UNIVERSIDADE FEDERAL DE SÃO JOÃO DEL-REI – UFSJ
NÚCLEO DE EDUCAÇÃO À DISTÂNCIA
DEPARTAMENTO DE MATEMÁTICA E ESTATÍSTICA – DEMAT

CLAUDEMILSON DA SILVA OLIVEIRA

CONGRUÊNCIA MODULAR E APLICAÇÕES

SÃO JOÃO DEL-REI
2016

CLAUDEMILSON DA SILVA OLIVEIRA

CONGRUÊNCIA MODULAR E APLICAÇÕES

Trabalho de conclusão de curso, apresentado como requisito parcial para obtenção do título de Licenciado em Matemática, do curso de Licenciatura em Matemática a Distância, da Universidade Federal de São João Del-Rei.

Orientador: Prof. Me. Stênio Vidal Menezes

SÃO JOÃO DEL-REI
2016

CLAUDEMILSON DA SILVA OLIVEIRA

CONGRUÊNCIA MODULAR E APLICAÇÕES

Trabalho de conclusão de curso, apresentado como requisito parcial para obtenção do título de Licenciado em Matemática, do curso de Licenciatura em Matemática a Distância, da Universidade Federal de São João Del-Rei.

Os componentes da banca de avaliação, abaixo identificados, consideram este trabalho aprovado.

BANCA EXAMINADORA

_____

Prof.ª Dr. (nome)

(instituição)

_____

Prof.º Dr. (nome)

(Instituição)

Data da aprovação: São João del-Rei, _____ de ___novembro___ de _2016_.

Dedico aos meus pais Durval José Oliveira e Celina Ribeiro da Silva, por terem me oportunizado experimentar o conhecimento e incentivaram-me a cultivá-lo.

AGRADECIMENTOS

A Deus, autor e mantenedor da vida.

Ao colega Leonardo Lopes Faria, por ter me convidado a prestar o vestibular, por ter nos recebido sua casa para os estudos coletivos e por ser um grande amigo, parceiro além da jornada acadêmica.

Aos colegas Cássia Cristina e Claudinei Santos, pelas horas dedicadas aos estudos coletivos, onde pudemos construir conhecimento e amizade.

Ao Pedro Jardel, pelo incentivo, pelo exemplo acadêmico e pelo companheirismo.

À amiga Ivonilde Loiola, grande incentivadora, pelo apoio.

Aos colegas do Polo de Francisco Sá, pela atenção, carinho e parceria.

Aos tutores Melina Paola Seixas Santos e Fábio Alves Ferreira, pela paciência e suporte.

À tutora Andrea Aparecida Sacramento Castro, que mesmo distante esteve atenta e dispensou cuidado e suporte necessários à nossa formação.

Ao professor Me. Stênio Vidal Menezes, por ter acolhido este trabalho e por realizar uma brilhante orientação.

Aos familiares e amigos, por sempre me incentivarem a querer alcançar mais.

Aos Professores Marco Aurélio Oliveira Pereira (E. E. Armênio Veloso), Geíza A. Cruz, Ivone Rodrigues de Jesus e Iury Gabriel Silva Muniz (E. E. Augusta Valle) por terem me ensinado, na prática, a ser um professor de matemática.

Às diretoras Jussara Cristina Nunes Barbosa Bastos (E. E. Armênio Veloso), Shirley Cândida dos Santos e Raimunda Raquel Freitas (E. E. Augusta Valle), bem como aos funcionários das referidas escolas, por me acolherem e fazerem me sentir parte do universo escolar.

À Universidade Federal de São João Del-Rei pela oportunidade de crescimento acadêmico e profissional.

Epígrafe

"A matemática, vista corretamente, possui não apenas verdade, mas também suprema beleza - uma beleza fria e austera, como a da escultura."

Bertrand Russell

RESUMO

Este trabalho aborda aplicações de congruência modular em sistemas de identificação e Criptografia. Apresenta breve discussão sobre aspectos históricos relacionados à aritmética, ressaltando as contribuições de matemáticos como Pierre de Fermat, Legendre, Lagrange, Euler e Friedrich Gauss, na construção da teoria dos números, bem como fundamentação teórica sobre os pressupostos matemáticos utilizados nas congruências modulares. Discorre sobre a aplicação dessa facilidade matemática no desenvolvimento de sistemas de verificação de códigos de barras, números de identificação e criptografia, através de exemplos práticos. Sugere oficinas de ensino de aritmética modular para a educação básica, utilizando a estrutura dos códigos de barras, números de CPF e técnicas de criptografia de mensagens. Justifica-se por salientar a importância da matemática na solução de problemas atuais e destacar suas funcionalidades no cotidiano das pessoas. A metodologia utilizada consistiu em revisão de produções acadêmico-científicas relacionadas à congruência modular.

Palavras chave: Congruência modular; Código de barras; Sistemas de identificação; Criptografia.

ABSTRACT

This work addresses applications of modular congruence in identification systems and Cryptography. It presents a brief discussion of historical aspects related to arithmetic, emphasizing the contributions of mathematicians such as Pierre de Fermat, Legendre, Lagrange, Euler and Friedrich Gauss, in the construction of number theory, as well as theoretical basis on the mathematical assumptions used in modular congruences. It discusses the application of this mathematical facility in the development of bar code verification systems, identification numbers and encryption, through practical examples. It suggests modular arithmetic teaching workshops for basic education, using the structure of bar codes, CPF numbers and message encryption techniques. It is worth emphasizing the importance of mathematics in solving current problems and highlighting their functionalities in people's daily lives. The methodology used consisted of a review of academic-scientific productions related to modular congruence.

Keywords: Modular congruence; Bar code; Identification systems; Encryption.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

CI - Carteira de Identidade
CNH - Carteira Nacional de Habilitação
CNPJ - Cadastro Nacional de Pessoa Jurídica
CNS - Cartão Nacional de Saúde
CPF - Cadastro de Pessoa Física
EAN-13 - European Article Number – 13 algarismos
fig. - figura
ISBN - International Standard Book Number
mod - módulo
RG - Registro Geral
séc. - século
UPC - Universal Product Code

SUMÁRIO

1. Introdução

A matemática tem fascinado curiosos e pesquisadores desde a antiguidade, seja para a solução de problemas do cotidiano, para explicação de situações complexas, ou para demonstração de sua versatilidade. Em todos os casos, os amantes dessa disciplina têm dedicado um esforço para aprimorar os conhecimentos adquiridos e consolidar a relevância da matemática para a humanidade. Ela, a matemática, "está presente em todos os campos do conhecimento e se faz necessária em qualquer atividade humana" (LORENZATO, 2010, p. 53).

O Crescimento das cidades e o aumento das populações exigiu a criação de um sistema de identificação como forma de manter um monitoramento dos habitantes e que possibilitasse a distinção entre indivíduos através de códigos numéricos ou alfanuméricos, considerando as inúmeras possibilidades de combinações distintas entre números, tornando-se mais abrangentes e efetivos quando envolvem letras e algarismos. Tendo sido criadas as carteiras de identidade, onde cada cidadão possui um número distinto, percebeu-se que outros tipos de controle individual também poderiam ser implementados para controlar transações comerciais, trânsito entre mercados, funções exercidas em corporações empresariais, dentre outras finalidades.

O consequente aumento da demanda mundial por produtos, mercadorias e serviços culminou na abertura das fronteiras e na expansão dos mercados como exigência econômica, fazendo suscitar a necessidade de estabelecer sistemas de segurança que assegurassem o controle da produção e distribuição desses bens econômicos, de modo que as empresas produtoras pudessem controlar os lotes e cargas de mercadorias quando da sua alocação nos mercados consumidores. Outra finalidade foi o rastreamento de informações sobre o produto distribuído, incluindo aspectos relativos à sua composição, características físico-químicas, condições de armazenamento e transporte, dentre outros dados julgados importantes na cadeia produção-distribuição-consumo.

Outro fator, diz respeito à necessidade de estabelecer códigos de segurança no tráfego de informações em processos de comunicação entre pessoas, entre organizações empresariais, ou entre pessoas e organizações. Esses sistemas de segurança permitem garantir que informações sigilosas não sejam acessadas por agentes mal intencionados e asseguram que seu uso atingirá apenas a finalidade idealizada. É o caso do uso de senhas numéricas ou alfanuméricas para proteger acesso a redes de computadores, contas bancárias, perfis de

usuário ou contas de internet. O uso das técnicas de modificação de códigos para proteger informações, criptografia, remonta à Grécia no último século antes de Cristo, quando o imperador propôs uma recodificação das mensagens para que em caso de interceptação, os exércitos inimigos não conseguissem se apropriar do seu teor.

A congruência modular tem sido utilizada para gerar um número de controle da veracidade do código. Esse número verificador possibilita constatar se um código de barras, um número padrão internacional de livro (ISBN), um número de passaporte, ou o número de Cadastro de Pessoa Física (CPF) estão corretos, já que todos os algarismos que compõem o número original são utilizados no método de geração do código verificador.

No caso da criptografia, a congruência modular é empregada na recodificação de mensagens e senhas, criando nova estrutura de códigos e impossibilitando que as pessoas, ou sistemas não detentores das chaves de decodificação façam uso do conteúdo em sua essência.

Percebe-se claramente o frequente uso de congruência modular, cuja aplicação produz efeitos positivos no cotidiano das pessoas, embora grande parte delas não se dê conta de que a matemática esteja sendo empregada.

Assim, justifica-se um estudo que elucide a importância desse conteúdo matemático para a sociedade e que atraia a atenção para as aplicações da matemática no dia a dia. Sobretudo, o desenvolvimento de estudos nessa área pode suscitar, em momento oportuno, o interesse em aprimorar as técnicas de identificação e criptografia para promover maior segurança de informações, já que os mercados estão em franca evolução e o uso das tecnologias cada vez mais frequente. O desenvolvimento de um trabalho bem elaborado servirá como subsídio para fomentar o conhecimento e a investigação científica, além de abrir caminho para incursões mais detalhadas sobre o assunto no futuro.

O principal objetivo deste trabalho é estudar as principais aplicações da congruência modular em sistemas de identificação e codificação usados na atualidade. Especificamente, pretendeu-se: a) Apresentar aspectos históricos relacionados à aritmética modular; b) Expor os fundamentos da matemática relacionada à congruência modular utilizada na composição de códigos de barras, CPF e criptografia; c) Descrever a utilização da congruência modular na composição de códigos de barras, CPF e criptografia; d) Levantar experiências de ensino na educação básica baseadas em congruência modular; e) Propor metodologias de ensino de congruência modular no ensino básico.

Trata-se de uma pesquisa bibliográfica, abrangendo dissertações, monografias e artigos científicos, bem como livros de matemática que abordem o assunto.

No primeiro capítulo, apresenta-se uma discussão sobre a aritmética modular, contemplando aspectos históricos e fundamentos matemáticos relacionados ao assunto. Enfocam-se os principais fundamentos aplicados na composição de códigos de barras, CPF e criptografia. Também, discorre-se sobre a possibilidade de estabelecer uma análise geral de sistemas modulares.

No segundo capítulo, discorre-se sobre as principais aplicações de congruências modulares em sistemas de identificação e criptografia, evidenciando a composição numérica dos códigos de barras e de CPF, bem como demonstração do uso de congruência modular na criptografia de mensagens e códigos numéricos.

O terceiro capítulo foi reservado para estabelecer uma discussão acerca do ensino de congruência modular na educação básica, explicitando sua importância para as pessoas em geral, para os mercados e consequentemente para a economia. Apresenta ainda uma proposta de trabalho em sala de aula onde os alunos serão envolvidos num processo de investigação e aplicação de congruência modular.

Ressalta-se que os resultados esperados a partir do desenvolvimento deste trabalho dão conta de possibilitar ao leitor a imersão no campo da escrita científica, bem como de fornecer uma discussão lúcida sobre a aplicação matemática no cotidiano das pessoas, tendo como base, ou ponto de partida, uma de suas aplicações.

2. Aritmética Modular

2.1. Aspectos históricos de aritmética modular

No decorrer da história muitas contribuições foram dadas, por diversos estudiosos, para o enriquecimento do conhecimento das matemáticas. Isso mesmo, "matemáticas", pois são tantas as áreas de estudo da matemática e muitos modos de chegar a resultados semelhantes, que pode-se pluralizar esta ciência, que vem despertando o interesse e atenção de indivíduos curiosos e intelectuais desde tempos remotos. É claro que as descobertas e aprimoramentos aconteceram na medida em que novos olhares foram lançados sobre essa matéria e ainda há contribuições a serem feitas em tempos atuais e futuros.

A Aritmética vem sendo construída com a contribuição de muitos teóricos matemáticos desde Euclides, com Os Elementos[1] (aproximadamente 300 a.C), tendo seu auge no século XVII, com os trabalhos realizados por Pierre de Fermat, que consistiram em importantes contribuições para a aritmética. Outros estudiosos matemáticos deram suas contribuições nos séculos XVIII e XIX, quando a matemática contou com os estudos realizados por, Leonhard Euler, Josefh Louis Lagrange, Adrien Marie Legendre, Jhon Wilson e Carl Friedrich Gauss. Vale ressaltar que a partir do século XIX, após o trabalho de Gauss, a aritmética passa a ser chamada de Teoria dos Números. (HEFEZ, 2005).

A teoria dos números, cuja aritmética é parte essencial, é o ramo da matemática responsável por estudar a estrutura dos números e as operações possíveis de serem estabelecidas entre eles. Por isso é utilizada por todas as pessoas ao desenvolver contagens, calcular um troco, realizar medidas, verificar relações entre grandezas, etc. A aritmética é um dos ramos mais antigos da matemática, porque as operações básicas são realizadas desde a antiguidade, embora estudos avançados, denominados aritmética superior, só tenham sido desenvolvidos nos séculos XVIII e XIX.

Euclides de Alexandria já havia proposto em seu livro *Os elementos*, há aproximadamente 300 anos antes de Cristo, algo parecido com o teorema fundamental da aritmética, apresentando uma demonstração para tal proposição, mas foi Gauss, séc. XIX, que

[1] Os Elementos, de Euclides, é um tratado composto por 13 livros, 9 de geometria e 4 de aritmética (uma versão grega de teoria dos números). Segundo site Wikipédia é o segundo livro mais publicado no mundo, perdendo apenas para a bíblia.

conseguiu demonstrar com exatidão, atribuindo notação apropriada e propondo-o como teorema, o que vem sendo aceito e utilizado até a atualidade. (HEFEZ, 2005)

Conta a história que desde criança Gauss apresentava um comportamento diferenciado em relação aos demais alunos de sua turma. Foi ele quem aplicou pela primeira vez um pensamento voltado para as progressões aritméticas, quando instigado por seu professor a somar todos os números possíveis entre 1 e 100, percebeu que ao somar 1+100, obtia 101, 2+99 também é 101, 3+97 também é 101, logo concluiu que poderia multiplicar a metade de 100, que é 50, por 101 e obter a soma de todos os números existentes entre 1 e 100, obtendo 5050 como resultado, o que é conhecido hoje como a soma de uma progressão aritmética, $n(n+1)/2$. (OLIVERO, 2007, p. 110).

Atento às relações existentes entre os números, Gauss observou que frequentemente eram usados termos como "(a) *dá o mesmo resto que (b) quando divididos por (m)*", (SÁ, 2007), e essa afirmação o intrigou levando-o a desenvolver o pensamento e as bases da aritmética modular. Como isso é possível? Ora, ao demonstrar que números diferentes divididos por um mesmo número distinto dos anteriores produzia o mesmo resto, ele então concluiu que esses números são congruentes, "iguais", em termos de divisibilidade por aquele divisor.

Ressalta-se que o termo congruência, para esse caso, foi usado pela primeira vez pelo próprio Gauss em sua obra intitulada *Disquisitiones Arithmeticae* (Investigações aritméticas) em 1801. Tal livro é considerado o marco inicial da moderna teoria de números. *"Nele*, [Gauss] *compilou o trabalho de seus predecessores e deu à área uma vida nova, desenvolvendo as teorias de congruências quadráticas, formas e resíduos"*. (MOL, 2013, p. 125).

Por esse motivo, e pelas grandes contribuições no estudo da teoria dos números é que Gauss ficou conhecido como o pai da aritmética modular. Foi ele quem introduziu uma notação específica para demonstrar matematicamente as questões relacionadas à congruência modular e outras relações aritméticas.

Não se pode descartar em discussões sobre aritmética modular, as contribuições de Pierre de Fermat, advogado francês, que tinha a matemática como um *hobby*, já que matemáticos de épocas posteriores debruçaram sobre suas proposições para fazerem demonstrações e comprovações. Um exemplo apresentado por Mol (2013) sobre o Pequeno Teorema de Fermat, afirma que: Se p é primo e a é um numero não divisível por p o número $a^{p-1}-1$ é divisível por p, embora não tenha apresentado uma demonstração quando o

propôs. A demonstração desse teorema foi publicada pela primeira vez por Leonhard Euler, cerca de 100 anos mais tarde.

Tempos depois, Gauss propôs que o Pequeno Teorema de Fermat é um caso de congruência, pois "se a é um número primo e p é um número inteiro qualquer, então p divide $(a^p - a)$, pode ser escrita usando uma notação de congruência como $a^p \equiv a \; mod \; p$".

Os achados sobre aritmética modular elucidados por Fermat mereceram a atenção de outros estudiosos da matemática, posteriormente, nos séculos XVIII, Euler, e XIX, Lagrange e Legendre, que também atentaram para as elucidações feitas por Gauss.

2.2. Noções de aritmética modular

A aritmética modular é utilizada durante todo o tempo pelas pessoas, por vezes inconscientemente, quando realizam divisões cujo resto é a resposta para seus questionamentos ou necessidades. Um exemplo: o relógio analógico de pulso possui doze divisões (1, 2, 3, ... , 12) e cada uma dessas frações correspondem a uma hora. Um dia possui 24 horas, duas vezes mais do que a quantidade de frações de horas mostradas no visor do relógio. Assim que o relógio dá uma volta completa, passando pelas doze frações, volta ao ponto inicial, marcando 1, 2, 3, ..., 12 horas novamente. Isso possibilita corresponder 13h a 1h, 14h a 2h e assim por diante. Nesse caso efetua-se uma divisão por 12, em que o resto é a hora corespondente. Veja: $16 \div 12 = 4$, logo, 16h corresponde a 4h quando dividido por 12. Diz-se que 16 é congruente a 4 módulo 12.

O conceito de aritmética modular passa pela teoria da divisibilidade de números inteiros e está contemplada no vasto campo das matemáticas, principalmente na teoria dos números e possui diversos níveis de aplicabilidade.

Todo número natural pode ser dividido por outro e mesmo que não haja uma relação de divisibilidade entre eles, a divisão pode ser feita com pequeno resto, "*divisão euclidiana*". (HEFEZ, 2007, p. 30).

São critérios de divisibilidade:

a) Divisibilidade por 2: Todo número cujo último algarismo é par ou zero é divisível por 2;
b) Divisibilidade por 3. Um número é divisível por 3 se, e somente se, a soma de seus algarismos for um número divisível por 3;

c) Divisibilidade por 4: Um número é divisível por 4 quando seus dois últimos algarismos formam um número divisível por 4;
d) Divisibilidade por 5: Um número é divisível por 5 se, e somente se, seu último algarismo for 0 ou 5;
e) Divisibilidade por 6: "Um número é divisível por 6 quando for divisível por 2 e por três simultaneamente;
f) Divisibilidade por 7: Para saber se um número é divisível por 7, retiramos seu último algarismo e multiplicamos por 2 e em seguida subtraímos dos algarismos restantes o produto obtido. Se a diferença encontrada for divisível por 7, o número também será divisível por 7. (196 é divisível por sete, pois $6 \cdot 2 = 12\ e\ 19 - 12 = 7$);
g) Divisibilidade por 8. Um número é divisível por 8 quando seus três últimos algarismos formam um número divisível por 8;
h) Divisibilidade por 9. Um número é divisível por 9 se e somente se a soma dos seus algarismos formar um número divisível por 9.

Para melhorar o entendimento sobre o assunto apresentam-se a seguir algumas definições e exemplos acerca dos fundamentos da divisibilidade, e congruência modular.

Definição 1. Sejam a e b números inteiros, diz-se que b divide a quando existe um número inteiro c, tal que $a = b \cdot c$. Se b divide a, escreve-se que $b|a$ (b divide a) e para a negativa, escreve-se $b \nmid a$ (b não divide a). Se b divide a, diz-se que b é um divisor de a.

Exemplo: Tomando $a = 42$, $b = 7$ e $c = 6$. Pode-se afirmar que $7 \mid 42$, pois $7 \cdot 6 = 42$.

Definição 2. Sejam a e b números inteiros, com $a \neq b$ e $a, b \neq 0$. Diz-se que $c \in \mathbb{N}$ é o máximo divisor comum de a e b, se $c|a$, $c|b$ e c é o maior dentre todos os divisores comuns de a e b, denotado $(a, b) = c$.

Exemplo: Tomando $a = 12$, $b = 16$ e $c = 4$. Pode-se afirmar que 4 é o máximo divisor comum de 12 e de 16, pois $\{1, 2, 3, 4\ e\ 12\}$ dividem 12, $\{1, 2, 4, 8, e\ 16\}$ dividem 16 e $\{1, 2\ e\ 4\}$ são os divisores comuns de 12 e de 16, sendo 4 o maior deles.

Teorema da divisão euclidiana: Dados os números inteiros positivos a (chamado dividendo) e b (chamado divisor), existe um número inteiro q (chamado quociente da divisão) e r (chamado resto da divisão), tais que $a = bq + r$ e $0 \leq r < b$.

A demonstração desse teorema pode ser encontrado em HEFEZ (2004, p. 35 a 36).

Exemplo. Tomando $a = 40, b = 3$, na divisão de a por b, obtém-se $q = 13$ e $r = 1$, tal que $40 = (13 \cdot 3) + 1$ e que $0 \leq 1 < 3$.

Por uma questão conceitual, cabe dizer que existe uma diferença entre os significados de igualdade e de congruência.

> A palavra "congruente" tem origem grega e significa "de mesma medida". Congruência é a propriedade a duas figuras que são geneticamente iguais, ou seja, figuras geométricas congruentes são aquelas com medidas respectivamente iguais. (CHUEIRI e GONÇALVES, 2012, P. 44).

Trazendo esse conceito para a teoria dos números, pode-se entender que os números "congruentes" são aqueles que possuem o mesmo tamanho ou valor quando divididos por um terceiro número, já que gerará um mesmo resto nas divisões. Entretanto, não se pode dizer que eles são iguais já que individualmente eles possuem valores absolutos diferentes.

Definição 3. Sejam $a, b, m \in \mathbb{Z}*$, diz-se que a e b são congruentes módulo m, quando os restos das divisões euclidianas a por m e b por m forem iguais. Denota-se por $a \equiv b \, mod \, m$.

Exemplo. Toma-se $a = 3, b = 15$ e $m = 12$. Pode-se afirmar que $a \equiv b \, mod \, 12$, pois $12 \mid (3 - 15)$.

Proposição 1. Sejam $a, b \in \mathbb{N}$, tal que $a \geq b$. Diz-se que $a \equiv b \, mod \, m$, se e somente se, $m \mid (a - b)$.

Uma demonstração dessa proposição pode ser encontrada em HEFEZ (2004, p. 111).

Exemplo. Toma-se $a = 30$, $b = 18$ e $m = 6$. Pode-se afirmar que $a \equiv b \, mod \, 6$, pois $6 \mid (30 - 18)$.

Várias aplicações de congruência modular vêm sendo feitas no sentido de aperfeiçoar sistemas de segurança de informações, bem como investigações no campo da matemática, o que propõe uma análise geral dos sistemas modulares. Compreender a generalidade desses sistemas permite estabelecer um modelo de aplicação e investigação que se aplica se não a todos, à sua maioria.

2.3. Análise geral de sistemas modulares

A utilização da congruência modular é uma ferramenta cuja aplicação trouxe importantes facilidades para o mundo moderno. Sobretudo em sistemas de identificação, que serão tratados com mais detalhamento no decorrer deste trabalho. São aplicações com diversos níveis de complexidade, envolvendo desde operações simples até sistemas complexos, mas todos eles com o intuito de resolver determinados problemas matemáticos, para os quais a divisibilidade é fator essencial.

Um exemplo do uso de congruência modular no cotidiano é a prova dos noves. Uma pessoa que aprendeu a utilizar a prova dos nove para conferir os resultados de operações com números naturais pode não saber, mas aprendeu a aplicar congruência módulo nove em suas averiguações. (ESQUINCA, 2013).

Ao que parece, a aplicação de congruência modular é tão corriqueira quanto olhar as horas num relógio ou conferir resultados de operações matemáticas através do uso da prova dos nove. De certo modo é, porém existem sistemas mais complexos para os quais se tem utilizado a aritmética modular como ferramenta para obter resultados ainda distantes para a matemática do dia a dia.

LOPES e ÁVILA (2013), por exemplo, demonstram a utilização de congruência modular na investigação matemática da existência de um possível número perfeito ímpar.

Ao redor do mundo, vários sistemas de identificação vêm sendo utilizados para facilitar transações comerciais, controles fiscais, controles de estoques, rastreamento de produtos e identificação de pessoas.

Observa-se o uso de congruência modular na identificação de publicações através do ISBN ou controles de lotes de produtos através de códigos de barras. Já referente à identificação de pessoas, utiliza-se congruência modular na composição dos números de CPF, Carteiras de Identidade (CI), Passaporte, dentre outros.

Vale ressaltar que os códigos de barras também vêm sendo incorporados aos documentos, como modo de facilitar a leitura e resgate de informações sobre aquele documento, já que, além do código numérico, é possível transcrever a sequência numérica através do uso de barras que podem ser lidas por dispositivos eletrônicos.

Além disso, o uso da criptografia na codificação de mensagens visando potencializar a segurança de informações sigilosas representa outro modo de aplicação de congruência modular. É certo que a criptografia, tem sido aplicada nas linguagens de computadores, sistemas informatizados de uso doméstico ou empresariais, sistemas bancários e aplicativos de utilização individual.

Para que isso seja possível, sistemas modulares são desenvolvidos a fim de facilitar a programação e aplicabilidade desses códigos de identificação.

LOURENÇO (2011) propõe uma análise “global e generalizada” dos sistemas de identificação modulares, dadas às semelhanças existentes entre eles e por serem pertencentes a um corpo finito, já que seus elementos são limitados, ou seja, estão agrupados em um intervalo.

Assim, é possível estabelecer uma forma geral para a maioria dos sistemas de identificação modular, o que facilita estabelecer uma análise desses sistemas sobre a sua aplicabilidade ou não no módulo definido. Essa forma geral pode ser encontrada na dissertação de Lourenço (2011, p. 12).

3. Aplicações de Aritmética Modular

3.1. Congruência modular e código de barras

As aplicações de aritmética modular trouxeram grande contribuição para o mundo moderno, visto que para promover um ordenamento social, comercial e financeiro, essa metodologia matemática tem sido aplicada em diversos setores.

A criação de um código que fosse capaz de identificar produtos e pessoas individualmente ou em lotes, no caso de produtos, cujas finalidades variam desde um controle de estoque até mecanismos complexos de rastreamento de produtos e cargas, fez com que através do uso da tecnologia da informação esse controle ficasse facilitado.

Esses códigos são chamados de códigos de barras, fruto de estudos que vem sendo realizados desde o ano de 1850 e utilizados pela primeira vez, no formato que conhecemos, em 1973 quando foi apresentado por George J. Laurer[2] com o nome de *Universal Product Code* (UPC), com 12 algarismos (fig. 1). Meses depois, o mesmo UPC recebeu um dígito a mais, passando a ser composto por 13 algarismos, através do qual seria possível a identificação do país de origem. O novo código recebeu o nome de *European Article Numbering system* (EAN-13) (fig. 2).

Figura 1 - Código de barras UPC
Fonte: Google imagens (modificada para exemplificação)

[2] George J. Lawrer, inventor do UPC, enquanto atuava como engenheiro da International Business Machines Corporation – IBM, empresa estadunidense de tecnologia da informação.

Figura 2 - Código de barras EAN-13
Fonte: Google imagens (modificada para exemplificação)

O nome código de barras se dá devido à existência de uma sequência de barras que são identificadas pela largura de sua impressão e correspondem a um código numérico, para o qual foi utilizado congruência modular. Um mesmo código de barras pode ser impresso em diversos produtos identificando um lote de produtos que possuem características comuns, ou podem ser impressos individualmente, sendo que nesse último caso identificam aquela peça de modo que cada peça do lote terá seu próprio código.

Esquinca defende que o código de barras é:

> [...] uma representação gráfica de dados. Ele permite uma rápida captação de dados, proporciona velocidade nas transações, precisão nas informações e admite atualização em tempo real e tudo isso implica em maior controle, diminuição de erros, gerenciamento remoto, garantindo velocidade no atendimento de pedidos e clientes, além de significativa redução de custos. (ESQUINCA, 2013, p. 41).

Atualmente, existem vários tipos de códigos de barras para identificar diversos tipos de produtos. Fernando Zaidan[3], no blog que leva o seu nome, identifica 21 tipos de códigos de barras, sendo algumas variações de UPC, com mais ou menos algarismos, variantes de EAN e outros, entre eles o Caracteres Magnéticos Codificados em 7 barras (CMC7) que é utilizado na parte inferior das folhas de cheques bancários, também chamado de banda magnética ou linha 2.

O código de barras do tipo EAN-13 é formado por 13 algarismos e está entre os mais utilizados em todo mundo. Usa congruência módulo 10, cuja base de multiplicação é constituída pelos algarismos 1 e 3. Essa base de multiplicação vai se repetindo da esquerda para a direita, multiplicando os 12 algarismos da sequência. O 13º algarismo é chamado de algarismo de controle.

Partindo desse pressuposto, nos parágrafos a seguir será apresentada uma demonstração de como o código EAN-13 é constituído e os passos para a obtenção do algarismo de controle.

[3] Fernando Zaidan é graduado em Ciências da Computação, mestre em Administração e Doutor em Ciência da Informação. Possui um blog: www.fernandozaidan.com.br.

i) Determine que a sequência de doze algarismos do código sejam os fatores:

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}\}$$

ii) Multiplica-se pela base de multiplicação na sequência a seguir:

$$\{1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3\}$$

iii) Em seguida somam-se os produtos obtidos, obtendo o total S. Logo,

$$S = (a_1 + a_3 + a_5 + a_7 + a_9 + a_{11}) + (a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12}) \times 3 \qquad (1)$$

iv) O 13º algarismo, a_{13}, será aquele que somado com *S* gere um múltiplo de 10, ou seja, $S + a_{13} \equiv 0\ mod\ 10$.

Um exemplo utilizando um código de barras real:

Figura 3 - Código de barras EAN-13 sem o último algarismo
Fonte: Google imagens (modificada para exemplificação)

Observa-se que o código de barras da figura 3, possui 12 algarismos, sendo os números $\{5, 9, 0, 1, 2, 3, 4, 1, 2, 3, 4\ e\ 5\}$. Em seguida, Multiplicam-se esses números pela sequência de fatores na ordem $\{1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3\}$, da seguinte forma: $S = \{5 + 27 + 0 + 3 + 2 + 9 + 4 + 3 + 2 + 9 + 4 + 15\} \Rightarrow S = 83$. O 13º algarismo, que está faltando na figura 3 será obtido pelo algarismo que somado a 83 gere um número múltiplo de 10 e assim seja congruente a 0 módulo 10. Para isso fazemos $83 \div 10 = 8\ resto\ 3$, logo $10 - 3 = 7$ é o 13º algarismo pois $83 + 7 = 90$, 90 é múltiplo de 10 e $90 \equiv 0\ mod\ 10$. , Como pode ser verificado na figura 4.

Figura 4 - Código de barras EAN-13 completo
Fonte: Google imagens

Sá (2007) ajuda a compreender a estrutura do código EAN-13 discriminando que:

> [...] no código de barras com 13 algarismos, os **três primeiros** dígitos do código representam o país de registro do produto (verifique que para produtos filiados no Brasil teremos sempre os dígitos 7, 8 e 9); os **quatro dígitos seguintes** identificam o fabricante; os **próximos cinco dígitos** identificam o produto e o último, como já sabemos, é o dígito verificador ou de controle, que se pode calcular através da congruência, módulo 10. (SÁ, 2007, p. 7).

As barras seguem um padrão representado por uma sequência de zeros e uns, cujas leitoras eletrônicas interpretam as cores e a espessura das barras, atribuindo a elas um algarismo que sofrerá uma avaliação e cálculo do dígito verificador através de um sistema lógico matemático traduzido em linguagem de máquina.

A compreensão da estrutura desses códigos de barras permite entender a importância da aritmética modular para a construção de mecanismos de controle que permitam o aprimoramento de sistemas industriais e comerciais mundo afora. Vale lembrar que outros setores já utilizam os códigos de barras como alternativa de otimização de processos organizacionais internos. Por exemplo, os códigos de barras inseridos nos crachás dos funcionários ajudam a controlar frequência, folha de pagamento e obtenção de dados gerais sobre o funcionário.

Quando um consumidor passa pelo caixa de um supermercado, cujo sistema é informatizado, percebe que o atendente registra suas compras passando o código de barras em frente a uma leitora que permite identificar todas as informações fiscais e de preço referentes aos produtos. As informações do produto foram cadastradas previamente num banco de dados integrado. Esse procedimento agiliza a emissão do documento fiscal e a computação dos valores a serem pagos, permitindo que a efetivação da transação comercial aconteça em curto espaço de tempo. Numa situação diferente, o caixa teria que digitar os nomes dos produtos num sistema informatizado, ou mesmo procurar os preços dos produtos em uma tabela impressa e efetuar a soma manualmente, o que aumentaria sobremaneira a permanência do cliente na loja.

Percebe-se que o código de barras facilitou o trabalho do atendente e reduziu o tempo de espera do cliente na fila do caixa, além de melhorar o fluxo de pessoas e mercadorias no estabelecimento comercial, possibilitando melhor capacidade de atendimento.

Através do mesmo código de barras as mercadorias compradas pelo cliente foram rastreadas desde a produção, passando pela distribuição e exposição nas gôndolas do supermercado. Os rastreamentos são efetuados para garantir a qualidade do produto no sistema de distribuição e só é possível pela possibilidade de identificar um produto, ou um lote de produtos a partir de seu código de identificação, o código de barras.

Os códigos de barras também têm sido utilizados em sistemas hospitalares internos, no intuito de controlar a permanência de pacientes em unidades de internação e acessar dados sobre o prontuário médico, entre outras informações.

3.2. Congruência modular e sistemas de identificação

O aumento da população humana e a necessidade de se implementar mecanismos de registro e controle dessa população, para fins comerciais, negociais e de identificação, fez com que fossem desenvolvidos documentos registrais com códigos através dos quais é possível identificar um indivíduo numa base de dados comum.

No sistema de identificação, os indivíduos são discriminados pelo número da Carteira de Identidade ou Registro Geral (RG), no sistema de informações fiscais, pelo número do CPF, se for pessoa física, ou Cadastro Nacional da Pessoa Jurídica (CNPJ), se for pessoa jurídica. Outras bases de dados como Cartão Nacional de Saúde (CNS), Carteira Nacional de Habilitação (CNH), Passaporte, entre outros.

Não existe um padrão de numeração dos documentos de identidade das pessoas naturais brasileiras, já que no Brasil, cada Estado é responsável pela manutenção do seu próprio sistema, há divergências na estrutura do código entre os diversos estados. Já o CPF possui o mesmo padrão de identificação no território nacional, pois a sua emissão é realizada apenas pela Secretaria da Receita Federal do Ministério da Fazenda. Por isso será utilizado nas demonstrações a seguir.

O CPF possui onze dígitos divididos em dois blocos, o primeiro bloco tem nove algarismos e o segundo bloco 2 algarismos (fig. 5). Este último é o dígito verificador com

duas posições. Nesse caso também, usa-se a congruência modular para determinar esses verificadores.

Figura 5 - Cédula do CPF
Fonte: Google imagens

O décimo algarismo, o primeiro dígito verificador, é o resultado de uma congruência, módulo 11, obtido através da operação dos primeiros nove algarismos, como apresentado no exemplo a seguir.

i) Determine que os primeiros nove números estejam organizados na sequência:

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\}$$

ii) A sequência de base de multiplicação é:

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

iii) Procede-se à multiplicação dos fatores dessas sequências respectivamente, obtendo a soma S, conforme abaixo:

$$S = a_1.1 + a_2.2 + a_3.3 + a_4.4 + a_5.5 + a_6.6 + a_7.7 + a_8.8 + a_9.9 \quad (2)$$

iv) O 10º algarismo, a_{10}, é o número que subtraído da soma obtida, gere um múltiplo de 11, de modo que $S - a_{10} \equiv 0\ mod\ 11$. Nesse caso é o próprio resto da divisão por 11.

Exemplo:

Será utilizado o CPF 234.167.398-XX. Nota-se que o código possui 9 algarismos conhecidos, faltando determinar quais são o 10º e o 11º, representados pela incógnita "X".

Através da aplicação do método de cálculo, será determinado o 10º algarismo, como segue.

i) Os primeiros nove números estão organizados na sequência:

$$\{2, 3, 4, 1, 6, 7, 3, 9, 8\}$$

ii) A sequência de base de multiplicação é (base padrão):

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

iii) Procedendo-se à multiplicação dos fatores dessas sequências respectivamente, obtém-se a soma S:

$$S = 2.1 + 3.2 + 4.3 + 1.4 + 6.5 + 7.6 + 3.7 + 9.8 + 8.9 \Rightarrow S = 261$$

iv) O 10º algarismo, a_{10}, é o número que subtraído da soma obtida, gere um múltiplo de 11, desse modo $S - a_{10} \equiv 0\ mod\ 11$. Nesse caso a_{10} é o próprio resto da divisão por 11. Para isso fazemos $261 \div 11 = 23\ resto\ 8$, logo $261 - 8 = 253$ é múltiplo de 11 e $253 \equiv 0\ mod\ 11$. Logo $a_{10} = 8$

Assim, o número do CPF apresentado passa a ter um 10º algarismo, sendo 234.167.398-8X.

O décimo primeiro algarismo, o segundo dígito verificador, é obtido de modo similar, acrescentando-se o décimo algarismo, encontrado na operação anterior. Além disso, a base de multiplicação passa a contar com o zero no início, conforme demonstração e exemplo.

i) Determine que os primeiros dez números estejam organizados na sequência:

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\}$$

ii) A sequência de base de multiplicação é:

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

iii) Procede-se à multiplicação dos fatores dessas sequências respectivamente, obtendo a soma *S*, conforme demonstração:

$$S = a_1.0 + a_2.1 + a_3.2 + a_4.3 + a_5.4 + a_6.5 + a_7.6 + a_8.7 + a_9.8 + a_{10}.9 \qquad (3)$$

iv) O 11º algarismo, a_{11}, é o número que subtraído da soma obtida, gere um múltiplo de 11, de modo que $S - a_{11} \equiv 0\, mod\ 11$. Nesse caso, como anteriormente, é o próprio resto da divisão por 11.

Exemplo:

Considere o CPF 234.167.398.8X.

i) Os primeiros dez números estão organizados na sequência:

$$\{2, 3, 4, 1, 6, 7, 3, 9, 8, 8\}$$

ii) A sequência de base de multiplicação é (base padrão):

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

iii) Procedendo-se à multiplicação dos fatores dessas sequências respectivamente, obtém-se a soma *S*:

$$S = 2.0 + 3.1 + 4.2 + 1.3 + 6.4 + 7.5 + 3.6 + 9.7 + 8.8 + 8.9 \Rightarrow S = 290$$

iv) O 11º algarismo, a_{11}, é o número que subtraído da soma obtida, gere um múltiplo de 11, desse modo $S - a_{10} \equiv 0\, mod\ 11$. Nesse caso a_{11} é o próprio resto da divisão por 11. Para isso fazemos $290 \div 11 = 26\ resto\ 4$, logo $290 - 4 = 286$ é múltiplo de 11 e $286 \equiv 0\ mod\ 11$. Logo $a_{11} = 4$.

Assim, o numero do CPF passa a ter os 11 algarismos conhecidos, sendo 234.167.398.84.

Cabe ressaltar que o 9º dígito representa o estado onde o CPF foi emitido. Por exemplo, se o 9º dígito é zero, implica que o CPF foi emitido no estado do Rio Grande do Sul e se é 8 como o exemplo utilizado, foi emitido no estado de São Paulo. Alguns estados como Rio de Janeiro e Espírito Santo compartilham o mesmo código, isso porque os códigos variam de zero a nove, mas o Brasil possui 27 Estados e um Distrito Federal.

Os códigos verificadores dos números de outros documentos são obtidos através de processo semelhante.

Quando alguém informa o número do seu CPF para efetuar um cadastro em algum banco de dados, nem imagina que o sistema informatizado faz um rápido cálculo do dígito verificador e atesta a veracidade ou incorreção do número informado. É possível que algumas pessoas já tenham ouvido do atendente ou lido mensagem emitida pelo computador, quando do autopreenchimento de formulário eletrônico, que o número informado estava incorreto e teve que informar a sequência numérica correta para dar prosseguimento ao cadastro.

De outro modo, quando não é possível verificar se o número está correto, a relação é precarizada dada à impossibilidade de identificação e responsabilização do indivíduo em casos de descumprimento dos acordos firmados.

Ressalta-se que o fato de o número estar correto não significa que pertence a um documento válido. O empresário deve fazer uso de outros mecanismos para se assegurar.

3.3. Congruência modular e criptografia

A criptografia é uma técnica muito utilizada em sistemas de segurança de informações desde o último século antes de Cristo. Registros dão conta de que o imperador Julio César, já fazia uso de mensagens criptografadas para transmitir informações sigilosas às forças de guerra.

Segundo OLIVEIRA (2013) “a palavra criptografia vem do grego, *Kriptós* significa escondido, oculto e *grápho* que quer dizer grafia, ou seja, é a arte de escrever mensagens de forma sigilosa em códigos”. Dessa forma, apenas quem possui informações precisas de que tipo de código foi utilizado consegue decifrar as mensagens e compreender as informações nela contidas.

Funciona assim, a mensagem original é recodificada num sistema de números, chamado de pré-codificação que considera uma concordância biunívoca das letras existentes na mensagem com um conjunto de números definidos de acordo com a variedade de letras utilizadas.

A pessoa que recebe a mensagem somente consegue fazer a tradução se for portadora da chave decodificadora, ou seja, se compreender o sistema em que a criptografia foi realizada.

Na criptografia utilizada pelo Imperador Julio Cesar, ao se comunicar com sua equipe, havia uma "chave 3", ou uma regra de pular três letras além da que estava escrita para chegar à letra correta. Nesse caso, se na mensagem constava a letra *b*, isso correspondia a *e*, ou seja, $b = c + 2$. Assim, a decodificação da mensagem era feita pela simples substituição da letra escrita pela terceira letra depois dela. O quadro abaixo (Quadro 1) apresenta a transposição da criptografia de César.

A codificação da palavra CRIPTOGRAFIA, usando "*chave 3*", ficaria assim:

FULSWRJUDILD

QUADRO 1

Criptografia de César (Chave 3)

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: Conforme modelo de OLIVEIRA, 2013, p. 36

No processo de pré-codificação as letras são transformadas em números, na codificação chega a outro número. O quadro abaixo exemplifica como isso é feito.

QUADRO 2

Criptografia de César (Chave 3)

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: Conforme modelo de OLIVEIRA, 2013, p. 36.

Nesse caso para pré-codificar a palavra CRIPTOGRAFIA, no sistema numérico assumiria a seguinte forma:

$$02 - 17 - 08 - 15 - 19 - 14 - 06 - 17 - 00 - 05 - 08 - 00$$

Na codificação, usando *"chave 3"*, obtém-se um novo número:

$$05 - 20 - 11 - 18 - 22 - 17 - 09 - 20 - 03 - 08 - 11 - 03$$

A congruência modular é importante recurso para o aprimoramento da criptografia, uma vez que estabelece além de uma chave k, um módulo para a recodificação das mensagens. Ao verificar o quadro 2, percebe-se que existem 26 símbolos (00 a 25), permitindo aplicar $mod\ 26$, ou seja, todos os restos de uma divisão onde o divisor é 26, tal que $0 < k < 26$.

Oliveira (2013) apresenta um exemplo prático da aplicação de congruência modular na Criptografia. Neste caso, será recodificada a palavra MARIA, usando a criptografia de César com "*chave 15*".

Pré-codificação segundo o quadro 2: $12 - 00 - 17 - 08 - 00$

Codificação:

$$12 + 15 = 27 \equiv 01\ mod\ 26$$
$$00 + 15 = 15 \equiv 15\ mod\ 26$$
$$17 + 15 = 32 \equiv 06\ mod\ 26$$
$$08 + 15 = 23 \equiv 23\ mod\ 26$$
$$00 + 15 = 15 \equiv 15\ mod\ 26$$

Logo, a codificação utilizando a congruência modular será:

$$01 - 15 - 06 - 23 - 15$$

Desse modo, pode-se afirmar que:

$$C(a) \equiv a + k \; mod \; 26 \tag{4}$$

Em que a = número pré-codificado, $C(a)$ = número codificado e K = chave da criptografia de Cesar. Cuja decodificação se dá pela aplicação da expressão:

$$D(a) \equiv b - k \; mod \; 26 \tag{5}$$

Onde: $D(a)$ = número decodificado e $b = C(a)$.

Quando um cliente de um banco dirige-se a um terminal de autoatendimento ou acessa o portal do banco na internet e informa sua senha, abre uma série de possibilidades para contratar serviços e produtos bancários, como empréstimos, pagamento de faturas, saques, transferência de recursos entre contas, dentre outras. Tudo possibilitado pela verificação por parte do banco de que a senha informada é condizente com as informações do usuário. De outro modo, o cliente teria que se dirigir a agencia bancária, apresentar sua documentação, solicitar a realização da transação em um formulário e aguardar a conferência da assinatura, para só depois suprir sua necessidade.

O mesmo ocorre quando as pessoas trocam mensagens através da rede internacional de computadores, quando acessam suas contas de *e-mail*, seus *microblogs* em redes sociais e compartilham informações através de aplicativos instalados em *smartphones*. As informações prestadas passam por uma verificação e o acesso só é liberado depois de verificar a confiança dos códigos informados.

Para que isso seja possível, as empresas de tecnologia têm investido em sistemas de criptografia voltados à proteção dessas transações. São cruzadas várias informações que garantem identificar veracidade das senhas fornecidas e permitir o acesso do usuário aos recursos computacionais desejados.

4. Aplicações de Aritmética Modular no ensino básico

4.1. Contribuições para o ensino de aritmética modular

Existe uma preocupação por parte dos professores de matemática da educação básica com relação à adesão dos alunos aos temas de aulas propostos, já que a maioria dos alunos reclama que os conteúdos matemáticos não são contextualizados. Ouve-se perguntas como "onde vou aplicar isso? Para que aprender isso se nunca vou utilizar? Para que serve essa quantidade de fórmulas?" Esse desestímulo pela matemática se dá por uma série de fatores, principalmente pela didática pouco atrativa, bem como a falta de estrutura e de recursos para o ensino de matemática nas escolas públicas.

É certo que apresentar aos alunos uma aplicação para o conteúdo abordado, servirá como estímulo para sua adesão e a desmistificação de que a matemática além de difícil, tem pouca aplicabilidade.

Na pesquisa bibliográfica realizada para a construção deste trabalho, encontraram-se as dissertações de três estudiosos no campo da aritmética modular, que propuseram a utilização dessa ferramenta para o ensino de divisibilidade e aplicações de matemática no cotidiano, reforçando a importância da matemática na produção de soluções para o dia a dia.

Em sua dissertação Lourenço (2011) relata a experiência de trabalhar as aplicações de congruência modular em sala de aula. Segundo seu relato, foram desenvolvidas atividades pedagógicas em turmas do 7º ano fundamental e em turmas do 1º ano do nível médio, totalizando 70 alunos. Seu objetivo foi analisar a capacidade dos alunos de compreender a aritmética e colocar em prática os conhecimentos adquiridos. A atividade se deu em duas etapas, uma com os alunos num laboratório de informática e a outra com a comunidade escolar numa conferência sobre aplicações de congruência modular.

O jogo "aritmética do relógio" foi construído em versões que utilizam modelos de relógio analógico e digital, onde os jogadores são convidados a praticar a congruência $mod\ 12$. Apresenta a figura de um relógio analógico marcando uma hora qualquer e lança desafios como: "Daqui a 22 horas o ponteiro das horas aponta para que número"? Quando o jogador responde corretamente o relógio é atualizado, fazendo a alteração da posição do ponteiro. Os desafios são semelhantes para o relógio digital.

Na primeira etapa, o pesquisador levou os alunos selecionados ao laboratório de informática onde acessaram o jogo “aritmética do relógio”, desenvolvido pelo próprio Lourenço e disponibilizado na internet, em sítio próprio. Os alunos foram motivados a resolver os problemas apresentados e o professor recolheu as respostas. Observou-se que eles recorreram a estratégias de contagem para encontrar as respostas. Em seguida os mesmos alunos tiveram uma aula sobre aritmética modular e voltaram a jogar “aritmética do relógio”, porém, com enunciados mais elevados que os utilizados anteriormente, dificultando o uso de contagem para resolução. Notou-se uma mudança na estratégia para obtenção dos resultados, reduzindo a estratégia de contagem e melhorando o desempenho individual.

Na segunda etapa, o pesquisador realizou uma conferência intitulada “Aplicações de congruência modular”, destinada a toda a comunidade escolar e com foco nos alunos do ensino secundário. O autor relata que no período de motivação, muitos alunos recusaram a participar do projeto por se tratar de matemática, já que tinham grande dificuldade com essa disciplina. Entretanto, depois de serem informados sobre o desenvolvimento, mostraram-se abertos a comparecerem. Relata grande entusiasmo por parte dos participantes ao perceberem as aplicações de congruência modular, tanto na “aritmética do relógio”, quanto nos sistemas de identificação.

De modo semelhante, Sant’Anna (2013) discorreu sobre a aritmética modular como ferramenta para as séries finais do ensino fundamental. Em sua dissertação, propõe testar as aplicações da congruência modular constituindo o dígito verificador do CPF, em codificações de mensagens e em determinação do dia de nascimento através da aritmética do calendário. Apresenta ainda uma aplicação cobrada nos exames de admissão das escolas militares de nível médio também utilizando a aritmética do calendário.

Através da aritmética do calendário é possível descobrir o dia da semana em que aconteceu um evento importante como o nascimento de uma pessoa, ou de um acontecimento histórico. Esse é um fator de motivação para o estudo da congruência modular, porque aciona a curiosidade do aluno para a aplicação da metodologia visando confirmar sua veracidade.

A proposta de Sant’Ana é apresentar um problema aos alunos e deixar que eles façam as conjecturas e testes que sua curiosidade sugerir, na tentativa de encontrar uma resposta. Em seguida, informar a metodologia correta e deixar que eles testem várias vezes a fim de comprovar a aplicabilidade da metodologia e fixar os conhecimentos.

Esquinca (2013) afirma que as aplicações de aritmética modular são importantes para ajudar o aluno a desenvolver a criticidade matemática, levando-o a resolver problemas matemáticos de diversos níveis, nos quais seja possível contextualizar a matemática ao

cotidiano das pessoas. Para tanto, em sua dissertação, apresenta uma discussão sobre conteúdos já apresentados em sala de aula, como critérios de divisibilidade. Propõe utilizar a prova dos nove e sistemas de identificação como recursos para ensino de congruência modular aos alunos do ensino médio.

A "prova dos nove" ou "regra dos noves fora" é amplamente utilizada para provar a veracidade de resultados de operações com números naturais e trata-se de uma aplicação simples de congruência modular. Na aplicação dessa prova, ao retirar os noves fora, encontra-se o resto da divisão de um número n por 9. Por exemplo: como saber se o resultado de $246 \cdot 624 = 172224$ está correto? Primeiro tiramos os noves fora do multiplicando 246 ($2 + 4 + 6 = 12 \div 9 = 1, resto\ 3$), descobrimos que $246 \equiv 3\ mod\ 9$. Em seguida tiramos os noves fora do multiplicador 624 ($6 + 2 + 4 = 12 \div 9 = 1 + resto\ 3$), donde descobrimos que $642 \equiv 3\ mod\ 9$. Depois retiramos os noves fora do produto de $3 \cdot 3$ ($3 \cdot 3 = 9 \div 9 = 1\ resto\ 0$), logo $9 \equiv 0\ mod\ 9$. Se ao tirarmos os noves fora do produto 172224 encontrarmos um resultado igual a 0 a multiplicação está correta. Então, $1 + 7 + 2 + 2 + 2 + 4 = 18 \div 9 = 2, resto\ 0$. Note que $172224 \equiv 0\ mod\ 9$, logo a conta está correta.

Embora a proposta de Esquinca seja abranger alunos do ensino médio, essa metodologia é muito apropriada para desenvolver habilidades de divisibilidade e pode ser aplicada com alunos do ensino fundamental a partir do sexto ano.

Lourenço assegura que a curiosidade dos alunos é um fator positivo e uma vantagem para os professores, pois é uma característica dos jovens e é a partir dela que surge a motivação para a aprendizagem. Segundo ele,

> [...] a melhor forma de os motivar, é apresentando os conteúdos recorrendo, sempre que possível, a exemplos próximos das suas vivências e utilizando as tecnologias que os absorvem nestas idades, despertando assim a curiosidade e a vontade de procurar os métodos para obter a solução dos problemas apresentados. (Lourenço, 2011. p. 44).

De modo análogo, Skovsmose (2008) ao apresentar suas contribuições à teoria sobre matemática crítica, onde os alunos e sua curiosidade são o principal objetivo do professor de matemática, defende que a matemática faz parte de muitas práticas cotidianas, ela está impregnada na vida das pessoas e deve ser tratada com esse enfoque. Afirma que toda iniciativa voltada para a valorização das experiências cotidianas interfere positivamente no processo de ensino-aprendizagem e que o desenvolvimento de ambientes e condições de aprendizagem diferenciadas são bem vindas para produzir um conhecimento sólido.

Na concepção de Skovsmose, a matemática quando ensinada voltada para uma perspectiva de "*empowerment*"[4], na qual o sujeito consegue desenvolver uma consciência política e imerge numa preocupação com a responsabilidade e confiabilidade, além de preparo para assumir a alfabetização e proficiência em matemática, desenvolve também certa emancipação e liberdade enquanto cidadão.

Assim, criar ambientes de aprendizagem que valorizem as aplicações da matemática, significa criar condições para a formação do conhecimento e não apenas para cumprir as formalidades propostas nos planos curriculares. Certamente, esses ambientes contextualizados de ensino se mostrarão eficientes na produção de um saber consolidado e emancipador.

4.2. Proposta de metodologia para o ensino de aritmética modular

Segundo Lorenzato (2010) é difícil encontrar aplicações para tudo na matemática, por isso, não se deve ter a preocupação de ensinar apenas o que possui aplicação conhecida. Entretanto, sempre que possível após ensinar determinado conteúdo para o qual existe uma aplicação, é bom que os alunos sejam estimulados a experimentar. Os experimentos têm o poder de fixar os conhecimentos e consolidar o saber.

Lourenço (2011) conclui que fazer a opção por metodologias "diversificadas, apelativas e interativas" promove condições para acessar os indivíduos que não gostam ou apresentam alguma dificuldade para aprender matemática. Para ele, a utilização de recursos inovadores representa a possibilidade de romper as barreiras da aprendizagem e possibilitar a desmistificação da matemática como uma ciência dura e destinada apenas a pessoas com intelecto privilegiado.

Partindo desse pressuposto, apresentam-se a seguir três propostas de oficinas abordando a congruência modular, e que podem ser desenvolvidas com alunos de diferentes séries, enfatizando aqueles que já passaram pelo 9º ano do ensino fundamental.

[4] "Empoderamento". Um neologismo que se refere as relações de poder, onde o indivíduo ascende do ponto de vista social e ocupa posições mais elevadas no grupo a que pertence.

4.2.1. Pesquisa de CPF

A proposta é desenvolver um processo de investigação da veracidade do número de um CPF através do cálculo de seu dígito verificador e a determinação da Unidade Federada emissora do documento.

A atividade pode ser desenvolvida com alunos do 9º ano do ensino fundamental ou alunos do ensino médio.

Para a realização dessa oficina o professor deve levantar previamente alguns números de CPF, seja por pesquisa na internet ou montagem de números de CPF fictícios contemplando várias unidades da federação, ou ainda utilizar os números de documentos dos próprios alunos, quando for possível.

O professor deve ministrar uma aula inicial introduzindo a congruência modular, apresentando as definições, demonstrações e exemplos sobre o assunto, preparando os alunos para a atividade. Reforçar os critérios de divisibilidade e apresentar a fórmula de cálculo do dígito verificador do CPF, apresentado no tópico 3.2 deste trabalho.

Para o desenvolvimento, devem ser utilizados apenas os 9 primeiros algarismos componentes do CPF, com vistas a compor o décimo e o décimo primeiro, conferindo posteriormente a aplicação da congruência.

Em seguida, os alunos devem ser estimulados a verificar a unidade da federação onde o documento foi emitido, através da lista de Estados emissores do CPF (anexo 1).

Os alunos devem avaliar a oficina. Ao final, o professor abre espaço para que os alunos relatem a experiência. Podem ser feitas perguntas como: O que você achou da experiência de verificar o uso da matemática na composição do numero do CPF? Qual a lição principal aprendida nessa oficina? Dentre outras que o professor achar pertinente.

4.2.2. Pesquisa do código de barras

Nessa oficina os alunos serão estimulados a desenvolverem a investigação da aplicação da congruência modular na composição de códigos de barras, determinando o dígito verificador nos códigos analisados.

O público para aplicação dessa oficina deve contemplar alunos do 9º ano do ensino fundamental ou alunos do ensino médio.

Os alunos serão avisados da atividade previamente e motivados a levarem alguma embalagem de produto com código de barras. Pode ser embalagem de produtos diversos, ou os códigos de barras impressos nos próprios materiais didáticos em posse dos alunos (caderno, livro, frasco de cola, etc.).

Inicialmente os alunos podem ser levados ao laboratório de informática e instigados a pesquisar sobre o código de barras, sua finalidade, os modos de uso e os tipos. Em seguida relatarem o que encontraram na pesquisa realizada. Deve-se enfatizar o uso desses códigos no controle de todos os tipos de produtos, que eles podem determinar uma unidade de determinado produto ou um lote deles.

O professor deve ministrar aula sobre a congruência modular, apresentando as definições, demonstrações e exemplos sobre o assunto, preparando os alunos para a atividade. Reforçar os critérios de divisibilidade e apresentar a formula de cálculo do dígito verificador do código de barras, apresentado no tópico 3.1 deste trabalho.

Para padronizar, a fim de facilitar o trabalho, serão escolhidos para a atividade apenas códigos de barras com 13 dígitos, EAN-13.

O desenvolvimento corresponde a separar os 12 primeiros algarismos componentes do código de barras, com vistas a compor o décimo terceiro (código verificador), utilizando o método de cálculo apresentado no tópico 3.1 e conferirem posteriormente a aplicação da congruência.

Os alunos podem ser estimulados a verificarem o país de origem do produto, com base na relação de códigos conforme anexo 2.

Os alunos devem avaliar a oficina. Ao final, o professor abre espaço para que os alunos relatem a experiência. Podem ser feitas perguntas como as sugeridas na oficina anterior.

4.2.3. Oficina de Criptografia

O objetivo principal dessa oficina é aplicar a congruência modular na criptografia, levando os alunos a investigarem as diversas possibilidades de aplicação da aritmética modular na codificação de mensagens.

A oficina deve ser desenvolvida com alunos do ensino médio.

Os alunos devem ser preparados para a atividade com aula sobre a congruência modular, enfatizando as definições, demonstrações e exemplos sobre o assunto. O professor deve apresentar a formula de codificação (4) e decodificação (5) apresentadas no tópico 3.3 deste trabalho.

Como exercício, os alunos podem desenvolver o mesmo exemplo apresentado no tópico 3.3.

Em seguida os alunos podem escolher outra palavra ou uma frase para criptografarem, utilizando a mesma chave utilizada no exercício ou criarem uma chave diferente. Deve-se ter o cuidado de realizar a criptografia utilizando a congruência modular $mod\ 26$, com chave de sua escolha.

Para promover uma dinâmica, o professor pode estimular os alunos trocarem as criptografias feitas entre eles e deixar que os colegas tentem decodificar a mensagem. Inicialmente sem conhecer a chave e depois conhecendo-a.

Ao final, o professor pode dispor os alunos em círculo e promover uma roda de conversa permitindo que os alunos avaliem a oficina e relatem a experiência com a criptografia. O professor deve formular perguntas previamente para orientar a discussão e torná-la mais proveitosa. As perguntas sugeridas na oficina sobre pesquisa de CPF podem ser adaptadas para essa oficina.

5. Considerações finais

A congruência modular foi amplamente discutida, ressaltando a sua aplicação tanto para a composição de sistemas de identificação, quanto para a criptografia de códigos de segurança, como também em outras aplicações citadas anteriormente neste trabalho.

Procurou-se apresentar as principais aplicações de congruência modular abordadas no conjunto de referências bibliográficas selecionadas, enfatizando as que abrangem os sistemas de identificação, códigos de barras e criptografia.

Uma vez explicitadas as aplicações mais abrangentes, passou-se a verificar as aplicações na educação básica, utilizadas na escola como forma de reforçar a habilidade com a divisibilidade e estudos de aritmética. Ressalta-se que não foram abordadas todas as aplicações possíveis, mas apenas algumas das contempladas pelos autores estudados.

Procurou-se apresentar propostas de trabalho com alunos do ensino fundamental e médio, onde os mesmos são convidados a experimentarem as aplicações da congruência modular nas situações destacadas no desenvolvimento deste trabalho. A intenção é provocar a inovação do processo de ensino, promovendo melhores condições para a aprendizagem.

Isso chama a atenção para a necessidade de implementar metodologias de ensino que reforcem a aplicação da matemática no dia a dia. Demonstrar as aplicações da matemática é essencial para motivar os alunos a estabelecerem processos de investigação nesse campo, bem como de valorização dessa disciplina como conteúdo curricular.

Cabe considerar os ganhos obtidos no empreendimento deste processo de investigação bibliográfica, cujos resultados referem-se à melhoria da capacidade crítica do acadêmico, possibilitando progresso da habilidade interpretativa e, sobretudo, de imergir no universo da pesquisa científica.

Principalmente, espera-se que este trabalho possa servir como subsídio para professores de matemática da educação básica, visando estabelecer novas metodologias em suas aulas sobre aritmética modular. Igualmente, preste-se como referência para o desenvolvimento de estudos futuros.

6. Referências Bibliográficas

CARVALHO, A. L. de; RODRIGUES, D. V. M; ARAUJO, L. H. R. **Aplicações da aritmética modular na criptografia**. 2015. Disponível em: <https://periodicos.set.edu.br/index.php/cadernoexatas/article/view/2157> Acesso em: 04 março 2016.

CASTRO, Jânio Kléo de Souza. **Teoria dos números**: introdução à teoria dos números. Fortaleza: UAB/IFCE, 2010.

CASTRO, M. A. C; ARANTES, F. B; COSTA, P. O. Matemática Elementar. São João Del Rei: UFSJ, 2012.

CHUEIRI, Vanilda Miziara Mello; GONÇALVES, Eliete Maria. **Dicionário comentado de matemática**: conteúdos de matemática dispostos em forma de dicionário. Rio de Janeiro: Editora Ciência Moderna, 2012. 645 p.

DALBÉRIO, O; DALBÉRIO, M. C. B. **Metodologia científica**: desafios e caminhos. São Paulo: Paulus, 2009.

ESQUINCA, J. C. P. **Aritmética**: códigos de barras e outras aplicações de congruências. Dissertação de mestrado. Disponível em: <http://repositorio.cbc.ufms.br:8080/jspui/handle/123456789/1746>. Acesso em: 04 março 2016.

HEFEZ, Abramo. **Elementos de aritmética**. 2. ed. Rio de Janeiro: SBM. 2011.

LOPES, J. V; ÁVILA, J. A. J. **Limitação de qualquer fator primo de um número perfeito ímpar**. Disponível em: <http://www.ufsj.edu.br/portal2-repositorio/File/profmat/TCC_09_Jaqueline.pdf> Acesso em: 11 março 2016.

LOURENÇO, P. J. P. **Aplicações da aritmética modular**. Dissertação de mestrado. Universidade de Coimbra. Julho de 2011. Disponível em: <http://sistemaidentificacao.n.o.sapo.pt/ficheiros/Relatorioarit%20Modular.pdf>. Acesso em: 04 março 2016.

LORENZATO, S. **Para aprender matemática**. 3. ed. Campinas, SP: Autores Associados, 2010.

MEDEIROS, J. B. **Redação científica**: A prática de fichamentos, resumos, resenhas. 12. ed. São Paulo: Atlas, 2014. 344 p.

MOL, Rogério Santos**. Introdução à história da matemática**. Belo Horizonte: CAED-UFMG, 2013. 138 p.

OLIVERO, Mário. **História da Matemática Através de Problemas**. vol. 1. Rio de Janeiro: UFF / CEP – EB, 2007. 160 p.

OLIVEIRA, Maycon Costa de. **Aritmética**: criptografia e outras aplicações de congruências. Dissertação de mestrado. Disponível em: <http://repositorio.cbc.ufms.br:8080/jspui/bitstream/123456789/2160/1/MAYKON%20COSTA%20DE%20OLIVEIRA.pdf>. Acesso em: 11 março 2016.

PICADO, Jorge. **A álgebra dos sistemas de identificação**: da aritmética modular aos grupos diedrais. Disponível em: <http://www.mat.uc.pt/~picado/SistIdent/isbn2.pdf>. Acesso em 04/03/2016. Acesso em: 04 março 2016.

SÁ, Ilydio Pereira de. **Aritmética modular e algumas de suas aplicações**. Disponível em: <http://www.magiadamatematica.com/diversos/eventos/20-congruencia.pdf>. Acesso em: 11 março 2016.

SANT'ANNA, I. K. de. **A aritmética modular como ferramenta para as séries finais do ensino fundamental**. Dissertação de mestrado. Disponível em: <http://www.impa.br/opencms/pt/ensino/downloads/PROFMAT/trabalho_conclusao_curso/2013/iury_kersnowsky.pdf>. Acesso em: 11 março 2016.

SKOVSMOSE, Ole. **Desafios da reflexão em educação matemática crítica**. Campinas, SP: Papirus, 2008. 138 p.

TORRES, Guilhermo Zamalloa. **Divisibilidade por 3, 7, 9, 11, 13, 17...** Revista do professor de matemática. 2005. Disponível em: <http://wwwp.fc.unesp.br/~mauri/TN/RPM58divisibilidade.pdf>. Acesso em: 04 jun 2016.

7. Anexos

Anexo 1 – Estados emissores do CPF

Para identificar o Estado em que foi emitido, basta verificar o 9º algarismo (o último antes dos dígitos de controle). A definição do Estado emissor obedece à tabela abaixo.

Código	Estado
1	Distrito Federal, Goiás, Mato Grosso do Sul e Tocantins
2	Pará, Amazonas, Acre, Amapá, Rondônia e Roraima
3	Ceará, Maranhão e Piauí
4	Pernambuco, Rio Grande do Norte, Paraíba e Alagoas
5	Bahia e Sergipe
6	Minas Gerais
7	Rio de Janeiro e Espírito Santo
8	São Paulo
9	Paraná e Santa Catarina
0	Rio Grande do Sul

Fonte: www.acetbs.net.br/samba/noticias/7-artigos/177-como-conferir-um-cpf

Anexo 2 – Países de origem dos produtos conforme código de barras

Os três primeiros algarismos do código de barras identificam o país de origem do produto.

Código	País
002–019	EUA
020 - 029	Distribuição restringida definido pela organização membro GS1
030 - 039	EUA (reservado para medicamentos)
040 - 049	Distribuição restringida definido pela organização membro GS1
050 - 059	*Coupons*
060–139	EUA
140	CS Sistemas
200–299	Distribuição restringida definido pela organização membro GS1
300–379	França Mônaco
380	Bulgária
383	Eslovênia
385	Croácia
387	Bósnia e Herzegovina
400–440	Alemanha
450–459 490–499	Japão
460–469	Rússia
470	Quirguistão
471	Ilha de Taiwan
474	Estônia
475	Letônia
476	Azerbaijão
477	Lituânia
478	Uzbequistão
479	Sri Lanka
480	Filipinas
481	Bielorrússia
482	Ucrânia
484	Moldávia

Código	País
485	Armênia
486	Geórgia
487	Cazaquistão
489	Hong Kong
500–509	Reino Unido
520	Grécia
528	Líbano
529	Chipre
530	Albânia
531	República da Macedônia
535	Malta
539	República da Irlanda
540–549	Bélgica, Luxemburgo
560	Portugal
569	Islândia
570–579	Dinamarca, Ilhas Feroé, Groenlândia
590	Polônia
594	Romênia
599	Hungria
600-601	África do Sul
603	Gana
608	Bahrein
609	lhas Maurício
611	Marrocos
613	Argélia
616	Quênia
618	Costa do Marfim
619	Tunísia
621	Síria
622	Egito
624	Líbia
625	Jordânia
626	Irã
627	Kuwait
628	Arábia Saudita
629	Emirados Árabes Unidos

Código	País
640–649	Finlândia
690–699	República Popular da China
700–709	Noruega
729	Israel
730–739	Suécia
740	Guatemala
741	El Salvador
742	Honduras
743	Nicarágua
744	Costa Rica
745	Panamá
746	República Dominicana
750	México
754 – 755	Canadá
759	Venezuela
760–769	Suíça, Liechtenstein
770	Colômbia
773	Uruguai
775	Peru
777	Bolívia
779	Argentina
780	Chile
784	Paraguai
786	Equador
789 – 790	Brasil
800–839	Itália, San Marino, Vaticano
840–849	Espanha, Andorra
850	Cuba
858	Eslováquia
859	República Checa
860	Sérvia e Montenegro
865	Mongólia
867	Coreia do Norte
869	Turquia
870–879	Holanda
880	Coreia do Sul

Código	País
884	Camboja
885	Tailândia
888	Singapura
890	Índia
893	Vietnam
899	Indonésia
900–919	Áustria
930–939	Austrália
940–949	Nova Zelândia
950	GS1 *Global Office*
955	Malásia
958	Macau
977	Publicações periódicas seriadas (ISSN)
978, 979	*Bookland* (ISBN) 979 é formalmente usado para pautas de música
980	*Refund receipts*
981, 982	*Coupons* e meios de pagamento
990–999	*Coupons*

Fonte: https://pt.wikipedia.org/wiki/Lista_de_c%C3%B3digos_de_pa%C3%ADs_GS1