Um Estudo de Aritmética Modular para a Educação Básica

Francisca Daniella Andreu Simões Moraes Lage danebencao@gmail.com

Thiago Fontes Santos santostf@ufop.edu.br
Universidade Federal de Ouro Preto, Ouro Preto, MG, Brazil

Resumo

Este estudo é voltado à aritmética modular e pretende ser uma contribuição para a prática de docentes da Educação Básica. O mesmo traz algumas aplicações 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, aplicações, dígito verificador, criptografia.

1 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 este estudo, esperamos que outros educadores possam compreender que algumas áreas da teoria dos números possibilitam muito à 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. Por meio do exposto, desejamos que eles possam ver tais conteúdos como algo real, podendo ser usados em seu cotidiano.

A estrutura deste trabalho é composta por mais duas seções, sendo a próxima voltada para algumas aplicações da aritmética modular. Nela, 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. Falamos, ainda, sobre a utilização 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.

A última seção relata sobre práticas feitas em sala de aula com o uso de congruência no algoritmo de Zeller. Colocamos, também, atividades envolvendo código de barras e cadastro de

pessoa física, ambos trazidos pelos alunos. Nessa seção, ainda foi feito um estudo teórico envolvendo criptografia, sua importância e aplicação de cifras para codificar e decodificar mensagens.

Por fim, chegamos à conclusão com as considerações finais visando melhorias nos trabalhos relativos ao ensino da aritmética dos restos.

2 Algumas Aplicações da Aritmética Modular

Nesta seção, abordamos 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, 6, 4, 8, 2].

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, produtos, documentos e cargas. A criação dos códigos se deu no intuito de ajudar o comércio a aumentar a velocidade para verificar a entrada e a saída de mercadorias.

Ao observar os códigos em vários tipos de produtos, é notório perceber que existem diferentes larguras em suas barras brancas e pretas. Assim, as mesmas podem ser finas, médias, grossas e muito grossas. Conforme a espessura da barra a quantidade de zero ou um altera 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 de barras adotados nos Unidos e Canadá são os denominados *Universal Product Code* (UPC), com 12 dígitos. Mais tarde, fabricantes de países europeus inventaram um sistema de códigos com 13 dígitos chamado *European Article Numbering Association* (EAN).

Nos códigos UPC, a leitura é realizada conforme mostra a Tabela (2) 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.

No que concerne ao sistema EAN-13, esse também é formado 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.

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

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 estão corretos. Para isso, é efetuada uma congruência, podendo ser definda conforme mostra [7], em linhas gerais:

Definição 1 (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:*

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

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:*

$$\overline{a_n} = \overline{p_n}^{-1} \left(\overline{w} - \sum_{i=1}^{n} \overline{a_i p_i} \right) \tag{2}$$

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

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 relata o matemático Jacobus Koos Verhoeff, os erros mais comuns são chamados de erro único e de transposição. O erro único ou consistente ocorre por meio da troca de um dígito por outro(a por b). Nos erros de transposição, os algarismos são digitados com mudança de ordem dos dígitos consecutivos(ab por ba ou abc por cba).

Tomaremos o teorema abaixo, descrevendo como os erros são encontrados nas congruências dos códigos de barras.

Teorema 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:*

$$c \cdot p^t = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \end{bmatrix} \cdot \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{bmatrix} = a_1p_1 + \cdots + a_np_n \equiv w \pmod{m} \quad (3)$$

Então:

1. *Todo erro consistente numa única alteração na posição i-ésima será detectado se, e somente se, $mdc(p_i, m) = 1$.*

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, $mdc(p_i - p_j, m) = 1$.*

Demonstração. A demonstração do teorema dado pode ser vista em [7].

□

2.2 Sistema 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.

Como cada sistema possui o operador módulo e a matriz peso pré- estabelecidos, segue abaixo a congruência realizada para encontrar D no ISBN - 10. Nele, sua sequência numérica é dada pela matriz:

$$c = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 & \cdots & a_9 & D \end{bmatrix} \quad (4)$$

e a matriz peso apresenta-se da seguinte forma:

$$p = \begin{bmatrix} 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix} \quad (5)$$

Para encontrar D usamos a congruência módulo 11 ao produto matricial entre c e p^t. Daí,

$$c \cdot p^t = a_110 + a_29 + a_38 + a_47 + \cdots + a_92 + D \equiv 0 \pmod{11}. \quad (6)$$

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 Cartões de Crédito

Outra aplicação de grande valia da congruência modular com dígitos verificadores está na área de cartões de crédito. O algoritmo usado nesses cartões 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, então fazemos $1 + 4 = 5$). No que se refere aos dígitos de posições pares, estes são conservados, ou seja, seus pesos valem 1. Em seguida, juntamos as respostas das somas da posição ímpar com as da posição par. Daí, o dígito verificador será o número que falta para se chegar em um múltiplo de 10.

Daí,

$$c = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 & \cdots & a_{15} & D \end{bmatrix} \tag{7}$$

e

$$p = \begin{bmatrix} 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 \end{bmatrix} \tag{8}$$

e o produto é dado por:

$$c \cdot p^t = 2a_1 + 1a_2 + 2a_3 + 1a_4 + \cdots + 2a_{15} + D \equiv 0 \pmod{10}. \tag{9}$$

2.4 O Documento de CPF

O Cadastro de Pessoa Física (CPF) é um banco de dados regido pela Secretaria da Receita Federal do Brasil (RFB). Como este documento 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.

O décimo dígito, ou primeiro verificador, vem da congruência módulo 11 operando com os nove primeiros algarismos do CPF:

$$c = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 \end{bmatrix} \tag{10}$$

esses algarismos são multiplicados, conforme a ordem dada no documento, pela primeira matriz de pesos pré-estabelecida por:

$$p = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{bmatrix} \tag{11}$$

Assim como nas outras aplicações, o produto matricial é feito entre c e p^t, dando uma soma (S) e a congruência usada é:

$$S - a_{10} \equiv 0 \pmod{11} \tag{12}$$

Para encontrar o segundo dígito verificador, o mesmo processo é realizado, todavia acrescen-

tando a_{10} em c e a matriz peso p passa a ser:

$$p = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{bmatrix} \tag{13}$$

2.5 Criptografia

A palavra criptografia se origina do grego *kryptós* - escondido e *gráphein* - escrita. 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 tange ao uso da criptografia nos dias de hoje, uma grande aplicação da mesma está relacionada a sites de vendas pela internet, permitindo que o cliente consiga realizar compras seguras.

Quando há a necessidade de se codificar um determinado texto, é imprescindível que se tenha uma chave cifradora. Esta possui um conjunto de bits onde existe um algoritmo capaz de codificar e decodificar/descodificar tal texto. Com isso, dentro da criptografia, a congruência modular é usada desde com recursos simples até os mais complexos.

Doravante, agora falando sobre as 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.

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 uma velocidade de processamento bem rápida. Todavia, a mesma traz consigo uma periculosidade quanto à segurança, já que necessita de um canal de comunicação bastante seguro de maneira que não haja um vazamento de informações por terceiros.

A criptografia assimétrica utiliza-se 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, 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.

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

2.5.1 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. Isso é feito para que não haja ambiguidade na interpretação da mensagem.

Na pré- codificação do método RSA, são utilizados dois números primos, os parâmetros, que necessitam ser bem grandes para dificultar a quebra das chaves. Aqui, os denotaremos por p e q e o produto entre eles será chamado de n. Logo,

$$n = p \cdot q \tag{14}$$

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 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:

$$\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1) \tag{15}$$

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 $C(b)$. Daí,

$$b^e \equiv C(b) \pmod{n} \tag{16}$$

Sendo $C(b)$ o resto da divisão de b^e por n.

2.5.3 Decodificação

Para decodificar a mensagem, precisamos da chave dada por (n, d). O valor do inteiro positivo d é dado pelo inverso de e módulo $\varphi(n)$. Ou seja, como o mdc(e, $\varphi(n)$) = 1, então existe $d \in \mathbb{Z}$, tal que:

$$e \cdot d \equiv 1 \pmod{\varphi(n)} \tag{17}$$

Pela chave de decodificação, $a = C(b)$ passará a ser $D(b)$. Com isso,

$$(C(b))^d \equiv D(b) \pmod{n} \tag{18}$$

Sendo $D(b)$ o resto da divisão de $(C(b))^d$ por n. Dessa maneira os dados são decodificados, permitindo que se entenda a mensagem original.

3 Usando a 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, esta seção traz algumas atividades realizadas com alunos do oitavo e do nono ano do Ensino Fundamental, além de também terem sido aplicadas com quatro turmas de primeiro ano do Ensino Médio.

Em todas as atividades, as salas foram divididas em grupos onde cada um continha 4 alunos. Os materiais utilizados pelos mesmos foram: folhas $A4$, réguas, telefones celulares, documentos de CPF e certidões de nascimento, recortes de códigos de barras, lápis, borrachas e lápis de colorir.

3.1 Algoritmo de Zeller e Calendários

Segundo [5], 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 [3], 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:

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

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).

As atividades abaixo foram retiradas de [3] e adaptadas, conforme o público atendido.

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

Tempo gasto: Dois horários de 50 minutos.

Atividades:

01. Conforme as explicações em sala, faça seus cálculos e descubra o dia da semana em que nasceu. Em seguida, confira se o resultado de seus cálculos está de acordo com sua certidão de nascimento ou utilize o telefone 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: Em duas turmas do primeiro ano, existiam grupos que continham alunos portadores de necessidades especiais. Para estes ficou 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 alunos a respeito de calendários: tipos, objetivo, criação. As mesmas ocorreram nas salas de informática das escolas e aconteceram questionamentos durante a prática, enfatizando sobre a necessidade de se trabalhar com calendários, suas utilidades, vantagens e desvantagens. Em outro momento, os alunos receberam um texto, onde o mesmo servia de embasamento para as aplicações do algoritmo.

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 para as turmas e as mesmas o utilizaram para conferir a veracidade do dia da semana dos nascimentos. 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. 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 04 foi trabalhada, os grupos 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 conseguiram chegar ao resultado correto pelo fato de considerarem o segundo domingo de maio como fator crucial. Um grupo chamou a atenção ao justificar que se o dia ocorre no segundo domingo, então o primeiro dia a ser analisado deveria ser 07 de maio. Assim, ao descobrirem o dia da semana desta data, ficava fácil chegar à resposta correta. Logo, como daria numa segunda, 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. As turmas de oitavo e nono anos 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 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 decodificação.

Aqui, estaremos usando o método da cifra por substitutição. O mesmo consiste em trocar uma letra por outra, porém mantendo a ordem dos caracteres do texto original.

3.2.1 Prática 02 (Relacionada às atividades 05 e 06)

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

Atividades:

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 3: 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 havia 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

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

Relato da prática em sala de aula: As atividades foram entregues aos alunos após uma discussão relativa à importância da criptografia em operações militares e no que tange o uso da mesma na parte de segurança em redes sociais.

Como os alunos eram os mesmos e já estavam bastante à 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 nas mensagens enviadas do computardor.

Em relação à participação dos alunos especiais, esse 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 é uma tabela que permite encontrar quais são os números primos existentes até um determinado número já estabelecido.

3.3.1 Prática 03 (Relacionada à atividade 07)

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

CRIVO DE ERATÓSTENES:

***	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

Atividade:

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

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.

Relato da prática em sala de aula: Foi solicitado que os alunos fizessem uma tabela, o crivo, usando apenas números ímpares maiores que um. 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.

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-se de acrescentar o 2 no resultado.

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 na seção de aplicações. Esse texto mostrava a importância dos códigos, além de trazer a explicação do uso da congruência e do operador módulo 10.

3.4.1 Prática 04 (Relacionada à atividade 08)

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

Atividade:

08. 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 $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{bmatrix}$ 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. Veja.

$$SOMA_{\alpha\beta} + A \equiv 0 \pmod{10}$$

Observação: Os alunos especiais ficaram de selecionar os códigos trazidos, além de fazer a escolha dos mesmos e a colagem nas folhas.

Relato da prática em sala de aula: Os alunos passaram pela interpretação do texto e, em seguida, foi explicado como se encontrava o dígito verificador no código.

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. No momento das explicações, falamos, superficialmente, das matrizes e citamos que seria um conteúdo dado mais adiante, em outra série.

3.5 Calculando Dígitos Verificadores em CPF

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

3.5.1 Prática 05 (Relacionada à atividade 09)

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

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}.

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

Relato da prática em sala de aula: Os alunos passaram pela interpretação do texto e depois deveriam mostrar como se trabalha com dígitos verificadores presentes em seus relativos cadastros de pessoas físicas.

A atividade foi a mais demorada e difícil, conforme relato dos alunos. O oitavo ano teve maior dificuldade que as outras turmas e os especiais ficaram ociosos desta vez. As turmas se mostraram com mesmo afinco para realizar a atividade, porém os primeiros anos gastaram bem menos tempo que o oitavo e o nono.

4 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.

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, mostrou-nos 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 envolvidos. Sendo assim, anelamos que este trabalho possa ser válido para outros que ainda virão, tanto na teoria quanto na prática.

5 Agradecimentos

Aos alunos que participaram das atividades com tanta dedicação e força de vontade.

Referências

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

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

[3] A. Hefez. *Aritmética:*. Coleção PROFMAT. Sociedade Brasileira de Matemática, 2014.

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

[5] 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.

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

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

[8] C. Severino Collier. *Números inteiros e criptografia RSA.* IMPA, 2014.