UNIVERSIDADE ESTADUAL DO SUDOESTE DA BAHIA

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

ABIZAI CAMPOS LIMA

APLICAÇÕES DE ARITMÉTICA MODULAR NA EDUCAÇÃO BÁSICA A PARTIR DA RESOLUÇÃO DE PROBLEMAS

Vitória da Conquista/BA

2019

UNIVERSIDADE ESTADUAL DO SUDOESTE DA BAHIA

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE

NACIONAL – PROFMAT

ABIZAI CAMPOS LIMA

APLICAÇÕES DE ARITMÉTICA MODULAR NA EDUCAÇÃO BÁSICA A PARTIR DA RESOLUÇÃO DE PROBLEMAS

Dissertação apresentada ao Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, oferecido pela Universidade Estadual do Sudoeste da Bahia – UESB, como requisito necessário para obtenção do grau de Mestre em Matemática. Orientadora: Profª. Drª Alexsandra Oliveira Andrade.

Vitória da Conquista/BA

2019

L696a Lima, Abizai Campos.
Aplicações de aritmética modular na educação básica a partir da resolução de problemas. / Abizai Campos Lima, 2019.
61f. il.
Orientador (a): Drª . Alexsandra Oliveira Andrade.
Dissertação (mestrado) – Universidade Estadual do Sudoeste da Bahia, Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, Vitória da Conquista - BA, 2019.
Inclui referências. 60 - 61.
1. Aritmética modular – Educação básica. 2. Códigos de barras. 3. Criptografia. 4. Aprendizagem Baseada em Problema. I. Andrade, Alexsandra Oliveira. II. Universidade Estadual Sudoeste da Bahia, Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, Vitória da Conquista, III. T.

CDD: 513

Catalogação na fonte: Juliana Teixeira de Assunção- CRB 5/1890
UESB – Campus Vitória da Conquista – BA

ABIZAI CAMPOS LIMA

APLICAÇÕES DE ARITMÉTICA MODULAR NA EDUCAÇÃO BÁSICA A PARTIR DA RESOLUÇÃO DE PROBLEMAS

Dissertação apresentada ao Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, oferecido pela Universidade Estadual do Sudoeste da Bahia – UESB, como requisito necessário para obtenção do grau de Mestre em Matemática.

BANCA EXAMINADORA

Professora Drª. Alexsandra Oliveira Andrade (Orientadora)
Universidade Estadual do Sudoeste da Bahia – UESB

Prof. Dr. Flaulles Boone Bergamaschi
Universidade Estadual do Sudoeste da Bahia – UESB

Prof. Dr. Ronildo Pinheiro de Araújo Moura
Universidade Federal do Rio Grande do Norte– UFRN

Vitória da Conquista/BA

2019

AGRADECIMENTOS

Quero agradecer primeiramente a Deus por tudo quanto Ele me proporcionou de ensino e aprendizagem durante todo a minha vida e também nesse curso de Mestrado.

Quero a agradecer aos meus pais, pela dedicação, pelo amor, pelos valores transmitidos, pelos ensinos e pelas correções. Todos os esforços deles foram importantes para que eu chegasse até aqui. Eles são os meus grandes mestres.

Quero agradecer aos meus irmãos e irmãs que caminharam comigo até o presente momento, com atitudes e palavras de conforto e incentivo, sempre me proporcionando a felicidade e tranquilidade de que tanto necessitei.

Quero agradecer aos meus colegas de mestrado que em muitas horas foram solidários e sempre dispostos para ajudar uns aos outros.

Quero agradecer aos idealizadores e realizadores do projeto Profmat. Suas atitudes são de extrema importância para melhorar os níveis de conhecimento da matemática em nosso país.

Quero agradecer aos professores do curso de Mestrado Profissional em Rede em Matemática da Universidade Estadual do Sudoeste da Bahia, que semearam seus conhecimentos e nos ajudaram a enxergar ainda com mais clareza a beleza, a importância da matemática.

Em especial, quero agradecer à minha orientadora, Professora Drª Alexsandra Oliveira Andrade, que desde a graduação tem me ensinado importantes e valiosos conhecimentos matemáticos, mas além disso, tem me ensinado atitudes de compreensão, de respeito ao ser humano. Guardarei para sempre suas palavras e atitudes de incentivo e fé.

LISTA DE FIGURAS

LISTA DE TABELAS

RESUMO

Esse é um estudo sobre a aritmética modular na educação básica a partir da resolução de problemas numa escola da rede pública de educação. A aritmética é uma importante área da matemática que trouxe inúmeras contribuições para o desenvolvimento tecnológico, social e econômico da sociedade através do tempo. Uma teoria muito importante na realização dessa pesquisa é a Aprendizagem Baseada na Resolução de Problemas (APB), uma metodologia inovadora que busca colocar o aluno como protagonista do ato de aprender e ensinar. Nesse estudo tanto a aritmética quanto a APB estão intrinsicamente conectados como instrumentos de aprendizagens em matemática. Seus conceitos estão presentes nos códigos de barras usados no mundo todo, inclusive os EAN-13, utilizado no Brasil. A aritmética modular também se fazem presentes nos dígitos do CPF e nas mensagens criptografadas do imperador romano Júlio César, criptografia também se faz presentes atualmente nas operações bancárias ou mesmo quando enviamos um pequeno texto através dos aplicativos de mensagens.

Palavras Chaves: Aritmética modular, Códigos de Barras, Criptografia, Aprendizagem Baseada na Resolução de Problemas.

ABSTRACT

This is a study about Modular Arithmetic in elementary school with problem based learning in a Public School. Arithmetic is an important area of mathematics that has made countless contributions to the technological, social and economic development of society over time. A very important theory in this research is Problem Based Learning (PBL), an innovative methodology that seeks to place the student as the protagonist of the act of learning and teaching. In this study, both arithmetic and PBL are intrinsically connected as learning tools in mathematics. Their concepts are present in barcodes used worldwide, including the EAN-13, used in Brazil. Modular arithmetic is also present in the CPF digits and encrypted messages of the Roman emperor Julius Caesar, encryption is also present today in banking or even when we send a small text through messaging applications

Keywords: Modular Arithmetic, Barcodes, Cryptography, Problem Based Learning.

SUMÁRIO

INTRODUÇÃO.

A matemática, ciência que historicamente vem sendo construída e aperfeiçoada, é parte integrante na evolução da humanidade. Assim, compreender os conceitos que essa ciência traz torna-se vital para evolução da sociedade do conhecimento. Dentre esses conceitos, estão as operações com a divisibilidade de números inteiros e os de congruências estudadas dentro de um campo da matemática chamado de Aritmética.

A aritmética modular, através da congruência de números inteiros, também chamada de matemática dos restos, é ensinada nos níveis superiores, mas devido à sua importância, funcionalidade e fácil compreensão poderiam ser ensinadas na educação básica. Desde o 6º ano do ensino fundamental se estuda divisibilidade de números inteiros e seus possíveis restos dentro do campo de estudo da matemática. Surge daí uma provocação para se estudar a aritmética modular e suas aplicações na educação básica.

Diante da importância e do papel que a aritmética possui na formação do cidadão, esta pesquisa se deparou com a seguinte questão: É possível ensinar conceitos de aritmética modular e suas aplicações na educação básica?

Diante desse questionamento, esta pesquisa tem como objetivo contribuir no aprofundamento de estudos sobre o ensino da aritmética modular e suas aplicações na educação básica e no cotidiano dos seres humanos. Outro objetivo que se pretende alcançar com essa pesquisa é investigar o papel da Aprendizagem através da Resolução de problemas aplicada ao ensino da aritmética modular.

Metodologicamente, essa pesquisa constitui de uma revisão da literatura e de estudos já feitos sobre aritmética modular, na qual buscou-se fazer análises e interpretações de pesquisas já existentes. Trata-se um estudo sistemático e criterioso da literatura existente sobre o nível mais alto de aplicações de aritmética modular. Também foi uma experiência com 28 alunos da turma do 1º ano C do Ensino Médio do Colégio Estadual de Livramento através da metodologia proposta pela Aprendizagem Baseada na Resolução de Problemas, na qual os alunos resolveram uma lista de cinco questões abertas (em anexo) sobre aritmética modular.

Os referenciais citados nessa pesquisa foram coletados de artigos publicados em depositórios de universidades, centros de pesquisas e também foram coletadas informações e também pesquisas de livros de autores clássicos.

O segundo capítulo dessa pesquisa é dedicado ao estudo da aritmética modular, onde são demonstradas propriedades de divisibilidade, máximo divisor comum e número primo. Também são demonstrados os critérios de divisibilidade de números inteiros entre 2 e 10, assunto este amplamente abordado no 6º e 7º ano do ensino fundamental. Ainda nesse capítulo aborda-se a ideia de congruência de números inteiros.

O terceiro capítulo trata das aplicações da aritmética modular no contexto das vivências do próprio ser humano, ou seja, como ele utiliza esse campo da matemática para desenvolver mecanismos e tecnologias que facilitam sua própria vida. Nesse capítulo são estudados os algoritmos de aritmética modular presentes nos dígitos de documentos como o Cadastro de Pessoas Físicas (CPF), nos cartões de crédito. Também é abordado um tema de muita relevância nas vendas, nas transações comerciais, que são os códigos de barras; abordaremos esse tema como objeto de pesquisa da aritmética modular. Ainda nesse capítulo, é estudado outra aplicação da aritmética; a Cifra de César ou Código de César, um tipo de criptografia que o imperador romano Júlio César utilizava para se comunicar com os chefes dos exércitos do império romano.

Já o quarto capítulo abordamos a importância de se ensinar a matemática, a aritmética modular através de uma metodologia inovadora e desafiante, que é a Aprendizagem Baseada em Problemas também conhecida pela sigla APB, no qual o aluno é estimulado a estudar a matemática através de um contexto. Ainda nesse capítulo trazemos algumas sugestões de problemas ou situações-problemas que podem ser trabalhados no contexto do ensino de aritmética modular na educação básica para alunos a partir do 6º ano do ensino fundamental até as últimas séries do ensino médio.

No quinto capítulo propomos algumas atividades de aritmética modular para serem aplicados aos alunos da educação básica. Nessas atividades os alunos puderam relacionar os conceitos de divisão euclidiana com os de congruência. Entre essas aplicações, pode-se destacar que eles tiveram a oportunidade de aprender como a aritmética está presente em situações do nosso dia-dia.

Por fim, concluímos o trabalho trazendo sugestões para que se amplie a discussão sobre o ensino de aritmética modular na educação básica.

2 ARITMÉTICA MODULAR

O ensino de aritmética no ensino básico, principalmente, no nível fundamental, talvez compreenda a parte mais elementar da matemática, sendo justamente nesse nível que matemática começa a se mostrar como um instrumento útil para vida na sociedade. Somar, diminuir, dividir e multiplicar são instrumentos poderosos na vida de todos nós. Mas muitos questionamentos são feitos no processo ensino aprendizagem deste tema

> *Se a matemática é uma disciplina base de todas as ciências e todas as artes; se o domínio dos números e das operações é decisivo para o sucesso numa sociedade competitiva; se o desenvolvimento tecnológico está fundamentado em cálculos e logaritmos; se o Brasil é a terra de Malba Tahan... por que 89% dos estudantes chegam ao final do Ensino Médio sem aprender matemática?(AZEVEDO, 2008)*

Talvez precisamos ressignificar o ensino da aritmética, aproximando conceito aparentemente complexos, para a realidade de alunos.

2.1 - DIVISIBILIDADE

Inicialmente, denotaremos simbolicamente com $\mathbb{Z}$ o conjunto dos números inteiros e $\mathbb{N}$ o conjunto dos números naturais, com as operações de soma (+), multiplicação (.) e as relações de ordem $<$. Considera-se também um importante principio da matemática, chamado de Princípio da Boa Ordenação. Os teoremas e propriedades abordados nessa pesquisa também podem encontrados em HEFEZ (2005).

Definição 2.1 (2.3 de HEFEZ (2005)): Seja S um subconjunto de $\mathbb{N}$. Dizemos que um número natural a é um menor elemento de S se possui as seguintes propriedades:

i) $a \in S$,

ii) $\forall\, n\, S \in , a \leq$n

Para HEFEZ (2005), é possível verificar que, se *S* possui um menor elemento, este é único. Observe que, se *a* e *a'* são menores elementos de *S*, então $a < a'$ e $a' < a$, o que implica que $a = a'$.

Sobre a divisibilidade de números inteiros, observe que dada uma equação do tipo $b \cdot x = a$, com $a, b \in \mathbb{Z}$, é possível que exista ou não soluções para ela dentro do conjunto dos números inteiros; dependendo dos valores dos coeficientes *a e b*. Caso exista uma solução, dizemos que *a é divisível por b*.

Definição 2.2: *Sejam a, b* $\epsilon \mathbb{Z}$*. Diz-se que a divide b se existir k* $\epsilon \mathbb{Z}$ *tal que* $b = a \cdot k$*. Se a divide b, diremos também que a é um divisor ou um fator de b. Podemos dizer ainda que b é um múltiplo de a.*

Para dizer que *a* divide *b*, usaremos a notação $a \mid b$. A negação da sentença, isto é, se *a* não dividir, ou b não ser um múltiplo de a, usaremos a notação $a \nmid b$. Assim, $a \nmid b$ se e somente se $b \neq a \cdot k$.

Exemplo 1: O conceito de divisibilidade é ilustrado nos exemplos a seguir.

$3 \mid 60$ *pois* $60 = 3 \cdot 20$;

$5 \mid 150$ *pois* $150 = 5 \cdot 30$;

$-32 \mid 544$ *pois* $544 = -32 \cdot (-17)$.

Analogamente, $2 \nmid 11$ pois $11 \neq 2 \cdot k$, para todo k $\epsilon \mathbb{Z}$.

Ressalta-se que se $b \neq 0$ na definição de divisibilidade acima, ele é único. Pois caso exista outro k', tal que $b = a \cdot k'$, teríamos $a \cdot k = a \cdot k'$, o que resultaria em k = k´. Tal inteiro, assim definido chama-se quociente de a *por* b, sendo indicado por $k = a \mid b = \frac{a}{b}$.

Ainda seguindo a definição de divisibilidade, note que se 0 | a se e somente se $a = 0$. Nesse caso, o quociente não é único, pois $0 \cdot k = 0$, para todo $k \epsilon \mathbb{Z}$. Por esse motivo, costuma-se excluir o caso em que o divisor é nulo. Aqui também faremos adesão a essa convenção, ou seja, sempre será excluído o caso em que o divisor é nulo.

Proposição 2.1: *Para quaisquer a, b, c, d* $\epsilon \mathbb{Z}$*, as seguintes propriedades são verdadeiras (vale lembrar que assumimos os divisores diferentes de zero)*

i) $a \mid a$.

ii) $Se\ a \mid b\ e\ b \mid c, então\ a \mid c.$

iii) $Se\ a \mid b\ e\ c \mid d, então\ a \cdot c \mid b \cdot d.$

iv) $Se\ a \mid b\ e\ a \mid c, então\ a \mid (b + c).$

v) $Se\ a \mid b, então\ para\ todo\ m \in \mathbb{Z}, \text{tem} - \text{se}\ que\ a \mid m \cdot b.$

vi) $a \mid b\ e\ a \mid c\ então, para\ todos\ \text{m, n} \in \text{Z, tem} - \text{se que}\ a \mid (m \cdot b + n \cdot c).$

Demonstração:

i) *É só observar que podemos escrever* $a \cdot 1 = a.$

ii) *Por definição, existem inteiros* $d\ e\ d'$*, tais que* $a \cdot d = b\ e\ b \cdot d' = c.$ *substituindo o valor de b dado pela primeira igualdade, temos que* $c = (a \cdot d) \cdot d' = a \cdot (d \cdot d')$*, assim a | c.*

iii) *Mais uma vez usando a definição, existem inteiros f e f´, tais que* $a \cdot f = b\ e$ $c \cdot f' = d$*. Efetuando ordenadamente ambos os termos da igualdade, temos* $a \cdot c\ (f \cdot f') = b \cdot d$*, concluímos dessa forma que* $a \cdot c \mid b \cdot d$.

iv) *Existem inteiros* $d\ e\ d'$*, tais que* $a \cdot d = d\ e\ a \cdot d' = c.$ *Somando ordenadamente ambas as igualdades, temos* $a \cdot (d + d') = b + c$*, assim* $a \mid (b + c)$.

v) *Se* $a \mid b$*, então deve existir um inteiro c tal que* $a \cdot c = b.$ *Multiplicando por m ambos os lados, temos* $a \cdot (cm) = b \cdot m.$ *Logo* $a \mid b \cdot m$*, segue diretamente de (v) e (iv).*

Exemplo 2 : Os exemplos a seguir são alusivos a cada uma das propriedades acima.

Propriedade (i): $7 \mid 7;\ 10 \mid 10;\ 275 \mid 275$

Propriedade(ii): Se $4 \mid 16\ e\ 16 \mid 336, logo\ podemos\ verificar\ que\ 4 \mid 336$

Propriedade (iii): Se$3 \mid 6\ e\ 5 \mid 10, logo\ podemos\ verificar\ que\ 3 \cdot 5 \mid 6 \cdot 10$

$Propriedade\ (iv)\ \ Se\ 7 \mid 56\ e\ 7 \mid 28, então\ como\ 28\ e\ 56\ são\ ambos\ múltiplos\ de\ 7, podemos\ perceber\ que\ 7 \mid (56 + 28)$

Propriedade (v): *Se* $6 \mid 24$, *tome* $3 \in Z$, *então* $6 \mid 3 \cdot 24$, *resolvendo o produto temos que* $6 \mid 72$

Propriedade (vi): $8 \mid 16$ *e* $8 \mid 32$, tome $3, 7 \in \mathbb{Z}$, *podemos verificar que* $8 \mid 3 \cdot 16 + 7 \cdot 32$, *que é equivalente a* $8 \mid 272$

Tome a *e* $b \in \mathbb{Z}$, pode acontecer que b não seja divisível por a. Nesse caso, é possível efetuarmos a divisão de b por a, no qual encontraremos um quociente q, admitiremos também a existência de um resto r, tal que $0 \leq r < a$. Tal processo de divisão é chamado de *Divisão Euclidiana.*

2.1 – Teorema 2.1: (*Divisão Euclidiana)***:** *Dados a e b dois números naturais com* $a < b$. *Existem dois únicos números naturais quaisquer tais que* $b = a \cdot q + r$, com $r < a$.

Demonstração:

Inicialmente, vamos mostrar a existência dos números q e r.

Seja a um número natural. Considere o conjunto

$$S = \{a - b \cdot x, onde\ x \in \mathbb{N}\ e\ a - b \cdot x \geq 0\}$$

Note que $S \subset N$ *e que* $S \neq \emptyset$, $pois\ a = a - b \cdot 0 \geq 0$. *Sendo assim, como S é um subconjunto não vazio de N, é possível afirmar, baseado no Princípio da Boa Ordenação, que S possui um menor elemento. Vamos denotá-lo por r. Como* $r \in S$, *existe um natural x tal que* $r = a - b \cdot x$. *Chamando x=q, temos*

$$a = b \cdot q + r$$

Como $r \in S, tem - se\ que\ r \geq 0$. *Suponha por absurdo que* $r \geq b$. *Segue imediatamente que* $r - b \geq 0$.

Sendo assim, como $r = a - bq \Leftrightarrow r - b = a - b \cdot q - b \Leftrightarrow r - b = a - b \cdot (q - 1) \in S$

observe que $r - b$ *é menor que r, o que é um absurdo, pois r é o menor elemento de S, logo* $r < b$

Sendo assim, no caso $a, b \in \mathbb{N}\ com\ b > 0$, *existem q e r naturais com a* $0 \leq r < B$

Agora consideremos o caso em que $a < 0$ *e* $b > 0$. *Temos então que* $-a \in \mathbb{N}$, *daí existem* $q', r' \in \mathbb{N}$, *tais que* $-a = b \cdot q' + r'$ *e* $0 \leq r' < b$.*Segue que* $+a = b \cdot (-q) - b + b - r'$. *Assim, podemos escrever* $a = b \cdot (-q' - 1) + b - r'$, *onde* $0 \leq b - r' < b$. *Logo, basta tomar* $q = -q' - 1$ *e* $r = b - r'$, *ou seja* $a = b \cdot q + r$, *onde* $0 \leq r < b$, *para* $a < 0$ *e* $b > 0$

Provaremos agora a unicidade.

Suponha que existam q' *e* r'*inteiros, tais que* $a = b \cdot q' + r'$, *como* $0 \leq r' < b$ *Afirmamos que* $0 \leq |r' - r| < b$

Como $0 \leq r < b$, *multiplicando esta desigualdade por-1, temos* $-b < -r \leq 0$. *Temos então as seguintes desigualdades :*

$$0 \leq r' \qquad r' < b$$
$$-b < r \qquad -r \leq 0$$

Somando os termos das desigualdades, obtemos:

$$0 - b < r - r' \quad e \quad r' - r < b$$

Podemos reescrever as desigualdades, nesta ordem, das seguintes maneiras:
$-(r' - r) < b$ *e* $r' < b$ *Sendo que ainda podem ser escritos como* $|r' - r| < b$
Como $a = b \cdot q + r$ *e* $a = b \cdot q' + r'$, *segue que:*

$$b \cdot q' + r' = b \cdot q + r \Leftrightarrow r - r' = b \cdot (q - q')$$

Segue que $|r' - r| = b \cdot |q' - q| < b$, *onde* $0 \leq |q' - q|$, *logo* $q' = q$ *e* $r' = r$.

Exemplo 3: Observe como fica a divisão euclidiana:

$55 = 8 \cdot 6 + 7$; $sendo\ b = 55, a = 8, q = 6\ e\ r = 7$. Observe também que $0 \leq 7 < 8$

$39 = 4 \cdot 9 + 3$; $sendo\ b = 39, a = 4, q = 9\ e\ r = 3$

2.2 - MÁXIMO DIVISOR COMUM

Sejam dados dois números naturais a e b, não simultaneamente nulos, diremos que o número natural $d \in \mathbb{N}$ é um *divisor comum* de a e b se $d|a$ e $d|b$.

Exemplo 4:

$\pm 3, \pm 5$ são divisores de 15.

$\pm\ 4, \pm 5$ são divisores de 20.

Proposição 2.2- Um número *d é* chamado *máximo divisor comum* (*mdc*) de a e *b* se possuir as seguintes propriedades:

i) d é um divisor comum de *a* e de *b*;

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

Demonstração*: Tome d e d´ máximos divisores comuns de a e b, então d | a e d | b. Mas observe que d´ é mdc entre a e b. Logo, por definição, d´| d. De forma análoga, d | d´. Como d e ´d* $\in$ $\mathbb{N}$*, segue pela proposição 1 (ii) que d e d´. Conclui-se assim, que o mdc quando existe é único.*

O mdc entre a e b será denotado por (a, b), não importando a ordem em que os números aparecem, ou seja (a, b) = (b, a).

Se d= (a, b), seja c um divisor comum desses números, logo c $\leq$ *d. O que significa que (a, b) é o maior divisor comum de a e b.*

Exemplo 5: Os números $\pm 2, \pm 3, \pm 4, \pm 8$ *e* $\pm\ 16$ são divisores comuns de 32 e 48, mas o maior deles é 16, logo (32, 48) = 16.

2.3 - NÚMERO PRIMO.

Um número natural maior do que 1 que só é divisível por 1 e por si próprio é chamado de *número primo.*

Proposição 2.3: Seja *p* um número primo e *a e b* inteiros:

Se p$\nmid$ *a* então *mdc (p, a) = 1.*

Se p | ab então p | a ou p | b.

Demonstração:

Se $p \nmid a$ então o único divisor comum entre *p e a* é o 1, onde segue a tese.

Admitamos que *p | ab.* Se *p | a* não há mais nada há provar. Em caso contrário, do item *(i) mdc (p, a) = 1 e do Teorema de Euclides (2.3.7 de MILES (2001)), segue que* p ∣ *b*.

Exemplos 6: De acordo com as propriedades são primos os seguintes números: 2, 3, 5, 7, 11, etc.

2.4 – CONGRUÊNCIA

Um dos mais importantes conceitos da aritmética é o de *Congruência.* Tal conceito foi introduzido por Karl Friedrich Gauss $(1777 - 1855)$ na sua obra intitulada *Disquisitiones Arithmeticae* no ano de 1801.

A título de motivação, vamos à seguinte questão: Se hoje é terça-feira, dia 01 de janeiro de 2019, que dia será daqui a 185 dias? Esse e outros tipos de questionamentos são objeto de estudo da aritmética e sua resolução é relativamente simples. Observe na tabela 01 como estão organizados os dias no calendário do mês de janeiro de 2019.

Tabela 1- Calendário de Janeiro de 2019

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Fonte: http://www.supercalendario.com.br/2019

Para responder a essa questão, vamos associar uma correspondência entre a sucessão de dias e os números inteiros. Ao dia de hoje (terça-feira), associamos o número 0, ao de dia de quarta 1, e assim sucessivamente

Como uma semana possui 7 dias, notemos que dois inteiros representam o mesmo dia da semana se, e somente se, a sua diferença for um múltiplo de 7. Sendo assim, podermos reescrever esta mesma tabela, na qual os números inteiros correspondentes aos dias são escritos na forma de divisão euclidiana

Tabela 2 - Calendário de Janeiro de 2019

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
			1 = 7· 0 +1	2 = 7· 0+2	3 =7· 0+3	4 =7· 0+4
5 = 7· 0+5	6 = 7· 0+6	7 = 7· 1+0	8 = 7· 1+1	9 = 7·1+2	10 =7·1+3	11 =7·2+4
12 =7·1+5	13 =7·1+6	14 =7·2+0	15 =7·2+1	16 =7·2+2	17 =7·2+3	18 =7·2+4
19 =7·2+5	20 =7·3+6	21 =7·3+0	22 =7·3+1	23 =7·3+2	24 =7·3+3	25= 7·3+4
26 =7·3+5	27 =7·3+6	28 =7·4+0	29= 7·4+1	30 =7·4+2		

Fonte: http://www.supercalendario.com.br/2019

De acordo com os dados da tabela 2, os números inteiros correspondentes aos dias da semana, escritos na forma da divisão euclidiana, são os mesmos quando apresentam os mesmos restos. Sendo assim, $185 = 7 \cdot 26 + 3$. Ao observar na tabela, verificamos que o dia cujo resto é igual a 3 é sexta-feira, sendo esta a resposta da questão em debate.

2.4.1 - DEFINIÇÃO DE CONGRUÊNCIA.

Ao efetuarmos a divisão de um número *a* por um número *m*, pode existir um resto *b*. A título de exemplo, podemos escrever que $5 \mid 12$ deixa resto 2. Podemos também escrever essa mesma sentença da seguinte forma $12 = 5 \cdot 2 + 2$. Se analisarmos mais criteriosamente, é possível observar que $5 \mid (12 - 2)$.

Definição 2.3: Sejam *a, b e m* números inteiros, com *m>0*. Dizemos que *a* é côngruo a *b* módulo *m* se $m|\ (a\ -b)$. A notação para esta sentença é $a\ \equiv b\ mod\ m$.

Exemplos 7: A seguir alguns exemplos relacionados à definição de congruência:

$15\ \equiv\ 1\ mod\ 7$, o que implica em dizer que a divisão de 15 por 7 deixa resto 1, ou seja

$$15\ \big|\ \underline{7}$$
$$1\quad 2$$

$58 \equiv 2 \bmod 8$.

$$58\ \big|\ \underline{8}$$
$$2\quad 7$$

Uma importante observação que se pode fazer nesse momento é que na aritmética modular, o valor do quociente não aparece na definição, importando tão somente o dividendo, o divisor e o resto.

Proposição 2.4: Sejam *a, b, c* e *m* números inteiros quaisquer, então valem:

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

ii) $Se\ a\ \equiv\ \ b\ (mod\ m)\ , então\ b\ \equiv\ a\ (mod\ m)$.

iii) $Se\ a\ \equiv b\ (mod\ m)\ e\ b\ \equiv\ c\ (mod\ m)\ , então\ a\ \equiv\ c\ (mod\ m)$.

iv) $Se\ a\ \equiv\ b\ (mod\ m)\ e\ c\ \equiv\ d\ (mod\ m), então\ a\ +\ c\ \equiv\ b\ +\ d\ (mod\ m)$.

v) $Se\ a\ \equiv\ b\ (mod\ m), então\ a\ +\ c\ \equiv\ b\ +\ c\ (mod\ m)$.

vi) $Se\ a\ \equiv\ b\ (mod\ m)\ e\ c\ \equiv\ d\ (mod\ m), então\ a \cdot c\ \equiv\ b \cdot d\ (mod\ m)$.

vii) $Se\ a\ \equiv\ b\ (mod\ m), então\ an\ \equiv\ bn\ (mod\ m), para\ todo\ inteiro\ positivo\ n.$

viii) $Se\ a\ +\ c\ \equiv\ b\ + c\ (mod\ m), então\ a\ \equiv\ b\ (mod\ m)$.

Demonstração:

i) $a \equiv a\ (mod\ m)$

Como m | 0 = (a – a), m, logo a≡a(mod m).

ii) Se a ≡ *b (mod m), então b ≡ a (mod m).*

Temos que m| (a - b), assim, m|−(a − b), ou seja, m|(b − a). Portanto, b ≡a (mod m).

iii) Se a ≡b (mod m) e b ≡ c (mod m) , então a ≡ c (mod m)

Da definição temos que m| (a – b) e m | (b – c), assim m | (a – b) + (b- c).

Logo m | (a – c).

iv) Se a ≡ b (mod m) e c ≡ d (mod m), então a + c ≡ b + d (mod m)

Temos que m | (a – b) e m | (c – d), assim m | (a + b) + (c – d) ⟹ m | (a +c) – (b + d).

v) Se a ≡ b (mod m), então a + c ≡ b + c (mod m)

Temos que m | (a – b) ⟹ como (a – b) = (a + c) – (b + c), segue que

m | (a + c) – (b + c).

vi) Se a ≡ b (mod m) e c ≡ d (mod m), então a·c ≡ b·d (mod m).

Podemos escrever a·*c*−*b*·*d* = *a*·*c*−*b*·*c* + *b*·*c* − *b*·*d* = *c*· *(a* − *b)* + *b*· *(c* − *d), assim, temos que a*·*c*−*b*·*d* = *c*· *(x*·*m)*+*b*· *(y*·*m)* = *m(cx* + *by). Logo, m | (a*·*c* − *b*·*d).*

vii) Se a ≡ b (mod m), então $a^n \equiv b^n$ *(mod m), para todo inteiro positivo n.*

Considere "n congruências" do tipo a ≡ b (mod m)

$$\begin{cases} a \equiv b \ (mod\ m) \\ a \equiv b \ (mod\ m) \\ a \equiv b \ (mod\ m) \\ \quad \ldots \\ \quad \ldots \\ a \equiv b \ (mod\ m) \end{cases}$$

Assim, pelo item anterior temos:

$$\underbrace{a \cdot a \cdot a \cdot a \ldots a}_{n\ vezes} \equiv \underbrace{b \cdot b \cdot b \cdot b \ldots b}_{n\ vezes} (mod\ m) \implies a^n \equiv b^n (mod\ m).$$

viii) *Se $a + c \equiv b + c\ (mod\ m)$, então $a \equiv b\ (mod\ m)$*

De acordo com a definição $m \mid (a + c) - (b + c) = (a - b)$.

2.5 – CRITÉRIOS DE DIVISIBILIDADE.

A aritmética elementar, ensinada na educação básica, tem grande importância no mundo moderno. O ensino desta importante área da matemática, a aritmética, é explorado desde as séries iniciais da educação básica.

Cotidianamente, as pessoas efetuam cálculos de divisão de números inteiros, seja na escola, seja no trabalho ou mesmo em situações corriqueiras. Em toda parte, a matemática e as operações de aritmética se fazem presentes. É nas séries iniciais do ensino fundamental que se inicia o estudo de divisibilidade. A partir do 6º ano do ensino fundamental começa-se a estudar de forma mais aprofundada esse assunto. Para que o aluno possa construir um bom conhecimento em matemática, no 6º ano o ele começa a ter conhecimento sobre os critérios de divisibilidade, isto é, quais são as condições para que um número inteiro seja divisível por um outro número inteiro menor que ele.

A seguir, estudaremos os critérios de divisibilidade de números inteiros, assunto esse bastante abordado em livros didáticos do ensino fundamental e médio. Para tanto, também traremos os enunciados de alguns critérios presentes em livros do 6º ano do ensino fundamental, trazendo assim as informações de como é feito esse estudo. Feitas as consultas e pesquisas necessárias, pode-se perceber que os livros não trazem as demonstrações dos teoremas, ou seja, dos critérios de divisibilidade. Talvez seja porque os alunos nessa etapa de ensino ainda não tenham condições de compreender demonstrações mais complexas e abstratas desses teoremas.

2.5.1 – CRITÉRIO DE DIVISIBILIDADE POR 2

Os alunos, ao iniciarem os estudos de divisibilidade, nem sempre tem em mente quais condições um número pode ser dividido por 2. Sendo assim, a bibliografia para o 6º ano assim traz o enunciado desse critério. Cabe fazer uma ressalva: como nesse nível de ensino ainda não se estudou os números inteiros, os enunciados são feitos considerando os números naturais. Tal fato irá se repetir para outros critérios da seção 2.5.

"Um número natural é divisível por 2 quando ele é par" (MORI, p. 113)

Numa linguagem matemática mais formal, esse enunciado seria feito de acordo com o teorema a 2.2.

Teorema 2.2 - Seja $x = x_n \,.\, 10^n + x_{n-1}.\, 10^{n-1} + \ldots + x_1.\, 10^1 + x_0$, a representação decimal de um número inteiro $x_k \in \mathbb{N}, 0 \leq x_k < 10, 1 \leq k \leq n \; e \; x_n \neq 0$. Então x é divisível por 2 se, e somente se, $2 | x_0, ou\ seja\ ,\ x_0 = 0, 2, 4, 6\ ou\ 8$

***Demonstração*:** *Sabe-se que 10≡ 0 (mod 2), da proposição 2.4 (vii) temos que* $10^n \equiv 0\ (mod\ 2), \forall\, n \in \mathbb{Z}\, e\, n > 0$. *Sendo assim* $10^n \equiv 0\ (mod\ 2), 10^{n-1} \equiv 0\ (mod\ 2), 10^{n-2} \equiv 0 (mod\ 2) \ldots, 10^1 \equiv 0\ (mod\ 2)$. *Logo* $(x_n \,.\, 10^n + x_{n-1}.\, 10^{n-1} + \ldots + x_1.\, 10^1) \equiv 0\ (mod\ 2)$, *pela proposição 2.4 (iv). Sendo assim basta verificar a congruência* $x \equiv x_0\ (mod\ 2)$. *Observe que 2 |* x_0 *se, e somente se,* $x_0 = 0, 2, 4, 6\ ou\ 8$.

Da mesma forma, suponha que $2 \mid x_0$. Sabe-se que $10^n \equiv 0\ (mod\ 2), 10^{n-1} \equiv 0\ (mod\ 2), 10^{n-2} \equiv 0, \ldots, 10^1 \equiv 0\ (mod\ 2)$. *Logo, pela proposição 2.4 (* $x_n \,.\, 10^n + x_{n-1}.\, 10^{n-1} + \ldots + x_1.\, 10^1 + x_0\ ) \equiv 0\ (mod\ 2)$.

Exemplo 8*: O número 2678 é um número par, pois termina em 8, logo 2 | 2678. Podemos também escrever* $2678 = 2 \cdot (1339)$. *Como* $2 \cdot (1339)$ *é um múltiplo de 2, logo ele é divisível por 2.*

2.5.2 - CRITÉRIO DE DIVISIBILIDADE POR 3

O critério de divisibilidade por 3 também é estudado no 6º ano. MORI(2015) traz dessa forma o enunciado desse critério.

> *"Um número natural é divisível por 3 quando a soma dos algarismos da sua escrita numérica for divisível por 3" (*MORI, *p. 114)*

Esse enunciado pode parecer não muito claro, uma vez que ele conclui dizendo para se dividir um número por três, é necessário que a soma dos algarismos da escrita desse número seja também divisível por 3. Já que se está estudando um critério de divisibilidade por 3, nessa etapa de ensino nem sempre se sabe quais são os múltiplos de 3.

O teorema 2.3 traz a demonstração da divisibilidade por 3.

Teorema 2.3 Seja $x = x_n . 10^n + x_{n-1}. 10^{n-1} + \ldots + x_1. 10^1 + x_0$, a representação decimal de um número inteiro $x_k \in \mathbb{N}, 0 \leq x_n < 10, 1 \leq k \leq n$ *e* $x_n \neq 0$. Dizemos que x é divisível por 3 se e somente se, *3|* $(x_n + x_{n-1} + \ldots + x_1 + x_0)$

***Demonstração*:** *De acordo com a definição de congruência, temos que 10≡1 (mod 3), do teorema 2.4 (vii) temos que* $10^n \equiv 1 \pmod 3$, $\forall\, n \in \mathbb{Z}$ *e* $n > 0$. *De forma semelhante,* $x_n. 10^n \equiv 1\ (mod\ 3), x_{n-1}. 10^{n-1} \equiv 1\ (mod\ 3) \ldots 10^n \equiv 1\ (mod\ 3)$. *Assim, de acordo com o mesmo teorema temos que ,* $x_n. 10^n \equiv x (mod\ 3)$, $x_{n-1}. 10^{n-1} \equiv x_{n-1}\ \ (mod\ 3), \ldots, x_0 \equiv x_0\ (mod\ 3)$. *Então, pela proposição 2.4 (iv) temos*

$(x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \ldots + x_1 \cdot 10^1 + x_0) \equiv (x_n + x_{n-1} + \ldots + x_1 + x_0)$ *(mod 3).*

Observe que se $3 \mid (x_n + x_{n-1} + \ldots + x_1 + x_0)$ *se, e somente se* $(x_n + x_{n-1} + \ldots + x_1 + x_0)$ *for um múltiplo de 3. O que significa que 3 | x e x ≡ 0 (mod 3).*

Exemplo 9 - Observe que 3 | 1791, pois 1 + 7 + 9 + 1 = 18, a soma dos algarismos é um múltiplo é 18, sendo este um múltiplo de 3. Também poderemos escrever $1791 = 3 \cdot (597)$, assim $3 \mid 3 \cdot (597)$.

2.5.3 - CRITÉRIO DE DIVISIBILIDADE POR 4

O critério de divisibilidade por 4 também está presente na maioria dos livros didáticos do 6º ano. Ele é assim enunciado

> *"Um número natural é divisível por 4 quando o número formado pelos algarismos das dezenas e das unidades simples desse número é divisível por 4" (*MORI, *p. 117)*

O teorema 2.4, traz uma demonstração formal desse enunciando.

Teorema 2.4 - Seja $x = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \ldots + x_1 \cdot 10^1 + x_0$, a representação decimal de um número inteiro $x_k \in \mathbb{N}, 0 \leq x_k < 10, 1 \leq k \leq n$ *e* $x_n \neq 0$. Dizemos que x é divisível por 4 se. e somente se, *4* | $x_1 \cdot 10^1 + x_0$

Demonstração: *Podemos escrever* $10 = 2 \cdot 5$, *também é possível escrever* $10^n = 2^n \cdot 5^n$, *o que implica, pela proposição 2.4 (vi) que* $10^n \equiv 0 \pmod{2^2}$, *para qualquer* $n \geq 3$. *De forma análoga,* $x_n \cdot 10^n \equiv 0 \pmod{2^2}$, $x_{n-1} \cdot 10^{n-1} \equiv 0 \pmod{2^2}$. *Sendo assim, conclui-se que* $x = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \ldots + x_2 \cdot 10^2 \equiv 0 \pmod{2^2}$. *Suponha então que 4 | x, pela proposição 2.4 (iv)* $4 \mid x_1 \cdot 10^1 + x_0$

Reciprocamente, se 4 | $x_1 \cdot 10^1 + x_0$ *, temos que* $x_1 \cdot 10^1 + x_0 \equiv 0 \pmod{2^2}$. *Como* $x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \ldots + x_2 \cdot 10^2 \equiv 0 \pmod{2^2}$, *pela proposição 2.4 (iv) 4 | x.*

Exemplo 10: Seja dado x = 24716, como o os algarismos das dezenas de das unidades simples é igual a 16, então podemos afirmar que 4 | 16, de acordo com o teorema 2. 4;

$3 \mid 24716$. Ora , $24716 = 4 \cdot 6179$.

2.5.4 - CRITÉRIO DE DIVISIBILIDADE POR 5.

A divisibilidade por 5 pode parecer uma das mais fáceis para os alunos quando estes passam a ter conhecimento desse critério.

> *"Um número natural é divisível por 5 quando ele termina em zero ou 5" (*MORI, *p. 114)*

'A demonstração desse enunciado é feita formalmente pelo teorema 2.5.

Teorema 2.5 - Seja $x = x_n . 10^n + x_{n-1}. 10^{n-1} + \ldots + x_1. 10^1 + x_0$, a representação decimal de um número inteiro $x_k \in \mathbb{N}, 0 \leq x_k < 10, 1 \leq k \leq n \; e \; x_n \neq 0$. Dizemos que x é divisível por 5 se, e somente se, x_0 é um múltiplo de 5, ou seja, se, e somente se, $x_0 = 0 \; ou \; x_0 = 5$.

***Demonstração*:** *De forma semelhantes à demonstração da divisibilidade por 2, observe que 10≡ 0 (mod 5), pela proposição2.4 (vii) temos que* $10^n \equiv 0 \; (mod \; 5), \forall \; n \in \mathbb{Z} \; e \; n > 0$ *. Sendo assim* $10^n \equiv 0 \; (mod \; 5)$, $10^{n-1} \equiv 0 \; (mod \; 5)$, $10^{n-2} \equiv 0 (mod \; 5)$, *..., 10¹ ≡ 0 (mod 5). Logo* $(x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \ldots + x_1 \cdot 10^1) \equiv 0 \; (mod \; 5)$, *pela proposição 2.4 (v). Sendo assim basta verificar a congruência* $x \equiv x_0 \; (mod \; 5)$. *Observe que 5 |* x_0 *se, e somente se,* $x_0 = 0 \; ou \; 5$.

Da mesma forma, suponha que $5 \mid x_0$. Sabe-se que $10^n \equiv 0 \; (mod \; 5)$, $10^{n-1} \equiv 0 \; (mod \; 5)$, $10^{n-2} \equiv 0 (mod \; 5)$, *. . .,10¹ ≡ 0 (mod 5). Logo, pela proposição 2.4;* $(x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \ldots + x_1 \cdot 10^1 + x_0) \equiv 0 \; (mod \; 5)$.

Exemplo 11: Seja $x = 15260$, de acordo com o teorema 2.5, $5 \mid 15260$, pois termina em 0. É fácil perceber $15260 = 5 \cdot 3052$.

2.5.5 - CRITÉRIO DE DIVISIBILIDADE POR 6.

A divisibilidade por 6 já requer um conhecimento prévio da divisibilidade por 2 e por 3. Ela também está presente nos livros didáticos do 6º ano.

> *"Um número natural é divisível por 6 quando é divisível por 2 e por 3 ao mesmo tempo" (*MORI, *p. 117)*

A demonstração desse enunciado é feita pelo teorema 2.6.

Teorema 2.6 - Seja $x = x_n . 10^n + x_{n-1}. 10^{n-1} + \ldots + x_1. 10^1 + x_0$, a representação decimal de um número inteiro $x_k \in \mathbb{N}, 0 \leq x_k < 10, 1 \leq k \leq n$ *e* $x_n \neq 0$. Dizemos que *6 | x* se, e somente se, *2 |x e 3 | x.*

Demonstração: *Como 6 é par, 2 | 6, como 6 é um múltiplo de 3, temos que 3 | 6, logo pela proposição 2.4 (iii), 2 | x e 3 | x. Logo x é um número par e 3 | (*$x_n + x_{n-1} + \ldots + x_1 + x_0$*).*

Analogamente, se x é um número par, ou seja x = 2k, tal que k ∈ ℤ, e se e 3 | ($x_n + x_{n-1} + \ldots + x_1 + x_0$*), ou seja 3 | x. Se 3|x, logo 3 | 2k, como 3 e 2 são primos entre si, temos que m.d.c (2,3) = 1, sendo assim 3 | k. Logo k = 3.w, com w ∈ ℤ. O que implica 3 | 2.3.w, logo 3 | 6w.*

Exemplo 12: Dado o número 5634, vamos verificar se ele é divisível por 6. Observe que 5634 é um número par, logo $2 \mid 5634$. Observe também que $5 + 6 + 3 + 4 = 18$ e como $3 \mid 18$, logo $3 \mid 5634$. Então, pelo teorema 2.6; $6 \mid 5634$

2.5.6 – CRITÉRIO DE DIVISIBILIDADE POR 7

Pesquisando sobre a divisibilidade por 7, percebemos que os livros didáticos não trazem uma regra para esse critério.

A divisibilidade por 7 é demonstração no teorema a 2.7.

Teorema 2.8 - Seja $x = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \ldots + x_1 \cdot 10 + x_0$, a representação decimal de um número inteiro $x_k \in \mathbb{N}, 0 \leq x_k < 10, 1 \leq k \leq n$ *e* $x_n \neq 0$. Dizemos que x é divisível por 7 se, e somente se, $7 \mid (x_k \cdot 10^{n-1} + x_{n-1} \cdot 10^{n-2} + \ldots + x_2 \cdot 10^1 + x_1) - 2 \cdot x_0$.

Demonstração: *Se x é divisível por 7, então podemos escrever* $= x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \ldots + x_1 \cdot 10^1 + x_0 = 7k, onde\ k \in \mathbb{Z}$*; logo*

$$x_0 = 7k - x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \ldots + x_1 \cdot 10$$

$$x_0 = 7k - 10 \cdot (x_n \cdot 10^{n-1} + x_{n-1} \cdot 10^{n-2} + \ldots + x_1)$$

Então, podemos escrever

$(x_n \cdot 10^{n-1} + x_{n-1} \cdot 10^{n-2} + \ldots + x_2 \cdot 10^1 + x_1) - 2 \cdot x_0 =$

$(x_n \cdot 10^{n-1} + x_{n-1} \cdot 10^{n-2} + \ldots + x_2 \cdot 10^1 + x_1) - 2 \cdot [7k - 10.(x_n \cdot 10^{n-1} + x_{n-1} \cdot 10^{n-2} + \ldots + x_1)]$

$= (x_n \cdot 10^{n-1} + x_{n-1} \cdot 10^{n-2} + \ldots + x_2 \cdot 10^1 + x_1) - 14k + 20 \cdot (x_n \cdot 10^{n-1} + x_{n-1}.10^{n-2} + \ldots + x_1)$

$= -14k + 21 \cdot (x_n \cdot 10^{n-1} + x_{n-1} \cdot 10^{n-2} + \ldots + x_1)]$

$= 7 \cdot [-2k + 3 \cdot (x_n \cdot 10^{n-1} + x_{n-1} \cdot 10^{n-2} + \ldots + x_1)]$

Logo, $7 \mid (x_n \cdot 10^{n-1} + x_{n-1} \cdot 10^{n-2} + \ldots + x_2 \cdot 10^1 + x_1) - 2 \cdot x_0$.

Analogamente, vamos supor que

$7 \mid (x_n \cdot 10^{n-1} + x_{n-1} \cdot 10^{n-2} + \ldots + x_2 \cdot 10^1 + x_1) - 2 \cdot x_0$.

Então

$(x_n \cdot 10^{n-1} + x_{n-1} \cdot 10^{n-2} + \ldots + x_2 \cdot 10^1 + x_1) - 2 \cdot x_0 = 7w, onde\ w \in \mathbb{Z}$.

Como

$$x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \ldots + x_1 \cdot 10 + x_0$$

$$= 10 \cdot (x_n \cdot 10^{n-1} + x_{n-1} \cdot 10^{n-2} + \ldots + x_1) + x_0$$

$$= 10 \cdot (7w + 2x_0) + x_0$$

$$= 70 \cdot w + 20 \cdot x_0 + x_0$$

$$= 70 \cdot w + 21 \cdot x_0$$

$$= 7 \cdot (10w + 3x_0).$$

Exemplo 13: Dado o número 315, será que ele é divisível por 7?

De acordo com o teorema 2.7, $7|(31 - 2 \cdot 5)$, ou seja $31 - 10 = 21$, como 21 é um múltiplo de 7, logo 315 é divisível por 7. É só observar que $315 = 45 \cdot 7$.

2.5.7 – CRITÉRIO DE DIVISIBILIDADE POR 8

Outra divisibilidade não muito explorada pelos livros didáticos da educação básica é que é feita por 8. Isso também talvez influencie na sua aprendizagem.

A divisibilidade por 8 é demonstrada no teorema 2.8.

Teorema 2.8 - Seja $x = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \ldots + x_1 \cdot 10^1 + x_0$, a representação decimal de um número inteiro $x_k \in \mathbb{N}, 0 \leq x_k < 10, 1 \leq k \leq n$ *e* $x_n \neq 0$. Dizemos que x é divisível por 8 se e somente se, $8 \mid x_2 \cdot 10^2 + x_1 \cdot 10^1 + x_0$

Demonstração: *Podemos escrever* $10 = 2 \cdot 5$, *também é possível escrever* $10^n = 2^n \cdot 5^n$, *o que implica, pela proposição 2.4 (vii) que* $10^n \equiv 0 \pmod{2^3}$, *para qualquer* $n \geq 3$. *De forma análoga,* $x_n \cdot 10^n \equiv 0 \pmod{2^3}$. $x_{n-1} \cdot 10^{n-1} \equiv 0 \pmod{2^3}$, *para qualquer* $n \geq 3$. *Sendo assim, conclui-se que*

Seja $x = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \ldots + x_3 \cdot 10^3 \equiv 0 \pmod{2^3}$. *Suponha então que* $8 \mid x$, *pela proposição 2.4 (iv) ,* $8 \mid x_2 \cdot 10^2 + x_1 \cdot 10^1 + x_0$

De forma análoga, se $8 \mid x_2 \cdot 10^2 + x_1 \cdot 10^1 + x_0$, *temos* $x_2 \cdot 10^2 + x_1 \cdot 10^1 + x_0, \equiv 0 \pmod{2^3}$. *Como* $x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \ldots + x_3 \cdot 10^3 \equiv 0 \pmod{2^3}$, *pela proposição 2.4 (iv)* $8 \mid x$.

Exemplo 14- O número 56120 é divisível por 8?

Pelo teorema 2.8; como $8| 120$, entã o 56120 também é divisível por 8. De fato, basta verificar que $7015 \cdot 8 = 56120$.

2.5.8- CRITÉRIO DE DIVISIBILIDADE POR 9.

A divisibilidade por 9 tem um processo semelhante à que é feita por 3. Eu estudo é explorado pela grande maioria dos livros didáticos do 6º ano.

> *"Um número natural é divisível por 9 quando a soma dos algarismos de sua escrita numérica for divisível por 9." (*MORI, *p. 115)*

Aqui também se faz as ressalvas feitas ao enunciando da divisibilidade por 3.

A demonstração desse enunciado é feita no teorema 2.9.

Teorema 2.9 -Seja $x = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \ldots + x_1 \cdot 10^1 + x_0$, a representação decimal de um número inteiro $x_k \in \mathbb{N}, 0 \leq x_n < 10, 1 \leq k \leq n$ *e* $x_n \neq 0$. Dizemos que x é divisível por 9 se e somente se $9 \mid (x_n + x_{n-1} + \ldots + x_1 + x_0)$

Demonstração: *De acordo com a definição de congruência, temos que* $10 \equiv 1 \pmod 9$*, da proposição 2.4 (vii) temos que* $10^n \equiv 1 \pmod 9$*,* $\forall\, n \in \mathbb{Z}$ *e* $n > 0$*. De forma semelhante,* $x_n . 10^n \equiv 1 \pmod 9$*,* $x_{n-1} . 10^{n-1} \equiv 1 \pmod 9 \ldots$*,* $10^n \equiv 1 \pmod 9$*. Assim, de acordo com o mesmo teorema temos que ,* $x_n \cdot 10^n \equiv x \pmod 9$*,* $x_{n-1} \cdot 10^{n-1} \equiv x_{n-1} \pmod 9, \ldots, x_0 \equiv x_0 \pmod 3$*. Então, pela proposição 2.4 (v) temos*

$(x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \ldots + x_1 \cdot 10^1 + x_0) \equiv (x_n + x_{n-1} + \ldots + x_1 + x_0) \pmod 9$*).*

Observe que se $9 \mid (x_n + x_{n-1} + \ldots + x_1 + x_0)$ *se, e somente se* $(x_n + x_{n-1} + \ldots + x + x_0)$ *for um múltiplo de 9. O que significa que* $9 \mid x$ *e* $x \equiv 0 \pmod 9$*.*

Exemplo 15 - O número 1791 é divisível por 9, pois $1 + 7 + 9 + 1 = 18$ e como 18 é um múltiplo de 9, a conclusão segue do teorema 2.9. Observe que $199 \cdot 9 = 1791$.

2.5.9- CRITÉRIO DE DIVISIBILIDADE POR 10

A divisibilidade por 10 é de suma importância para estudo de outros temas da matemática, como tais como potência, radiciação, entre muitos outros. É bastante explorado no ensino fundamental e médio.

> *"Um número natural é divisível por 10 quando termina em zero" (*MORI, *p. 114)*

A demonstração dessa divisibilidade é feita pelo teorema 2.10.

Teorema 2.11 - Seja $x = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \ldots + x_1 \cdot 10^1 + x_0$, a representação decimal de um número inteiro $x_k \in \mathbb{N}, 0 \leq x_k < 10, 1 \leq k \leq n \; e \; x_n \neq 0$. Então x é divisível por 10 se, e somente se, $x_0 = 0$

Demonstração: *Observe que* $10 \equiv 0 (mod\ 10)$. *O restante da demonstração é semelhante à do critério da divisibilidade por 2.*

Exemplo 16 – Conforme o teorema 2.10; número 12390 é divisível por 10, pois terminar em 0.

3 - ARITMÉTICA MODULAR NO CONTEXTO SOCIAL E TECNOLÓGICO.

A aritmética se faz presente em diversas atividades humanas. Embora os leigos possam pensar que esse ramo da matemática seja algo de interesse apenas de pesquisadores, professores e alunos, existem muitas aplicações de aritmética modular do que supõe nossa imaginação.

Ao comprar um produto em um supermercado na maioria das vezes nos deparamos com um conjunto de barrinhas verticais onde também são escritos uma sequência de números que muitos desconhecem o seu significado. Outra situação em que vemos conjuntos numéricos que por vezes desconsideramos seus significados estão presentes no Cadastro de Pessoas Físicas (CPF), nos cartões de crédito, etc. Todos esses números que aparecem nos códigos de barra, em documentos como o CPF, nos cartões de créditos não são aleatórios, são aplicações de aritmética modular que foram desenvolvidas para facilitar o dia a dia das pessoas, diminuindo erros, contribuindo para o desenvolvimento econômico, social e tecnológico da humanidade.

3.1 – DÍGITO VERIFICADOR.

Dígito verificador, também chamado algarismo de controle, método de autenticação utilizado para verificar a validade e a autenticidade de um valor numérico, evitando dessa forma, possíveis fraudes ou erros de transmissão ou digitação de dados e informações. São muito utilizados e difundidos em números de documentos, cartões de crédito, códigos de barras e em muitos códigos numéricos que possa demandar maior segurança.

O dígito verificador consiste em um ou mais algarismos que são acrescentados ao valor original e calculados a partir deste através de um determinado algoritmo.

3.1.2 - ARITMÉTICA MODULAR NO CADASTRO DE PESSOAS FÍSICAS (CPF)

Uma importante aplicação da aritmética modular está presente no cadastro das pessoas físicas (CPF). O CPF é um documento emitido pela Receita Federal do Brasil e é composto de 11 dígitos numéricos, sendo que os dois últimos são chamados de dígitos verificadores.

Os nove primeiros dígitos são a base de cálculo para encontrar o décimo e o décimo primeiro dígito, sendo estes os dígitos verificadores. O nono dígito define a região fiscal, revelando assim onde o CPF foi emitido. A tabela 3 identifica o número e a região fiscal de cada estado brasileiro.

Tabela 3 - Regiões Fiscais

NÚMERO	REGIÃO FISCAL
0	RS
1	DF, GO, MS, MT, TO
2	AC, AM, AP, PA, RO, RR
3	CE, MA, PI
4	AL, PB, PE, RN
5	BA, SE
6	MG
7	ES, RJ
8	SP
9	PR, SC.

Fonte: http://receita.economia.gov.br

De acordo com a tabela 3, uma pessoa cujo nono dígito do seu CPF é 5, verifica-se que tal documento foi emitido no estado da Bahia ou de Sergipe; assim como é possível afirmar que o estado emissor é São Paulo caso o nono dígito desse CPF for igual a 8.

Mas um importante questionamento que se pode fazer é: como encontrar os dígitos verificadores de um CPF?

De acordo com OLIVEIRA (2013), sejam $a_1a_2a_3a_4a_5a_6a_7a_8a_9$os 9 primeiros dígitos de um determinado CPF. Para encontrar o primeiro dígito verificador, devemos multiplica-los, nesta ordem, por {1, 2, 3, 4, 5, 6, 7, 8, 9} e somar os resultados (S). O décimo dígito (a_{10}) é o resto da divisão de S por 11, com a exceção para o caso em que o resto é 10, no qual será utilizado o dígito zero. Para encontrar o segundo dígito verificador, devemos multiplicar, nesta ordem, os dígitos $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}$ por {0 , 1 ,2, 3, 4, 5, 6, 7, 8, 9 } e somar os resultados (S'). O décimo primeiro dígito é o resto da divisão de S' por 11, com exceção para o caso em que o resto for igual a 10, no qual é utilizado o dígito zero.

Sendo assim, para encontrar os dígitos verificadores de um CPF, devemos escrever as seguintes congruências para o primeiro e segundo dígitos:

$$1^o \text{ digito verificador } \rightarrow \text{ S - } a_{10} \equiv 0\ (mod\ 11) \qquad (3.1)$$

$$2^o \text{ digito verificador } \rightarrow \text{ S' – } a_{11} \equiv 0\ (mod\ 11) \qquad (3.2)$$

Exemplo 17: Para exemplificar melhor, vamos considerar o caso de um CPF hipotético em que os 9 primeiros dígitos são 136.487.635 e vamos descobrir o décimo e o décimo segundo termos, que são os dígitos verificadores.

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

$$S = 1 + 6 + 18 + 16 + 40 + 42 + 42 + 24 + 45$$

$$S = 234$$

Logo, 234 - $a_{10} \equiv 0\ (mod\ 11)$ ou 234 $\equiv 3\ (mod\ 11)$ logo a_{10} = 3, nesse caso será utilizado o dígito 3, já que o resto da divisão de 233 por 11 é igual a 3.

Para calcular S', seguimos o seguinte algoritmo.

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

$$S' = 0 + 3 + 12 + 12 + 32 + 35 + 36 + 21 + 40 + 27$$

$$S' = 218$$

Logo, $218 - a_{11} \equiv 0\ (mod\ 11) ou\ 218 \equiv 9 (mod\ 11)$ logo $a_{11} = 9$.

Sendo assim, o CPF hipotético teria os seguintes dígitos 136.487.635-39. Um conhecedor do algoritmo que determina os dígitos verificadores de um CPF saberia que

tal documento seria falso caso os dois últimos dígitos fossem diferentes de 39. Também é possível afirmar, de acordo com a tabela 3.1, esse documento hipotético poderia ter sido emitido nos estados da Bahia ou de Sergipe, pois seu antepenúltimo dígito é igual a 5.

3.1.3 – ARITMÉTICA MODULAR NO CARTÃO DE CRÉDITO.

Uma pessoa desinformada poderá achar que os números presentes nos cartões de crédito são aleatórios, mas todos os números ali presentes possuem uma razão de ser. Por exemplo, os primeiros números de um cartão de crédito identificam a bandeira do cartão. Todos os cartões de bandeira Visa começam com o número 4, Mastercard pode começar com 51, 52, 53, 54 ou 55. American Express começam com 34 ou 37. Essa regra serve para todo o mundo, tendo sido definida em 1989 como forma de padronizar movimentações financeiras. Normalmente, a quantidade de dígitos de um cartão de crédito (figura 1) pode variar de 14 a 19. No Brasil, a quantidade de dígitos mais comum é 16. Para além dos primeiros dígitos, os outros, com exceção do último, servem para identificar o cliente.

Figura 1: Cartão de Crédito

Fonte: https://gizmodo.uol.com.br/

O algoritmo para o cálculo do dígito verificador de um cartão de crédito foi desenvolvido por Hans Peter Luhn em 1954, sendo por isso chamado de algoritmo de Luhn. Tal algoritmo se efetua pela multiplicação dos números de posição ímpares por 2;

caso o resultado dessa multiplicação for um número de dois algarismos, soma-se os valores absoluto dos mesmos, o que equivale a colocar o resto da divisão desse número de dois algarismos por 9. Vamos citar o caso de multiplicarmos 6 por 2, logo teríamos resultado 12, assim poderíamos fazer o seguinte cálculo 1 + 2 = 3 , sendo que este também é o resto da divisão de 12 por 9. Os algarismos de posição par multiplicamos por 1. O passo seguinte é adicionar os resultados das multiplicações das posições pares com as posições ímpares. O dígito verificador será o número que pode ser acrescentado a essa soma para que seja um múltiplo de 10.

Sendo assim, vamos supor que um determinado cartão tenha a seguinte sequência.

$$c = [a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10} a_{11} a_{12} a_{13} a_{14} a_{15} a_{16}] \qquad (3.3)$$

sendo a_{16} o dígito verificador.

e

$$p = [\,2\ 1\ 2\ 1\ 2\ 1\ 2\ 1\ 2\ 1\ 2\ 1\ 2\ 1\ 2\ 1] \qquad (3.4)$$

logo, o produto obtido seria dado por

$$c.p = 2a_1 + 1a_2 + 2a_3 \ldots + 2a_{15} + 1a_{16} \equiv 0\ (mod\ 10) \qquad (3.5)$$

Exemplo 18: Vamos supor que o número hipotético de um cartão de crédito seja 4016 5491 3678 852, assim vamos determinar o dígito verificador desse cartão.

Observe que os números de posição ímpar multiplicaremos por 2, caso o resultado seja um número de dois algarismos, somamos os valores absolutos dele.

$2 \cdot a_1 = 2 \cdot 4 = 8$

$2 \cdot a_3 = 2 \cdot 1 = 2$

$2 \cdot a_5 = 2 \cdot 5 = 10$, logo 1+0 = 1

$2 \cdot a_7 = 2 \cdot 9 = 18$, logo 1+8 = 9

$2 \cdot a_9 = 2 \cdot 3 = 6$

$2 \cdot a_{11} = 2 \cdot 7 = 14$, logo 1+4 = 5

$2 \cdot a_{13} = 2 \cdot 8 = 16$, logo 1+6 = 7

$2 \cdot a_{15} = 2 \cdot 2 = 4$

$$(8 + 0 + 2 + 6 + 1 + 4 + 9 + 1 + 6 + 6 + 5 + 8 + 7 + 5 + 4 + a_{16}) \equiv 0 \ (mod\ 10)$$

$$(72 + a_{16}) \equiv 0 \ (mod\ 10)$$

Concluímos então que o dígito verificador desse cartão é a_{16} = 8. Sendo assim, esse cartão de crédito hipotético terá 4016 5491 3678 8528 como números. Outra informação que é possível identificar é que esse cartão teria a bandeira VISA, já que começa com o algarismo 4.

Numa situação apresentada como a do exemplo 18**,** em que seja necessário digitar os números do cartão, caso por um descuido qualquer, fosse trocado algum desses dígitos, a máquina de cartão de crédito identificaria o erro, uma vez que o dígito verificador não seria o resultado dos algarismos digitados.

3.1.4 - CÓDIGOS DE BARRAS

Os códigos de barras, figura 2, estão presentes em muitas áreas do nosso cotidiano. Podemos percebê-los quando vamos ao supermercado, quando pagamos contas de água, luz, telefone, etc. São muito utilizados devido à praticidade, eficiência e pouca probabilidade de erros.

Figura 2: Código de Barras

Fonte: Wikipédia

Os códigos de barras representam uma sequência numérica representada por listras brancas e pretas. A espessura de cada listra representa um número: a uma listra branca fina é associada ao símbolo 0, a uma listra branca média é associado ao 00, a uma listra branca grossa é associada ao 000 e a uma listra branca muito grossa é associada o 0000. Analogamente, a sequência 1, 11, 111, 1111 representa uma listra preta, fina, média, grossa e muito grossa, respectivamente.

Os códigos de barras nasceram das necessidades de se aumentar o grau de eficiência de processos de logísticos e de vendas de mercadorias. É caracterizado como um conjunto de barras, apresentando logo abaixo das mesmas uma sequência numérica, facilmente identificada. Os sistemas de códigos de barras mais comuns são "European Article Numbering" com 13 dígitos (EAN - 13), (figura 03), e o Universal Product Code (UPC), muito comuns nos EUA e no Canadá, possuindo 12 dígitos.

Figura 3: Exemplo de Código de Barras EAN-10

Fonte: Wikipédia

Nos códigos de barras, os três primeiros dígitos servem para identificar o país onde o produto foi produzido; nos produtos fabricados no Brasil, por exemplo, os três primeiros dígitos dos códigos de barras é 789. Os quatro números seguintes são designados para identificar a empresa; ressalta-se que os dígitos identificadores da empresa podem variar de quatro a sete. Os cinco dígitos seguintes, servem para identificar as características do produto. O último dígito é chamado de dígito de controle, sendo o resultado de operações feitos com os dígitos anteriores.

3.1.4.1- A DETECÇÃO DE ERROS

O princípio de funcionamento dos códigos de barras é dinamizar o processo de entradas de saídas de produtos. Devido a isso, a detecção de erros é de fundamental importância. Para uma melhor compreensão do processo de detecção de erros, sugerimos um estudo mais aprofundado de SANT´ANNA (2013).

Para compreendermos o processo, de acordo com SANT´ANNA (2013), vamos supor que um certo produto está identificado no sistema EAN -13, de acordo com uma dada sequência de dígitos $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}a_{12}a_{13}$. Já sabemos que os primeiros dígitos identificam o país de origem, o fabricante e o produto. Os primeiros doze dígitos dessa sequência, estão determinados, por um método padrão, sob responsabilidade de uma autoridade classificadora em cada país. O décimo terceiro dígito, chamado de dígito verificador, denotaremos por K.

Sendo assim, o algoritmo que permite a detecção de erros, pode ser escrito como o da matriz

$$\alpha = (a_1a_2, a_3, \ldots, a_{10}, a_{11}, a_{12},\ K) \tag{3.6}$$

por uma matriz, que no sistema EAN -13 é chamado de vetor peso, que é dado por

$$w = \ (1\ ,3\ ,1, 3, 1, 3, 1, 3, 1\ ,3, 1, 3, 1) \tag{3.7}$$

Assim, o produto escalar das matrizes tem a seguinte configuração

$$\alpha.w = (a_1a_2, a_3, \ldots, a_{10}, a_{11}, a_{12},\ K)\ .\ (1\ ,3\ ,1, 3, 1, 3, 1, 3, 1\ ,3, 1, 3, 1)$$

$$= a_1 + 3a_2 + a_3 + 3a_4 + a_5 + 3a_6 + a_7 + 3a_8 + a_9 + 3a_{10} + a_{11} + 3a_{12} + K \tag{3.8}$$

Por fim, o dígito verificador é encontrado através um processo tal que a soma acima seja um múltiplo de 10, ou seja

$$\alpha.w \equiv 0\ (mod\ 10) \tag{3.9}$$

Exemplo 19: Tomando como exemplo a o código de barra da figura 4, vamos supor que não se conhecesse o seu último dígito, chamado de dígito de controle. A sequência de numérica que será utilizada para se encontrar o dígito de controle, de acordo com a figura, é 789490053100

Figura 4: Códigos de Barras

Fonte: Wikipédia

$$(7 \cdot 1 + 8 \cdot 3 + 9 \cdot 1 + 4 \cdot 3 + 9 \cdot 1 + 0 \cdot 3 + 0 \cdot 1 + 5 \cdot 3 + 3 \cdot 1 + 1 \cdot 3 + 0 \cdot 1 + 0 \cdot 3 + k) \equiv 0(mod\ 10)$$

$$(7 + 24 + 9 + 12 + 9 + 0 + 0 + 15 + 3 + 3 + 0 + 0 + k) \equiv 0(mod 10)$$

$$(82 + k) \equiv 0(mod\ 10)$$

$$\Leftrightarrow$$

$$k = 8$$

Logo, verifica-se que o algoritmo (3.8) revela quão fundamental são os conceitos de aritmética modular na simplificação e otimização na dinâmica dos mercados, nas trocas de produtos, evitando erros e facilitando os negócios entre empresas, pessoas, etc.

3.1.4.4 - SISTEMA ISBN

O sistema ISBN (International Standard Book Number) foi desenvolvido para identificação numérica de livros, editoras, autores, títulos, etc. É um sistema semelhante ao código de barras, seu surgimento se deu no ano de 1967 por editores ingleses, mas a oficialização do ISBN só se deu no ano de 1972, como norma internacional dada pela Organization for Standartization – ISO 2108 – 1972.

Inicialmente, o sistema ISBN era composto por 10 dígitos e é descrito como ISBN-10. A partir de 1º de janeiro de 2007 passou a ter 13 dígitos, sendo conhecido como ISBN-13.

Determinar o dígito verificador do ISBN é outra importante aplicação da aritmética modular. O processo é semelhante ao do código de barras, ou seja, multiplicaremos os dígitos pelo vetor

$$w = (1,3,1,3,1,3,1,3,1,3,1,3,1)$$

Exemplo 20: Vamos determinar o dígito verificador do livro Aritmética, da coleção PROFMAT, HEFEZ (b) (2016). Analisando a obra, podemos observar que os 12 primeiros dígitos são 978858337105k (onde a k significa o digito verificador), logo

$$(9\cdot 1 + 7\cdot 3 + 8\cdot 1 + 8\cdot 3 + 5\cdot 1 + 8\cdot 3 + 3\cdot 1 + 3\cdot 3 + 7\cdot 1 + 1\cdot 3 + 0\cdot 1 + 5\cdot 3 + k) \equiv 0(mod\ 10)$$

$$(9 + 21 + 8 + 24 + 5 + 24 + 3 + 9 + 7 + 3 + 0 + 15 + k) \equiv 0(mod 10)$$

$$(128 + k) \equiv 0(mod\ 10)$$

$$\Leftrightarrow$$

$$k = 2$$

Logo, o ISBN do livro Aritmética, coleção PROFMAT do autor Abramo Hefez é dado por 9788583371052. Tal fato poderá ser confirmado ao consultar a obra citada.

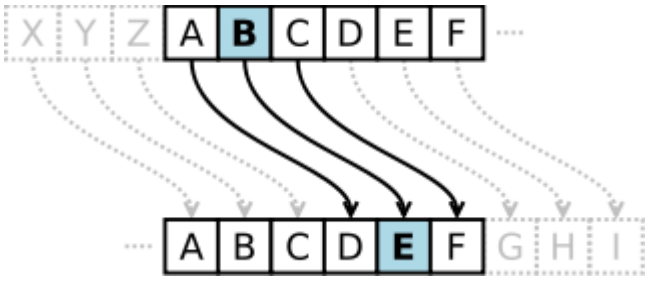
3.1.5- CRIPTOGRAFIA

Na sociedade da informação e comunicação, o sigilo das informações que circulam nos diversos canais de comunicação presentes na atualidade é cada vez maior. Empresas, universidades, centros de pesquisas, governos, pessoas, etc., precisam manter os sigilos das informações que recebem e transmitem. Uma técnica que se manter esse sigilo é feita através da criptografia. A palavra "CRIPTOGRAFIA" vem do grego, *kriptós*: escondido, oculto e *grápho*: grafia. Logo, Criptografia vem a ser a técnica de se escrever uma mensagem de maneira sigilosa, através de códigos de tal forma que apenas os destinatários possam decodificá-la.

3.1.5.1 - CRIPTOGRAFIA DE CÉSAR.

A criptografia de César ou Cifra de César foi uma das primeiras formas utilizadas para se manter o sigilo das mensagens enviadas. Tal método surgiu com finalidades militares, quando o Imperador romano Júlio César necessitava enviar alguma mensagem aos seus comandados durante as guerras que eles enfrentavam. Tal técnica consistia na transposição de um certo número de casas para frente das letras do alfabeto. A figura 5 mostra essa técnica transpondo as letras em três casa para frente, ou seja, cada letra é substituída por uma outa que está três posições a sua frente. Com essa técnica, o exército romano se protegia de possíveis interceptadores de mensagens enviadas pelo Imperador Júlio César.

Figura 5: Transposição em três casas para frente



Fonte: Wikipedia

A tabela 4, conforme SANT´ANNA (2013), traz em minúsculo, a transposição em três casas para frente das letras do alfabeto, utilizando a técnica da cifra de César e que é

estudada até dos dias atuais pela sua importância e pelo fato de ter sido umas das primeiras técnicas para proteção de mensagens.

Tabela 4 - Transposição do Alfabeto em Três Casas Para Frente

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
d	*E*	*F*	*G*	*H*	*i*	*j*	*K*	*L*	*m*	*n*	*o*	*P*
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
q	*R*	*S*	*T*	*U*	*V*	*w*	*X*	*Y*	*z*	*a*	*b*	*C*

Fonte: SANT´ANNA (2013)

Sendo assim, quando o imperador queria se comunicar com os seus subordinados do exército romano, ele fazia a transposição de três casas para frente das letras do alfabeto em cada palavra do texto da mensagem.

Exemplo 21 – Vamos supor que se queria escrever a seguinte frase com a Cifra de César:

"O MUNDO SE FAZ ATRAVÉS DA MATEMÁTICA"

Aplicando a técnica da cifra de César, temos:

"r pxqgr vh idc dwudyhr gd pdwhpdwlcd"

Embora não pareça, a cifra de César é uma importante aplicação de aritmética modular. Considere a seguinte tabela do alfabeto, na qual à cada letra é atribuído um número correspondente, conforme a tabela 05.

Tabela 5 - Pré- Codificação do Alfabeto

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

Fonte: SANT´ANNA (2013)

Esse recurso, transforma as mensagens em números, que através da codificação são transformadas em outros números. Uma codificação utiliza um número natural *k*, chamado de chave. No caso da Cifra de César, $k = 3$.

Exemplo 22: Vamos fazer uma correspondência entre os números e as letras da palavra abaixo e depois aplicaremos o método da Cifra de César.

"BAHIA"

A sequência numérica correspondente ao nome BAHIA, é escrita da seguinte forma

$$01 - 00 - 07 - 08 - 00$$

Aplicado o método da cifra de César, ou seja, aplicando a chave *k= 3*, temos

$$04 - 03 - 10 - 11 - 03$$

Fazendo a correspondência número-letra, temos uma sequência de letras que difere muito da palavra original.

EDKLD

Será que é possível aplicarmos o método da Cidra de César para uma chave $k > 3$? Como o alfabeto possui 26 letras, seja *t* o número correspondente a uma letra do texto, *k* uma determinada chave e *C* o número de uma letra de um texto codificado. Assim,

$$C(t) \equiv t + k\ (mod 26), com\ 0 \leq C \leq 25$$

Exemplo 23: Vamos codificar o nome abaixo para $k = 12$

"PROFMAT"

Fazendo a correspondência de cada letra da palavra PROFMAT com os seus respectivos números, temos:

$$15 - 17 - 14 - 05 - 12 - 00 - 19$$

Como *k=12,* usaremos a congruência $C(t) \equiv t + 12\ (mod 26)$ para codificar esses números. Logo:

$C(15) \equiv 15 + 12\ (mod 26) \equiv 01(mod 26)$

$C(17) \equiv 17 + 12\ (mod 26) \equiv 03(mod 26)$

$C(14) \equiv 14 + 12\ (mod 26) \equiv 00(mod 26)$

$C(5) \equiv 5 + 12\ (mod 26) \equiv 17(mod 26)$

$C(12) \equiv 12 + 12\ (mod 26) \equiv 24(mod 26)$

$C(0) \equiv 12\ (mod 26)$

$C(19) \equiv 19 + 12\ (mod 26) \equiv 05(mod 26)$

Assim, o código da mensagem é

$$01 - 03 - 00 - 17 - 24 - 12 - 05$$

Fazendo a correspondência com as letras, temos

"BDARVMF"

A codificação de mensagens pelo método da Cifra de César é uma maneira de proteger o conteúdo das mesmas, mas um questionamento que poderá surgir é o que trata sobre a decodificação das mesmas: Como fazer para decodificar uma mensagem? Sendo assim, para decodificar as mensagens, utilizamos a seguinte congruencia

$$t \equiv C(t) - k\ (mod 26)$$

Chamando $C(t)$ de p temos

$$Q(p) \equiv p - k\ (mod 26)$$

Exemplo 24: Vamos descodificar e descobrir o que quer dizer a mensagem abaixo com o método da Cifra de César, portanto *k*=3.

17– 21 16– 23– 15– 07– 18– 17– 21 09– 17– 24– 07– 20– 16– 03– 15 17 15– 03– 16– 06– 17

Então, vamos decodificar esses códigos

$Q(17) \equiv 17 - 3\ (mod 26) \equiv 14(mod 26)$

$Q(21) \equiv 21 - 3\ (mod 26) \equiv 18(mod 26)$

$Q(16) \equiv 16 - 3\ (mod 26) \equiv 13(mod 26)$

$Q(23) \equiv 23 - 3\ (mod 26) \equiv 20(mod 26)$

$Q(15) \equiv 15 - 3\ (mod 26) \equiv 12(mod 26)$

$Q(07) \equiv 07 - 3\ (mod 26) \equiv 04(mod 26)$

$Q(18) \equiv 18 - 3\ (mod 26) \equiv 15(mod 26)$

$Q(17) \equiv 17 - 3\ (mod 26) \equiv 14(mod 26)$

$Q(21) \equiv 21 - 3\ (mod 26) \equiv 18(mod 26)$

$Q(09) \equiv 09 - 3\ (mod 26) \equiv 06(mod 26)$

$Q(17) \equiv 17 - 3\ (mod 26) \equiv 14(mod 26)$

$Q(24) \equiv 24 - 3\ (mod 26) \equiv 21(mod 26)$

$Q(07) \equiv 07 - 3\ (mod 26) \equiv 04(mod 26)$

$Q(20) \equiv 20 - 3\ (mod 26) \equiv 17(mod 26)$

$Q(16) \equiv 16 - 3\ (mod 26) \equiv 13(mod 26)$

$Q(03) \equiv 03 - 3\ (mod 26) \equiv 00(mod 26)$

$Q(15) \equiv 15 - 3\ (mod26) \equiv 12(mod26)$

$Q(17) \equiv 17 - 3\ (mod26) \equiv 14(mod26)$

$Q(15) \equiv 15 - 3\ (mod26) \equiv 12(mod26)$

$Q(03) \equiv 03 - 3\ (mod26) \equiv 00(mod26)$

$Q(16) \equiv 16 - 3\ (mod26) \equiv 13(mod26)$

$Q(06) \equiv 06 - 3\ (mod26) \equiv 03(mod26)$

$Q(17) \equiv 17 - 3\ (mod26) \equiv 14(mod26)$

A mensagem, decodificada terá a seguinte sequência

$$14 - 18\ 13 - 20 - 12 - 04 - 15 - 14 - 18\ 06 - 14 - 21 - 04 - 17 - 13 - 00 - 12\ 14\ 12 - 00 - 13 - 03 - 14$$

Fazendo a correspondência entre os números e as letras, temos a seguinte mensagem

OS NÚMEROS GOVERNAM O MUNDO

4 – APRENDIZAGEM BASEADA EM PROBLEMAS

Ao observarmos as práticas pedagógicas vigentes, percebemos que ainda persiste o método de ensino em que o professor realiza suas aulas através da reprodução e da transmissão de conteúdo, com aulas expositivas, seguindo um plano previamente estabelecido, no qual ele é a figura central dessa aula.

O ensino de matemática e de outras ciências ainda é feito através de uma metodologia centrada na figura do professor como detentor do saber. Tal prática ainda se faz presente em escolas do Brasil e no mundo em pleno século XXI.

Uma alternativa para se superar o modelo de ensino centrado numa metodologia meramente reprodutiva é a Aprendizagem Baseada na Resolução de Problemas (APB). A APB é um método inovador, focado na aprendizagem e que vem ganhando espaço em todos os níveis de ensino no Brasil e no mundo. A primeira aplicação dessa metodologia se deu no ano de 1969 no curso de Ciências da Saúde da Universidade de McMaster University, no Canadá.

Vários estudiosos da APB tentaram conceituar essa temática, trazendo grandes contribuições acerca da abrangência, da importância, da relevância, etc., dessa temática. Para BARROWS (1986) *apud* SOUZA e DOURADO (2015) a APB é um método de aprendizagem que tem como base a utilização de problemas como ponto de partida para integrar e adquirir novos conhecimentos. Assim, a APB parte de um contexto e a partir daí é que se desenvolve a aprendizagem e a integração dessa com outras áreas do conhecimento.

Para MAMEDE (2001), a APB se configura como uma estratégia educacional e uma filosofia curricular, em que os discentes autodirigidos constroem o conhecimento de forma ativa e colaborativa, aprendendo de forma contextualizada, apropriando-se de um saber com significado pessoal. Sendo assim, pode-se perceber que a APB não vê na figura do professor o centro da aprendizagem, mas no discente, rompendo dessa forma com aquele modelo de ensino que perdura por vários séculos e que não tem acompanhado a evolução da humanidade e da própria forma de aprender.

LEITE E ESTEVES (2005) *apud SOUZA* e DOURADO (2015) entendem a ABP como um caminho que conduz o aluno para a aprendizagem. Nesse contexto, a relação entre o aluno e os problemas de uma área de conhecimento vai promovendo,

gradativamente, uma evolução na aprendizagem desse aluno, visto que este desempenha um papel ativo através da investigação, da análise e da síntese do conhecimento investigado.

4.1- APRENDIZAGEM BASEADA EM PROBLEMAS NA MATEMÁTICA

A proposta de se ensinar a matemática através da APB ainda é desafiador no contexto de muitas escolas. A abordagem problematizadora pode motivar os alunos a descobrir a beleza da matemática e que ela se faz presente em vários campos da atividade humana. Para SOUZA e DOURADO (2015) o problema pode ser modesto, mas se ele desafiar a curiosidade e colocar em jogo as faculdades inventivas, quem o resolver por seus próprios meios experimentará a tensão e gozará o triunfo da descoberta."

Ensinar a matemática através da APB pode ser uma ferramenta capaz de motivar a raciocínio lógico dos alunos, através de uma ação motivadora, exigindo do mesmo uma postura reflexiva diante da situação em que ele é exposto.

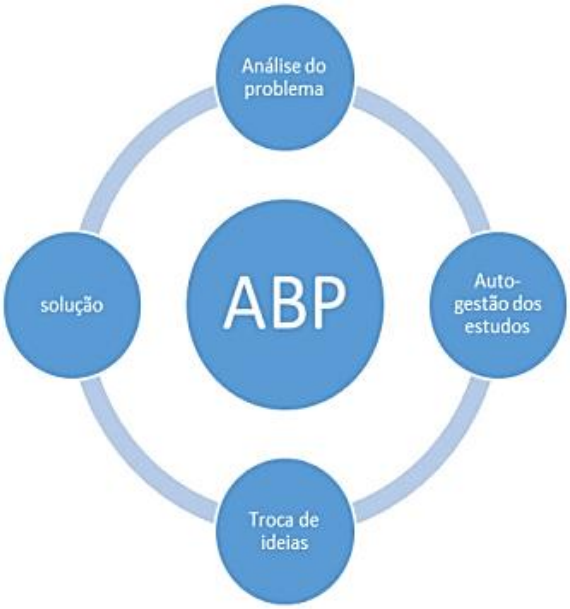
Ainda de acordo com SOUZA e DOURADO (2015)

> *Um professor de Matemática tem, assim, uma grande oportunidade. Se ele preenche o tempo que lhe é concedido a exercitar seus alunos em operações rotineiras, aniquila o interesse e tolhe os desenvolvimentos intelectuais dos estudantes, desperdiçando, dessa maneira, a sua oportunidade. Mas se ele desafia a curiosidade dos alunos, apresentando-lhes problemas compatíveis com os conhecimentos destes e auxiliando-os por meio de indagações estimulantes, poderá incutir-lhes o gosto pelo raciocínio independente e proporcionar-lhes certos meios para alcançar este objetivo. (SOUZA e DOURADO, p. 5)*

Percebe-se nas palavras de SOUZA e DOURADO (2015) que propor problemas aos alunos serve como um estimulante para que estes aprendam matemática. Desenvolver o gosto pelo raciocínio independente, como afirma o autor, contribuirá para que alunos possam desenvolver novas aplicações que poderão trazer novos benefícios para toda a

sociedade. Esses caminhos (ver figura 6) ajudam os alunos a desenvolver um ciclo de aprendizagem através da metodologia proposta pela APB, levando-os a se tornarem protagonistas da sua própria aprendizagem.

Figura 6: Aprendizagem Baseada em Problemas



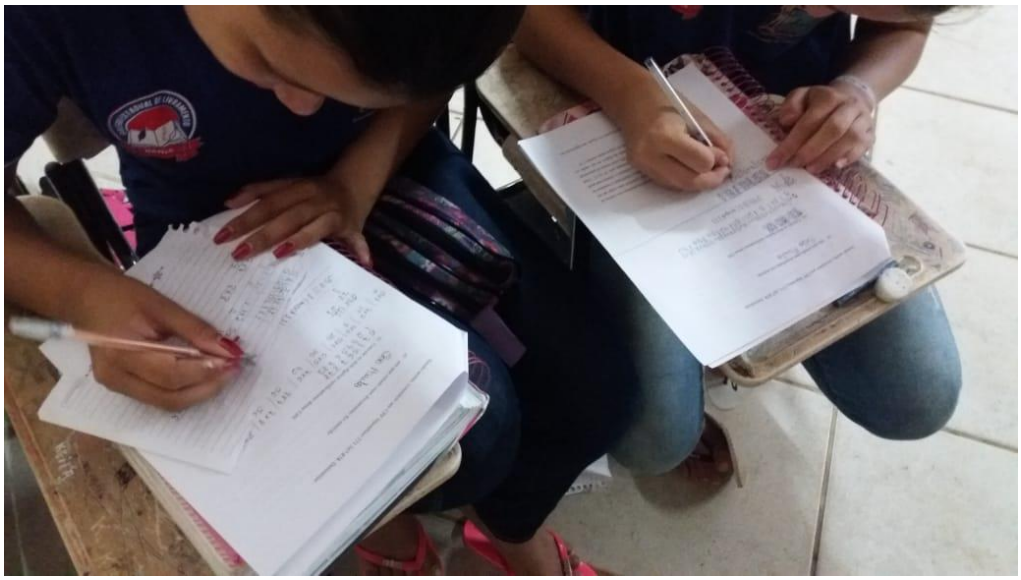
Fonte: Wikipedia

A APB ajuda a ressignificar o processo ensino aprendizagem, trazendo ideias e metodologias que colocam sempre o aluno como principal sujeito no processo ensino aprendizagem. Por isso, conforme SOUZA e DOURADO (2015) o trabalho em grupo destaca-se como uma forma de atividade em que o aluno valoriza a convivência e se dispõe a participar, de forma criativa, do processo de aprendizagem, buscando criar espaços para o trabalho cooperativo, no qual todos são protagonistas, colaborando para uma aprendizagem mútua e integral.

5 - ARITMÉTICA MODULAR NA SALA DE AULA

O objetivo desse trabalho é dissertar sobre a inserção do tema aritmética modular no ensino básico. Para tanto, foram aplicadas algumas questões relacionadas numa turma da 1ª série do ensino médio do Colégio Estadual de Livramento, na cidade de Livramento de Nossa Senhora, no estado da Bahia. Os alunos foram divididos em duplas, conforme figura 7, e foram necessárias duas aulas de 50 minutos cada para aplicação de toda a atividade. O experimento consistia em resolver problemas de aritmética modular através da metodologia proposta pela Aprendizagem Baseada na Resolução de Problemas (APB). As questões foram elaboradas de forma tal que os níveis de dificuldades fossem aumentando à medida que os alunos fossem avançando na resolução de cada questão. A adoção da metodologia proposta pela Aprendizagem Baseada na Resolução de Problemas foi importante na elaboração dessas questões visto que os problemas presentes nesse experimento fazem parte de um contexto social e tecnológico no qual todos nós estamos inseridos, facilitando assim a compreensão desse estudo. Os materiais necessários para a realização da atividade foram papel A4, lápis, caneta e borracha. Participaram da atividade 28 alunos entre 15 e 18 anos.

Figura 7: Alunos Resolvendo Aplicações de Aritmética na Educação Básica



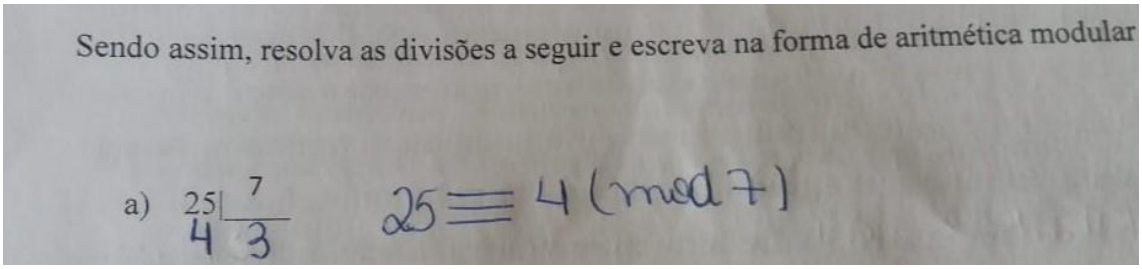
Fonte: Arquivo Pessoal

5.1- RESULTADOS DAS ATIVIDADES

A primeira questão dessa atividade consistia em escrever duas questões de divisão euclidiana na forma de congruência, de aritmética modular. O objetivo da é estabelecer relações entre uma divisão e o assunto de congruência

Os 28, ou seja 100% dos alunos, conseguiram compreender o conceito de congruência, dentro do tema aritmética modular. Essa atividade inicial serviu como ponto de partida para um conceito mais amplo. Como o conceito congruência é de fácil interpretação, os alunos fizeram a divisão euclidiana (ver figura 8 e figura 9), calcularam quociente e o resto, e escreveram a divisão na forma de congruência.

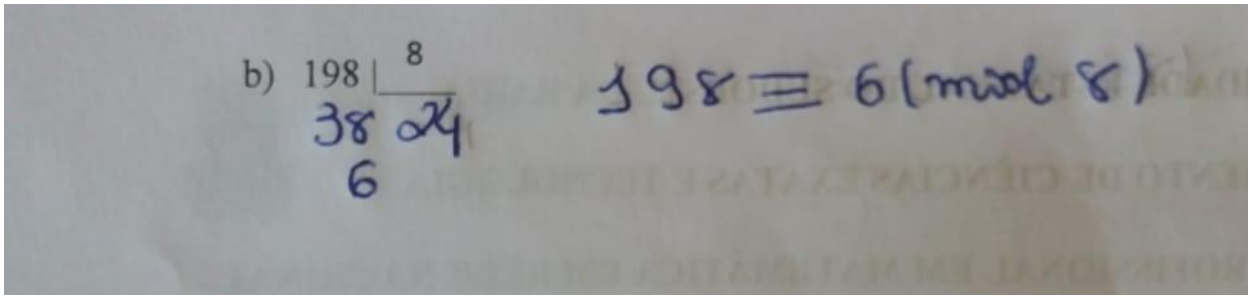
Figura 8: Relacionando divisão com congruência



Fonte: Arquivo Pessoal

Nessa atividade, a maioria dos alunos conseguiram estabelecer relações entre divisão e congruência.

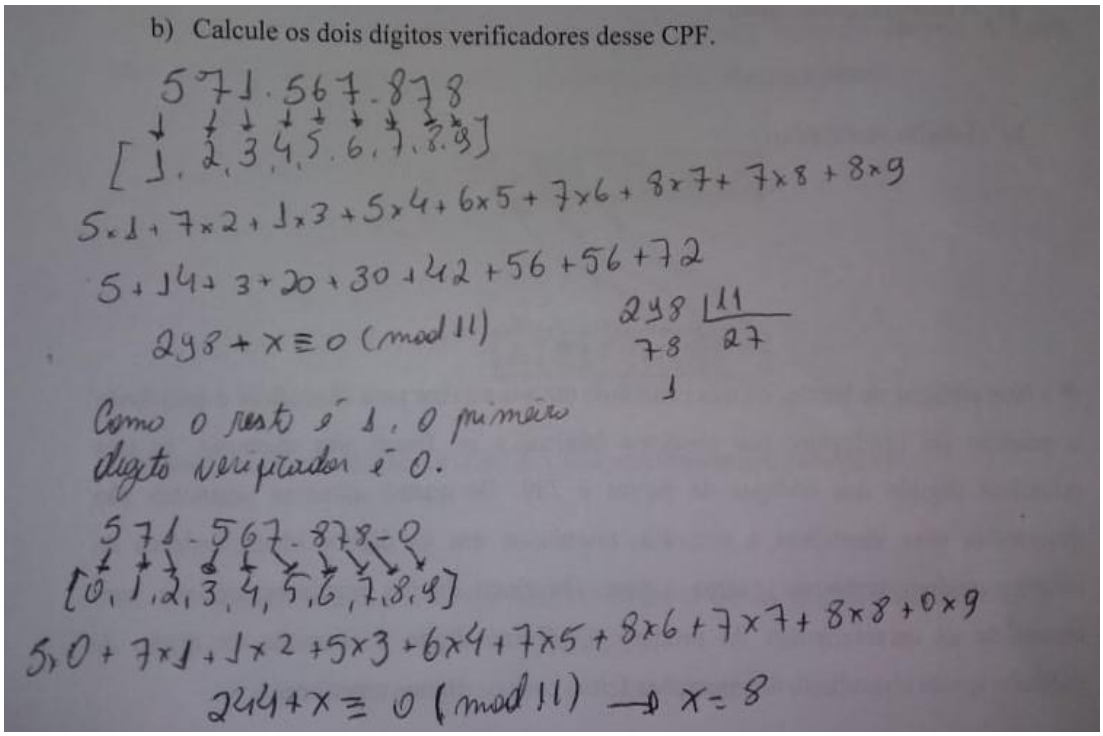
Figura 9: Congruência de Números Inteiros



Fonte: Arquivo Pessoal

A Segunda questão trouxe para os alunos um tema importante e já abordado nessa pesquisa que são os dígitos verificadores do CPF. Conhecer os fundamentos e a razão de ser de cada número ali presente é de fundamental importância para compreender como a matemática se faz presente em todos os segmentos da sociedade pós-moderna. Nessa questão foram dadas uma tabela contendo os números correspondente a cada estado pertencente as regiões fiscais do Brasil, disponibilizados pela Receita Federal. Também foram dados o algoritmo do cálculo dos dígitos verificadores do um CPF fictício, sendo os nove primeiros dígitos 571.567.878 . Cabiam aos alunos identificar a região fiscal onde aquele documento foi emitido e calcular os seus dígitos verificadores. Aproximadamente 78% alunos conseguiram responder completamente às questões, sendo que o restante conseguiram responder apenas parcialmente .Os alunos, conforme figura 10, conseguiram calcular o algoritmo e determinar os dígitos verificadores.

Figura 10: Cálculo de Dígitos Verificadores do CPF

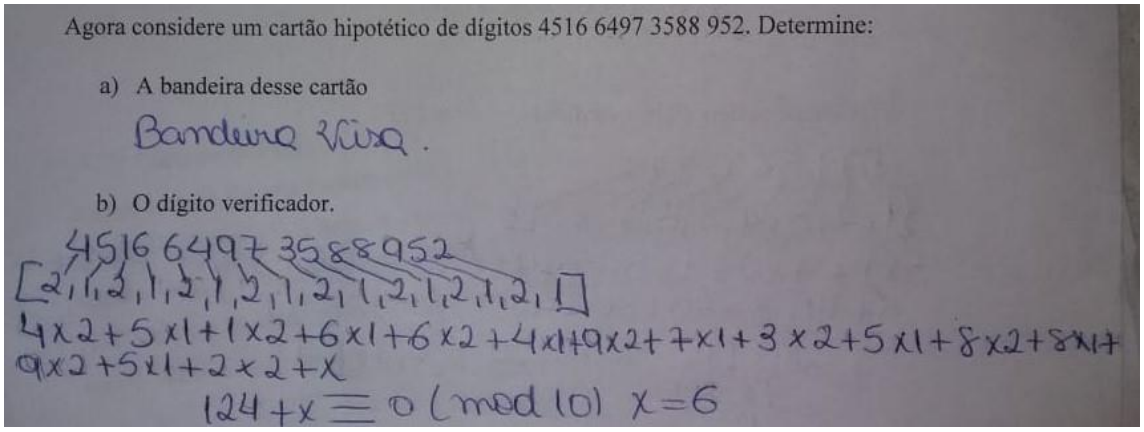


Fonte: Arquivo Pessoal

Ressalta-se que algumas duplas apresentaram alguma confusão no entendimento de como se determinava esses dígitos verificadores, alguns considerando apenas os restos da congruência como os dígitos verificadores e não levando em consideração o que faltava àqueles restos para que a congruência tivesse o zero com resto.

A terceira questão desse trabalho aplicados aos alunos trouxe um instrumento muito utilizado nas transações comerciais e que desperta muitos questionamentos sobre a sua eficiência e funcionamento por parte das pessoas: o cartão de crédito. Na questão foi dado aos alunos alguns dígitos fictícios de cartão de crédito, sendo estes 4516 6497 3588 952; e foi pedido a eles que a partir desses dados, que identificassem a bandeira de cartão, e o seu dígito verificador, ver figura 10. Como já tinham feito algo semelhante no processo do cálculo do CPF, os alunos pareciam ter mais segurança para determinar o dígito verificador do cartão de crédito. Dentre os 28 alunos, 20 conseguiram responde às questões integralmente, o que corresponde a aproximadamente 71%.

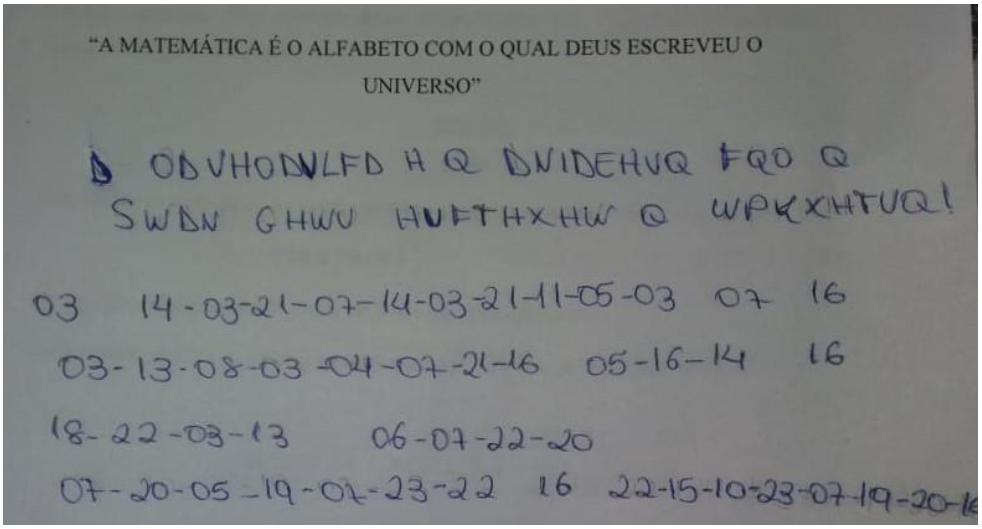
Figura 11: Cálculo do Dígito Verificador do Catão de Crédito



Fonte: Arquivo Pessoal

A quinta e última questão a ser respondida pelos alunos está relacionada à cifra de César. Método utilizado pelo imperador romano Júlio César para manter o sigilo das mensagens que ele enviava para os seus comandados do exército romano. É uma espécie de criptografia, se for considerado sua principal finalidade, que é proteger o sigilo das mensagens. A atividade consistia em transpor em três casa para frente as letras da frase "A MATEMÁTICA É O ALFABETO COM O QUAL DEUS ESCREVEU O UNIVERSO", (figura 12) e escrevê-la de acordo com essa transposição. A última parte dessa atividade consistia em codificar numericamente essa atividade. Nessa atividade, cerca de 28,5 % dos alunos, o que corresponde a 8 alunos responderam essa questão. Outros 21,4 % responderam apenas parcialmente, sendo 6 o número desses alunos.

Figura 12: Codificando com a Cifra de César



Fonte: Arquivo Pessoal

6 – CONCLUSÃO

Inferir sobre a aritmética modular na educação básica através da metodologia proposta pela Aprendizagem Baseada na Resolução de Problemas nos ajudou a perceber que tanto a aritmética modular quanto a APB podem ser propostas que ajudarão os alunos a compreender melhor a aprendizagem em matemática.

Os resultados da experiência com a aritmética modular através da APB dão sinais possíveis de que esse ramo da matemática pode ser ensinado na educação básica. O fato de 100% dos alunos conseguirem estabelecer uma relação entre uma divisão euclidiana e uma congruência podem ajuda-los a compreender melhor a divisibilidade de números inteiros, operação esta tão importante para o exercício da cidadania. Outro aspecto a se observar é que através da APB foi possível fazer com que os alunos compreendessem o significado dos dígitos verificadores de um CPF. No problema proposto para se descobrir a região fiscal e os dígitos verificadores, cerca de 78 % dos alunos conseguiram resolver o problema.

Nos problemas que foram propostos aos alunos que eles encontrassem o dígito verificador de um cartão de crédito hipotético, 71% dos alunos conseguiram resolver a atividade com êxito. Tal fato evidencia que tanto a APB como a aritmética modular são temas que ganham relevância para serem trabalhados na educação básica.

Sendo assim, a compressão dos resultados da pesquisa Aplicações de Aritmética Modular através da Resolução de Problemas sinaliza para que esse ramo da matemática seja inserido no contexto dos conteúdos de estudo da educação básica. Sua funcionalidade e importância falam por si.

ANEXOS

UNIVERSIDADE ESTADUAL DO SUDOESTE DA BAHIA

DEPARTAMENTO DE CIÊNCIAS EXATAS E TECNOLOGIA

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

Escola:

Série:

Nome Idade:

Esse questionário faz parte de uma pesquisa do Mestrado Profissional em Matemática em Rede (PROFMAT) da Universidade Estadual do Sudoeste da Bahia (UESB), com o intuito de investigar as Aplicações de Aritmética Modular no Ensino Básico.

QUESTIONÁRIO

1º - A aritmética modular é um ramo da matemática que estuda os Números Inteiros, suas características e propriedades. Ela busca facilitar a compreensão e o estudo desse conjunto numérico. Um exemplo dessa simplificação, está nada divisibilidade de números inteiros e seus restos.

$$58 \mid \_\_8\_\_$$
$$2 \quad 7$$

Esse problema pode ser assim escrito na forma de aritmética modular:

$$58 \equiv 2 \bmod 8.$$

ou seja, quando dividimos 58 por 8, ele deixa um resto igual a 2.

Sendo assim, resolva as divisões a seguir e escreva na forma de aritmética modular

a) $25 \mid \underline{\quad 7 \quad}$

b) 198 |8___

2º - O Cadastro de Pessoas Físicas (CPF) é um documento muito importante no Brasil e é emitido pela Receita Federal do Brasil. Esse documento contém 11 dígitos. Os nove primeiros dígitos são a base de cálculo para encontrar o décimo e o décimo primeiro dígitos, sendo estes os dígitos verificadores. O nono dígito define a região fiscal, revelando assim onde o CPF foi emitido. A tabela a seguir identifica o número e a região fiscal de cada estado brasileiro.

Tabela de Regiões Fiscais

NÚMERO	REGIÃO FISCAL
0	RS
1	DF, GO, MS, MT, TO
2	AC, AM, AP, PA, RO, RR
3	CE, MA, PI
4	AL, PB, PE, RN
5	BA, SE
6	MG
7	ES, RJ
8	SP
9	PR, SC.

Para encontrar o primeiro dígito verificador, devemos multiplicá-los, nesta ordem, por pela sequência [1, 2, 3, 4, 5, 6, 7, 8, 9] e somar os resultados (S). O décimo dígito (a_{10}) é o resto da divisão de S por 11, com a exceção para o caso em que o resto é 10, no qual será utilizado o dígito zero. Para encontrar o segundo dígito verificador, devemos multiplicar, nesta ordem, os dígitos $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}$ por [0 , 1 ,2, 3, 4, 5, 6, 7,

8, 9] e somar os resultados (S'). O décimo primeiro dígito é o resto da divisão de S' por 11, com exceção para o caso em que o resto for igual a 10, no qual é utilizado o dígito zero.

Os cálculos obedecem à seguinte regra:

1º digito verificador → S - $a_{10} \equiv 0\ (mod\ 11)$ (3.1)

2º digito verificador → S' – $a_{11} \equiv 0\ (mod\ 11)$

Sendo assim, considere um CPF hipotético 571.567.878. Determine:

a) em que estado esse documento foi emitido

b) Calcule os dois dígitos verificadores desse CPF.

3º - Uma pessoa desinformada poderá achar que os números presentes nos cartões de crédito são aleatórios, mas todos os números ali presentes possuem uma razão de ser. Por exemplo, os primeiros números de um cartão de crédito identificam a bandeira do cartão. Todos os cartões de bandeira Visa começam com o número 4, Mastercard pode começar com 51, 52, 53, 54 ou 55. American Express começam com 34 ou 37. Essa regra serve para todo o mundo, tendo sido definida em 1989 como forma de padronizar movimentações financeiras. Normalmente, a quantidade de dígitos de um cartão de crédito pode variar de 14 a 19. No Brasil, a quantidade de dígitos mais comum é 16.

Para determinar o dígito verificador, basta multiplicarmos os valores dos dígitos de um cartão, na ordem em que aparecem, por

$$p = [\,2\ \ 1\ \ 2\ \ 1\ \ 2\ \ 1\ \ 2\ \ 1\ \ 2\ \ 1\ \ 2\ \ 1\ \ 2\ \ 1\ \ 2\ \ 1]$$

adicionado os resultados e dividindo por 10. O valor do resto dessa divisão será o dígito verificador desse cartão de crédito.

Agora considere um cartão hipotético de dígitos 4516 6497 3588 952. Determine:

a) A bandeira desse cartão

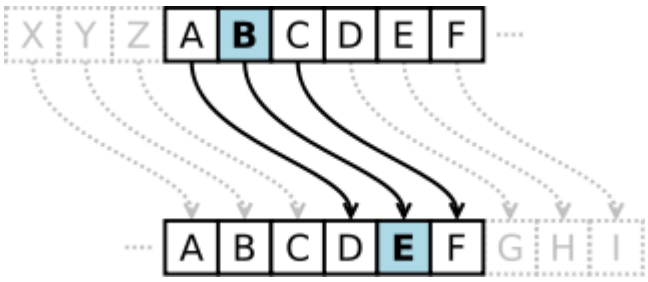
b) O dígito verificador.

4º - Nos códigos de barras, os três primeiros dígitos servem para identificar o país onde o produto foi produzido; nos produtos fabricados no Brasil, por exemplo, os três primeiros dígitos dos códigos de barras é 789. Os quatro números seguintes são designados para identificar a empresa; ressalta-se que os dígitos identificadores da empresa podem variar de quatro a sete. Os cinco dígitos seguintes, servem para identificar as características do produto. O último dígito é chamado de dígito de controle, sendo o resultado de operações feitos com os dígitos anteriores.

Para se calcular o dígito de controle, multiplicarmos os valores dos dígitos do código de barras, nessa ordem, por $[1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1]$ adicionarmos os resultados e dividirmos o resultado por 10. O valor do resto será o dígito de controle.

Suponha que os valores dos dígitos de um determinado código de barras sejam 789581043010. Determine o seu dígito de controle. Escreva essa divisão na forma de aritmética modular.

5º - A criptografia de César ou Cifra de César foi uma das primeiras formas utilizadas para se manter o sigilo das mensagens enviadas. Tal método surgiu com finalidades militares, quando o imperador romano Júlio César necessitava enviar alguma mensagem aos seus comandados durante as guerras que eles enfrentavam. Tal técnica consistia na transposição de um certo número de casas para frente das letras do alfabeto. A figura abaixo utiliza essa técnica transpondo as letras em três casa para frente.



Escreva frase abaixo usando a cifra de César com três casas para frente.

"A MATEMÁTICA É O ALFABETO COM O QUAL DEUS ESCREVEU O UNIVERSO"

REFERÊNCIAS

AZEVEDO, V. A.; PIRES, G. L. Análise da produção em educação física/esporte e mídia veiculada nos congressos do CBCE e da Intercom. In: IV Congresso Sul-Brasileiro de Ciências do Esporte. Anais... Faxinal do Céu, Paraná. Disponível em: < http://cbce.tempsite.ws/congressos/index.php/csbce/ivcsbce/paper/view/44>, acesso em 20/03/2019.

DOMINGUES. Hygino H. Fundamentos de Aritmética. Atual Editora. São Paulo, 1991.

HEFEZ, Abramo. Elementos da Aritmética, 2ª edição, SBM, 2005.

HEFEZ (b), Abramo. Aritmética. Rio de Janeiro; SBM; 2016.

LEOPOLD, Guilherme Liegem. Dissertação de Mestrado. Congruências e Aplicações. Disponível em <http://www.sites.uem.br/profmat/GuilhermeLiegelLeopold.pdf >, acesso em 10/03/19.

MAMEDE, S. Aprendizagem baseada em problemas: características, processos e racionalidade. In: MAMEDE, S.; PENAFORTE, J. (Org.). *Aprendizagem baseada em problemas:* anatomia de uma nova abordagem educacional. Fortaleza: Hucitec, 2001. p. 25-48.

MILIES, F. C. P., Números: Uma Introdução à Matemática. São Paulo: Editora da Universidade de São Paulo, 3. ed., 2001.

MILIES (b), Francisco César Polcino Milies. A Matemática dos Códigos de Barras. PIC. OBMEP.2009. Disponível em: obmep.org.br/docs/apostila6.pdf

MORI, Iracema. Matemática: Ideias de Desafios, 6º ano / Iracema Mori, Dulce Satiko Onaga. 18—18. ed. – São Paulo: Saraiva 2015.

OLIVEIRA, Maycon Costa de. Dissertação de Mestrado. Aritmética: Criptografia e Outras Aplicações de Congruências. Disponível em < https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?id=42822> . Acesso em 05/05/2019

SANT´ANNA. Iury Kersnowsky de. A Aritmética Modular como Ferramenta para as Séries Finais do Ensino Fundamental. IMPA, 2013. Disponível em < https://impa.br/wp-content/uploads/2016/12/iury_kersnowsky.pdf>, acesso em 28/04/2019.

POLYA, G. A Arte de Resolver Problemas. Rio de janeiro: Interciência, 1995.

SANTOS, T. Cássia Regina dos. Ensinando Matemática Através dos Códigos de Barras.

SOUZA, S.C e DOURADO, L. Aprendizagem Baseada em Problemas: Um Método de Aprendizagem Inovador para o Ensino Educativo. IFRN, 2015. Disponível em< http://www2.ifrn.edu.br/ojs/index.php/HOLOS/article/download/2880/1143 >. Acesso em agosto de 2019.