo e $p \mid a.b$ então $p \mid a$ ou $p \mid b$.
Demonstração: Suponha que $p \nmid a$, se $p \mid a.b$ então existe um natural n, tal que $n.p = a.b$, logo $n = \frac{a.b}{p}$. Como n é natural e $p \nmid a$, então $p \mid b$. Analogamente $p \nmid b \Rightarrow p \mid a$.

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

Teorema 1.6 (Fundamental da Aritmética) Todos os inteiros positivos $n > 1$ possuem uma decomposição única em fatores primos.

Demonstração: A demonstração será dividida em duas etapas. Inicialmente, prova-se que existe uma decomposição em fatores primos e, em seguida, que essa decomposição é única.Na primeira parte utiliza-se o método de indução. Para $n = 2$, é trivial pois o próprio número é primo e portanto se apresenta como uma decomposição em fator primo. Supondo que o teorema seja

válido para n, prova-se a validade para n+1. Se n+1 é um número primo, é um caso idêntico ao n = 2, logo não há nada a demonstrar. Caso não sejam, pelo princípio da indução como $n \geq d$ e $n \geq q$, podem ser escritos como fatores primos. Logo $d = p_1.p_2...p_r$ e $q = q_1.q_2...q_s$, então $n + 1 = d.q = p_1.p_2...p_r.q_1.q_2...q_s$, com $p_1, p_2, ..., p_n, q_1, q_2..., q_s$ 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, $n = p_1.p_2...p_r$, com $p_1 \leq p_2 \leq ... \leq p_r$ e $n = q_1.q_2...q_n$, com $q_1 \leq q_2 \leq ... \leq q_s$. Então $p_1.p_2...p_r = q_1.q_2...q_s$. Logo p_1 divide $q_1.q_2...q_s$ e pelo corolário 1.5, $p_1 \mid q_j$ para algum j, $p_1 = q_j \geq q_1$. Analogamente q_1 divide $p_1.p_2...p_r$, para algum i, $q_1 = p_i \geq p_1$. Portanto $p_1 = q_1$, pela minimalidade de n. De $p_1.p_2...p_r = q_1.q_2...q_s$ e com o mesmo argumento, encontram-se as relações $p_2 = q_2$, $p_3 = q_3$,..., $p_r = q_s$. 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 $\varphi(x)$ é definida para um número natural x como sendo a quantidade de números menores ou iguais a x co-primos a ele. Matematicamente a função é expressa por

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

Se $n = p_1^{k_1}.p_2^{k_2}...p_n^{k_n}$, 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 $n = (p_1 - 1)^{(k_1-1)}.(p_2 - 1)^{(k_2-1)}...(p_n - 1)^{(k_n-1)}$. 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 $\varphi(n) = (p - 1).(q - 1)$.

Definição 1.8 Seja n um número natural tal que $n \geq 2$. Dados $a, b \in Z$ dizemos que **a** é congruente a **b** módulo n, denotado por $a \equiv b$ (mod n), se $a - b$ é múltiplo de n. O número **n** é chamado de módulo da congruência.

Teorema 1.9 Seja $n \geq 2$ um inteiro. A relação de congruência módulo n é uma relação de equivalência.

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

1. Reflexividade: Seja a um inteiro. Tem-se que 0 é múltiplo de **n**, $0 = a - a$, logo $a - a$ é múltiplo de n. Portanto $a \equiv a$ (mod n).

2. Simetria: Sejam a e b inteiros tais que $a \equiv b$ (mod 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 $\Rightarrow (-1).(a - b) = (-1).n.k$. Por fim, $(b - a) = n.(-k)$, como $k \in Z$, tem-se que $b - a$ é múltiplo de n e portanto, $b \equiv a$ (mod n).

3. Transitividade: Sejam a, b e c inteiros tais que $a \equiv b$ (mod n) e $b \equiv c$ (mod n), então por definição de congruência, segue que $a - b$ e $b - c$ são múltiplos de n, isto é, existe $k_1, k_2 \in Z$, tais que $a - b = n.k_1$ e $b - c = n.k_2$. Somando-se 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 $a \equiv c$ (mod n).

Teorema 1.10 Se $a \equiv a'$ (mod n) e $b \equiv b'$ (mod n), então:

1. $(a + b) \equiv (a' + b')$ (mod n);

2. $a.b \equiv a'.b'$ (mod n).

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

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

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

Teorema 1.14 Sejam $a \geq 2$ e $n \geq 2$ números inteiros. As seguintes afirmativas são equivalentes:

1. $\bar{a}$ possui inverso multiplicativo em Z_n ;
2. mdc(a,n) = 1;
3. existe um inteiro positivo k tal que $a^k \equiv 1$ (mod 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.
Demonstração Como mdc $(a, b) = 1$, $\exists k$ inteiro tal que $a^k \equiv 1$ (mod b), onde $a^{(k-1)}.a \equiv 1$ (mod b), sendo $a^{(k-1)}$ o elemento inverso de a.

Lema 1.16 (Euclides)- Se $x, y \neq 0$, $mdc(x, y) = mdc(x, x + y)$.

Corolário 1.17. $mdc(n, n + 1) = 1$.
Demonstração De fato, como $mdc(n, 1) = 1$ então mdc $(n, n + 1) = 1$.

Teorema 1.18 Seja $k \in Z$, então mdc $(3, 6k - 2) = 1$.
Demonstração: Suponha que exista um divisor $d \neq 1$, tal que, $d \mid 3$ e $d \mid (6k - 2)$. Como 3 é primo e $d \mid 3$ temos que $d = 3$ ou $d = 1$. Se $d \mid (6k - 2)$, existe um inteiro m, tal que, $6k - 2 = 3d$, implicando em $6k - 3d = 2$. Mas $3(2k - d) = 2$. Assim $3 \mid 2$, levando a uma contradição. Portanto $d = 1 = mdc(3, 6k - 2)$.

Teorema 1.19 O inverso de 3 módulo $6k - 2$, com $k \in Z$ 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
$n = 6.k - 2 \Rightarrow n - 1 = 6.k - 3 \Rightarrow n - 1 = 3.(2.k - 1) \Rightarrow n = 3.(2.k - 1)$
Assim,
$3.(2.k - 1) + 1 \equiv 0$ (mod n)
$\Rightarrow 3.(2.k - 1) \equiv (-1)$ (mod n)
$\Rightarrow 3.(1 - 2.k) + 1 \equiv 1$ (mod n)
Logo $1 - 2.k$ é o inverso de 3 módulo n. Quando $k > 0$, o inverso é negativo. Utilizando o resíduo temos $1 - 2k + n = 1 - 2.k + 6.k - 2 = 4.k - 1$, positivo para $k > 0$, demonstrando o teorema.

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

Demonstração: Os possíveis resíduos de p são $1, 2, ..., p-1$. Multiplicando cada resíduo por a temos $a, 2.a, \ldots, (p-1).a$, 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: $r_1 \equiv a$ (mod p)
$r_2 \equiv 2a$ (mod p)
$\vdots$
$r_{p-1} = (p-1).a(modp)$.
Multiplicando-se as congruências, segue que $r_1.r_2...r_{p-1} \equiv a.2.a.\ldots.(p-1).a$ (mod p)
$r_1.r_2...r_p - 1 \equiv a^{p-1}.1.2\ldots(p-1)$ (mod p). ($\star$) Demostraremos 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 $a.r_k \equiv a.k \equiv a.l \equiv a.r_l(modp)$
$a.k \equiv a.l$ (mod p).
Como p não divide a, segue que mdc $(a, p) = 1$. Pelo teorema 1.14, a é inversível módulo p, resultando em $k \equiv l$ (mod p). Como k e l são congruentes e $1 \leq k, l \leq (p-1)$, concluímos que $k = l$, provando que os resíduos $r_1, r_2, \ldots, r_{p-1}$ não são iguais. Logo $r_1, r_2, \ldots, r_{p-1} = 1.2\ldots(p-1)$.
Substituindo essa igualdade em ($\star$), segue que $r_1, r_2, \ldots, r_{p-1} \equiv a^{p-1}.1.2\ldots(p-1)$ (mod p)
$1.2\ldots(p-1) \equiv a^{p-1}.1.2\ldots(p-1)$ (mod p).
Mas mdc $(2, p) = 1, mdc(3, p) = 1, \ldots, mdc(p-1, p) = 1$, então $2, 3, \ldots, p-1$ são inversíveis módulo p, resultando em $a^{p-1} \equiv 1$ (mod 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

$$\begin{cases} x \equiv a \ \ mod(m) \\ x \equiv b \ \ mod(n). \end{cases}$$

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 tal que $* : G \times G \to G$, satisfaz as seguintes propriedades:

1. Associatividade: para todo $a, b, c \in G$, $(a * b) * c = a * (b * c)$;
2. Existência de elemento neutro: existe um elemento $e \in G$ tal que, para todo $a \in G$, $a * e = e * a = a$;
3. Existência de inversos: para todo $a \in G$, existe um elemento $a^{-1} \in G$ 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 **abeliano** se além das propriedades de grupo, ele satisfaz a comutatividade, isto é, para todo $a, b \in G$, $a * b = b * a$.

Definição 1.24 Define-se $U(n) = \{\bar{a} \in Z_n / mdc(a, n) = 1\}$, como o conjunto de todos os elementos de Z_n que possuem inverso multiplicativo.

Teorema 1.25 O par $(U(n), \cdot)$, onde "$\cdot$"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 $n \geq 2$, temos que mdc$(1, n) = 1$, logo, $\bar{1} \in U(n)$. Vamos mostrar se $a, b \in U(n)$ então $a \cdot b \in U(n)$. Se $a \in U(n)$ então existe $a^{-1} \in U(n)$

que é inverso de a. Analogamente, dado $b \in U(n)$ então existe $b^{-1} \in U(n)$ que é inverso de b. Seja u o inverso de $a \cdot b$, então
$a \cdot b \cdot u = 1$ (mod n)
$a \cdot (b \cdot u) = 1$ (mod n)
$a^{-1} \cdot a \cdot (b \cdot u) = a^{-1} \cdot 1$ (mod n)
$1 \cdot (b \cdot u) = a^{-1}$ (mod n)
$b \cdot u = a^{-1}$ (mod n)
$b^{-1} \cdot (b \cdot u) = b$
$b^{-1} \cdot a^{-1}$ (mod n)
$(b^{-1} \cdot b) \cdot u = b^{-1} \cdot a^{-1}$ (mod n)
$1 \cdot u = b^{-1} \cdot a^{-1}$ (mod n)
$u = b^{-1} \cdot a^{-1}$ (mod n)
logo $b^{-1} \cdot a^{-1}$ é o inverso de $a \cdot b$ e portanto, $a \cdot b \in U(n)$.

Definição 1.26 A ordem de um grupo $G = (G, *)$ é definida pela 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 $a \in G$ um de seus elementos. Define-se 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, diz-se que $H = (H, *)$ é um subgrupo de G se as seguintes propriedades são satisfeitas:
(i) $H \subseteq G$;
(ii) Para todo $h, j \in H$, temos que $h * j \in H$;
(iii) $e \in H$, onde e é o elemento neutro da operação;
(iv) Para todo $h \in H$, existe um elemento $h^{-1} \in H$ tal que $h * h^{-1} = h^{-1} * h = e$.

Definição 1.30 Considere que $(H, *)$ é um subgrupo cíclico de G gerado por **a**, então **a** é uma raiz primitiva do grupo $(H, *)$.

Definição 1.31 - Um grupo diz-se cíclico se for gerado por um único elemento.

Lema 1.32 (Chave) Seja $G = (G, *)$ um grupo finito e $a \in G$. Então $a^t = e \Leftrightarrow$ 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 $a = a^{kt'} = (a^k)^{t'} = e^{t'} = e$.
($\Rightarrow$) Suponha que $a^t = e$. Vamos dividir t por k, obtendo $t = kq + r$, com $r < k$. 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 1.33 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**.

Lema 1.34 Sejam p primo e $f(x) = a_k x^k + a_{k-1} x^{k-1} + \ldots + a_1 x + a_0$ um polinômio tal que os

coeficientes a_i, $0 \leq i \leq k$, são inteiros, a variável x também assume valores inteiros e $a_k \not\equiv 0$ (mod p). Então, a congruência $f(x) \equiv 0$ (mod p) possui, no máximo k soluções distintas módulo p.
Demonstração: Prova-se por indução em k. Para k = 0, valem as congruências:
$f(x) \equiv 0$ (mod p);
$a_0 \equiv 0$ (mod p)
Contradizendo a hipótese, $a_0 \equiv 0$ (mod p) admite 0 (zero) soluções. Considera-se a validade para $k-1$ e demonstra-se para k. Se a congruência $f(x) \equiv 0$ (mod 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 $s_1, s_2, \ldots, s_k$. Será demonstrado que não existe outra solução módulo p, destas k soluções listadas para a congruência.Seja $g(x) = f(x) - a_k(x-s_1)(x-s_2)\ldots(x-s_k)$. Note que o grau de $g(x) < k$, uma vez que o termo $a_k x^k$ de $f(x)$ é cancelado em $a_k(x-s_1)(x-s_2)\ldots(x-s_k)$. Pela hipótese de indução, se g(x) satisfaz as hipóteses do enunciado, a congruência $g(x) \equiv 0$ (mod p) terá menos de k soluções distintas módulo p. Entretanto, temos que $g(s_i) \equiv 0$ (mod p) para todos os valores s_i, $1 \leq i \leq k$. Logo, a hipótese de que o termo líder do polinômio não é congruente a zero módulo p e que não poderá ser satisfeita por g(x), implica que $g(x)$ é o polinômio identicamente nulo (módulo p). Assim, a partir da equação, obtem-se: $f(x) \equiv a_k(x-s_1)(x-s_2)\ldots(x-s_k)$ (mod p). Desta forma, $f(x) \equiv 0$ (mod p) $\Leftrightarrow$ p divide o $a_k(x-s_1)(x-s_2)\ldots(x-s_k)$. Como p é primo e se p divide um produto, ele divide um dos termos deste produto. Por hipótese, p não divide a_k, pois $a_k \not\equiv 0$ (mod p). Desta forma, p divide $x - s_i$, para algum $1 \leq i \leq k$, o que significa que $x \equiv s_i$ (mod p). Portanto, $f(x) \equiv 0$ (mod p)$\Leftrightarrow x \equiv s_i$ (mod p), para algum $1 \leq i \leq k$. Assim, todas as soluções da congruência $f(x) \equiv 0$ (mod p) são congruentes a uma das k soluções listadas anteriormente.

Teorema 1.35 Se p é primo, então U(p) é cíclico.
Demonstração Como p é primo, $U(p) = Z_p - \{\bar{0}\}$, de forma que a ordem de $U(p)$ é $p-1$. Fatorando $p-1$:

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

onde $1 < q_1 < q_2 < \ldots < q_k$ são primos distintos e $e_i \geq 1$, para todos $1 \leq i \leq k$. 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 $\bar{a}_i$ tal que

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

com $\bar{a}_i \in U(p)$. Este elemento deve existir, pois os elementos $\bar{u} \in U(p)$ são 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 1.34. Conhecendo o valor a_i, calcula-se o valor de h_i.

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

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:

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

o que implica 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 em $a_i^{\frac{(p-1)}{q_i}} \equiv 1$ (mod p), também pelo Lema 1.33, o que contradiz a escolha de a_i. Portanto a ordem de $\bar{h}_i$ é igual a $q_i^{e_i}$. Realizada esta operação para cada $q_i^{e_i}$ da fatoração, obtem-se elementos $\bar{h}_1, \bar{h}_2, ..., \bar{h}_k \in U(p)$ tais que suas respectivas ordens são $q_1^{e_1}, q_2^{e_2}, ..., q_k^{e_k}$. Como estas ordens são potências de primos distintos e se **m** é a ordem de $\bar{h}_i$ e **n** é a ordem de $\bar{h}_j$, com $i \neq j$, então $mdc(m, n) = 1$. Temos que o elemento $\bar{g}$, onde

$$\prod_{1 \leq i \leq k} h_i (mod p)$$

tem ordem

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

de acordo com o lema 1.32. Logo $\bar{g}$ é uma raiz primitiva de $U(p)$, portanto é um grupo cíclico.

Definição 1.36 De acordo com [2], define-se o Problema do Logaritmo Discreto (PLD), da seguinte forma: dados um grupo finito cíclico $G = (G, \star)$ de ordem n, um gerador **g** de G e um elemento $h \in G$, determinar o valor de x no intervalo $0 \leq x < n$, tal que $g^x = h$ em G.

Definição 1.37 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 $g^x \equiv h$ (mod p).

3 Aplicações da aritmética modular

A aritmética modular fornece uma base para vários sistemas de identificação, muito utilizados atualmente como por exemplo: em livros, cartões, produtos, e mais especificamente, na criptografia que dentre várias utilidades, tem papel fundamental na codificação e decodificação de mensagens. Aqui serão abordadas algumas das suas utilizações, de modo particular, em exemplos que serão utilizados como aplicações tanto Ensino Fundamental quanto no Médio.

3.1 Cadastro de pessoa física - CPF

O CPF é um documento que utiliza dígitos para identificar uma pessoa. Segundo [3], o uso de códigos numéricos tem muitas vantagens, por se tratar de uma identificação universal além de possibilitar registrar uma maior quantidade de informações que um nome. Composto por onze dígitos, onde os dois últimos são separados do restante por hífen (também chamados de dígitos de controle), têm como finalidade evitar fraudes ou erros de digitação e são gerados através dos noves primeiros dígitos.Para isso, é seguida a seguinte regra. Sejam a n-úpla $(a_1, a_2, a_3, a_4, a_5, a_6, a_7 a_8, a_9)$

formada pelos 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 estes produtos obtendo S_1, isto é, $S_1 = a_1.1 + a_2.2 + a_3.3 + a_4.4 + a_5.5 + a_6.6 + a_7.7 + a_8.8 + a_9.9$. O termo a_{10} será o resto da divisão de S_1 por 11 (caso seja 10, considera-se $a_{10} = 0$). O último dígito, a_{11}, que dependerá dos noves dígitos anteriores, será gerado de maneira análoga, isto é, multiplica-se 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 $S_2 = a_2.1 + a_3.2 + a_4.3 + a_5.4 + a_6.5 + a_7.6 + a_8.7 + a_9.8 + a_{10}.9$. O termo a_{11} será o resto da divisão de S_2 por 11. Da aritmética modular, os dígitos de controle satisfarão o sistema:
$S_1 - a_{10} \equiv 0 \pmod{11}$
$S_2 - a_{11} \equiv 0 \pmod{11}$.
Considerando, por exemplo, o C.P.F. $134.806.752 - XX$, calcula-se os dígitos de controle da seguinte forma:
$S_1 = 1.1 + 3.2 + 4.3 + 8.4 + 0.5 + 6.6 + 7.7 + 5.8 + 2.9 = 194$
Segue que $194 - a_{10} \equiv 0 \pmod{11}$
$a_{10} \equiv 7 \pmod{11}$
$a_{10} = 7$
$S_2 = 3.1 + 4.2 + 8.3 + 0.4 + 6.5 + 7.6 + 5.7 + 2.8 + 7.9 = 221$
$221 - a_{11} \equiv 0 \pmod{11}$
$a_{11} \equiv 1 \pmod{11}$
$a_{11} = 1$.

3.2 Cartão de crédito

Os cartões de crédito possuem dezesseis dígitos onde o primeiro e o segundo dígitos têm a função de distinguir a função como uso para compras em geral ou distinção entre bancos; do sétimo ao décimo quinto são os algarismos responsáveis pela identificação do cliente e o último algarismo é calculado através dos anteriores, análogo ao dígito de controle do cpf.

Figura 1: Cartão de crédito no formato mais utilizado

O cálculo é realizado do seguinte modo: considere um cartão de crédito com dezesseis dígitos denotados por $(a_1, a_2, \ldots, a_{16})$, onde $1 \leq n \leq 16$. Realizam-se duas somas, onde a primeira contém a soma de todos os dígitos em posições ímpares multiplicados por 2, isto é, $S_1 = (a_1 + a_3 + \ldots + a_{15}).2$ e a segunda soma entre os elementos de posições pares, ou seja, $S_2 = a_2 + a_4 + \ldots + a_{14}$. 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, isto é,
$S + a_{16} \equiv 0 \pmod{10}$.
Por exemplo, considerando um cartão de crédito com o número $441643218765901X$, calcula-se o último dígito da seguinte forma: $S1 = (4 + 1 + 4 + 2 + 8 + 6 + 9 + 1).2 = 70$

$S_2 = 4 + 6 + 3 + 1 + 7 + 5 + 0 = 26$
$S = S_1 + S_2 = 70 + 26 = 96$
$96 + a_{16} \equiv 0 \pmod{10}$
Portanto, o último dígito que validará o cartão será $a_{16} = 4$.

3.3 Código de barras

O código de barras, 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).

Figura 2: Código de Barras UPC - Fonte [4]

"Em uma definição técnica, o código de barras é uma representação gráfica de dados que permite rápida captação 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" [4]. Em um código de barras, os três primeiros dígitos representam o código do país, os próximos quatros referem-se ao código da empresa, os cinco números posteriores informam o código do produto e o último representa o dígito verificador.Na sua leitura, é aferida 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 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 1. Tal fato foi necessário para que um mesmo leitor realizasse leituras tanto no sistema UPC quanto no EAN-13.O código EAN 13 é uma combinação única de números com 13 dígitos para identificar um objeto ou produto com base em um sistema europeu ("EAN" que significa Numeração Européia de Artigos tradução de "European Article Number"). Ele também é chamado hoje de GTIN 13 (Global Trade Item Number) na nova nomenclatura em que é utilizada[5].

Na tabela 1, os números do lado esquerdo dependem da quantidade par ou ímpar de algarismos "1"para serem identificados, e com essa classificação gera-se o primeiro algarismo do código de barras, seguindo a sequência.

Considerando o modelo EAN−13, descrito na tabela 2, uma sequência de treze dígitos $\alpha = (a_1, a_2, \ldots, a_{12})$ e um vetor w= $(1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3)$, para determinar o valor do dígito verificador a_{13}, primeiramente calcula-se o produto escalar $\alpha \cdot w = a_1.1 + a_2.3 + a_3.1 + a_4.3 + \ldots + a_{12}.3$. O dígito verificador será a soma do produto escalar $\alpha \cdot w$ com a_{13} e $\alpha \cdot w - a_{13} \equiv 0 \pmod{10}$. Por exemplo, no código de barras $600580965503X$, calcularemos o seu dígito verificador. Considerando a sequência com o vetor $\alpha = (6, 0, 0, 5, 8, 0, 9, 6, 5, 5, 0, 3)$ e o vetor fixo

Tabela 1: Sequência de dígitos do código de Barras

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

Tabela 2: Sequência binária de dígitos no sistema EAN-13

Dígito Inicial	1.	2.	3.	4.	5.	6
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

w= $(1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3)$, então o produto escalar será:
$\alpha \cdot w = 6.1 + 0.3 + 0.1 + 5.3 + 8.1 + 0.3 + 9.1 + 6.3 + 5.1 + 5.3 + 0.1 + 3.3 = 75.$
Assim:
$\alpha \cdot w - a_{13} \equiv 0 \pmod{10}$
$75 - a_{13} \equiv 0 \pmod{10}$
$75 - a_{13} = 10.q$, com $q \in Z$
Logo $a_{13} = 5$. Portanto, o dígito verificador é 5.

3.4 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, dentre os quais destacam-se : gregoriano, hebraico, islâmico, indiano, chinês, persa, bahaí, 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 [6]. O calendário mais utilizado atualmente é o gregoriano criado na Europa em 1582, por incentivo do papa Gregório XIII, em substituição ao juliano. Dentre algumas curiosidades, uma das mais citadas, está em prever em qual dia da semana, ocorrerá determinada data. De forma geral, um ano

no calendário gregoriano possui 365 dias, 7 dias na semana, utilizando a aritmética modular, basta calcular o resto: $365 \equiv 1 \pmod 7$, ou seja, em um ano comum, a data atual será transferida para o dia posterior da semana, no ano posterior. No caso do ano bissexto, calcula-se o resíduo, sendo neste caso $366 \equiv 2 \pmod 7$. Portanto, deduz-se que em um ano bissexto, uma determinada data avançaria dois dias na semana. Embora pareça coerente, está incorreto pois, o dia adicional é acrescido no final do mês de fevereiro, posterior ao dia 28. O problema fica um tanto complicado quando busca-se uma data em um intervalo maior de anos. Considerando este 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.
$S(d, m, A) = d + 1 + [\frac{13m-1}{5}] + A + [\frac{A}{4}] - [\frac{A}{100}] + [\frac{A}{400}] \pmod 7$.
onde d representa o dia, m = mês e A = ano. Antes do algoritmo, torna-se necessária uma definição.

Definição 1.38 Dados $a, b \in N$, define-se $[\frac{a}{b}]$ como o maior inteiro menor ou igual ao número $\frac{a}{b}$, com $b \neq 0$.

O algoritmo é uma função de três variáveis: dia, mês e ano.Como os meses tem nomes, no algoritmo associam-se números da seguinte forma: março = 1, abril = 2,. . ., janeiro = 11 e fevereiro = 12, A ano e $S(d, m, A)$, 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, ou seja, $d = 16$, $m = 5$ e $A = 1957$,tem-se:

$S(16, 5, 1957) = 16 + 1 + [\frac{(13.5-1)}{5}] + 1957 + [\frac{1957}{4}] - [\frac{1957}{100}] + [\frac{1957}{400}] \pmod 7$
$S(16, 5, 1957) = 2460 \pmod 7$.
Então
$2460 \equiv 3 \pmod 7$.
Logo, $S(16, 5, 1957) = 3$ e portanto o dia da semana que ocorreu em 16 de julho de 1957 foi uma terça-feira.

3.5 Criptografia

A criptografia (do grego kryptós = escondido e gráphien = escrita) é uma área da criptologia que estuda princípios e técnicas para comunicação segura na presença de terceiros. Mas geralmente, a criptografia refere-se à construção e análise de protocolos que impedem terceiros, ou o público, de lerem mensagens privadas[7]. Muitos aspectos em segurança da informação, como confidencialidade, integridade de dados, autenticação e não-repúdio são centrais à criptografia moderna. A criptografia moderna existe na interseção das disciplinas de matemática, ciência da computação, engenharia elétrica, ciência da comunicação e física. Aplicações de criptografia incluem comércio eletrônico, cartões de pagamento baseados em chip, moedas digitais, senhas de computadores e comunicações militares [8]. 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 [9]. No período pós-guerra as empresas começaram a utilizar técnicas de criptografia com a finalidade de proteger seus dados,

promovendo um grande desenvolvimento além de fins militares. Com o impulso 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, isto é,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 exige uma chave diferente a cada par de indivíduos. Portanto as chaves devem ser distribuídas aos pares (emissor e receptor) tornando-a vulnerável, enquanto que na chave pública, a chave usada pode ser de conhecimento público e apenas utilizada para decodificá-la pelo destinatário da mensagem. Com a popularização da 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. A seguir, serão apresentados os dois métodos criptográficos de chave pública mais conhecidos: modelos RSA e El Gamal, descrevendo cada um e e sua utilização na aritmética modular.

3.5.1 Modelo RSA

Descrito em [10] como o mais conhecido dos métodos de criptografia de chave pública, o RSA, cuja a sigla corresponde às iniciais dos inventores do código que foi inventado em 1977 por R. L. Rivest; A. Shamir e L. Adleman, (M.I.T.) e tem sua base na Teoria dos Números. As 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: $\varphi(n) = (p-1).(q-1)$;
4. Escolha um inteiro e tal que $1 < e < \varphi(n)$, de forma que e e $\varphi(n)$ sejam primos entre si;
5. Calcule $d.e \equiv 1 \bmod \varphi(n)$, ou seja, d é o inverso multiplicativo de **e** mod $\varphi(n)$.
Logo a chave pública é o par (n, e) e a chave privada é o terno (p, q, d).
Para cifrar uma mensagem m, onde $1 < m < n-1$, em 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 cifrada c, usando a respectiva chave privada do receptor n e d, basta resolver a equação: $c^d \equiv m$ mod n.

Definição 1.39 Define-se bloco b como um trecho de uma sequência numérica em que o primeiro algarismo deve ser diferente de zero e $b < n$, $n = p.q$, com p e q primos.

Definição 1.40 Dado um bloco b, denomina-se codificação de b, denotado por $C(b)$, a seguinte expressão $C(b) \equiv b^3$ (mod n).

Definição 1.41 Dada uma codificação $C(b)$, denomina-se de decodificação, a expressão $D(C(b)) \equiv (C(b))^d$ (mod n), onde **d** é o inverso multiplicativo de um número inteiro **e** tal que $1 < e < \varphi(n)$ mod $\varphi(n)$, isto é, $d.e \equiv 1 \bmod \varphi(n)$.

Demonstração do 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.
$D(C(b)) \equiv b$ (mod n).
Pela definição de D e C, segue que:
$C(b) \equiv b^3$ (mod n)
$D(a) \equiv ad$ (mod n).
Substituindo, temos que:
$D(C(b)) \equiv D(b^3) \equiv b^{3d} \equiv b$ (mod n).

Por definição, $3d \equiv 1$ (mod $(p-1).(q-1)$), onde $3d = 1+k(p-1)(q-1)$ com $k \in Z$, calcula-se os resíduos de b^{3d} mod(p) (e mod(q)), usando o teorema do resto chinês, afim de obter os resíduos mod(n). Como $n = p.q$, com p e q primos, calcula-se 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:
$b^{3d} \equiv b.b^{(p-1)k.(q-1)}$ (mod p).
Como p não divide b, temos que $b^{p-1} \equiv 1$ (mod p). Substituindo na congruência acima, obtém-se:
$b^{3d} \equiv b.b^{(p-1).k.(q-1)} \equiv b$ (mod p).
Se p divide b, é trivial, logo $b^{3d} \equiv b$ (mod p).
Sendo análogo para q, obtemos o par de congruências $b^{3d} \equiv b$ (mod p).
$b^{3d} \equiv b$ (mod q).
Logo b é uma solução de
$x \equiv b$ (mod p)
$x \equiv b$ (mod 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 $b^{3d} \equiv b$ (mod $p.q = n$), provando a congruência.

3.6 Método El Gamal

Desenvolvida pelo egípcio Taher El Gamal (1985) este método é outro de chave pública bastante empregado. De acordo com [11], 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), com p primo, sendo que o Teorema da Raiz Primitiva [12] garante que tais grupos são necessariamente cíclicos.Ainda, o método pode ser generalizado para utilizar quaisquer outros grupos abelianos finitos cíclicos. 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 $a \equiv r^x$ (mod p), onde r é a raiz primitiva de U(p).

Tabela 3: Sequência binária de dígitos no sistema EAN-13

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

Tabela 4: Sequência binária de dígitos no sistema EAN-13

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

Os valores r, p e a são valores públicos e o valor x é o segredo da chave. A mensagem é convertida em uma sequência de dígitos, utilizando um procedimento, exemplificado através das tabela 3 e 4, formando um bloco K, se $K \leq p$. A mensagem deve ser dividida em blocos menores M, tal que $M \leq p-1$. Cada sub-bloco será encriptado separadamente, escolhendo-se um número natural $2 \leq y \leq p-2$ aleatoriamente. Calcula-se $r^y \equiv b$ (mod p) e o código será obtido por meio de $C \equiv M.a^y$ (mod p), resultando na dupla cifrada (b, C).O procedimento para decifrar a mensagem, utilizará a chave privada x, em $P \equiv C.b^{(p-1-x)}$ (mod p).

3.7 Demonstração do El Gamal

A mensagem cifrada é o par (b, C), onde $C \equiv M.a^y$ mod (p) e $b \equiv r^y$ mod (p), então
$P \equiv C.b^{(p-1-x)}$ mod (p)
$P \equiv (M.a^y)(r^y)^{(p-1-x)}$ mod (p)
Mas, $a \equiv r^x$ mod (p), logo
$P \equiv (M.r^x)^y(r^{(y(p-1)-xy)})$ mod (p)
$P \equiv M.r^{(p-1)y}$ mod (p).
Como r é raiz primitiva de p, então $r^{(p-1)} \equiv 1$ mod (p).

4 Aplicações para o ensino médio e fundamental

Como aplicações da Criptografia, foram propostas as seguintes atividades para alunos de ensino fundamental e médio, descritas a seguir:

1. Matrizes e o cálculo dos dígitos verificadores do CPF para alunos do 2^o ano do Ensino Médio;
2. Código de Barras para alunos do 7^o ano do Ensino Fundamental;
3. Análise de futuras datas em calendários para o 1^o ano do Ensino Médio;
4. Criptografia para alunos do 6^o ano do Ensino Fundamental.

4.1 Matrizes e o cálculo dos dígitos verificadores do cpf para alunos do 2^o ano do ensino médio

No início desta atividade realizou-se uma abordagem sobre caracterização de matrizes e operações de adição, subtração e multiplicação por um escala. Fazendo um levantamento das dúvidas, foi proposta uma discussão com a sala, estruturando um resumo na lousa.Após a recapitulação, a sala se reuniu em grupos de 5 ou 6 pessoas, sendo proposto um problema inicial.

Para avaliar o conhecimento deste público em matrizes foi proposto o seguinte problema: (VUNESP-2009) Uma rede de comunicação tem cinco antenas que transmitem uma para outra, conforme a 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.

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

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

1. De $b_{41} = 0$, significa que a antena 4 não transmite para a antena 1.
2. De $b_{41} = 1$, significa que a antena 4 transmite para a antena 1.
3. De $b_{41} = 3$, significa que a antena 4 transmite para a antena 1.
4. De $b_{41} = 3$, isso significa que existem 3 maneiras diferentes da antena 4 transmitir para a antena 1, usando apenas uma retransmissão entre elas.No entanto, $b_{41} = 3$, não tem significado, pois b_{ij} só pode valer 0 ou 1.

Durante a multiplicação de matrizes, um grupo desenvolveu um esquema, com o auxílio do docente, que facilitava o processo [13] e foi posteriormente adaptado conforme Figura 3.
Quanto ao produto de matrizes $C = A.B$, a imagem representa duas matrizes quadradas de ordem

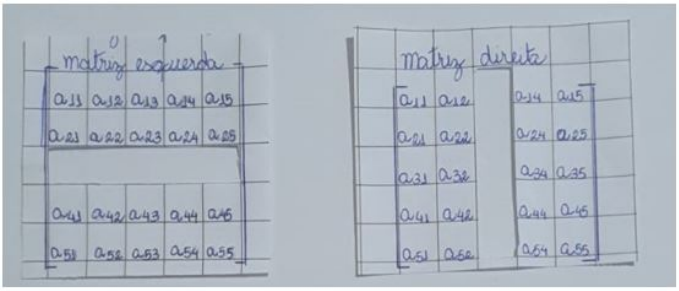

Figura 3: Esquema de multiplicação de matrizes

5 com uma linha recortada na matriz esquerda e uma coluna 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, além de auxiliar na compreensão da operação. Para o estudo do dígito verificador, foi proposto o seguinte problema:
(ENEM-2009) Para cada indivíduo, a inscrição no Cadastro de Pessoas Físicas (C.P.F.) é composto de 9 algarismos mais 2 dígitos verificadores, d_1 d_2, calculados da seguinte forma:

1. 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);
2. 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, $d_1 = 0$, caso contrário, $d_1 = (11 - r)$;
3. 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, $d_2 = 0$ se o resto s da divisão por 11 das somas das multiplicações for 0 ou 1, caso contrário, $d_2 = (11 - s)$.

Outro problema:
João perdeu seus documentos, inclusive o cpf e, ao registrar a perda, não lembrava dos dígitos verificadores, apenas dos 9 dígitos iniciais, 123.456.789. Pergunta-se: quais seriam os dígitos verificadores d_1 e d_2.
A resolução do cálculo do cpf, utilizando a multiplicação de matrizes, não apresentou grandes problemas, indicando uma nova estratégia de introduzir um conceito ao aluno, propondo um problema, uma estratégia para solucioná-lo, conduzindo-o finalmente à resolução do problema.

4.2 Cartão de crédito para alunos do 7^o ano do ensino fundamental

Para esta atividade, foram propostos vários problemas, dentre os quais, destacam-se:

1. Qual a finalidade do dígito validador de um cartão de crédito?

2. José perdeu seu cartão de crédito e precisou cancelá-lo. Ao verificar o local onde guardava algumas informações, notou que o último dígito do número de seu cartão estava ilegível. Tendo o cartão o número 123456789123456..., calcule o dígito verificador.

Nestas atividades, os alunos se depararam com um conteúdo de muitos cálculos, demonstrando-se uma boa ferramenta de aprendizado onde, além da realização de diferentes tipos de algoritmos que envolvem as operações fundamentais, abordou-se alguns tópicos sobre propriedades operatórias,etc. A organização da sala em grupos, constituiu-se uma boa estratégia, devido aos próprios alunos se auxiliarem, compreenderem suas dúvidas e por fim, aplicar conceitos envolvendo a álgebra, variáveis e equações.

4.3 Análise de datas futuras em calendários para o 1^o ano do ensino médio

Inicialmente, foram propostos os seguintes problemas:

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

2. 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?

3. Calcule o dia da semana que você nasceu.

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

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

Uma estratégia que demonstrou-se efetiva, foi a leitura realizada dos problemas, visto a maior participação dos alunos com questões sobre significados de algumas palavras. Ao final, muitos se mostraram interessados na resolução dos problemas e no debate dos itens propostos. Quando iniciaram as discussões relativas às datas, grande parte dos alunos utilizaram o calendário em seu celular para verificar a resposta do problema. A partir da intervenção do mediador, questionando sobre outra forma de resolver a questão utilizando as operações básicas e, após retomar as características do calendário gregoriano, surgiram as primeiras tentativas de solucionar os problemas. Ao elaborarem uma solução, o mediador questionava cada parte do procedimento. Para verificar a validade, foi solicitado que aplicassem o mesmo procedimento nos anos seguintes e conferissem com calendários futuros para validar o raciocínio. Foram obtidas estratégias diferentes de solução, mas grande parte dos grupos apresentaram dificuldades nas situações do dia referente ao ano de 2024 (ano bissexto). Através da apresentação de um método desenvolvido por um grupo, todos obtiveram um resultado satisfatório, demonstrando a compreensão do tema. Ao resolver o problema 2, todos

os grupos conseguiram replicar o mesmo raciocínio utilizado no problema anterior. Ao conferirem as respostas, verificou-se que estavam incorretas para a data referente à 2024. Concluiu-se que a data do aniversário de Beatriz avança um dia da semana, pois ocorre antes do 29 de fevereiro. No entanto, houve muitos questionamentos se existiria um método mais simples, devidas as condições para resolver este problema, criando o ambiente perfeito para introduzir o algoritmo de Zeller (figura 4) para a resolução dos problemas 3,4 e 5. Embora inicialmente, alguns demonstrassem dificuldades com o algoritmo da divisão, a atividade transcorreu de maneira satisfatória.

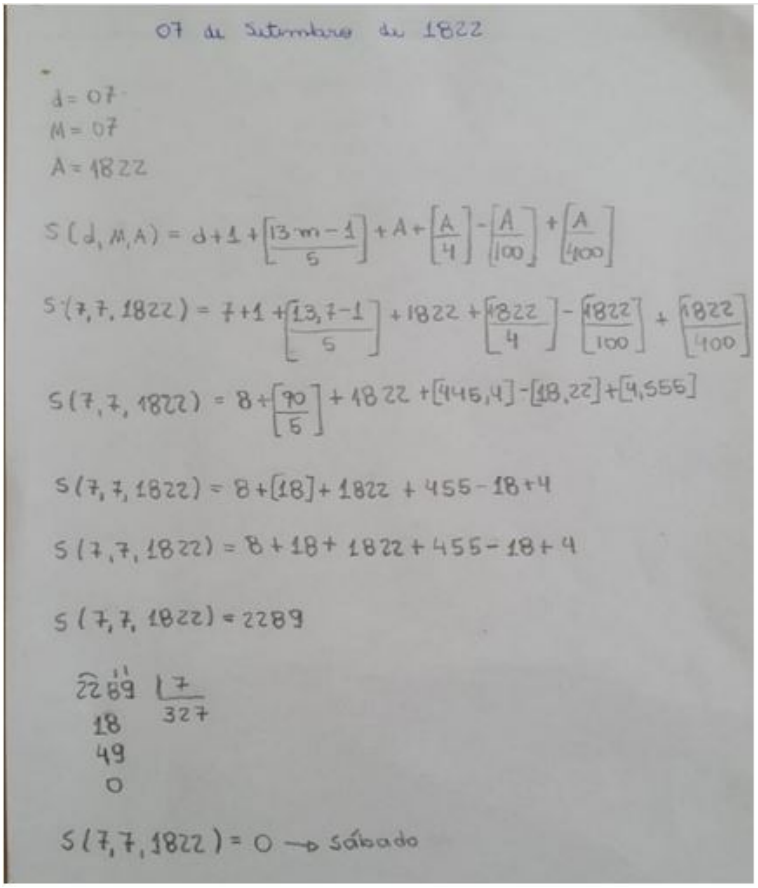

Figura 4: Utilização do algoritmo de Zeller - problema 4

4.4 Criptografia para alunos do 6^o ano do ensino fundamental

Para esta atividade, foi projetada a seguinte frase:
"Sem dvdúia, vcoê é cpaaz ler e etneednr etse ttexo com lreats tcaorads e plaarvas ftalndao."
É possível compreender esta 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. Foram propostas outras atividades:

1. Descubra o segredo do código utilizado na seguinte frase:"Tf wpdf dpotfhvf mfs jttp, foubp eftdpcsjv p tfhsfep".

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

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

Tabela 5: Tabela Letra X Dígito

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

Tabela 6: Tabela Letra X Dígito

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

A frase encriptada da introdução demostrou-se uma ferramenta ineficaz em algumas salas, devido a defasagem na formação de alguns alunos. Para contornar tais obstáculos, realizou-se uma avaliação diagnóstica com a finalidade de identificar os alunos que apresentaram dificuldades, pois de acordo com [14], há necessidade de correção de rotas no planejamento do ensino de Matemática em nível fundamental e médio, prática fundamental para a atividade docente. Adaptar a frase introdutória, substituindo-a por uma palavra simples, trouxe maior participação e aproveitamento na condução da atividade. A leitura compartilhada sobre textos auxiliares, abordando o tema, despertou maior interesse nos alunos. Com isso, pode-se discutir as características da criptografia, avaliando sua função, quando é empregada, onde é usada atualmente e até sobre o grau de dificuldade em decifrar certos códigos. No problema 1, embora alguns grupos conseguissem realizar rapidamente, outros gastaram mais tempo para desvendar. Quando questionados sobre o segredo, o símbolo $\check{b}$ conduziu ao raciocínio correto, pois só poderia ser as vogais a ou o, por serem 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, como pode ser observado na Figura 5.

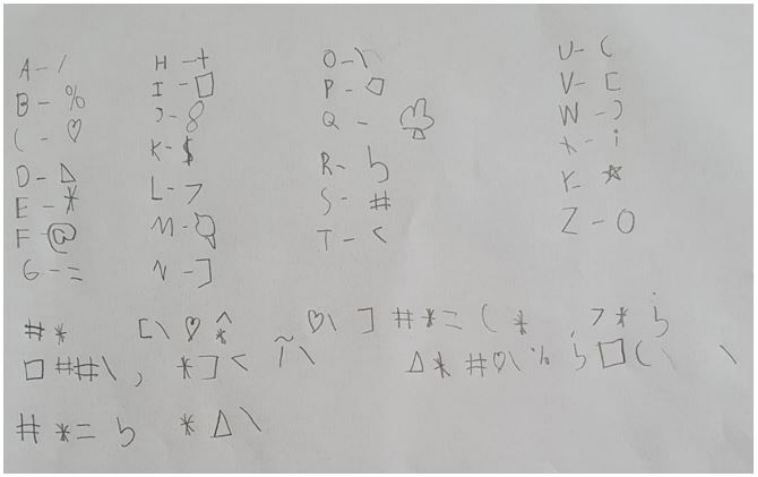

Figura 5: Código criado por aluno

5 Considerações finais

Durante a elaboração dos planos de aula, priorizou-se uma aprendizagem significativa, que segundo [15], é necessária para desenvolver táticas que motivem educandos, fazendo com que o aprendizado deixe de ser passivo e se torne ativo. Portanto, a estruturação de um plano de aula e planejamento de ações tornam-se ferramentas indispensáveis para o trabalho docente. Dentro desta óptica, foram utilizadas abordagens de criptografia utilizando a aritmética modular, demostrando-se efetivas no ensino, aprendizagem e na formação contínua do professor. Foi observado que planos de aula que adotaram uma leitura inicial sobre determinados temas, resultou em maior participação dos discentes. A utilização de fatos históricos da matemática e realização de atividades interdisciplinares demonstrou uma boa estratégia para maior participação. Apesar de abordar habilidades específicas para cada série de ensino, as atividades propostas demostraram-se excelentes oportunidades de abordar conteúdos defasados, sanando deficiências da progressão continuada, observando uma melhora e um incentivo ao aprendizado de matemática e demais habilidades do público alvo. Por fim, observou-se que a defasagem, na formação do aluno, pode ser sanada utilizando a metodologia empregada em várias disciplinas com a promoção de aulas estruturadas, contemplando conteúdos não oferecidos pela grade curricular, proporcionando uma nova possibilidade para este público.

Referências

[1] EUCLID. **The thirteen books of Euclid's elements**. Translated from the text of Heiber. Introduction and commentary Thomas L. Health. 2nd ed. New York: Dover Publications, 1956. v. 1.

[2] TERANISHI, K.; SHIMADA, N.; KOGISO, K. Stability-guaranteed dynamic El Gamal cryptosystem for encrypted control systems. **IET Control Theory & Applications**, v. 14, n. 16, p. 2242-2252, 2020.

[3] MACHADO, D. A. **Uma abordagem de dígitos verificadores e códigos corretores no ensino fundamental**. 2016. 63 f. Dissertação (Mestrado Profissional em Matemática) - Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos, 2016.

[4] ESQUINCA, J. C. P. **Aritmética:** códigos de barras e outras aplicações de congruências. 2013. 63 f. Dissertação (Mestrado Profissional em Matemática) - Centro de Ciências Exatas e Tecnologia, Universidade Federal de Mato Grosso do Sul, Campo Grande, 2013.

[5] SOARES, A.; VASCONCELLOS, H. Códigos de barras: a presença visível da automação. **Revista de Administração de Empresas** [online], v. 31, n. 1, p. 59-68, 1991. Disponível em: https://doi.org/10.1590/S0034-75901991000100009. Acesso em: 5 jun. 2022.

[6] RODRIGUES JUNIOR, M. A. **Os calendários e a sua contribuição para o ensino da astronomia**. 2012. 128 f. Dissertação (Mestrado em Ensino de Astronomia) - Faculdade de Ciências, Universidade do Porto, Porto, 2012.

[7] BELLARE, M.; ROGAWAY, P. **Introduction to modern cryptography**. [*S. l.: s. n.*], 2005. Disponível em: https://web.cs.ucdavis.edu/ rogaway/classes/227/spring05/book/main.pdf. Acesso em: 31 maio 2022.

[8] KNUDSEN, J. **Java cryptography**. Sebastopol, CA: O'Reilly, 1998.

[9] SILVEIRA, J. P. C. **Aplicações de criptografia baseada em identidade com cartões de identificação eletrônica**. 2013. 80 f. Dissertação (Mestrado em Engenharia Informática)-Universidade da Beira Interior, Covilhã, 2013.

[10] COUTINHO, S. C. **Criptografia**. Rio de Janeiro: IMPA, 2015.

[11] SCHECHTER, L. M. **Uma introdução à criptografia de chave pública através do método El Gamal**. São Carlos: SBMAC, 2014 (Notas em Matemática Aplicada; v. 77).

[12] COHEN, H. **A course in computational algebraic number theory**. Berlin: Springer-Verlag, 1993.

[13] MONTANHER, J. F. **Introdução da criptografia no ensino básico sob a óptica da aritmética modular**. 2022. 63 f. Dissertação (Mestrado em Matemática) - Faculdade de Ciências, Universidade Estadual Paulista "Julio de Mesquita Filho", Bauru, 2022.

[14] RABELO, F. B. **Análise da avaliação diagnósticada aprendizagem do estado de Goiás:** um olhar sobre a área de Matemática. 2018. 98 f. Dissertação (Mestrado em Matemática) - Unidade Acadêmica Especial de Matemática e Tecnologia, Universidade Federal de Goiás, Catalão, 2018.

[15] BRUINI, E. C. **Aprendizagem significativa**. Brasil Escola UOL, 2022. Disponível em: https://educador.brasilescola.uol.com.br/trabalho-docente/aprendizagem-significativa.htm. Acesso em: 10 jun. 2022.