DEPARTAMENTO DE
MATEMÁTICA
UNIVERSIDADE FEDERAL DE OURO PRETO

PROFMAT
MESTRADO PROFISSIONAL
EM MATEMÁTICA EM
REDE NACIONAL

Francisca D. A. S. M. Lage

UM ESTUDO DE ARITMÉTICA MODULAR PARA A EDUCAÇÃO BÁSICA

Ouro Preto - MG, Brasil

Fevereiro de 2018

Francisca D. A. S. M. Lage

UM ESTUDO DE ARITMÉTICA MODULAR PARA A EDUCAÇÃO BÁSICA

Dissertação de mestrado apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional da Universidade Federal de Ouro Preto, como parte dos requisitos para obtenção do título de Mestre.

Universidade Federal de Ouro Preto (UFOP)

Instituto de Ciências Exatas e Biológicas (ICEB)

Departamento de Matemática (DEMAT)

Mestrado Profissional em Matemática em Rede Nacional (PROFMAT)

Orientador: Prof. Dr. Thiago F. Santos

Coorientador: Prof. Dr. Sebastião M. Xavier

Ouro Preto - MG, Brasil

Fevereiro de 2018

L135e Lage, Francisca Daniella Andreu Simões Moraes.
Um estudo de aritmética modular para a educação básica [manuscrito] / Francisca Daniella Andreu Simões Moraes Lage. - 2018.
61f.: il.: color; tabs.

Orientador: Prof. Dr. Thiago Fontes Santos.
Coorientador: Prof. Dr. Sebastião Martins Xavier.

Dissertação (Mestrado) - Universidade Federal de Ouro Preto. Instituto de Ciências Exatas e Biológicas. Departamento de Matemática. Programa de Pós-Graduação em Matemática em Rede Nacional.
Área de Concentração: Matemática com oferta nacional.

1. Aritmética. 2. Congruências (Geometria). 3. Criptografia. I. Santos, Thiago Fontes. II. Xavier, Sebastião Martins. III. Universidade Federal de Ouro Preto. IV. Titulo.

CDU: 511.1

Catalogação: www.sisbin.ufop.br

Um Estudo De Aritmética Modular Para A Educação Básica

Autor(a): Francisca Daniella Andreu Simões Moraes Lage

Dissertação defendida e aprovada, em **20 de Fevereiro de 2018**, pela banca examinadora constituída pelos professores:

Thiago Fontes Santos - Orientador
Universidade Federal de Ouro Preto

Sebastião Martins Xavier - Coorientador
Universidade Federal de Ouro Preto

Gilberto Duarte Cuzzuol
Universidade Federal de Itajubá

Rodrigo Geraldo do Couto
Universidade Federal de Ouro Preto

Dedico este trabalho aos meus alunos de ontem, hoje e amanhã. Que eles possam entender o verdadeiro sentido da educação!

Agradecimentos

Agradeço a Deus por não deixar que eu desanimasse, mesmo nos momentos mais difíceis, colocando em mim bastante força de vontade e coragem para enfrentar as longas viagens e os grandes desafios de ficar longe das minhas pequenas filhas. Este curso me mostrou o quanto a fé nos faz crescer em sabedoria, misericórdia e graça.

A Universidade Federal de Ouro Preto pela oportunidade de fazermos o curso.

Aos professores do curso, em especial Thiago Santos, Sebastião Martins, Ediney, Gil, Monique e Jamil por todo empenho, preocupação e paciência. Também aos professores da banca, Gilberto Duarte e Rodrigo Couto, pelas sábias palavras e grande valia nas sugestões dadas nas correções de meu trabalho.

Aos meus pais Encarnacion e Astrogildo, meus irmãos Gustavo e Guilherme, meu sogro Ciro e minha sogra Leice pelas palavras de afeto e compreensão nas ausências. Devo muito a vocês pela grande força quanto à criação de minhas filhas.

A Isadora e Marina, minhas filhas, e ao meu esposo Júnior por tantas vezes que deixei de estar com eles por causa dos estudos.

Aos lindinhos Dani, Mari, Fabian e Lívia pelo carinho e parceria; ao Willsander pela grande ajuda, ao Gilberto, secretário do PROFMAT e aos colegas de turma, em especial: Renato, Marcelo, Márcio, Juvenal, Geraldo, Bruno e Rodney pelo aprendizado, companheirismo e trocas de conhecimento.

A Karine pelas voltas para João Monlevade, sempre com palavras doces e de perseverança.

Também agradeço aos meus colegas de trabalho e aos irmãos da igreja pelas palavras de incentivo e pelas orações.

Resumo

Este estudo é voltado à aritmética modular e pretende ser uma contribuição para o trabalho de professores da Educação Básica. O mesmo tem início com uma fundamentação teórica, servindo de base para as aplicações desta área da matemática. Tais aplicações compõem o capítulo dois, atuando com congruência em código de barras, ISBN, cartões de crédito, CPF, além de relatar sobre o funcionamento da criptografia e do método RSA. Em sua última parte, o trabalho mostra atividades realizadas em sala de aula. O intuito é de que elas sirvam como ferramentas a serem usadas e adaptadas por professores, já que as mesmas quase não aparecem em livros didáticos.

Palavras chave: aritmética modular, congruência, criptografia.

Abstract

This study is focused on modular arithmetic and aims to be a contribution to the work of teachers of Elementary Education. The same begins with a theoretical foundation, serving as the basis for the applications of this area of mathematics. Such applications make up chapter two, working with congruence in bar code, ISBN, credit cards, CPF, as well as reporting on the operation of encryption and the RSA method. In his last part, the work shows activities carried out in the classroom. The intention is that they serve as tools to be used and adapted by teachers, since they hardly appear in didactics books.

Keywords: modular arithmetic, congruence, cryptography.

Sumário

Introdução

A aritmética modular ou aritmética dos restos, desenvolvida por Argand Gauss, é um grande instrumento no que tange à teoria dos números, envolvendo o conceito de congruência e operador módulo no conjunto dos números inteiros. Com isso, a motivação para a escolha do tema deste trabalho foi o interesse em compreender as aplicações da aritmética modular na educação básica, além de perceber o quanto é importante sua função no cotidiano dos nossos alunos. Isto porque o ensino de alguns tópicos da aritmética dos restos é muitas vezes dado apenas por meio de abordagens introdutórias, focando geralmente em regras de divisibilidade, mínimo múltiplo comum e máximo divisor comum, dentre outros.

Com este estudo esperamos que outros educadores possam compreender que algumas áreas da teoria dos números possibilitam muito a aquisição de novas ferramentas para o entendimento de diferentes problemas. Para mais, trazemos propostas de atividades focadas nos ensinos fundamental e médio, objetivando tornar os conteúdos matemáticos menos abstratos e mais interessantes aos alunos.

A estrutura de nosso trabalho é composta por três capítulos. O primeiro deles traz a fundamentação teórica, servindo de base para o entendimento dos cálculos e das aplicações mostradas posteriormente. Nele enfatizamos o conceito e a importância dos números primos, dissertamos sobre a divisão nos inteiros, concentramos nos estudos das congruências e demonstramos alguns teoremas pertinentes ao estudo aqui apresentado.

O capítulo dois está voltado a algumas aplicações da aritmética modular. No mesmo mostramos o uso de congruência em código de barras, cadastro de pessoa física, cartões de crédito, códigos em publicações de livros e dígitos de verificação. Apresentamos também uma aplicação da criptografia de forma clara e bastante acessível ao entendimento de docentes e discentes, assim como estampamos a importância do método RSA no que se refere à segurança

de informações em redes sociais.

Já o terceiro capítulo relata sobre as práticas feitas em sala de aula com a utilização de congruência no algoritmo de Zeller em calendários. Colocamos também atividades envolvendo código de barras e cadastro de pessoa física, ambos trazidos pelos alunos. Nesse capítulo ainda foi feito um estudo teórico envolvendo criptografia, sua importância e a aplicação de cifras para codificar e decodificar mensagens.

Por fim, chegamos à conclusão com as considerações finais e algumas propostas visando melhorias nas práticas de sala de aula, relativas ao ensino da aritmética dos restos.

CAPÍTULO 1

Fundamentos Teóricos

Em nossos estudos sobre a aritmética modular veremos que a mesma é um vasto campo da matemática que se ocupa da resolução de operações envolvendo restos de divisões entre números inteiros. Assim, dentro deste campo, iremos desenvolver noções elementares sobre divisibilidade a fim de prestar esclarecimentos para as aplicações que iremos expor no próximo capítulo. Dentre as principais definições e resultados que apresentaremos, destacamos: Máximo Divisor Comum-MDC, Mínimo Múltiplo Comum-MMC, Função $\varphi(n)$ de Euler e o Pequeno Teorema de Fermat-PTF. Outros resultados, bem como as respectivas provas dos teoremas podem ser vistos e aprofundados em [4, 10, 2, 5].

Ao final estudaremos sobre congruências, via definição, uma vez que este tópico é a chave para criptografia RSA, mostrada no capítulo dois.

Neste trabalho estamos considerando tanto o conjunto dos números naturais ($\mathbb{N}$), quanto dos inteiros ($\mathbb{Z}$), e suas respectivas operações de adição ($+$) e multiplicação ($\cdot$), como já conhecidos.

1.1 Princípio da Boa Ordenação e Princípio da Indução Matemática

O grande matemático Giuseppe Peano enunciou no século XX axiomas que descrevem precisamente o conjunto dos números naturais. O último deles é chamado de Axioma da Indução. Este, juntamente com o Princípio da Boa Ordenação são bases de demonstrações que envolvem, dentre outros campos da aritmética, problemas de divisibilidade.

Esses dois princípios são equivalentes, ou seja, admitindo-se um deles é possível provar o outro. Aqui admitiremos o Princípio da Boa Ordenação e, na sequência, demonstraremos o

Princípio da Indução Matemática.

Teorema 1.1 (Princípio da Boa Ordenação)**.** *Todo subconjunto $S \subset \mathbb{Z}$ não vazio e limitado inferiormente possui menor elemento.*

Teorema 1.2 (Princípio da Indução Matemática)**.** *Seja $X \subset \mathbb{N}$ com as seguintes hipóteses:*

(i) $1 \in X$*;*

(ii) Dado $n \in \mathbb{N}$, se $n \in X$, então $n + 1 \in X$.

Logo, $X = \mathbb{N}$.

Demonstração. O que queremos provar é que sendo X um conjunto pertencente aos naturais e se 1 é elemento de X, com os sucessores de 1 também em X, então $X = \mathbb{N}$.

Seja $Y = \mathbb{N} - X$ e suponhamos que $Y \neq \emptyset$. Como $\mathbb{N}$ é bem ordenado, Y possui um menor elemento b_0 que é maior do que 1, em virtude da hipótese (i).

Como $b_0 - 1 \notin Y$, então $b_0 - 1 \in X$. Mas, pela hipótese (ii), $(b_0 - 1) + 1 = b_0 \in X$, o que é uma contradição e, portanto, Y não pode ser diferente de vazio e, sendo $Y = \mathbb{N} - X = \emptyset$, então temos que $X = \mathbb{N}$, como queríamos demonstrar. □

1.2 Divisibilidade

Segundo relata [5], como a divisão de um inteiro por outro nem sempre é possível, expressa-se essa possibilidade através da relação de divisibilidade. Quando não existir a relação de divisibilidade entre dois inteiros, ainda assim será possível efetuar uma divisão denominada divisão euclidiana, que veremos mais adiante.

Definição 1.1. *Dados $a, b \in \mathbb{Z}$, dizemos que a divide b se existir $k \in \mathbb{Z}$ tal que*

$$b = k \cdot a \tag{1.1}$$

Quando isto ocorre, denotaremos por $a \mid b$. Do contrário, escreveremos $a \nmid b$. É comum dizer que quando $a \mid b$ o número a é divisor de b ou que b é divisível por a.

Chamamos a atenção que $a \mid b$ é diferente de a/b ou $\dfrac{a}{b}$. Estas últimas formas de escrita são usadas para representar frações enquanto que $a|b$ representa a definição acima.

Apenas com esta definição podemos concluir várias propriedades, as quais sintetizamos na proposição a seguir, cuja prova pode ser visualizada em [4]:

Proposição 1.1. *Sejam a, b, c, d, m e n números inteiros.*

1. *Se* $a \mid b$ *e* $b \mid c$ *então* $a \mid c$.
2. *Se* $c \mid a$ *e* $c \mid b$ *então* $c \mid (am + bn)$.
3. $n \mid n$, $\forall n \neq 0$.
4. *Se* $d \mid n$ *então* $(ad) \mid (an)$.
5. *Se* $(ad) \mid (an)$ *e* $a \neq 0$ *então* $d \mid n$
6. $1|n$, $\forall n$.
7. $n|0$, $\forall n$.
8. *Se* $d|n$ *e* $n \neq 0$ *então* $|n| \geq d$.
9. *Se* $d|n$ *e* $n|d$ *então* $|n| = |d|$.

A fim de ilustrar a ideia de divisibilidade, vejamos o exemplo a seguir.

Exemplo 1.1. *Encontre todos os* n *inteiros positivos, tais que*

$$(n + 1) \mid (n^2 + 1).$$

Primeiro, note que $n^2+1 = (n^2-1)+2 = (n+1)(n-1)+2$. Agora, vamos mostrar a seguinte afirmação:

$$\text{Se } a \mid (b + c) \text{ e } a \mid b \text{ então } a \mid c.$$

De fato, se $a \mid (b + c)$ e $a \mid b$ então existem inteiros k_1 e k_2 tais que

$$\begin{aligned} b + c &= k_1 a \\ b &= k_2 a \end{aligned}$$

Daí, $c = (k_1 - k_2)a$ e portanto $a \mid c$.

Voltando ao exemplo, se n é tal que $(n + 1) \mid (n^2 + 1)$ então $(n + 1) \mid 2$. Segue que $n + 1 = 1$ ou $n + 1 = 2$. No primeiro caso, temos que $n = 0$ não pertence aos naturais. Por outro lado, se $n + 1 = 2$ então $n = 1$, único valor que satisfaz o pedido.

Agora, pensando na definição $a \mid b$, seria interessante supor a situação em que b não é múltiplo de a. Com isto em mente, existe um resultado deveras importante de teoria dos números, a saber, o Algoritmo da Divisão de Euclides, que enunciaremos a seguir com a sua respectiva prova. Como tal teorema fornece uma rotina para executar a divisão de a por b, ele é geralmente chamado de *Algoritmo da Divisão*. A prova que segue é a mesma feita em [10].

Teorema 1.3 (Algoritmo da Divisão de Euclides)**.** *Sejam* $a, b \in \mathbb{N}$*, com* $b < a$*. Então existem únicos* $q, r \in \mathbb{Z}$*, chamados respectivamente de quociente e resto, tal que*

$$a = bq + r \tag{1.2}$$

com $0 \leq r < b$.

Demonstração. Primeiramente devemos provar a existência e, após, a unicidade de tais q e r. Para provar a existência, considere o conjunto X abaixo definido

$$X = \{a - bx \in \mathbb{N} \cup \{0\} \,/\, x \in \mathbb{Z}\}$$

Evidentemente $X \neq \emptyset$, pois $x = 1$ e $a - b \in X$. Assim, existe um menor elemento que denotaremos aqui por $r = a - bq \in X$, para algum $q \in \mathbb{Z}$. Se $r = 0$ então $b \mid a$ e não temos mais nada a fazer. Suponha que $0 < r$. Temos que provar que $r < b$. Suponha que não, ou seja, $r \geq b$. Isto nos permite observar que

$$\begin{aligned} a - b(q+1) &= a - bq - b \\ &\geq r - b \\ &\geq 0 \end{aligned}$$

e portanto $a - b(q+1) \in X$. Além disso, como $-(q+1) < -q$, temos que

$$\begin{aligned} a - b(q+1) &< a - bq \\ &< r \end{aligned}$$

Mas isso não pode ocorrer, pois r é o menor elemento de X e portanto $r < b$.

Por fim, nos resta provar a unicidade de tais elementos. Vamos supor que existam dois pares q, q_1 e r, r_1, que atendam às condições dadas por (1.2) e no final concluiremos que são os mesmos. De fato, tomando os inteiros q_1 e r_1 que atendem (1.2), então temos que:

$$\begin{aligned} bq + r &= bq_1 + r_1 \\ b(q - q_1) &= r_1 - r \end{aligned}$$

Podemos dizer que $b \mid (r_1 - r)$. Como $r < b$ e $r_1 < b$, temos da equação dada acima que $0 < r_1 - r = b(q - q_1) < b$, o que é um absurdo.

□

Este teorema nos dá a possibilidade de particionar o conjunto $\mathbb{Z}$ em uma união finita de conjuntos infinitos de acordo com o resto da divisão por um certo $n \in \mathbb{N}$. Por exemplo, se $n = 2$ os restos possíveis são 0 ou 1 e podemos tomar dois conjuntos P e I com $\mathbb{Z} = P \cup I$ da seguinte forma:

$$P = \{2k \mid k \in \mathbb{Z}\} = \{\text{Conjunto dos números pares}\}$$

$$I = \{2k + 1 \mid k \in \mathbb{Z}\} = \{\text{Conjunto dos números ímpares}\}$$

Esta será a ideia básica que iremos abordar na seção 1.4.

Assumindo que seja do conhecimento do leitor os conceitos de múltiplos comuns e divisores, ao tomarmos dois inteiros a e b, queremos saber sobre seus divisores e múltiplos comuns. Ou seja, quem são os divisores simultâneos ou múltiplos simultâneos de a e b. De antemão é sabido que 1 é um divisor comum de a e b e também que ab é um múltiplo comum de a e de b.

Definição 1.2 (Máximo Divisor Comum - MDC)**.** *Dados dois números inteiros a e b, não simultaneamente nulos, dizemos que um inteiro d é o máximo divisor comum de a e b se:*

(i) $d \mid a$ *e* $d \mid b$*.*

(ii) Se existe um inteiro c tal que $c \mid a$ e $c \mid b$ então $c \leq d$.

Se d é o MDC de a e de b, o denotaremos por $d = (a, b)$. Uma consequência imediata da definição acima é que $d = (a, b) > 0$, além disso, temos que $(a, b) = (b, a)$.

Proposição 1.2. *Sejam a e b dois inteiros. Então valem as seguintes afirmações:*

(i) Se a é múltiplo de b , então $(a, b) = b$.

(ii) Se $a = bq + c$, $c \neq 0$, então o conjunto dos divisores comuns dos números a e b coincide com o conjunto dos divisores comuns dos números b e c.

Demonstração. Começaremos provando (i). Com efeito temos que todo divisor comum dos números a e b é divisor de b. Reciprocamente, usando que a é múltiplo de b, todo divisor de b também é um divisor de a, ou seja, um divisor comum dos números a e b. Portanto, o conjunto dos divisores comuns dos números a e b é o mesmo conjunto dos divisores de b. Mas, como o maior divisor de b é ele mesmo, então $(a, b) = b$.

Para a prova de (ii), usando o item (2) da Proposição (1.1), temos que todo divisor comum de a e b também divide c e, consequentemente, é divisor de b e c. Pela mesma razão todo divisor comum de b e c também divide a e, consequentemente, é divisor de a e b. Portanto, os divisores comuns de a e b são os mesmos que os divisores comuns de b e c. Particularmente, também coincidem os maiores divisores comuns, ou seja, $(a, b) = (b, c)$. □

Definição 1.3. *Quando a e b são inteiros tais que $(a, b) = 1$, então dizemos que a e b são co-primos.*

Apesar de conhecermos algumas propriedades teóricas básicas para calcular o mdc, o algoritmo abaixo é uma importante ferramenta para encontrar o mdc de forma bastante simples e prática. A prova foi retirada de [5].

Teorema 1.4 (Algoritmo de Euclides)**.** *Dados dois inteiros positivos, a e b, aplicamos sucessivamente a divisão euclidiana para obter a seguinte sequência de igualdades:*

$$\begin{cases} b = aq_1 + r_1, & 0 \leq r_1 < a, \\ a = r_1q_2 + r_2, & 0 \leq r_2 < r_1, \\ r_1 = r_2q_3 + r_3, & 0 \leq r_3 < r_2, \\ \vdots & \vdots \\ r_{n-2} = r_{n-1}q_n + r_n, & 0 \leq r_n < r_{n-1}, \\ r_{n-1} = r_nq_{n+1}, & \end{cases} \tag{1.3}$$

até algum r_n dividir r_{n-1}. Assim, $(a, b) = r_n$, ou seja, é o último resto não nulo do processo de divisão anterior.

Demonstração. Se tomarmos a primeira equação contida em (1.3), temos duas possibilidades:

$a)$ $r_1 \mid a$. Neste caso, $r_1 = (a, r_1) = (a, b - aq_1) = (a, b)$ e o algoritmo termina.

$b)$ $r_1 \nmid a$. Neste caso, efetuando a divisão de a por r_1, obtemos $a = r_1q_2 + r_2$, com $0 < r_2 < r_1$, conforme mostra a segunda equação de (1.3). Daí, temos também duas possibilidades:

$a_1)$ $r_2 \mid r_1$. Neste caso, $r_2 = (r_1, r_2) = (r_1, a - r_1q_2) = (r_1, a) = (b - q_1a, a) = (a, b)$ e paramos, pois o algoritmo termina.

$b_1)$ $r_2 \nmid r_1$. Neste caso, podemos dividir r_1 por r_2, obtendo $r_1 = r_2q_3 + r_3$, com $0 < r_3 < r_2$.

O procedimento continua até que pare. Isso ocorre, pois, caso contrário, teremos uma sequência de números $a > r_1 > r_2 > \cdots$ que não possui menor elemento, o que não é possível pelo Princípio da Boa Ordenação. Assim, para algum n, temos que $r_n \mid r_{n-1}$, o que implica que $(a, b) = r_n$. Logo, examinando as igualdades em (1.3) de cima para baixo e usando a proposição (1.2), temos que:

$$(a, b) = (a, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = r_n$$

. □

Agora iremos para mais um conceito importante desta seção. Ele está relacionado com os múltiplos simultâneos de dois inteiros fixos, denominado por mínimo múltiplo comum.

Definição 1.4 (Mínimo Múltiplo Comum - MMC)**.** *Sejam a e b inteiros diferentes de zero. O mínimo múltiplo comum entre a e b é o inteiro positivo m que satisfaz as seguintes condições:*

(i) m é um múltiplo comum de a e de b, isto é, $a \mid m$ e $b \mid m$;

(ii) m é o menor inteiro positivo com a propriedade (i).

O mínimo múltiplo comum de a e b será denotado por $mmc(a, b)$. De forma análoga ao mdc quanto à ordem dos números a e b, temos que $mmc(a, b) = mmc(b, a)$.

1.3 Números Primos

Um conceito de suma importância em teoria dos números, e portanto neste trabalho, é o de número primo. Os números primos nos servirão de pano de fundo no estudo do método RSA, que veremos mais adiante. Notaremos, no decorrer do trabalho, que esses números são relevantes não apenas na aritmética modular, mas em vários ramos da matemática.

Definição 1.5. *Um número $p \in \mathbb{N}$, $p > 1$, é dito primo se seus únicos divisores forem 1 e o próprio p. Um número que não é primo é dito composto.*

Nesta seção trabalharemos com alguns teoremas voltados ao estudo dos números primos. No final do próximo capítulo necessitaremos dos mesmos para demonstrar o funcionamento da criptografia assimétrica e de seus algoritmos por meio de chaves para codificar e decodificar mensagens. Assim, para melhor entendimento de suas propriedades, enunciaremos e demonstraremos os seguintes resultados:

Teorema 1.5. *Seja $n \in \mathbb{N}$. Então o menor divisor $p > 1$ de n é primo.*

Demonstração. Denotando p como sendo o menor divisor de n e sendo $p > 1$, vamos supor que p seja composto. Daí, $p = k \cdot m$, com $1 < k, m < p$.

Mas, se dissermos que $n = q \cdot p$, então temos também que $n = q \cdot k \cdot m$. Logo, $k \mid p$ e como $p \mid n$, então $k \mid n$ e isso contradiz a hipótese de que p é o menor divisor de n.

□

Como podemos ver no teorema a seguir, os números primos são a base para a formação dos números naturais, uma vez que os naturais são formados pelo produto dos mesmos.

Teorema 1.6 (Teorema Fundamental da Aritmética - TFA)**.** *Todo número natural maior que 1 ou é primo ou pode ser escrito como produto de números primos.*

Demonstração. Tomemos $n \in \mathbb{N}$. Se n for primo, não há nada a fazer. Agora, vamos assumir que n é composto e seja q_1 seu menor divisor. Pelo teorema 1.5, sabemos que q_1 é número primo. Segue que podemos escrever, para algum $n_1 \in \mathbb{N}$ com $1 < n_1 < n$,

$$n = q_1 \cdot n_1.$$

Novamente, se n_1 for primo então terminamos a prova. Do contrário, seja q_2 o menor primo que divide n_1. Daí, temos que, para algum $n_2 \in \mathbb{N}$ com $1 < n_2 < n_1$.

$$n = q_1 \cdot q_2 \cdot n_2.$$

Continuando o argumento, teremos ao final de n etapas uma cadeia $n > n_1 > n_2 > \cdots > 1$ e:

$$n = q_1 \cdot q_2 \cdots q_s. \tag{1.4}$$

Assim, podemos rearrumar esses primos que obtemos e escrever n da seguinte maneira:

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_j^{a_j}, \tag{1.5}$$

com $a_i > 0$, $\forall i = 1, 2 \cdots j$, e $p_1 < p_2 < \cdots p_j$. □

Pelos teoremas dados a seguir, vejamos a importância de se estudar a existência dos números primos.

Teorema 1.7. *Existem infinitos números primos.*

Demonstração. Vamos supor que existe apenas um número finito de números primos,

$$p_1, p_2, \cdots, p_i, \cdots, p_n.$$

Agora consideremos o número natural b de forma que:

$$b = (p_1 \cdot p_2 \cdots p_i \cdots p_n) + 1 \tag{1.6}$$

Daí, pelo TFA, o número b possui um fator primo p que, portanto, deve ser um dos p_i, com $1 \leq i \leq n$ e, consequentemente, divide o produto $p_1 \cdot p_2 \cdots p_n$. Mas temos que se $p \mid (a + b)$ e $p \mid a$, então $p \mid b$. Logo, observando a equação dada em (1.6), então $p \mid 1$, o que é absurdo. □

1.3.1 Crivo de Eratóstenes

Apesar da infinidade dos números primos, apresentada no teorema anterior, e da alta capacidade computacional, nos livros didáticos presentes na Educação Básica não há um método que mostre como produzir números primos. Todavia, ao longo dos tempos, alguns algoritmos úteis foram desenvolvidos para descobrirmos quais números primos existem dentro de uma quantidade pré-estabelecida.

O primeiro matemático, que se tem conhecimento, a construir um algoritmo que permite encontrar todos os números primos menores que um número natural dado n, foi o grego Eratóstenes de Cirene. Tal algoritmo ficou conhecido como Crivo de Eratóstenes.

O crivo funciona com um algoritmo simples, feito manualmente, sendo baseado no lema a seguir:

Lema 1.1. *Todo número composto $a > 1$ admite um divisor primo p tal que $p^2 \leq a$.*

Demonstração. Usando a hipótese de que $p \mid a$, sendo a composto, então existe um número b tal que $a = b \cdot p$. Assim, temos que $p \leq b$. Daí, segue que $a = b \cdot p \geq p \cdot p = p^2$. Logo, $p^2 \leq a$. □

1.4 Congruência

Na seção (1.2) vimos o importante teorema da divisão euclidiana. Com ele verificamos que na divisão de dois inteiros, se um não é múltiplo do outro, ocorre a existência de restos não nulos. Muitos matemáticos se ocuparam em estudar a aritmética dos restos na divisão por um número fixo. Isso deu início a um considerável campo da teoria dos números chamado de congruência modular, a qual enunciaremos da seguinte forma:

Definição 1.6. *Seja m um número natural. Diremos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se*

$$a \equiv b \pmod{m} \tag{1.7}$$

Quando a relação $a \equiv b \pmod{m}$ for falsa, diremos que a e b são incongruentes, módulo m. Escrevemos, neste caso, $a \not\equiv b \pmod{m}$.

Aqui tomaremos sempre $m > 1$, pois o resto da divisão de qualquer inteiro por 1 é nulo e isso não nos é interessante. Da definição, temos que a congruência módulo m é uma relação de equivalência e isso pode ser explicitado abaixo, conforme os enunciados das propriedades

que seguem. Apesar da congruência possuir várias propriedades, estamos demonstrando as mais usadas na Educação Básica. Daremos destaque às seguintes, tendo em vista que as aplicaremos nas resoluções de alguns exemplos voltados à codificações e decodificações de mensagens, presentes no capítulo dois.

Dados os números inteiros a, b, c, k, q e m um inteiro maior que 1, seguem as seguintes propriedades:

Propriedade Reflexiva: $a \equiv a \pmod{m}$;

Propriedade Simétrica: se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$;

Propriedade Transitiva: se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

Demonstração. Propriedade Reflexiva: Como m divide 0, então m divide $(a-a)$, ou seja, $a \equiv a \pmod{m}$. □

Demonstração. Propriedade de Simetria: Se $a \equiv b \pmod{m}$, então $a - b = km$, com $k \in \mathbb{Z}$. Portanto, $b - a = -(k)m \Rightarrow b \equiv a \pmod{m}$. □

Demonstração. Propriedade Transitiva: Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então existem k e q, tais que:

$$a - b = km \quad \text{e} \quad b - c = qm \tag{1.8}$$

Somando membro a membro dessas equações em (1.8), temos que:

$$a - b + b - c = km + qm \Rightarrow a - c = m(k + q),$$

ou seja, $a \equiv c \pmod{m}$

□

Quando desejarmos saber se dois números $a, b \in \mathbb{Z}$ são congruentes módulo m, não se faz necessária aplicar a divisão euclidiana de a e b por m para comparar seus restos a seguir. Para isso, é suficiente utilizarmos o resultado dado por:

Proposição 1.3. *Dados $a, b, m \in \mathbb{Z}$, com $m > 1$, tem-se que $a \equiv b \pmod{m}$ se, e somente se, $m \mid (b - a)$.*

Demonstração. Vamos supor que $a \equiv b \pmod{m}$. Pela definição sabemos que a e b têm o mesmo resto quando estes são divididos por m. Com isso, existem os inteiros q_1 e q_2, tais que:

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

e

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

com $0 \leq r \leq m-1$. Daí temos:

$$b - a = q_2 \cdot m + r - (q_1 \cdot m + r) = q_2 \cdot m + r - q_1 \cdot m - r = (q_2 - q_1)m \Rightarrow m \mid (b-a)$$

Agora estamos dizendo que $m \mid (b-a)$. Se considerarmos a divisão euclidiana, temos que $a = q_1 \cdot m + r_1$ e $b = q_2 \cdot m + r_2$, com $0 \leq r_1, r_2 \leq m-1$. Supondo r_1 e r_2 distintos e tendo $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, então:

$$b - a = q_2 \cdot m + r_2 - (q_1 \cdot m + r_1) = q_2 \cdot m + r_2 - q_1 \cdot m - r_1 = (q_2 - q_1)m + (r_2 - r_1).$$

Mas como $m \mid (b-a)$ e $m \mid (q_2 - q_1)m$, então temos que $m \mid (r_2 - r_1)$. Sem perda de generalidade, se tomarmos $r_1 \leq r_2$, como $0 \leq r_1 \leq m-1$ e $0 \leq r_2 \leq m-1$, $r_1 - r_2 \leq m-1$, o que é um absurdo pelo fato de que $m \mid (r_2 - r_1)$. Portanto $r_1 = r_2$ e $a \equiv b \pmod{m}$.

□

A congruência é uma importante relação de equivalência na adição e multiplicação dos inteiros. Essas operações podem ser vistas nas proposições que seguem.

Proposição 1.4. *Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$.*

i) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$.

ii) se $a \equiv b \pmod{m}$, e $c \equiv d \pmod{m}$, então $ac \equiv bd \pmod{m}$.

Demonstração. Suponhamos que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$. Logo, temos que $m \mid b-a$ e $m \mid d-c$.

(i) Basta observar que $m \mid (b-a) + (d-c)$ e, portanto $m \mid (b+d) - (a+c)$, o que prova esta parte do resultado.

(ii) Basta notar que $bd - ac = d(b-a) + a(d-c)$ e conluir que $m \mid bd - ac$.

□

Pela proposição abaixo, podemos notar que em se tratando de congruência modular o cancelamento sempre é válido com relação à adição.

Proposição 1.5. *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$. Tem-se que*

$$a + c \equiv b + c \pmod{m} \iff a \equiv b \pmod{m}$$

Demonstração. Se $a \equiv b \pmod{m}$, segue-se imediatamente da Proposição (1.4)(i) que $a+c \equiv b+c \pmod{m}$, pois $c \equiv c \pmod{m}$. Reciprocamente, se $a+c \equiv b+c \pmod{m}$, então $m \mid b+c-(a+c)$, o que implica que $m \mid b-a$ e, consequentemente, $a \equiv b \pmod{m}$. □

Em aritmética modular não temos uma operação de divisão. No entanto, temos os inversos multiplicativos ou inversos modulares. Os mesmos são de grande utilidade para encontrar chaves de decodificação na criptografia. E isso poderá ser visto nas demonstrações e nos exemplos do próximo capítulo.

Definição 1.7. *Dados dois números inteiros a e m com $(a,m)=1$, chama- se inverso de a módulo m a qualquer um dos inteiros x tais que*

$$a \cdot x \equiv 1 \pmod{m} \tag{1.9}$$

Observação: Se $(a,m)=1$, então existem os números x e y tais que $a \cdot x + m \cdot y = 1$, daí resultando na equação (1.9).

Outra forma de escrevermos $a \cdot x \equiv 1 \pmod{m}$ é colocando $a \cdot a^{-1} \equiv 1 \pmod{m}$. Vale ressaltar que apenas os números primos de m, ou seja, números que não possuem fatores primos com m têm inverso multiplicativo módulo m.

Pela divisão euclidiana, podemos ver que todo inteiro é congruente módulo m ao seu resto. Daí, é congruente a um dos números $0, 1, 2, \cdots, m-1$ e dois desses números diferentes não serão congruentes módulo m. Logo, para encontrar o resto da divisão de um inteiro a por m só é preciso achar um natural r dentre os números de 0 a $m-1$ que seja congruente a a módulo m.

Definição 1.8. *Um sistema completo de resíduos módulo m é todo conjunto de números inteiros cujos restos pela divisão por m são os números $0, 1, \cdots, m-1$, sem repetições e numa ordem qualquer. Simbolicamente, podemos representar este sistema por:*

$$\mathbb{Z}_m = \{0, 1, 2, \cdots, m-1\}$$

Conforme a definição acima, vemos que o sistema completo de resíduos módulo m tem m elementos. Com isso, se $a_1, a_2, \cdots, a_m$ são m números inteiros, não congruentes módulo m dois a dois, formando um sistema completo de resíduos. A seguir temos proposições mostrando aplicações voltadas ao sistema completo de resíduos.

Corolário 1.1. *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$ e $(c,m)=1$. Temos que:*

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

Proposição 1.6. *Sejam $a, k, m \in \mathbb{Z}$, com $m > 1$ e $(k, m) = 1$. Se $\{a_1, \cdots, a_m\}$ é um sistema completo de resíduos módulo m, então,*

$$\{a + ka_1, \cdots, a + ka_m\}$$

também é um sistema completo de resíduos módulo m.

Demonstração. Do corolário acima, para $i, j = 0, \cdots, m-1$, temos:

$$a + ka_i \equiv a + ka_j \pmod{m} \iff ka_i \equiv ka_j \pmod{m}$$

$$\iff a_i \equiv a_j \pmod{m} \iff i = j.$$

Isso mostra que $a + ka_1, \cdots, a + ka_m$ são, dois a dois, não congruentes módulo m e, portanto, formam um sistema completo de resíduos módulo m. □

Proposição 1.7. *Se $\{a_1, a_2, \cdots, a_m\}$ é um sistema completo de resíduos módulo m, onde $a_1 \equiv 0 \pmod{m}$, então $a_2 \cdot a_3 \cdots a_m \equiv 1 \cdot 2 \cdot 3 \cdots (m-1) \pmod{m}$.*

Demonstração. Temos que para cada i, com $2 \leq i \leq m$ existe um único b_i com $1 \leq b_i \leq m-1$, tal que $a_i \equiv b_i \pmod{m}$. Mas como $\{a_2, a_3, \cdots, a_m\}$ tem $m-1$ elementos não congruentes dois a dois e $\{b_2, b_3, \cdots, b_m\}$ também possui $m-1$ elementos, temos que $\{b_2, b_3, \cdots, b_m\} = \{1, 2, \cdots, m-1\}$. Assim,

$$a_2 \cdot a_3 \cdots a_m \equiv b_2 \cdot b_3 \cdots b_m \equiv 1 \cdot 2 \cdots (m-1) \pmod{m}$$

□

Proposição 1.8. *Seja p um número primo e a um inteiro tal que $p \nmid a$. Então*

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

Demonstração. Como $p \nmid a$ temos que $(p, a) = 1$. Considerando o sistema completo de resíduos módulo p, $\{0, 1, 2, \cdots, p-1\}$ e usando a primeira dessas três proposições, temos que:

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

□

As três proposições acima servirão para auxiliar na demonstração do próximo teorema, o Pequeno Teorema de Fermat, que atua nas congruências usando divisão por número primo.

Teorema 1.8 (Pequeno Teorema de Fermat - PTF)**.** *Dado um número primo p e a um natural não divisível por p, tem-se que p divide o número $a^{p-1}-1$.*

Demonstração. Considerando os $p-1$ múltiplos de a, temos: $a, 2a, 3a, \cdots, (p-1)a$. Sabemos que nenhum desses números é congruente módulo p com outros deles e nem é congruente a zero módulo p.

Se tomarmos $ra \equiv sa \pmod{p}$, com $1 \leq r < s \leq (p-1)$, como $p \nmid a$, temos $r \equiv s \pmod{p}$, o que é uma contradição. Dessa maneira, tais números formam um sistema completo de resíduos. Logo, eles são congruentes a $1, 2, 3, \cdots, (p-1)$ em alguma ordem. Assim,

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

onde,

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

Agora, observando que $mdc(p, 1 \cdot 2 \cdots (p-1)) = 1$, segue que $a^{p-1} \equiv 1 \pmod{p}$. □

Definição 1.9. *Um sistema reduzido de resíduos módulo m é um conjunto de inteiros $(r_1, r_2, r_3, \cdots, r_s)$, tais que:*

(i) $(r_i, m) = 1$*, para todo* $i = 1, 2, 3, \cdots, s$*;*

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

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

Podemos formar um sistema reduzido de resíduos $\{r_1, r_2, r_3, \cdots, r_s\}$ módulo m a partir de um sistema completo de resíduos $\{a_1, a_2, a_3, \cdots, a_m\}$ módulo m eliminando os elementos a_i que não são primos com m.

Definição 1.10. *Designamos por $\varphi(m)$ o número de elementos presentes em um sistema reduzido de resíduos módulo $m > 1$. Isto corresponde à quantidade de números naturais entre 0 e $m-1$ primos com m, como já informado. Se colocarmos $\varphi(1) = 1$ isso definirá uma importante função dada por:*

$$\varphi : \mathbb{N} \to \mathbb{N} \quad \textit{(denominada função fi de Euler).}$$

Pela definição dada por [5], temos que

$$\varphi(m) \leq m-1, \quad \textit{para todo } m \geq 2$$

Para mais, se $m \geq 2$, então $\varphi(m) = m-1$ se, e somente se, m é primo. De fato, m é primo se, e somente se, $1, 2, \cdots, m-1$ formam um sistema reduzido de resíduos módulo m, o que equivale dizer que $\varphi(m) = m-1$.

Para calcular $\varphi(m)$, vejamos a proposição a seguir:

Proposição 1.9. *Sejam $a, b \in \mathbb{N}$, tais que $(a, b) = 1$. Então $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.*

Demonstração. Se $a = 1$ ou $b = 1$ o resultado é trivial. Então vamos supor que $a > 1$ e $b > 1$. Conforme mostra [5], consideremos a tabela formada pelos naturais de 1 a $(a \cdot b)$:

1	2	$\cdots$	k	$\cdots$	b
$b+1$	$b+2$	$\cdots$	$b+k$	$\cdots$	$2b$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$(a-1)b+1$	$(a-1)b+2$	$\cdots$	$(a-1)b+k$	$\cdots$	$a \cdot b$

Como temos que $(t, a \cdot b) = 1$ se, e somente se, $(t, a) = (t, b) = 1$, para calcular $\varphi(a \cdot b)$ devemos determinar os inteiros da tabela acima que são simultaneamente primos com a e b.

Se o primeiro elemento de uma coluna não for primo com b, então todos os elementos desta coluna também não serão. Portanto, os elementos primos com b estão necessariamente nas colunas restantes que são em número $\varphi(b)$.

Pensemos em quais elementos são primos com a em cada coluna. Como $(a, b) = 1$, a sequência $k, b+k, \cdots, (a-1)b+k$ forma um sistema completo de resíduos módulo a e, portanto, $\varphi(a)$ desses elementos são primos com a. Daí, o número de elementos simultaneamente primos com a e b é dado por $\varphi(a) \cdot \varphi(b)$.

□

O Pequeno Teorema de Fermat que vimos é um caso particular do teorema a seguir, pois enquanto o teorema de Fermat trabalha com congruências envolvendo módulo primo, o próximo lida com módulos em números compostos.

Teorema 1.9 (Teorema de Euler)**.** *Se m é um número inteiro positivo e a um inteiro tal que $mdc(a, m) = 1$, então, $a^{\varphi(m)} \equiv 1 \pmod{m}$.*

Demonstração. A prova deste teorema pode ser vista em [8]. Temos que se $\{r_1, r_2, \cdots, r_{\varphi(m)}\}$ é um sistema reduzido de resíduos módulo m e tendo a um número natural tal que $mdc(a, m) = 1$, então $\{ar_1, ar_2, \cdots, ar_{\varphi(m)}\}$ também será um sistema reduzido de resíduos módulo m. De fato, temos que $mdc(ar_i, m) = 1$ para todo i, já que $ar_i \equiv ar_j \pmod{m}$, então $r_i \equiv r_j \pmod{m}$ pois a é invertível módulo m, logo $r_i = r_j$. Daí, $i = j$. Com isso, cada ar_i será congruente com algum r_j e, portanto,

$$\prod_{1\leq i\leq \varphi(m)} (ar_i) \equiv \prod_{1\leq i\leq \varphi(m)} r_i \pmod{m}$$

$$\iff a^{\varphi(m)} \cdot \prod_{1\leq i\leq \varphi(m)} r_i \equiv \prod_{1\leq i\leq \varphi(m)} r_i \pmod{m}$$

Porém, como cada r_i é invertível módulo m, simplificando o fator $\prod_{1\leq i\leq \varphi(m)} r_i$, obtemos o resultado desejado.

□

Teorema 1.10 (Teorema de Wilson - TW)**.** *Sendo p um número primo, então* $(p-1)! \equiv -1 \pmod{p}$.

Demonstração. Se tomarmos $p = 2$ ou $p = 3$ o teorema é válido e nada há para se fazer, pois:

$$(2-1)! \equiv -1 \pmod{2}$$

$$1! \equiv -1 \pmod{2}$$

$$(3-1)! \equiv -1 \pmod{3}$$

$$2! \equiv -1 \pmod{3}$$

$$2 \equiv -1 \pmod{3}$$

Agora vamos supor $p \geq 5$, com p primo. Então fatorando $(p-1)!$ teremos:

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdot 4 \cdots (p-2) \cdot (p-1)$$

Para todo $i \in \{1, 2, \cdots, p-1\}$ existe um único $j \in \{1, 2, \cdots, p-1\}$ tal que $i \cdot j \equiv 1 \pmod{p}$. Por outro lado, se $i \in \{1, 2, \cdots, p-1\}$ é tal que $i^2 \equiv 1 \pmod{p}$, então $p \mid (i+1)$ ou $p \mid (i-1)$ e isso só pode ocorrer se $i = 1$ ou se $i = p-1$. Daí,

$$2 \cdot 3 \cdot 4 \cdots (p-2) \equiv 1 \pmod{p} \Leftrightarrow 2 \cdot 3 \cdot 4 \cdots (p-2)(p-1) \equiv 1(p-1) \pmod{p}$$

Logo,

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

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

Uma vez que $p - 1 \equiv -1 \pmod{p}$.

□

CAPÍTULO 2

Algumas Aplicações da Aritmética Modular

Neste capítulo serão abordados temas relativos à aritmética modular com foco em aplicações presentes no cotidiano dos alunos da educação básica, porém muitas vezes ignoradas por não saberem sua origem e/ou seu funcionamento.

As bases que serviram de referência para os estudos aqui feitos foram [1, 11, 6, 13, 3].

2.1 Código de Barras

Registros históricos relatam que a primeira patente dos códigos de barras foi atribuída aos engenheiros Norman Joseph Woodland e Bernard Silver, em 1952, nos Estados Unidos da América. Tais códigos são definidos como sendo uma representação gráfica de uma sequência numérica, servindo para identificar, dentre outras coisas, unidades logísticas, produtos, documentos, cargas e contêineres. A criação dos códigos se deu no intuito de ajudar o comércio a aumentar a velocidade para verificar a saída de produtos, visando melhorias quanto ao controle de inventários. Com o passar do tempo constatou-se que esses códigos eram eficientes para serem usados em todo varejo. Mesmo sendo de grande valia, é importante citar que a utilidade dos códigos só foi reconhecida algumas décadas após sua invenção. Isso se deu graças ao aumento de componentes eletrônicos na fabricação de leitores de códigos de barras com preços baixos.

Os códigos de barras adotados nos Estados Unidos e no Canadá são os denominados *Universal Product Code* (UPC), possuindo 12 dígitos. Devido à tamanha repercussão do sistema UPC, alguns fabricantes de países europeus criaram uma associação e se aprofundaram em novos estudos nessa área da tecnologia, inventando um sistema de códigos chamado *European*

Article Numbering Association (EAN) no ano de 1987. Como existiam muitos países ligados à importação e exportação de produtos comerciais, era preciso inserir na estrutura dos códigos o país de fabricação de cada produto. Dessa forma, ocorreu a criação de mais um dígito nos códigos e as leitoras necessitavam ler tanto códigos UPC quanto EAN. Com isso, nos locais onde se usava UPC foi inserido o zero antes dos outros dígitos e o sistema passou a se chamar UPC-A, já no EAN os primeiros três dígitos, da esquerda para a direita, serviam e ainda servem para identificar o país de onde foi feito o cadastro do produto, os próximos quatro mostram qual a empresa proprietária do prefixo, o outro conjunto de cinco dígitos traz a identificação do produto e o último dígito é chamado verificador. Mais adiante falaremos de maneira detalhada sobre o mesmo. No caso do Brasil, este utiliza o código EAN e seus produtos são cadastrados sendo iniciados pela sequência 789. Existem outros códigos como os usados em caixas de papelão que têm quatorze dígitos, informando até a quantidade de produtos dentro das caixas e existem ainda códigos de oito dígitos, usados em embalagens muito pequenas.

Para que a leitura dos códigos seja feita, existe o leitor de código de barras. Este é um aparelho que faz a decodificação dos dados a partir da emissão de um raio na cor vermelha, atingindo todas as barras. Daí, por intermédio da reflexão da luz pelos módulos contidos no espaço ou pela ausência desses módulos o leitor ou *scanner* vai interpretando os códigos. Essa interpretação acontece com o uso de um conversor digital ou analógico produzido pela luz enviada por um sensor fotoelétrico. No caso da ausência de luz, a reflexão transmite um sinal distinto caracterizando a barra. Dessa forma, cada caractere presente no código fica sendo interpretado como um número binário e cada módulo reproduz o dígito 0 para os espaços em branco e o dígito 1 para as barras onde a luz não está sendo refletida. Para efeito de ilustração foram colocados nesta seção leitores ou *scanners* de códigos de barras representados na Figura (1).

(a) Leitor de código de barras 1D. (b) Leitor de código de barras 2D.

Figura 1: Exemplos de leitores.

Ao observar os códigos em vários tipos de produtos, percebemos que existem diferentes larguras para as barras brancas e pretas e cada uma delas possui um significado de caractere diferente. Assim, as barras podem ser finas, médias, grossas e muito grossas. Conforme a espessura, a quantidade de 0 ou 1 varia e isso pode ser entendido por meio da Tabela (1).

Tabela 1: Interpretação das listras em códigos de barras.

Tipos de listras	Cor branca	Cor preta
finas	0	1
médias	00	11
grossas	000	111
muito grossas	0000	1111

Os códigos mais conhecidos por causa do comércio são UPC e EAN-13. Nos códigos UPC a leitura é realizada conforme mostra a tabela a seguir e cada número do sistema decimal é simbolizado por uma sequência diferente. Neste tipo de código, cada quatro barras associa-se a uma sequência de sete dígitos, dispostos entre zeros e uns.

Tabela 2: Dígitos no sistema UPC.

Dígito	Lado Esquerdo	Lado Direito
0	0001101	1110010
1	0011001	1100110
2	0010011	1101100
3	0111101	1000010
4	0100011	1011100
5	0110001	1001110
6	0101111	1010000
7	0111011	1000100
8	0110111	1001000
9	0001011	1110100

Exemplo 2.1. *Pela Tabela* (2)*, o número* $084300 - 235713$ *fica sendo:*
Lado esquerdo:

$$0001101 - 0110111 - 0100011 - 0111101 - 0001101 - 0001101$$

Lado direito:

$$1101100 - 1000010 - 1001110 - 1000100 - 1100110 - 1000010$$

E o código gerado fica sendo:

Figura 2: Código UPC.

No que concerne ao sistema EAN-13, que possui um dígito a mais que o UPC, ele também é representado pela sequência de zeros e uns. Em qualquer um desses sistemas os dígitos possuem codificações distintas, conforme os lados em que estão. Se estiverem do lado direito iniciarão em um, se estiverem do esquerdo iniciarão por zero. Em consequência disso, a leitura do código pode ser realizada até de cabeça para baixo que produzirá o mesmo número.

2.1.1 O Dígito Verificador na Estrutura dos Códigos de Barras

O dígito verificador, que denotaremos por D, é o último número que aparece no código de barras, da esquerda para a direita, e o mesmo tem a incumbência de confirmar matematicamente se os dígitos que o precedem no código estão corretos. Com isso, para encontrar o dígito verificador tomaremos o que mostra [12] em linhas gerais.

Definição 2.1. *Sejam* $p = \begin{bmatrix} p_1 & p_2 & p_3 & p_4 & \cdots & p_n \end{bmatrix}$, *com* $p_i \in \mathbb{Z}_m$, $1 \leq i \leq n$ *uma matriz de pesos e* $w \in \mathbb{Z}_m$ *um número inteiro fixado. Chamaremos de* $\mathbb{Z}_m$ *o conjunto de valores que podem assumir os dígitos usados no código. Dados dois inteiros positivos* m *e* n *e a sequência de números* $a_1, a_2, a_3, a_4, \cdots, a_{n-1}$ *tais que* $a_i \in \mathbb{Z}_m$, $1 \leq i \leq n-1$, *define-se o número de verificação* a_n *como o único elemento de* $\mathbb{Z}_m$ *que verifica a equação:*

$$\sum_{i=1}^{n} a_i p_i \equiv w \pmod{m} \tag{2.1}$$

Um sistema de codificação assim definido será denotado por $C = (\mathbb{Z}_m, m, n, w, p)$.

Como $\mathbb{Z}_m = \{0, 1, 2, \cdots, m-1\}$, *daí tomando as classes residuais módulo* m, *teremos que* $D = a_n$ *é o único elemento de* $\mathbb{Z}_m$ *tal que:*

$$a_n = {p_n}^{-1} \left(w - \sum_{i=1}^{n} a_i p_i \right) \tag{2.2}$$

sempre que $p_i \in \mathbb{Z}_m$ *possuir elemento inverso em* $\mathbb{Z}_m$.

2.1.2 Detecção de Erros em Códigos de Barras

A teoria de códigos voltada aos dígitos verificadores não só analisa tipos de erros, mas os detecta e os corrige, quando são mais comuns. Conforme o matemático Jacobus Koos Verhoeff, os erros mais comuns são chamados de erro único e de transposição.

O erro único ou consistente ocorre em setenta e nove por cento dos casos e ele acontece por meio da troca de um dígito por outro (a por b). Neste caso, se o produto matricial não for múltiplo de 10, o erro será detectado possibilitando a correção.

Nos erros de transposição os algarismos são digitados com mudança de ordem dos dígitos consecutivos. Esses erros acontecem em onze por cento dos casos (ab por ba ou abc por cba).

Tomaremos o teorema abaixo, presente em [12], descrevendo como os erros são encontrados nas congruências dos códigos de barras.

Teorema 2.1. *Sejam m um inteiro positivo e $p = \begin{bmatrix} p_1 & p_2 & \cdots & p_n \end{bmatrix}$ uma matriz de pesos. Suponhamos que uma matriz de identificação $c = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \end{bmatrix}$, possuindo o dígito de verificação (onde temos que $0 \leq a_i < n$ para todo i, $1 \leq i \leq n$), satisfaz a condição:*

$$c \cdot p^t = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \end{bmatrix} \cdot \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{bmatrix} = a_1p_1 + \cdots + a_np_n \equiv w \pmod{m} \tag{2.3}$$

Então:

1. *Todo erro consistente numa única alteração na posição i-ésima será detectado se, e somente se, $(p_i, m) = 1$.*
2. *Todo erro de transposição da forma $\cdots a_i \cdots a_j \cdots \rightarrow \cdots a_j \cdots a_i \cdots$ será detectado se, e somente se, $(p_i - p_j, m) = 1$.*

Demonstração. (1) $\Rightarrow$ Vamos supor que a sequência digitada teve a troca do dígito a_i na posição i por b_i, ou seja, passou por um erro único e $a_i \neq b_i$. Agora vamos denotar por r a matriz resultante deste erro. Daí,

$$r = \begin{bmatrix} a_1 & a_2 & \cdots & b_i & \cdots & a_n \end{bmatrix}.$$

Segue que $c \cdot p^t - r \cdot p^t = (a_i - b_i)p_i$ e o erro não poderá ser detectado se:

$$c \cdot p^t - r \cdot p^t \equiv 0 \pmod{m} \Leftrightarrow m \mid (a_i - b_i)p_i$$

Caso o $(p_i, m) = 1$ temos que a classe inversa de p_i é inversível em $\mathbb{Z}_m$, donde a condição acima implica que, tendo $a_i \neq b_i$, então suas classes inversas também serão distintas, e assim o erro é detectado.

($\Leftarrow$) Se tivermos $(p_i, m) = 1$, a classe inversa de p_i é invertível em $\mathbb{Z}_m$. Como as classes inversas de a_i e b_i são distintas, então o erro é detectado.

(2) ($\Rightarrow$) Supondo que ocorreu um erro de transposição, e a matriz c implicou na c' por causa da mudança de ordem dos dígitos. Nesse caso, calculando $c \cdot p^t - c' \cdot p^t$, teremos:

$$(a_i p_i + a_j p_j) - (a_j p_i + a_i p_j) = (a_i - a_j)(p_i - p_j)$$

Assim, o erro não será detectado caso aconteça de $(a_i - a_j)(p_i - p_j) \equiv 0 \pmod{m}$, ou seja, $m \mid (a_i - a_j)(p_i - p_j)$.

($\Leftarrow$) A demonstração é análoga de (1). Portanto, é detectado o erro se e somente se $((p_i - p_j), m) = 1$. □

Com base no teorema acima, podemos concluir que para detectar erros consistentes ou de transposição, um sistema de verificação de dígitos precisa ter um número primo como número de $\mathbb{Z}_m$, ou seja, m deve ser primo.

Por simplicidade, segue abaixo um exemplo mostrando como encontrar o dígito verificador usando congruência. Para tal foi utilizada a Figura (3).

Exemplo 2.2. *Confira a veracidade do dígito verificador na figura a seguir, onde a mesma possui seu código de barras no sistemas EAN-*13*. De acordo com esse tipo de sistema, sua matriz* p *sempre tem pesos* 3 *em casas pares e pesos* 1 *em casas ímpares.*

Figura 3: Ilustração do código.

Pelas informações, temos que:

$p = \begin{bmatrix} 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 & 1 \end{bmatrix}$ e que a matriz c que compõe o código é dada por:

$$c = \begin{bmatrix} 7 & 8 & 9 & 6 & 6 & 4 & 4 & 4 & 1 & 8 & 1 & 8 & D \end{bmatrix}.$$

Aqui denotamos p^t como sendo a matriz transposta de p. Logo, realizando o produto matricial entre c e p^t:

$$\begin{aligned} c \cdot p^t &= 7\cdot 1 + 8\cdot 3 + 9\cdot 1 + 6\cdot 3 + 6\cdot 1 + 4\cdot 3 + 4\cdot 1 + 4\cdot 3 + 1\cdot 1 + 8\cdot 3 + 1\cdot 1 + 8\cdot 3 + D\cdot 1 \\ &= 7 + 24 + 9 + 18 + 6 + 12 + 4 + 12 + 1 + 24 + 1 + 24 + D \\ &= 142 + D \end{aligned}$$

Como $142 + D \equiv 0 \pmod{10}$, então o valor de D é 8 e isso pode ser verificado pelo código da figura em questão.

2.2 Dígito Verificador no ISBN

O *International Standard Book Number* (ISBN) é um sistema criado no ano de 1969 para identificar desde livros até publicações em braille. Tal sistema é conhecido mundialmente e os códigos de barras do ISBN de livros lançados entre 1969 até 2007 possuem 10 dígitos. Já os lançados após esse período têm 13 dígitos.

Os códigos do sistema ISBN com 13 dígitos são do tipo EAN -13, trazendo informações dadas por uma sequência numérica listada da seguinte forma: prefixo EAN (3 dígitos); identificador de grupo, país ou área idiomática (2 dígitos); identificador de editor (3 dígitos); identificador de título (5 dígitos, incluindo o verificador). Suas regras são as mesmas dos códigos de barras e a congruência realizada para encontrar D é análoga à já feita na seção anterior, só mudando o operador módulo e a matriz peso, pois para cada tipo de sistema há um operador e uma matriz peso pré- estabelecidos para o mesmo.

No caso do ISBN-10, sua sequência numérica é dada pela matriz:

$$c = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 & \cdots & a_9 & D \end{bmatrix} \tag{2.4}$$

e a matriz peso fica sendo:

$$p = \begin{bmatrix} 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix}. \tag{2.5}$$

Para encontrar D no ISBN usamos a congruência módulo 11 ao produto matricial entre c e p^t. Daí,

$$c \cdot p^t = a_1 10 + a_2 9 + a_3 8 + a_4 7 + \cdots + a_9 2 + D \equiv 0 \pmod{11}. \tag{2.6}$$

Portanto, o valor de D será dado pelo número que falta para que a divisão da resposta de $c \cdot p^t$ por 11 seja de resto zero.

2.3 Dígito Verificador em Cartão de Crédito

Outra aplicação de grande valia dos dígitos verificadores está na área de cartões de crédito. Estes cartões geralmente possuem 16 dígitos, onde os 6 primeiros estão relacionados à bandeira do cartão, os outros 9 identificam o cliente e o último dígito, como sempre, é o verificador. O algoritmo usado nos cartões de crédito é o algoritmo de Luhn, criado por Hans Peter Luhn em 1954. Tal algoritmo se dá pela multiplicação pelo peso 2 dos dígitos do cartão em posição ímpar e, no caso de alguma multiplicação resultar em um número de dois algarismos, somamos os valores absolutos dos mesmos (um exemplo seria a multiplicação de 7 por 2. Como 14 tem dois algarismos, logo faríamos $1 + 4 = 5$), ou pegamos o resto da divisão desse número por nove. No que se refere aos dígitos de posições pares, estes são conservados, ou seja, seus pesos valem 1. Em seguida, juntamos as respostas da soma da posição ímpar com as da posição par. Daí, o dígito verificador será o número que falta para se chegar em um múltiplo de dez.

Assim, teríamos:

$$c = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 & \cdots & a_{15} & D \end{bmatrix} \tag{2.7}$$

e

$$p = \begin{bmatrix} 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 \end{bmatrix} \tag{2.8}$$

e o produto seria dado por:

$$c \cdot p^t = 2a_1 + 1a_2 + 2a_3 + 1a_4 + \cdots + 2a_{15} + D \equiv 0 \pmod{10}. \tag{2.9}$$

Onde vale lembrar da situação dos dígitos em casas ímpares antes de ocorrer a soma final presente na congruência dada.

2.4 Dígitos Verificadores do CPF

O Cadastro de Pessoa Física (CPF) é um banco de dados regido pela Secretaria da Receita Federal do Brasil (RFB). Ele armazena informações cadastrais de cidadãos que se inscrevem de forma voluntária ou de contribuintes que são obrigados a se inscreverem no CPF. Este documento vale como identificador de crédito e por meio dele é possível saber como está a situação de débito de alguém em relação a alguma empresa.

O CPF é um dos principais documentos dos brasileiros, sendo constituído por onze dígitos. O nono dígito, da esquerda para a direita, indica o estado onde a pessoa fez seu registro. No caso de Minas Gerais o algarismo é o 6 e no Rio Grande do Sul fica sendo o zero. Mesmo em casos de perdas ou roubos o número de um CPF não fica sendo cancelado. Como este documento

Figura 4: Ilustração de um suposto CPF.

tem onze dígitos, os mesmos ficam distribuídos em dois blocos, um com nove algarismos e o outro com apenas dois. Este último par de algarismos constitui os dígitos de verificação de erros, sendo essa mais uma aplicação de congruência.

O décimo dígito, ou primeiro verificador, resulta de uma congruência módulo 11, operando com os nove primeiros algarismos do documento:

$$c = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 \end{bmatrix} \tag{2.10}$$

esses algarismos ficam sendo multiplicados, conforme a ordem dada no documento, pela primeira matriz de pesos pré-estabelecida em CPF's por:

$$p = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{bmatrix}. \tag{2.11}$$

Assim como nos códigos de barras, o produto matricial é feito entre c e p^t, dando uma soma (S) e a congruência usada é:

$$S - a_{10} \equiv 0 \pmod{11}. \tag{2.12}$$

Para encontrar o segundo dígito verificador o mesmo processo é realizado, todavia acrescentando a_{10} em c e a matriz peso p passa a ser:

$$p = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{bmatrix}. \tag{2.13}$$

Usaremos abaixo um exemplo da aplicação de congruência presente no CPF.

Exemplo 2.3. *Encontre os dígitos verificadores do CPF dado por* $040317523 - xx$.

Para encontrar o primeiro dígito, tomemos as matrizes:

$c_1 = \begin{bmatrix} 0 & 4 & 0 & 3 & 1 & 7 & 5 & 2 & 3 \end{bmatrix}$ e $p_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{bmatrix}$, daí encontrando a soma (S) em cada caso, temos:

$$S_1 = 0 \cdot 1 + 4 \cdot 2 + 0 \cdot 3 + 3 \cdot 4 + 1 \cdot 5 + 7 \cdot 6 + 5 \cdot 7 + 2 \cdot 8 + 3 \cdot 9$$

$$S_1 = 0 + 8 + 0 + 12 + 5 + 42 + 35 + 16 + 27$$

$$S_1 = 145$$

Logo,

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

$$145 - a_{10} \equiv 0 \pmod{11}.$$

Pela congruência, a_{10} vale 2.

Agora, para calcular o último dígito, tomemos

$$c_2 = \begin{bmatrix} 0 & 4 & 0 & 3 & 1 & 7 & 5 & 2 & 3 & 2 \end{bmatrix}$$

e

$$p_2 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{bmatrix}$$

Daí, encontrando a outra soma:

$$S_2 = 0 \cdot 0 + 4 \cdot 1 + 0 \cdot 2 + 3 \cdot 3 + 1 \cdot 4 + 7 \cdot 5 + 5 \cdot 6 + 2 \cdot 7 + 3 \cdot 8 + 2 \cdot 9$$

$$S_2 = 0 + 4 + 0 + 9 + 4 + 35 + 30 + 14 + 24 + 18$$

$$S_2 = 138$$

Mas como

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

temos que

$$138 - a_{11} \equiv 0 \pmod{11}.$$

Então a_{11} vale 6.

2.5 Criptografia

A palavra criptografia se origina do grego *kryptós* - escondido e *gráphein* - escrita. Na década de setenta existiam poucos métodos para se manter sigilo sobre certas informações e os mesmos eram usados basicamente por poderes militares e instituições governamentais. Com o passar do tempo, estudos acadêmicos começaram a se dedicar à criptologia e os criptoanalistas, que são profissionais que se ocupam de cifrar e decifrar mensagens criptográficas, deram início aos estudos desta natureza.

Relatos históricos mostram que a criptografia existe desde a antiguidade e já foi bastante utilizada em ações secretas, disfarçando informações por intermédio de codificações e decodificações. No que concerne ao uso da criptografia nos dias de hoje, uma grande aplicação da mesma está relacionada a sites de compras pela internet utilizando protocolos que funcionam com o auxílio da mesma, permitindo que o cliente consiga realizar compras seguras. Desta feita, o processo denominado encriptação é responsável por transformar informações originais de tal modo que somente os destinatários com permissão prévia tenham acesso à estas informações. A tais destinatários, podemos entender como pessoas, máquinas e processos autorizados.

Quando há a necessidade de se codificar um determinado texto, é imprescindível que se tenha uma chave cifradora. Esta possui um conjunto de bits, sendo estes a menor unidade de medida de transmissão de dados usada na computação e informática.Nesse conjunto existe um algoritmo capaz de codificar e decodificar/descodificar tal texto. Com isso, dentro da criptografia a congruência modular é aplicada, desde com recursos simples até os mais complexos. Em se tratando dos recursos simples, usaremos uma chave k no alfabeto de 26 letras, com $0 < k < 26$. Se olharmos a tabela 3,retirada de [9], veremos que é possível trabalhar com as 26 letras denotadas com os símbolos 00 a 25, atuando com congruência módulo 26, onde os restos possíveis pela divisão por 26 variam de $0 < k < 26$.

Tabela 3: Uso de chaves para congruência módulo 26.

A-00	B-01	C-02	D-03	E-04	F-05	G-06	H-07	I-08
J-09	K-10	L-11	M-12	N-13	O-14	P-15	Q-16	R-17
S-18	T-19	U-20	V-21	W-22	X-23	Y-24	Z-25	

Exemplo 2.4. *Usando uma cifra de chave* 15*, faça a codificação e a decodificação da palavra RIMA.*

Codificando as letras, temos:

$R = 17$*;* $I = 08$*;* $M = 12$*;*$A = 00$*.*

Agora, usando a chave:

$$17 + 15 = 32 \equiv 06 \pmod{26}$$

$$08 + 15 = 23 \equiv 23 \pmod{26}$$

$$12 + 15 = 27 \equiv 01 \pmod{26}$$

$$00 + 15 = 15 \equiv 15 \pmod{26}$$

Dessa forma, passamos a ter $06 - 23 - 01 - 15$ *como sendo as partes codificadas da mensagem textual.*

De modo geral, denominado por a o número pré-codificado e por $C(a)$ o número codificado, teremos:

$$C(a) \equiv a + k \pmod{26}. \tag{2.14}$$

Para decodificar:

$$D(a) \equiv C(a) - k \pmod{26}, \tag{2.15}$$

com $D(a)$ sendo o número decodificado.

Assim, o exposto acima usa o método da cifra por transposição e mostra o que ocorre quando um remetente usa uma chave para criptografar um texto, relatando também o que acontece quando o destinatário o recebe e o decodifica.

Agora, apresentaremos outro tipo de cifra também conhecida como método de substituição. Este método é conhecido por ser o mais fácil para cifração e decifração, trocando uma letra por outra, porém mantendo a ordem dos caracteres do texto original.

Para explanar o método da substituição, a tabela abaixo foi construída trocando as letras do alfabeto de lugar, porém obedecendo a ordem de troca da primeira letra pela última, da segunda pela penúltima e assim por diante.

Tabela 4: Alfabeto Usando Cifras por Substituição.

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

Deste modo, aplicando o método da substituição na palavra MATEMÁTICA, encontramos NZGVNZGRXZ.

Doravante, no que tange às chaves usadas pela criptografia, elas podem ser de dois tipos: a secreta ou simétrica e a pública ou assimétrica. Esses tipos de chaves são definidos como sendo um conjunto de bits que formam uma senha baseada em um algoritmo.

2.5.1 Criptografia Simétrica ou de Chave Secreta

Na criptografia simétrica, de chave secreta ou privada o mesmo algoritmo cifra e decifra as mensagens, utilizando uma só chave. Com isso, é importante que destinatário e remetente possuam o algoritmo e a chave. Este tipo de criptografia atua com privacidade e a velocidade do processamento é bem rápida. Todavia, essa categoria de chave traz consigo certa periculosidade quanto à segurança, pois necessita de um canal de comunicação bastante seguro de maneira que não haja um vazamento de informações por terceiros.

O *Data Encription Standard* (DES) foi um algoritmo desenvolvido na década de setenta e processava blocos de textos no tamanho de 64 bits por vez, possuindo chave de 56 bits. Esse algoritmo de chave secreta já foi muito seguro, porém com o passar do tempo e com o desenvolvimento da era digital, o mesmo foi quebrado. Hoje já existe o DES com três chaves de 56 bits cada, conhecido como 3-DES. Outro algoritmo de chave privada é o *Advanced Encryption Standard* (AES), esse algoritmo com criptografia simétrica tem chaves maiores de 256; 192 ou 128 bits, com blocos de 128 bits.

2.5.2 Criptografia Assimétrica e o Algoritmo RSA

No cotidiano muitas vezes a criptografia assimétrica é usada de maneira a combinar uma chave que deverá ser usada pela criptografia secreta. Isso ocorre porque a criptografia assimétrica se utiliza de dois tipos de chaves, a secreta e a pública, onde a pública pode ser divulgada a qualquer pessoa ou máquina e a secreta fica apenas com seu remetente. Dito isso, quando uma mensagem é codificada com uma chave, apenas a outra chave irá decodificá-la. A velocidade do processamento neste tipo de chave é mais lenta se comparada com a criptografia simétrica, pois exige maior poder computacional, garantindo a segurança, por exemplo, na área da internet.

Um exemplo de algoritmo assimétrico é o RSA, sendo inventado pelos pesquisadores R. Rivest, A. Shamir e L. Adleman que se valeram de conceitos voltados à teoria dos números na década de setenta, porém avaliado ainda hoje por muitos estudiosos como o principal algoritmo de chave pública. Assim, para se compreender o funcionamento do método RSA é fundamental o entendimento do algoritmo euclidiano aplicado sucessivas vezes, dos teoremas de Fermat e Euler, mdc, números primos, além da função de Euler, representada pela letra φ. Em tempo, vale ressaltar que os números primos são de grande valia no método RSA, já que as chaves que guardam informações sigilosas dependem deles e tais conceitos ditos aqui foram mostrados no capítulo anterior. Ainda falando em números primos, no método RSA são usados primos com uma média de 300 dígitos, mais adiante veremos o motivo dos mesmos necessitarem ser tão grandes.

O funcionamento do algoritmo RSA passa por três etapas, as quais mostraremos a seguir.

2.5.2.1 Pré - Codificação

Essa etapa consiste em tomar uma mensagem e o espaço entre suas palavras, transformando ambos em uma única sequência numérica. Na sequência, cada letra corresponde a um número de dois algarismos, a partir do 10. Isto é feito para que não haja ambiguidade na interpretação da mensagem.

Na pré- codificação do método RSA são utilizados dois números primos, os parâmetros. Aqui os denotaremos por p e q e o produto entre eles será chamado de n. Logo,

$$n = p \cdot q \tag{2.16}$$

O valor de n é um dos números da chave de codificação.

O final da etapa aqui mostrada consiste na quebra da sequência obtendo vários blocos, b, menores que n. A escolha de cada bloco pode ser feita de diferentes maneiras, porém blocos iniciados em zero não devem ser formados por causa da decodificação.

2.5.2.2 Codificação

Para codificar uma mensagem precisamos do valor de n, já escolhido, e também de um inteiro positivo, e, que seja invertível módulo $\varphi(n)$. Isso significa dizer que $(e, \varphi(n)) = 1$. Conhecendo p e q é fácil achar $\varphi(n)$, pois:

$$\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1), \quad \text{com} \quad (p, q) = 1. \tag{2.17}$$

A chave de codificação é formada por (n, e). Com essa chave cada bloco será codificado e vale dizer que após a codificação os mesmos não podem ser reunidos novamente na sequência. Isso se deve ao fato de ficar impossível decodificar a mensagem, como veremos mais adiante. Depois de codificado cada bloco passará a ser $C(b)$definido por:

$$b^e \equiv C(b) \pmod{n}. \tag{2.18}$$

Sendo $C(b)$ o resto da divisão de b^e por n. Dizemos que $C(b)$ é a forma reduzida de $b^e \equiv C(b) \pmod{n}$.

2.5.2.3 Decodificação

Para decodificar a mensagem teremos uma chave dada por (n, d). O valor do inteiro positivo d é dado pelo inverso de e módulo $\varphi(n)$. Ou seja, como (e, $\varphi(n)$) = 1, então existe

$d \in \mathbb{Z}$, tal que:

$$e \cdot d \equiv 1 \pmod{\varphi(n)}. \tag{2.19}$$

A chave de decodificação, $a = C(b)$, passará a ser $D(b)$ dado por:

$$(C(b))^d \equiv D(b) \pmod{n}, \tag{2.20}$$

sendo $D(b)$ o resto da divisão de $(C(b))^d$ por n. Isso significa dizer que $D(b)$ é a forma reduzida de $(C(b))^d \equiv D(b) \pmod{n}$. E dessa maneira os dados são decodificados, permitindo que se entenda a mensagem original.

2.5.2.4 Funcionamento do Método RSA

O método só vale se, após a codificação dos blocos codificados, obtém-se os blocos da mensagem original. Com isso, para saber se o método funciona de maneira correta, é preciso provar o que se encontra em (2.18). Ou seja,

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

Proposição 2.1. *O funcionamento do método RSA é válido quando* $D(C(b)) = b$.

Demonstração. Considere d o inverso de e módulo $\varphi(n)$, tem-se que $ed = 1 + k \cdot \varphi(n)$, $k \in \mathbb{Z}$, com $k, d, e \in \mathbb{Z}$ e ainda $d, e > 2$. Mas como $\varphi(n) > 0$, então $k > 0$ e isso possibilita trocar ed por $1 + k\varphi(n)$. Daí,

$$D(C(b)) \equiv (b^e)^d \equiv b^{1+k\varphi(n)} \pmod{n} \equiv b \cdot b^{k\varphi(n)} \pmod{n}$$

Mas, como $\varphi(n) = (p-1)(q-1)$, então:

$$D(C(b)) \equiv b \cdot b^{k(p-1)(q-1)} \pmod{n}$$

Assim,

- Suponha que $p \nmid q$, então usando o Pequeno Teorema de Fermat,

  $$b^{p-1} \equiv 1 \pmod{p}$$

  Logo,

  $$b^{ed} \equiv b \pmod{p}$$

- Suponha que $p \mid q$, logo, sendo eles primos, então $p = q$:

$$b \equiv 0 \pmod{p}$$

Logo,

$$b^{ed} \equiv b \pmod{p}, \quad \text{para qualquer } b.$$

Portanto, $b^{ed} \equiv b \pmod{n}$, ou seja, $D(C(b)) = b$.

□

2.5.2.5 Segurança do Método RSA

Como o método tem a chave pública, a mesma é de livre acesso a qualquer usuário. Assim, a segurança do RSA tem um de seus focos voltado à dificuldade de se calcular d a partir de n e e, conhecidos.

O cálculo de d só é possível se forem conhecidos e e $\varphi(n)$. Mas, vale lembrar que os parâmetros, p e q, não são públicos. Dessa forma, para encontrar $\varphi(n)$ é preciso fatorar n e obter os parâmetros. Isso nos leva a entender que a outra preocupação da segurança do método baseia- se na dificuldade de fatorar n, usando os algoritmos de fatoração que conhecemos. Logo, os valores dos parâmetros necessitam ser muito grandes para que a fatoração de n seja impossibilitada de ser efetuada.

Efetivamente, se n é fatorado, então é possível achar $\varphi(n)$ usando os cálculos feitos na outra seção, para decodificar mensagens. Todavia, caso seja inventado um algoritmo que consiga calcular $\varphi(n)$ sem ter os parâmetros conhecidos, teremos $n = pq$ e $\varphi(n) = (p-1)(q-1)$ conhecidos. Daí,

$$\varphi(n) = (p-1)(q-1) = pq - (p+q) + 1 = n - (p+q) + 1,$$

portanto,

$$p + q = n - \varphi(n) + 1.$$

Em compensação, temos que:

$$(p+q)^2 - 4n = (p^2 + q^2 + 2pq) - 4n = (p^2 + q^2 - 2pq) = (p-q)^2$$

assim,

$$p - q = \sqrt{(n - \varphi(n) + 1)^2 - 4n}$$

e das duas equações segue que:

$$p = \frac{\sqrt{(n-\varphi(n)+1)^2 - 4n} + n - \varphi(n) + 1}{2}$$

e

$$q = -\frac{\sqrt{(n-\varphi(n)+1)^2 - 4n} + n - \varphi(n) + 1}{2}.$$

Logo, temos n fatorado se conhecemos $\varphi(n)$.

Faremos a seguir uma aplicação do método RSA, partindo de um exemplo pequeno, porém relevante, indicando cada etapa do método de maneira separada.

1. Pré-codificação

Para realizar esta etapa, usamos a tabela retirada de [13] p. 181.

Tabela 5: Tabela de Conversão.

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

De posse da tabela acima, será feita a pré- codificação da palavra FAMÍLIA. Daí, convertendo a palavra na sequência numérica, seu resultado será:

$$15102218211810 \tag{1}$$

Para continuar a utilizar o método RSA o próximo passo é ter o número n, formado pelo produto dos números primos p e q. Tomaremos aqui para p e q os valores 11 e 17, respectivamente, e a sequência (1) passará agora pela quebra dos blocos (b). Como a quebra é aleatória e como $n = 11 \cdot 17 = 187$, então $b < 187$. Assim, os blocos formados são:

$$15 - 102 - 21 - 82 - 11 - 8 - 10, \tag{4}$$

onde $b_1 = 15$, $b_2 = 102$, $b_3 = 21$, $b_4 = 82$, $b_5 = 11$, $b_6 = 8$ e $b_7 = 10$.

2. Codificação

Nesta etapa o valor de $n = 187$ é usado. Mas, além de n é preciso ter outro número inteiro, no caso e, com $mdc\,(e, \varphi(n)) = 1$. Logo, se $p = 11$, $q = 17$ e $n = 187$, então temos:

$$\varphi(n) = (11-1)(17-1) = 10 \cdot 16 = 160.$$

Dando continuidade, se $\varphi(n) = 160$, fica escolhido o número 3 para ser e, uma vez que este é o menor número primo que não divide 160, ou seja, $e \nmid 160$.

Com efeito, a pré-codificação já dividiu a mensagem em blocos menores que n e a codificação desses blocos é denotada por $C(b)$. Além disso, o par $(187, 3)$ é a chave de codificação e o valor de $C(b)$ consiste no resto da divisão de b^e por n, ou seja,

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

Dito isso, as codificações dos blocos de (4) serão:

Para $b_1 = 15$,

$$15^3 \equiv C(15) \pmod{187}, \quad \text{logo} \quad C(15) = 9.$$

Para $b_2 = 102$,

$$102^3 \equiv C(102) \pmod{187}, \quad \text{logo} \quad C(102) = 170.$$

Para $b_3 = 21$,

$$21^3 \equiv C(21) \pmod{187}, \quad \text{logo} \quad C(21) = 98.$$

Para $b_4 = 82$,

$$82^3 \equiv C(82) \pmod{187}, \quad \text{logo} \quad C(82) = 92.$$

Para $b_5 = 11$,

$$11^3 \equiv C(11) \pmod{187}, \quad \text{logo} \quad C(11) = 22.$$

Para $b_6 = 8$,

$$8^3 \equiv C(8) \pmod{187}, \quad \text{logo} \quad C(8) = 138.$$

Para $b_7 = 10$,

$$10^3 \equiv C(10) \pmod{187}, \quad \text{logo} \quad C(10) = 65.$$

Desta feita, a mensagem codificada será:

$$9 - 170 - 98 - 92 - 22 - 138 - 65. \tag{5}$$

3. Decodificação

Esta fase é realizada conhecendo n e o inverso de e por $\varphi(n)$, sendo denotado aqui por d. Numericamente falando, fazendo a divisão de $\varphi(187) = 160$ por $e = 3$, teremos

$$160 \equiv 1 \pmod 3$$

pois,

$$160 = 3 \cdot 53 + 1$$

$$1 = 160 + 3 \cdot (-53)$$

ficando o inverso de 3 módulo 160 sendo -53, mas como d deve ser positivo, temos que

$$d = 160 - 53 = 107$$

já que

$$-53 \equiv 107 \pmod{160}.$$

Logo, o par $(187, 107)$ é a chave decodificadora.

Prosseguindo, denotando por $a = C(b)$ os blocos das mensagens codificadas, então $D(a)$ será a resposta da decodificação e, da mesma forma, $D(a)$ é o resto da divisão de a^d por n.

Vejamos:

Para $a = 9$,

$$D(9) \equiv 9^{107} \pmod{187} = 15$$

Para $a = 170$,

$$D(170) \equiv 170^{107} \pmod{187} = 102$$

Para $a = 98$,

$$D(98) \equiv 98^{107} \pmod{187} = 21$$

Para $a = 92$,

$$D(92) \equiv 92^{107} \pmod{187} = 82$$

Para $a = 22$,

$$D(22) \equiv 22^{107} \pmod{187} = 11$$

Para $a = 138$,

$$D(138) \equiv 138^{107} \pmod{187} = 8$$

Para $a = 65$,

$$D(65) \equiv 65^{107} \pmod{187} = 10.$$

Portanto, a mensagem decodificada está da mesma forma que a codificada.

CAPÍTULO 3

Uso da Aritmética Modular na Sala de Aula

Ao trabalhar na educação básica o docente necessita buscar diferentes meios de promover o conhecimento em sua área de atuação. No que se refere à aritmética modular e à construção do conhecimento na sala de aula, tal campo da matemática é entendido corriqueiramente por muitos, sendo trabalhado abstratamente. Desta feita, este capítulo traz algumas atividades realizadas com alunos do oitavo e do nono ano do Ensino Fundamental, além de também terem sido aplicadas em quatro turmas de primeiro ano do Ensino Médio.

3.1 Os Calendários e o Algoritmo de Zeller

Existem diferentes tipos de calendários pelo mundo, muitos criados antes de Cristo, cuja finalidade está voltada à carência de explicar fenômenos, divisões de tempo, festividades religiosas, épocas de plantio e colheita, além de satisfazer necessidades políticas, econômicas e culturais.

Por longos anos os astros eram observados da Terra e isso permitia ao homem quantificar seu tempo estabelecendo certos critérios na medição da passagem do tempo por intermédio dos movimentos de rotação e translação. O homem pré-histórico precisava observar o céu e adquirir informações relevantes à sua tribo no que se refere à utilização da luz solar, das geadas, das colheitas e posteriormente das épocas de plantio. Desse modo, o sol, a lua e as suas fases eram usados como relógios. Muitas culturas antigas reverenciavam a lua, dentre eles: egípcios, gregos, sumérios e romanos.

Segundo [7], há uma estimativa de que existam cerca de quarenta tipos de calendários

ainda usados pelo mundo, alguns deles são: indiano, islâmico, chinês e gregoriano. Também existem relatos de calendários que hoje não são mais usados, tais como o hindu, o juliano, o francês e o maia.

Conforme mostra [5], o algoritmo ou Regra de Zeller permite calcular o dia da semana referente a uma data passada ou futura. Esse algoritmo possui tal nome devido ao seu inventor, o alemão Reverendo Julius Christian Johannes Zeller, nascido em 1822 e falecido em 1899.

Em 1882 Zeller publicou o algoritmo, também presente em [5]:

$$s(d, m, A) = d + 1 + [(13m - 1)/5] + A + [A/4] - [A/100] + [A/400] \pmod 7.$$

Pelo algoritmo dado, tendo uma divisão $[a/b]$, com $a, b \in \mathbb{N}$, denotamos o quociente de a por b, com $b \neq 0$, como sendo o maior inteiro menor do que ou igual ao número racional a/b.

Segundo a regra, uma data é composta por três números:

$d =$ dia;

$m =$ mês;

$A =$ ano.

Vale citar que nesse algoritmo o mês 1 é março, daí janeiro e fevereiro são os meses 11 e 12, respectivamente. Tendo, por exemplo, a data de 20 de fevereiro de 1948, sua representação será $(20, 12, 1948)$.

Para os dias da semana, a numeração é feita como sendo: domingo (1), segunda-feira (2), $\cdots$, sexta- feira (6), sábado (0).

3.1.1 Prática 01 (Relacionada às atividades 01, 02, 03, 04)

Público alvo: alunos do oitavo e do nono ano de uma escola privada da cidade de João Monlevade, além de quatro turmas do primeiro ano do ensino médio de uma escola estadual da mesma cidade. No que se refere aos alunos da escola pública, as atividades foram realizadas com 02 alunos portadores de necessidades especiais inseridos nos grupos de trabalho . Esses alunos possuem desenvolvimento mental de uma criança com idade de sete a oito anos, laudados.

Materiais utilizados: folha $A4$ com as atividades, aparelhos celulares, certidões de nascimento dos alunos, lápis e borracha.

Distribuição das turmas: grupos de quatro alunos em cada.

Tempo gasto: Dois horários de 50 minutos.

Figura 5: Aluna portadora de necessidades especiais participando da atividade do algoritmo de Zeller.

Descrição: Começamos o trabalho fazendo uma pesquisa sobre tipos de calendários e debatemos a importância dos mesmos. Em outro momento os alunos receberam um texto, onde o mesmo servia de embasamento para as aplicações do algoritmo de Zeller. Em decorrência disso, as atividades abaixo aconteceram nos grupos e as intervenções eram feitas, quando necessárias.

ATIVIDADES USANDO O ALGORITMO DE ZELLER:

01. Conforme as explicações em sala, faça seus cálculos e descubra o dia da semana em nasceu. Em seguida, confira se o resultado de seus cálculos está de acordo com sua certidão de nascimento ou utilize o celular para conferir a resposta na parte de calendários.

02. Encontre em que dia da semana aconteceu a abolição da escravidão. Como lembrete vale relatar que esse evento foi em 13 de maio do ano de 1888.

03. Em que dia da semana ocorrerá o natal do ano de 2064?

04. Agora, descubra o dia do mês de maio em que acontecerá o dia das mães do ano de 2085.

Observação: Na escola estadual os grupos que continham os alunos especiais, deixaram para esses a tarefa de conferir nos celulares se os dias da semana batiam com os valores encontrados pelos colegas na congruência módulo 7 de cada atividade.

Relato da prática em sala de aula: Inicialmente foram realizadas pesquisas com os educandos do primeiro ano do Ensino Médio e com os alunos do Ensino Fundamental. As pesquisas foram feitas nas salas de informática das escolas e ocorreram questionamentos durante as mesmas, enfatizando sobre a necessidade de se trabalhar com calendários, suas utilidades, vantagens e desvantagens.

Aos alunos foi pedido que perguntassem em casa qual dia da semana em que nasceram e conferissem em suas certidões de nascimento, quando estas possuíssem tal informação. Na aula seguinte, o algoritmo de Zeller foi apresentado em sala e os meninos o utilizaram para conferir a veracidade do dia da semana de seus nascimentos. Mas, como muitas certidões não continham qual era o dia da semana, o celular serviu de instrumento de verificação pelos alunos na parte dos calendários.

Dando continuidade, as três primeiras atividades foram feitas com êxito pela maioria dos grupos e uma quantia de pequenos grupos chegou a errar nos momentos das divisões. Os grupos com maiores erros foram os da turma de oitavo ano. Todos os alunos demonstraram um enorme interesse e fizeram mais utilizações do algoritmo com relação à datas que julgavam importantes em suas vidas.

Quando a atividade 4 foi trabalhada os alunos estavam livres para realizar o raciocínio que fosse mais vantajoso, mas sempre usando o algoritmo. Nesta atividade, o tempo para a conclusão foi mais lento e muitos grupos conseguiram chegar ao resultado correto pelo fato de considerarem o segundo domingo de maio como fator crucial. Um grupo nos chamou atenção ao justificar que se o dia ocorre no segundo domingo, então a primeira data a ser analisada deveria ser 07 de maio. Assim, ao descobrirem o dia da semana desta data, ficava fácil de se chegar à resposta correta. Logo, como daria numa segunda-feira, então dia 06 seria o primeiro domingo e, respectivamente, o dia 13 seria o dia das mães.

As atividades em todas as turmas duraram quase um horário de 50 minutos, sobrando um tempo para os alunos descobrirem os dias da semana de outras datas relativas aos seus interesses. As turmas de oitavo e nono tiveram ainda a tarefa de ensinar a aplicação do algoritmo em casa para algum familiar e isso trouxe relatos surpreendentes dos pais.

3.2 Uso da Criptografia com a Cifra de Substituição

Quando mensagens são enviadas por meio de códigos, o que ocorre é que a mensagem original passa por um processo de codificação, se tornando uma mensagem secreta. Em seguida, a mensagem secreta é enviada e sofre uma decifração. As letras, números ou outros símbolos usados na criptografia para decifrar mensagens são chamados de chaves ou senhas e tais chaves

devem ser conhecidas apenas por quem envia e por quem recebe a mensagem.

3.2.1 Prática 02 (Relacionada às atividades 05 e 06)

Público alvo: mesmo, já citado.

Materiais utilizados: folha $A4$ com as atividades, lápis e borracha.

Distribuição das turmas: grupos de quatro alunos em cada.

Tempo gasto: Uma média de 25 minutos, incluindo o debate sobre a importância da criptografia e suas aplicações por governantes e militares.

Observação: Na escola estadual os grupos com os alunos especiais permitiram que os mesmos, em seu tempo mais delongado, fizessem as duas atividades.

Descrição: As atividades a seguir foram entregues aos alunos após uma discussão relativa à importância da criptografia em operações militares e no que tange ao uso da mesma na parte de segurança em redes sociais.

ATIVIDADES USANDO CRIPTOGRAFIA BÁSICA:

05. Pela tabela dada, use a cifra por substituição e descubra a frase dita por um pensador famoso. Em seguida, encontre também quem foi esse pensador.

Tabela 6: Cifras por Substituição.

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

LH-MFNVILH-TLEVIMZN-L-NFMWL. (KOZGZL)

06. Em um avião tinham 4 romanos e 1 inglês. Sabendo disso, qual o nome da aeromoça?

Caso tenha dúvidas sobre a resposta desta questão de lógica, use a mesma tabela para verificar se sua resposta está correta, conforme a cifra dada por:

RELMV

Relato da prática em sala de aula: Como os alunos eram os mesmos e já estavam bastante a vontade em seus grupos, foi possível evidenciar uma maior participação oral no momento das discussões sobre o tema. Mesmo sendo atividades pequenas e de rápida resolução, as mesmas despertaram tamanho interesse nos alunos e, com o tempo que sobrou, todos eles usaram a tabela de cifras para fazer um bilhete para um colega de maior afinidade. Na hora da conversa, foi relatada a existência de tipos mais elaborados de criptografia e falou-se um pouco,

mesmo que brandamente, sobre o método RSA. Tal método despertou a curiosidade dos alunos e alguns do nono ano trouxeram para a outra aula algumas questões relativas à segurança de dados na internet.

Em relação à participação dos alunos especiais, este foi um momento muito gratificante, pois os alunos em questão relataram sobre a falta que sentem em poder trabalhar com atividades iguais às de seus colegas de turma.

3.3 Encontrando Números Primos pelo Crivo de Eratóstenes

O crivo de Eratóstenes, mostrado na fundamentação teórica, permite encontrar quais são os números primos existentes até um determinado número já estabelecido.

3.3.1 Prática 03 (Relacionada à atividade 07)

Público alvo: mesmo, já citado.

Materiais utilizados: folha $A4$, lápis de escrever, lápis de cor ou canetas coloridas, régua e borracha.

Distribuição das turmas: grupos de quatro alunos em cada.

Tempo gasto: Uma média de 20 minutos, contando com a explicação sobre a construção do crivo.

Observação: Mesmo com a explicação dada, os alunos especiais necessitaram ser auxiliados na contagem dos números. Esses alunos iam riscando os números que eram múltiplos, apesar de não entenderem a profundidade do conceito dos mesmos.

Descrição: Foi solicitado que os alunos fizessem uma tabela, o crivo, usando apenas números ímpares maiores que um. Em seguida, os alunos deveriam ir riscando os números de três em três, depois de cinco em cinco, de sete em sete e assim por diante até que não restasse mais nada a ser riscado na tabela. Logo, foi mostrado que os números restantes eram os primos, lembrando de acrescentar o 2 no resultado.

Para alunos do oitavo ano o número máximo pedido foi o 60, como na tabela. Para as outras turmas foi pedido que fizessem o crivo até 100.

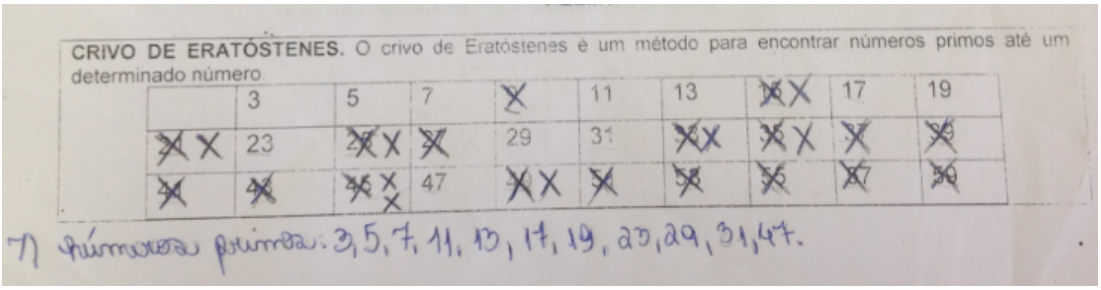

Figura 6: Atividade do crivo de Eratóstenes feita incorretamente por um grupo do oitavo ano.

CRIVO DE ERATÓSTENES. O crivo de Eratóstenes é um método para encontrar números primos até um determinado número.

***	3	5	7	9	11	13	15	17	19
21	23	25	27	29	31	33	35	37	39
41	43	45	47	49	51	53	55	57	59

07. Pelo método do crivo de Eratóstenes, explicado em sala, encontre quais os números primos até 60.

Relato da prática em sala de aula: Nesta atividade os alunos foram bem rápidos e a mesma foi mais prazerosa com os alunos do oitavo ano, porém nessa turma alguns alunos se esqueceram do número 2 na resposta. Como mostra a foto com a atividade, também erraram na quantidade dos números primos e acharam que o último deles seria o 47 . Para as demais turmas, o processo se deu sem muito diálogo entre os componentes dos grupos.

Alguns alunos disseram se lembrar da técnica aplicada, porém relataram que os docentes de anos anteriores pediam para que colocassem os naturais de 2 até o valor estipulado. Depois os alunos iam riscando todos os números pares com exceção do 2. Só após essa parte, é que eles começavam a riscar os múltiplos dos números ímpares.

3.4 O Uso dos Dígitos Verificadores em Códigos de Barras

Para a atividade com códigos de barras foi utilizado um texto base, retirado de estudos feitos no capítulo 2. Esse texto mostrava a importância desses códigos, além de trazer a explicação do uso de congruência e do operador módulo.

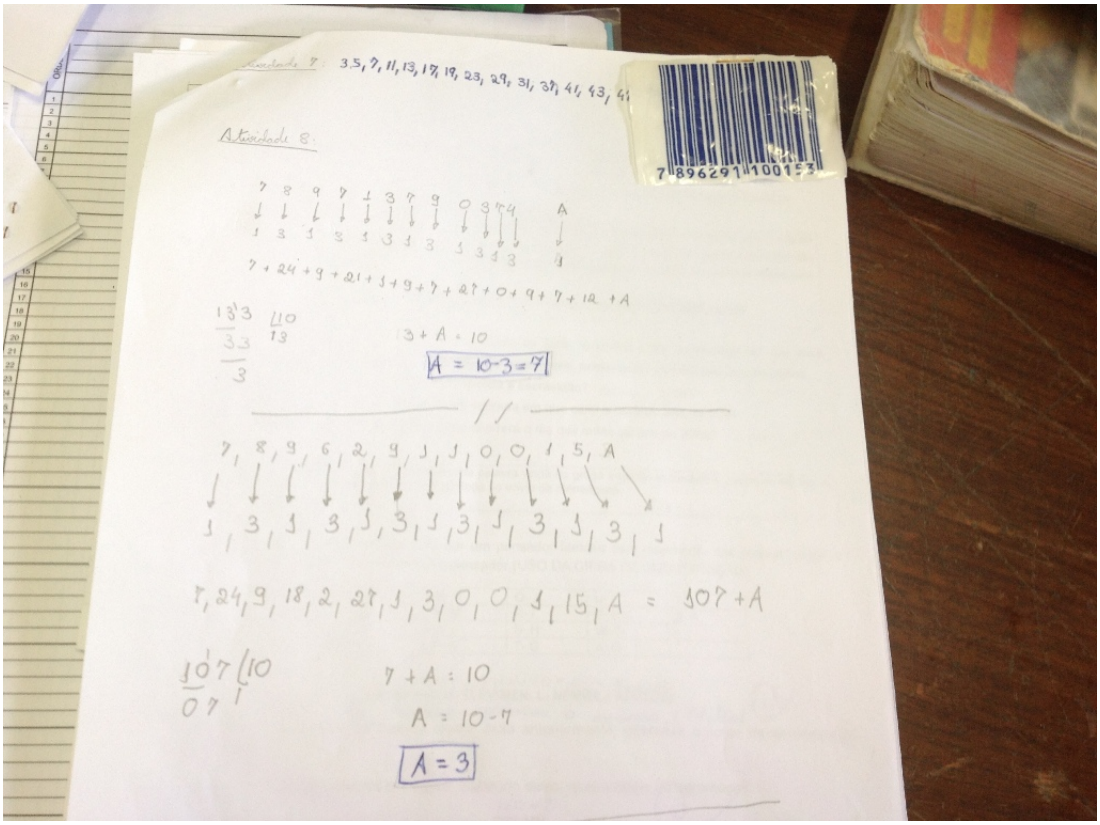

Figura 7: Atividade envolvendo dígitos verificadores em códigos de barras.

3.4.1 Prática 04 (Relacionada à atividade 08)

Público alvo: mesmo, já citado.

Materiais utilizados: folha $A4$ com o texto e a atividade, lápis de escrever, códigos de barras, cola e borracha.

Distribuição das turmas: mesmos grupos.

Tempo gasto: Uma média de 40 minutos, contando com a explicação da congruência aplicada e a interpretação do texto dado.

Observação: Os alunos especiais ficaram de selecionar os códigos trazidos, analisando quais começavam com os três primeiros dígitos iguais.

Descrição: Os alunos passaram pela interpretação do texto, aprendendo como identificar o país de origem do produto, além das outras partes da sequência numérica. Em seguida, foi explicado como se encontrava o dígito verificador no código.

08. Conforme o código de barras que está no quadro, separe a sequência numérica com base nos exemplos dados em sala, mostrando o país, a empresa, o produto e o dígito verificador,

contidos no mesmo.

Em seguida, utilize o código de barras trazido por você para realizar o processo de constatação do dígito verificador presente no seu código(Favor colar seu código na folha e deixar todos os cálculos na mesma).

Para esta atividade, vamos tomar α como sendo a sequência do código que você trouxe e $\beta = \begin{bmatrix} 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 & 1 \end{bmatrix}$ será nossa matriz peso. Colocaremos A no lugar do último dígito, ou seja do dígito verificador.

Em seguida, para encontrar o dígito verificador, A, é necessário satisfazer a seguinte congruência dada abaixo:

$$SOMA + A \equiv 0 \pmod{10}$$

Relato da prática em sala de aula: Mesmo sem os alunos saberem o conceito e as operações com matrizes, com ajuda das explanações básicas dadas em sala, eles conseguiram entender a forma de trabalhar e desenvolver a atividade proposta. Pela figura que mostra a atividade com código de barras, é possível notar que os alunos desenvolveram a atividade sem necessitar do uso de operação com matrizes. No momento da explicação falamos superficialmente das matrizes e citamos que seria um conteúdo dado mais adiante, em outra série.

O desfecho da atividade ocorreu de forma tranquila, com exceção do oitavo ano e de dois grupos do nono que erraram na parte final de seus cálculos. No ensino médio muitas dúvidas apareceram, mas os resultados saíram corretos.

3.5 Calculando Dígitos Verificadores em CPF

Para a atividade abaixo um texto base serviu para conceituar e retirar pequenas dúvidas trazidas pelos alunos. Da mesma forma do outro texto, este também foi construído a partir do capítulo precedente, contendo maiores informações relativas ao assunto aqui trabalhado.

3.5.1 Prática 05 (Relacionada à atividade 09)

Público alvo: mesmo, já citado.

Materiais utilizados: folha $A4$ com o texto e a atividade, lápis de escrever, documentos dos próprios alunos e borracha.

Distribuição das turmas: mesmos grupos.

Tempo gasto: Uma média de 50 minutos, contando com a explicação das congruências e a interpretação do texto dado.

Figura 8: Atividade sobre dígitos verificadores no CPF.

Observação: Nos grupos com os alunos especiais, os documentos usados foram os deles.

Descrição: Os alunos passaram pela interpretação do texto e depois deveriam mostrar como se trabalha com os dígitos verificadores presentes no seus relativos cadastros de pessoas físicas.

09. De acordo com as explicações dadas em sala, encontre os dois dígitos verificadores do CPF trazido por você. Deixe seus cálculos na folha da atividade e lembre-se: existem duas matrizes de peso distintas, uma para encontrar o a_{10} e outra para o a_{11}.

Relato da prática em sala de aula: A atividade foi a mais demorada e difícil, conforme relato dos alunos. O oitavo ano continuou com maior dificuldade que as outras turmas e os especiais ficaram ociosos desta vez. Os alunos se mostraram com mesmo afinco para realizar a atividade, porém as turmas do Ensino Médio gastaram a metade do tempo oferecido para desempenhar a atividade.

3.6 Relato das Atividades de Modo Geral

No decorrer do planejamento das atividades aqui relatadas, não fazíamos ideia do quanto a aplicação das mesmas seria um diferencial em nosso trabalho. Mesmo fazendo as práticas em turmas de séries distintas o interesse foi o mesmo.

Colegas se ajudando e perguntando como as coisas funcionavam; dúvidas relativas às divisões eram sanadas; respostas em torno da serventia dos documentos usados e como verificar se os mesmos são verdadeiros; curiosidades sobre criptografia eram pesquisadas, dentre outras observações feitas foi um marco para percebermos o quanto podemos trabalhar com a aritmética modular na Educação Básica.

Nas atividades descobrimos que aqueles alunos com notas menores foram os mais focados e com as melhores participações orais.Tais alunos procuraram professores de outras áreas, como o de História, para responder questões envolvendo a criptografia em operações militares.

Alguns pais nos procuraram e mandaram bilhetes elogiando o trabalho feito, pois viram como seus filhos chegaram em casa relatando sobre algumas atividades.

Em suma, vale descrever o quanto foi gratificante fechar nosso estudo com esta parte prática. A mesma nos fez ver mais uma vez que necessitamos buscar o aperfeiçoamento de nosso trabalho na sala de aula, já que os livros didáticos não trazem tudo o que nossos alunos precisam para entender de forma satisfatória a matemática do cotidiano.

Conclusão

Com este trabalho conseguimos perceber que a aritmética modular pode ser usada na Educação Básica de maneira satisfatória para ambas as partes, tanto com professores quanto com alunos. Com isso, para maior aprendizagem, recomendamos que pesquisas teóricas sejam realizadas com os alunos a fim de motivá-los ao alcance da compreensão e do interesse de cada área voltada às práticas com a aritmética dos restos.

Recomendamos também que o momento das atividades em grupo seja bem planejado, de forma que existam atividades voltadas para diferentes níveis de aprendizagem, incluindo aquelas focadas nos alunos portadores de necessidades especiais, sendo isso alvo de extrema importância. Por meio das observações feitas constatamos que o uso da contextualização de conteúdos com as pesquisas e os textos, facilitou bastante a compreensão dos conhecimentos matemáticos. Essa prática dos grupos trazendo seus próprios materiais, tais como códigos de barras e seus documentos nos mostrou que pode ser aplicada com regular frequência pelos professores e que os alunos acabam dando maior valor.

Concluindo, esperamos que este estudo possa auxiliar profissionais da educação básica no entendimento e na inserção de atividades voltadas ao uso da aritmética modular. Isso porque consideramos que essa área da matemática seja de tamanha relevância na construção do conhecimento dos alunos. Dada sua importância, pensamos que ainda há muito a ser explorado , já que existe um vasto campo para estudos posteriores dos assuntos aqui apresentados. Sendo assim, anelamos que este trabalho possa ser válido para outros que ainda virão, tanto na teoria quanto na prática.

Referências

[1] T. Cássia Regina dos Santos. Ensinando matemática através dos códigos de barras. *Ciência e Natura - 35 anos*, 37:278–288, 2015. 28

[2] J.P. de Oliveira Santos. *Introdução teoria dos números*. Coleção Matemática Universitária. Instituto de Matemática Pura e Aplicada, 2011. 12

[3] B. Fernando B. et al. Rsa: Criptografia assimétrica e assinatura digital., outubro 2017. 28

[4] A. Gonçalves. *Introdução à Algebra*. Projeto Euclides. Instituto de Matemática Pura e Aplicada, 2003. 12, 13

[5] A. Hefez. *Aritmética:*. Coleção PROFMAT. Sociedade Brasileira de Matemática, 2014. 12, 13, 17, 25, 26, 48

[6] H. Jeffrey, P. Jill, and S. Joseph H. *An introduction to mathematical cryptography.*, volume 1. Springer, 2009. 28

[7] J. Manoel A. R. Os calendários e a sua contribuição para o ensino da física. Master's thesis, Universidade do Porto, Porto, Portugal, 2012. Acesso em: julho de 2017. 47

[8] F. B. Martinez, C. G. Moreira, N. Saldanha, and E. Tengan. *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*. IMPA, 2015. 26

[9] O. Maykon Costa de. Arimética: Criptografia e outras aplicações de congruências. Master's thesis, Universidade Federal do Mato Grosso do Sul, Campo Grande, MS, 2013. 74p. 38

[10] K.I.M. Oliveira and A.J.C Fernández. *Iniciação a Matemática: um curso com problemas e soluções*. Sociedade Brasileira de Matemática, 2012. 12, 14

[11] M. Pedro L. *Atividades de contagem a partir da criptografia.* IMPA/OBMEP, 2015. 77p. 28

[12] C. Polcino Milies. A matemática dos códigos de barras. pages 1–19, 2006. 31, 32

[13] C. Severino Collier. *Números inteiros e criptografia RSA*. IMPA, 2014. 28, 44