UNIVERSIDADE ESTADUAL DO MARANHÃO - UEMA
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO - PPG

PROFMAT
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

CONGRUÊNCIA MODULAR NOS ANOS FINAIS DO ENSINO FUNDAMENTAL: INTEGRAÇÃO DE TECNOLOGIA NA EDUCAÇÃO MATEMÁTICA.

Karllos Alexandre Sousa Pereira

São Luís - MA
2024

CONGRUÊNCIA MODULAR NOS ANOS FINAIS DO ENSINO FUNDAMENTAL: INTEGRAÇÃO DE TECNOLOGIA NA EDUCAÇÃO MATEMÁTICA.

Karllos Alexandre Sousa Pereira

Dissertação apresentada ao Programa de Mestrado em Matemática em Rede Nacional (PROFMAT) da Universidade Estadual do Maranhão (UEMA), como parte dos requisitos para obtenção do título de Mestre em Matemática.
Orientador: Prof. Dr. Sérgio Nolêto Turibus.

São Luís - MA
2024

Pereira, Karllos Alexandre Sousa
Congruência modular nos anos finais do ensino fundamental: integração de tecnologia na educação matemática. / Karllos Alexandre Sousa Pereira. – São Luis, MA, 2024.
70 f

Dissertação (Mestrado Profissional Matemática em Rede Nacional - PROFMAT) - Universidade Estadual do Maranhão, 2024.

Orientador: Prof. Dr. Sérgio Nolêto Turibus

1.Congruência Modular. 2.Divisão Euclidiana. 3.Integração de Tecnologia. 4.Criptografia. I.Título.

CDU: 51:373.3

Elaborado por Cássia Diniz - CRB 13/910

CONGRUÊNCIA MODULAR NOS ANOS FINAIS DO ENSINO FUNDAMENTAL: INTEGRAÇÃO DE TECNOLOGIA NA EDUCAÇÃO MATEMÁTICA.

Karllos Alexandre Sousa Pereira

Dissertação apresentada ao Programa de Mestrado em Matemática em Rede Nacional (PROFMAT) da Universidade Estadual do Maranhão (UEMA), como parte dos requisitos para obtenção do título de Mestre em Matemática.
Orientador: Prof. Dr. Sérgio Nolêto Turibus.

Aprovada em: 19 de Julho de 2024.

Banca Examinadora:

gov.br Documento assinado digitalmente
SERGIO NOLETO TURIBUS
Data: 21/08/2024 08:35:59-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Sérgio Nolêto Turibus (Orientador)
Universidade Estadual do Maranhão - UEMA

gov.br Documento assinado digitalmente
JOAO COELHO SILVA FILHO
Data: 20/08/2024 22:49:43-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. João Coelho Silva Filho (Examinador interno)
Universidade Estadual do Maranhão - UEMA

gov.br Documento assinado digitalmente
VALESKA MARTINS DE SOUZA
Data: 19/08/2024 11:30:38-0300
Verifique em https://validar.iti.gov.br

Profa. Dra. Valeska Martins de Souza (Examinadora externa)
Universidade Federal do Maranhão - UFMA

São Luís - MA
2024

Dedico esse trabalho a Deus que fez todas as coisas
e me permitiu chegar até aqui.

Agradecimentos

Primeiramente agradecer a Deus por tudo que ele tem feito na minha vida, incluindo a conquista de mais esse sonho que é a obtenção do título de Mestre.

À minha digníssima esposa Joyne Rodrigues, que teve que abdicar do trabalho e se dedicar integralmente a nossa primeira filha, Elisa, que nasceu poucos meses antes do início do mestrado, além de todo o apoio moral e incentivo para seguir em frente no mestrado mesmo com todas as dificuldades.

Aos meus familiares por todo apoio e suporte em especial o meu sogro que apesar da idade sempre ficar disponível para ir me deixar e buscar todas as madrugadas na rodoviária ao chegar de viagem, a minha sogra por ser uma segunda mãe durante esses dois anos e a minha cunhada por ser uma tia sempre disponível pra a minha filha.

À minha mãe que infelizmente não se encontra mais entre nós, mas foi quem sempre me incentivou, nunca deixou faltar-me nada mesmo nos momentos mais difíceis. O meu padrasto que durante toda a convivência sempre me guiou pelos caminhos dos estudos.

Aos meus colegas de turma do PROFMAT por sempre se mostrarem dispostos e engajados a tirar dúvidas e trocar ideias sobre os mais diversos conteúdos estudados no programa. A Valterlli de Urbano Santos que contribui muito com os seus conhecimentos durante a preparação pro exame de qualificação e por ser o responsável pelo nosso deslocamento apartamento a UEMA durante todo o mestrado.

Os meus irmãos que a matemática me deu durante a graduação pelo incentivo, por sempre acreditarem nessa conquista, por estarem sempre disponíveis quando precisei. Agradecer ao Maciel por todas as dicas durante o PROFMAT e pelo suporte na dissertação. Luanderson por todo apoio e dicas desde quando vim disputar uma vaga no mestrado e durante todo o PROFMAT, foi quem me guiou por São Luís.

A minha segunda mãe Marion Carvalho, que foi a base da minha criação, sempre me mostrou as melhores oportunidades durante toda a nossa convivência. A minha madrinha Lucirene Carvalho que foi fundamental com todo apoio e investimento financeiro feito por ela principalmente durante todo o ciclo da graduação. A minha vó Maria das Dores, que em momentos de dificuldade foi quem deu suporte para comprar obras literárias para estudar pro vestibular. Todos os familiares que contribuíram de alguma forma.

Aos professores Marlon, Ivanildo, Celina, Felix, Leandro, Waléria, Roberto, Sandra, Lélia e Brandão por compartilhar os seus conhecimentos nas disciplinas do mestrado.

Ao professor e o meu orientador Prof. Dr. Sérgio Nolêto Turibus, por conceder-me liberdade para trabalhar o tema que escolhi, por compartilhar os seus conhecimentos e experiências, dando ótimas sugestões, entre outras contribuições que foram essenciais para esta pesquisa.

RESUMO

Este trabalho visa explorar aplicações de congruência modular anos finais do ensino fundamental, juntamente com a integração de tecnologia. Examina a evolução histórica da aritmética, com contribuições de Pierre de Fermat, Euler, Friedrich Gauss dentre outros. Este estudo ainda detalha a divisão Euclidiana e os critérios de divisibilidade como pré-requisitos para a compreensão da congruência modular, buscando desenvolver a aprendizagem dos alunos, exemplificando por meio de oficinas de resolução de problemas práticos do cotidiano sobre códigos de barras, números de CPF e técnicas de criptografia de mensagens, tudo isso aliado ao uso de uma calculadora digital em formato de aplicativo para apresentar restos inteiros e fazer o uso da definição de congruência. Usando de uma abordagem metodológica multifacetada, combinando revisão bibliográfica e análise qualitativa de campo, com foco em observações participantes, entrevistas semiestruturadas, análise documental e grupos focais em uma escola municipal de Magalhães de Almeida – MA, buscando alternativas para o ensino aprendizagem mais eficaz.

Palavras Chave: Congruência modular; Divisão Euclidiana; Integração de Tecnologia; Criptografia.

ABSTRACT

This work aims to explore applications of modular congruence in the final years of elementary school, together with the integration of technology. Examines the historical evolution of arithmetic, with contributions from Pierre de Fermat, Euler, Friedrich Gauss, among others. This study also details the Euclidean division and the divisibility criteria as prerequisites for understanding modular congruence, seeking to develop student learning, exemplifying through workshops on solving practical everyday problems about barcodes, CPF numbers and message encryption techniques, all combined with the use of a digital calculator in application format to present integer remainders and make use of the definition of congruence. Using a multifaceted methodological approach, combining bibliographic review and qualitative field analysis, focusing on participant observations, semi-structured interviews, document analysis and focus groups in a municipal school in Magalhães de Almeida – MA, seeking alternatives for more effective teaching and learning.

Keywords: Modular congruence; Euclidean Division; Technology Integration; Cryptography..

Sumário

Lista de Figuras

LISTA DE QUADROS

1 INTRODUÇÃO

Congruência modular, é um tópico matemático fascinante de teoria dos números. A motivação da escolha do tema e os assuntos abordados se deram pelo aprofundamento dos estudos durante a preparação para o Exame Nacional de Qualificação do PROFMAT-UEMA, que durante as resoluções de problemas, percebeu-se a grande importância e uma vasta aplicação do conteúdo.

A educação matemática nos anos finais do ensino fundamental no Brasil enfrenta desafios significativos, como evidenciado pelos resultados estáveis, porém insatisfatórios, no Programa Internacional de Avaliação de Estudantes (PISA) de 2022. Essa estagnação aponta para a necessidade urgente de revisitar e inovar as abordagens pedagógicas em matemática.

Em um contexto em que os estudantes brasileiros continuam apresentando desempenho abaixo da média em matemática, ciências e leitura, conforme os dados do PISA 2022, surge a questão da eficácia das metodologias de ensino atuais. Este estudo visa explorar como a integração de ferramentas digitais, especificamente com o uso de uma calculadora de restos inteiros, pode revitalizar o ensino e a aprendizagem da congruência modular, um aspecto vital da matemática.

A congruência modular é um conceito fundamental na teoria dos números, que estuda os padrões de repetição dos números inteiros quando divididos por um certo número inteiro, chamado de módulo (PONTES, 2021). Esse conceito é essencial para compreendermos a aritmética modular, que é uma extensão da aritmética convencional, na qual as operações básicas como adição, subtração, multiplicação e divisão são realizadas dentro de um conjunto finito.

Neste contexto, explorar a congruência modular pode ser uma excelente oportunidade para utilizar a tecnologia de forma eficaz e envolvente (VILAÇA, 2023). Ao introduzir esse tema, os estudantes podem não apenas desenvolver suas habilidades matemáticas, mas também aprender a aplicar esses conceitos de forma prática e criativa, utilizando ferramentas digitais (FREITAS et al., 2023).

A integração de tecnologia na educação matemática se tornou uma prática cada vez mais comum e necessária nos dias de hoje (FREITAS et al., 2023). Com a rápida evolução da tecnologia, os educadores têm à sua disposição uma vasta gama de ferramentas e recursos que podem enriquecer o processo de aprendizagem e tornar os conceitos matemáticos mais acessíveis e interessantes para os alunos (FRAZ, 2023).

Ao introduzir a congruência modular nos anos finais do Ensino Fundamental, os educadores podem estimular o pensamento crítico e a resolução de problemas, além de proporcionar uma base sólida para o estudo de conceitos mais avançados de matemática e ciência da computação (FREITAS et al., 2023).

Através da integração de tecnologia na educação matemática, os alunos podem experimentar uma abordagem mais *hands-on* e participativa, onde têm a oportunidade de explorar, experimentar e descobrir os conceitos matemáticos por si mesmos (FREITAS et al., 2023). Isso não apenas torna o aprendizado mais significativo e memorável, mas também prepara os estudantes para enfrentar os desafios do mundo digital em que vivemos (FRAZ, 2023).

Além disso, a integração de tecnologia na educação matemática pode ajudar a tornar a matemática mais acessível e inclusiva para todos os alunos, incluindo aqueles com dificuldades de aprendizagem ou deficiências. Por meio de recursos digitais, é possível adaptar o ensino para atender às necessidades individuais de cada estudante,

proporcionando uma experiência de aprendizado mais personalizada e eficaz (VILAÇA, 2023).

O presente trabalho se concentra em propor o ensino de congruência modular para alunos dos anos finais do ensino fundamental, utilizando uma calculadora desenvolvida para essa pesquisa para vincular o conteúdo matemático a aplicações práticas do dia a dia. A motivação para este foco decorre da constatação de que a proficiência em operações básicas de matemática é essencial para resolver problemas cotidianos por meio da congruência modular.

A pesquisa aborda a necessidade de melhorar a compreensão da aritmética fundamental, especialmente a divisão, que é única entre as operações básicas que resulta em dois valores: o quociente e o resto. Este estudo se propõe a explorar a divisão Euclidiana e os critérios de divisibilidade como pré-requisitos para a compreensão da congruência modular, buscando desenvolver a habilidade dos alunos em divisão, a operação que apresenta maior dificuldade de aprendizado.

O problema central que norteia esta pesquisa é: Como a implementação de uma ferramenta digital, especificamente uma calculadora para dispositivos móveis, pode influenciar o ensino e a aprendizagem da congruência modular entre os estudantes dos anos finais do ensino fundamental em uma escola municipal de Magalhães de Almeida - MA? Este problema reflete a necessidade urgente de abordagens pedagógicas mais eficazes e engajadoras no ensino de matemática.

Para respondermos a essa problemática foram traçados os seguintes objetivos:

O objetivo geral: Investigar a eficácia da utilização de uma calculadora que apresenta restos inteiros de uma divisão como ferramenta pedagógica para o ensino e a aprendizagem de congruência modular.

Os objetivos específicos: Examinar a evolução histórica da aritmética modular; exemplificar alguns critérios de divisibilidade; Orientar os estudantes através da divisão Euclidiana e Demonstrar aplicações práticas da congruência modular com o uso da Calculadora modular desenvolvida para essa pesquisa.

Considerando o objeto desta pesquisa, optou-se por uma abordagem de pesquisa qualitativa. Essa escolha foi feita devido à necessidade de analisar as causas e consequências dos fenômenos envolvidos durante a realização de um projeto de ensino e aprendizagem de congruência modular usando uma calculadora modular.

Segundo Godoy (1995, p. 52), A pesquisa qualitativa se caracteriza pelas práticas interpretativas que nos aproximam do nosso cotidiano. possibilita ter ambiente natural com fonte direta de dados e o pesquisador como instrumento fundamental; Essas práticas são transformadoras e trazem várias representações.

> A pesquisa qualitativa é uma atividade situada que posiciona o observador no mundo. Ela consiste em um conjunto de práticas interpretativas e materiais que tornam o mundo visível. Essas práticas transformam o mundo, fazendo dele uma série de representações, incluindo notas de campo, entrevistas, conversas, fotografias, gravações e anotações pessoais. Nesse nível, a pesquisa qualitativa envolve uma postura interpretativa e naturalística diante do mundo. Isso significa que os pesquisadores desse campo estudam as coisas em seus contextos naturais, tentando entender ou interpretar os fenômenos em termos dos sentidos que as pessoas lhes atribuem. (DENZIN; LINCOLN, 2006, p. 3).

Foi realizado uma pesquisa de campo com os alunos do ensino fundamental anos finais da Escola Municipal Antônio Lopes de Carvalho como forma de analisar o objeto de estudo deste trabalho. A escola fica localizada na zona rural de Magalhães de Almeida no povoado Custódio Lima, os alunos são do próprio povoado e de povoados vizinhos.

A escolha da escola deve-se ao fato do autor deste trabalho exercer suas atividades na mesma. O projeto consistiu na aplicação da proposta de forma presencial nas turmas do 8º e 9º ano vespertino ensino fundamental que ambas contém 16 alunos, onde todos participaram do projeto sendo 17 meninas e 15 meninos. O intuito foi analisar os impactos da utilização de uma ferramenta educacional, mais especificamente uma calculadora modular durante a resolução de problemas relacionados a teoria de congruências nos anos finais do ensino fundamental, verificar aceitação com relação ao novo conteúdo e investigar as contribuições do novo conhecimento com o uso da ferramenta tecnológica para essa etapa de ensino.

O presente trabalho está organizado em seis seções: Na primeira está a introdução, nela é feita a apresentação dos tema, a problemática, metodologia, justificativa e objetivos. A segunda aborda os aspectos históricos de teoria dos números; A terceira aborda as definições e propriedades de congruência modular e alguns critérios de divisibilidade; A quarta trás algumas aplicações de congruência modular no cotidiano; A quinta temos os resultados e discursões e a sexta trás as considerações finais do trabalho.

Este estudo visa contribuir para o campo da educação matemática, oferecendo *insights* valiosos sobre a integração de ferramentas digitais no ensino e aprendizagem da congruência modular. Além disso, espera-se que os resultados deste estudo possam informar práticas pedagógicas futuras e auxiliar na formulação de políticas educacionais mais eficazes.

2 ASPECTOS HISTÓRICOS DE TEORIA DOS NÚMEROS

A teoria dos números é um dos campos mais antigos e fascinantes da matemática, que se dedica ao estudo das propriedades dos números inteiros e suas relações. Ao longo da história da humanidade, desde as civilizações antigas até os dias de hoje, a teoria dos números tem desempenhado um papel crucial no desenvolvimento da matemática e da ciência como um todo (CARVALHO et al., 2020). Nesta seção, exploraremos os aspectos históricos gerais da teoria dos números, desde suas origens na antiguidade até os avanços mais recentes nesta área de estudo.

As origens da teoria dos números remontam às civilizações antigas, como os egípcios, babilônios e gregos, que já exploravam questões relacionadas aos números e suas propriedades. Na antiga Mesopotâmia, por exemplo, os babilônios desenvolveram um sistema de numeração baseado no número 60, que influenciou o sistema de medida de tempo que ainda utilizamos hoje. Os egípcios também tinham um sistema de numeração, embora menos desenvolvido que o dos babilônios, que utilizava símbolos para representar números (RUSSO et al., 2024).

Na Grécia Antiga, matemáticos como Pitágoras e Euclides deram contribuições significativas para a teoria dos números. Pitágoras, famoso por seu teorema sobre os triângulos retângulos, também estabeleceu importantes relações entre os números inteiros, como as propriedades dos números primos. Euclides, por sua vez, é conhecido por sua obra "Elementos", na qual apresentou os fundamentos da geometria euclidiana, mas também incluiu uma seção dedicada à teoria dos números, abordando questões como a decomposição em fatores primos e o algoritmo de Euclides para encontrar o maior divisor comum de dois números (IDEM, 2022).

Durante a Idade Média, a teoria dos números continuou a se desenvolver, principalmente no mundo islâmico. Matemáticos como Al-Khwarizmi e Omar Khayyam fizeram importantes contribuições para a resolução de equações polinomiais e para o estudo dos números irracionais. Al-Khwarizmi também introduziu o sistema de numeração indo-arábico na Europa, que substituiu gradualmente os sistemas de numeração romano e grego (NUNES, 2020).

No Renascimento, a teoria dos números experimentou um renascimento significativo na Europa, com matemáticos como Fibonacci e Fermat fazendo importantes avanços nesta área. Fibonacci, em sua obra "Liber Abaci", introduziu os números arábicos na Europa e popularizou a sequência de Fibonacci, que tem aplicações em várias áreas, incluindo a biologia e a economia. Fermat, por sua vez, enunciou o chamado "último teorema de Fermat", uma das conjecturas mais famosas da teoria dos números, que só foi provada mais de 350 anos após sua formulação (KASAHARA; DE SÁ, 2023).

No século XVIII, a teoria dos números começou a se consolidar como um campo distinto da matemática, com o trabalho de matemáticos como Euler e Gauss. Euler fez contribuições importantes para a teoria dos números, especialmente no campo das funções geratrizes e nas congruências. Gauss, por sua vez, é conhecido por suas obras sobre aritmética modular, teoria dos números algébricos e a demonstração do teorema fundamental da aritmética, que estabelece a unicidade da decomposição em fatores primos (RODRIGUES; GONZAGA, 2022).

Também no século XIX, a teoria dos números continuou a se expandir e se ramificar em várias direções, com o surgimento de novos conceitos e técnicas matemáticas. Destacam-se os trabalhos de matemáticos como Dirichlet, Dedekind e Riemann, que de-

ram contribuições significativas para a teoria dos números algébricos, teoria dos números analíticos e a teoria dos números transcendentais (RUSSO et al., 2024).

Já no século XX, a teoria dos números experimentou um grande florescimento, com o desenvolvimento de novas técnicas e métodos matemáticos. Destacam-se os trabalhos de matemáticos como Hardy, Littlewood, Ramanujan, Wiles e muitos outros, que fizeram importantes contribuições para áreas como a teoria dos números analíticos, a teoria dos números algébricos e a teoria dos números aditivos. O século XX também viu a resolução de várias conjecturas famosas na teoria dos números, como o último teorema de Fermat, provado por Andrew Wiles em 1994 (RUSSO et al., 2024).

Hoje, a teoria dos números continua sendo um campo ativo e vibrante da matemática, com muitos problemas em aberto esperando por soluções. Com o advento da computação e da teoria dos números computacionais, novas ferramentas e métodos matemáticos estão sendo desenvolvidos para lidar com problemas cada vez mais complexos nesta área de estudo. Assim, a teoria dos números permanece como um dos pilares fundamentais da matemática, com aplicações em diversas áreas, desde a criptografia até a física teórica (KASAHARA; DE SÁ, 2023).

A Teoria dos números é um ramo da Matemática utilizada como sinônimo de Aritmética, e estuda os números inteiros com suas propriedades e operações, sendo esta utilizada em tarefas do cotidiano, em cálculos científicos e negócios (SILVA 2022), ou seja, é a parte prática de quase todo o ramo teórico da Matemática, e uma das áreas que também compõe a base curricular do ensino fundamental.

A Aritmética em si na sala de aula é dada principalmente por meio dos conteúdos de números naturais e inteiros, múltiplos e divisores, números primos e compostos, regras de divisibilidade, máximo e mínimo divisor comum, bem como todas as suas propriedades e aplicações. Dentro disso ainda temos a Congruência Modular, que é a parte mais detalhista da Aritmética (KASAHARA; DE SÁ, 2023).

O estudioso Euclides de Alexandria no seu escrito chamado "Os elementos"- uma versão grega de teoria dos números - datado provavelmente 300 anos antes de Cristo, demonstrou algo parecido com o teorema fundamental da aritmética em sua proposição, mas foi Gauss, no séc. XIX, que conseguiu demonstrar com veracidade, atribuindo notação apropriada e gerando o teorema, o que vem sendo aceito e utilizado até a atualidade (OLIVEIRA 2017).

> Enquanto ainda estudante em Gottingen, Gauss tinha começado a trabalhar em uma importante publicação em teoria dos números. Aparecendo dois anos depois de sua dissertação de doutoramento, as Disquisiotiones arithmeticae constituem um dos grandes clássicos da literatura matemática. Consiste em sete seções. Culminando com duas demonstrações da lei de reciprocidade quadrática, as quatro primeiras seções são essencialmente uma reformulação mais compacta da teoria dos números do século dezoito. Fundamentais na discussão são os conceitos de congruência e classe de restos. (BOYER; MERZBACH, 2012, p.344)

Ele introduziu a noção de congruência, que descreve como números dividem um módulo comum, retornando um mesmo resto. Esta ideia revolucionou a maneira como os matemáticos abordam problemas de divisibilidade e teoria dos números. Além disso, a divisão, sendo fundamental para a compreensão da congruência modular, permanece como uma das operações matemáticas mais desafiadoras para os estudantes (CARVALHO et al., 2020).

Porém, a congruência modular, conceito-chave na aritmética modular, apesar de frequentemente ensinada nas aulas teóricas, caso não seja demonstrada a devida conexão

com aplicações práticas, pode contribuir para a falta de interesse dos alunos em relação ao conteúdo. O problema é agravado pelo contexto pós-pandemia, que exige novas abordagens pedagógicas e a integração de ferramentas digitais que se alinhem com as habilidades e interesses dos alunos (RUSSO et al., 2024).

> Sabemos das dificuldades presentes no ensino da matemática, devemos procurar tornar as aulas mais atrativas, especialmente quando falamos dos atuais estudantes mais imediatistas e menos interessados em aulas apenas teóricas. Nessas condições, o que podemos tentar fazer é tornar nossas aulas as mais atrativas possíveis, aos olhos deles. (Melo, 2014, p.53).

Historicamente, a aritmética modular não era um tópico comum nos currículos de matemática do ensino básico. Contudo, nas últimas décadas, tem sido cada vez mais reconhecida sua importância e incluída no ensino fundamental e médio. Isso é evidenciado em currículos educacionais que começam a incorporar conceitos de teoria dos números e álgebra em níveis mais básicos de educação (National Council of Teachers of Mathematics, 2000).

Santos (2013), em seu trabalho de pesquisa demonstra que o rendimento apresentado pelos alunos de escolas públicas que participam da OBMEP, em dados extraídos do site da instituição, teve rendimento insatisfatório e baixo aproveitamento. Dentro dessa problemática, é importante a realização de um trabalho prático a fim de ajudar o estudante da área da matemática a de fato usar na prática cotidiana dele o conceito base de congruência modular e desenvolva a capacidade de resolver problemas de repetições periódicas de eventos.

O ensino de aritmética modular enfrenta desafios, principalmente devido à sua natureza abstrata. Pesquisadores em educação matemática têm explorado diferentes abordagens para tornar esse tópico mais acessível aos alunos. Por exemplo, Zazkis e Campbell (1996) destacam a importância de estratégias pedagógicas que contextualizem a aritmética modular em problemas do mundo real para facilitar a compreensão dos alunos.

Borba e demais autores (2023), demostra com ênfase a importância do aprofundamento do uso de tecnologias no ensino na matemática como uma maneira de driblar algumas dificuldades existentes há tempos e incrementar o ensino. Se segue:

> Tentaremos ver como coletivos formados por professores, alunos, softwares, internet, e telefones celulares podem gerar novas opções educacionais e como as partes deste coletivo se influenciam mutuamente. Em outras palavras, este livro pode ser pensado como uma forma de ação local, como uma maneira de abrir possibilidades para que a inclusão digital se faça de forma que realce o que de novo essas tecnologias podem trazer para a educação, para expandir a sala de aula, ou mudar a noção do que entendemos por sala de aula. (BORBA, p. 20-21)

As aplicações da aritmética modular se estenderam para além da teoria dos números. Na criptografia, por exemplo, a aritmética modular é um pilar central em algoritmos como o RSA, que é um dos primeiros sistemas de criptografia de chave pública, amplamente utilizado para segurança de dados. [1] Além disso, seu uso em ciência da computação é bem documentado, particularmente em estruturas de dados e algoritmos.

[1] O algoritmo RSA foi descrito em 1977 por Ron Rivest, Adi Shamir, e Leonard Adleman. Este tipo de algoritmo é chamado de criptografia assimétrica ou de chave pública, pois existem duas chaves que são usadas.

2.1 Divisão Euclidiana de Números Inteiros

Como nem sempre é possível expressar uma relação de divisibilidade de um inteiro por outro, segue do Princípio da Boa Ordem que embora que nos inteiros não possamos fazer divisões em geral, existe um processo de divisão muito útil e importante chamado de divisão com resto.

O conceito e a prática da divisão Euclidiana são essenciais para a compreensão da congruência modular, um tópico fundamental na matemática avançada.

Teorema 2.1: (Divisão Euclidiana): Sejam a e b dois números naturais, com $b \neq 0$. Existem dois únicos números naturais q e r, tais que:

$$a = b \ . \ q + r, \text{ com } 0 \leq r < |b|.$$

Demonstração: Considere o conjunto,

$$S = \{x = a - by; y \in \mathbb{Z}\} \cap (\mathbb{N} \cup 0)$$

Existência: Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$, então existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$, logo $a - nb > 0$, o que mostra que S é não vazio. O conjunto S é limitado inferiormente por 0, logo, pelo Principio da Boa Ordenação, temos que S possui um menor elemento r. suponhamos então que $r = a - bq$. Sabemos que $r \geq 0$. Vamos mostrar que $r < |b|$. Suponhamos por absurdo que $r \geq |b|$.

Portanto, existe $s \in \mathbb{N} \cup 0$, tal que $r = |b| + s$, logo $0 \leq s < r$. Mas isso contradiz o fato de r ser o menor elemento de S, pois $s = a - (q \pm 1)b \in S$, com $s < r$.

Unicidade: Suponha que $a = bq + r = bq + r = bq' + r'$, onde $q, q'r, r' \in \mathbb{Z}$, $0 \leq r < |b|$ e $0 \leq r' < |b|$, Assim, temos que $-|b| < -r \leq r' - r \leq r' < |b|$. Por outro lado, $b(q - q') = r' - r$, o que implica que

$$|b||q - q'| = |r' - r| < |b|,$$

o que só é possível se $q = q'$ e consequentemente, $r = r'$

■

Este conceito foi fundamentado por Euclides em sua obra "Elementos", estabelecendo a base para a teoria dos números como conhecemos hoje (Heath, 1908). Heath (1908) destaca que a abordagem de Euclides para a divisão com resto é mais do que um simples método de cálculo, é a fundação da compreensão de números inteiros e suas propriedades.

Imaginemos a seguinte problemática: Desejamos dividir 9 pirulitos entre 4 crianças. Com quantos pirulitos cada criança ficará? Como 4 não divide 9. Precisaríamos dividir os 9 pirulitos em 4 partes iguais, ficaria cada uma das crianças com 2 pirulitos e sobraria 1, que seria o resto da divisão de 9 por 4. Na prática, esta seria a Divisão Euclidiana básica, feita de maneira manual com objetos comuns do dia a dia.

Portanto, no nosso uso, chamamos a de dividendo (número que será dividido), b de divisor (número que divide), q de quociente (resultado da divisão) e r de resto (o que sobra).

Exemplo 2.1.1. Sejam os números inteiros 236 o dividendo e 7 o divisor temos:

$$236 = 7 \cdot 33 + 5.$$

O Algoritmo da divisão euclidiana também pode ser estendida para dividendo negativo (ou divisor negativo) usando a mesma abordagem afinal a definição é para quaisquer inteiros a e b.

Exemplo 2.1.2. Sejam os números inteiros (-19) o dividendo e 4 o divisor temos:

$$-19 = 4 \cdot (-5) + 1.$$

Exemplo 2.1.3. Na prática podemos imaginar a seguinte situação: Sejam 15 cavalos a serem divididos entre 4 amigos. Nesse caso o dividendo é o número de cavalos e o divisor o número de amigos.

$$15 = 4 \cdot 3 + 3.$$

Nesse caso, cada amigo ganharia 3 cavalos e ainda restaria 3 cavalos.

Exemplo 2.1.4. Qual o quociente e o resto da divisão de -17 por 3?

$$-17 = 3 \cdot (-6) + 1.$$

Logo, o Quociente é -6 e o Resto 1.

3 CONGRUÊNCIA MODULAR

A aritmética modular é um sistema de aritmética para inteiros, onde os números "retrocedem"quando atingem um certo valor, o módulo. O pioneiro na abordagem de congruência foi matemático suíço Euler por volta de 1750, quando ele explicitamente introduziu a ideia de congruência módulo um número natural N.Porém a abordagem moderna da aritmética modular foi desenvolvida por Carl Friedrich Gauss em seu livro *Disquisitiones Arithmeticae*, publicado em 1801.

A congruência modular baseia-se no conceito de divisão Euclidiana. Ela é definida quando dois números inteiros têm o mesmo resto ao serem divididos por um número inteiro positivo n. Ou seja, a é congruente a b módulo n, escrito como $a \equiv b \bmod n$, se n divide a-b (Andrews, 1994).

Andrews (1994) explica como a congruência modular é uma extensão natural do conceito de divisão Euclidiana, enfatizando a importância de entender a divisão com resto para explorar as propriedades das congruências.

Introduzir a divisão Euclidiana no ensino fundamental e médio prepara os estudantes para conceitos mais complexos como a congruência modular. Ao entender como um número pode ser decomposto em um produto mais um resto, os alunos começam a perceber os padrões subjacentes na matemática (Burn, 2005). Burn (2005) ressalta ainda a importância da divisão Euclidiana como um precursor para o entendimento da congruência modular, apontando que este conhecimento básico é essencial para o avanço em matemática.

A prática e o entendimento da divisão Euclidiana são indispensáveis para a compreensão plena da congruência modular. Esta relação é fundamental não apenas em teoria dos números, mas também em diversas aplicações práticas na matemática, na ciência da computação e na criptografia.

> A grande aplicabilidade das Congruências modulares em diversas áreas, como sistemas de identificação (ISBN, CPF, RG, códigos de barras), criptografia, calendários, relógios etc. é base de muitos artigos científicos e gera contribuições para o processo ensino e aprendizagem no ensino fundamental. (SILVA, 2022, p. 59)

Agora vamos a algumas definições, proposições e exemplos:

Definição 3.1. Seja m um número natural. Diz-se que dois números a e b são congruentes módulo m e, escreve-se $a \equiv b \bmod m$, se os restos de sua divisão por m são iguais. Caso contrário, diz-se que a e b são incongruentes e, denota-se $a \neq b \bmod m$.

Exemplo 3.1. Seja $23 \equiv 11 \bmod 4$, pois os restos da divisão de 23 e 11 por 4 são iguais a 3.

Exemplo 3.2. Seja $17 \not\equiv 8 \bmod 5$, pois os restos da divisão de 17 e 8 por 5 são 2 e 3 respectivamente.

Pela definição 3.1, Temos a impresão que para verificar se dois números são congruentes módulo m é necessário efetuar a divisão euclidiana de ambos por m para depois comparar seus restos. porém é suficiente a aplicação do resultado apresentado na proposição 3.1.

Proposição 3.1. Suponha que a, b e $m \in Z$, com $m > 1$. Então $a \equiv b \bmod m$ se, e somente se, $m \mid b - a$.

Demonstração: Sejam $a = mq+r$, com $0 \leq r < m$ e $b = mq'+r'$, com $0 \leq r' < m$, as divisões euclidianas de a e b por m, respectivamente. Suponha que $a \equiv b \bmod m$. Segue, da definição, que, $r = r'$ e daí $b - a = m(q' - q) + r' - r = m(q' - q)$, portanto, $m|b - a$.

■

Decorre da definição, que a congruência, módulo um inteiro fixado m, é uma relação de equivalência, conforme a proposição 3.2.

Proposição 3.2. Seja $m \in N$. Para todos a, b, $c \in Z$, tem-se que:

(a) Reflexiva: $a \equiv a \bmod m$;

(b) Simétrica: se $a \equiv b \bmod m$, então $b \equiv a \bmod m$;

(c) Transitiva: se $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então $a \equiv c \bmod m$.

Demonstração:
(a) Como $m|0$, então, $m|(a - a)$ o que implica que $a \equiv a \bmod m$.

(b) Se $a \equiv b \bmod m$, então $a = b + k_1 m$, $k_1 \in Z$. Logo, $b = a - k_1 m$, o que implica pela proposição 3.1, que $a \equiv b \bmod m$.

(c) Se $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então existem inteiros k_1 e k_2 tais que $a - b = k_1 m$ e $b - c = k_2 m$. Somando membro a membro estas últimas equações, obtem-se $a - c \equiv m(k_1 + k_2) \bmod m$, de onde segue que, $a \equiv c \bmod m$. Reciprocamente, suponha que $m|b - a$. Como $r' - r = b - a - m(q' - q)$ e $m|b - a$, concluimos que $m|r' - r$. Sendo $0 \leq r'$, $r < m$, tem-se que $|r' - r| < m$, logo $r' = r$. Portanto, $a \equiv b \bmod m$.

■

Proposição 3.3. Sejam $a, b, c, d, m \in Z$, com $m > 1$.

(a) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a + c \equiv b + d \bmod m$;

(b) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a - c \equiv b - d \bmod m$;

(c) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $ac \equiv bd \bmod m$;

(d) Se $a \equiv b \bmod m$, então $ak \equiv bk \bmod m$, $\forall k \in Z$;

(e) Se $a, b, m, k \in Z$, com $k > 0$ e $a \equiv b \bmod m$, então $a^k \equiv b^k \bmod m$.

Demonstração:
(a) De $a \equiv b \bmod m$ e $c \equiv d \bmod m$, segue que existem $k_1, k_2 \in Z$ tais que, $a - b = mk_1$ e $c - d = mk_2$. Somando as duas últimas equações membro a membro, obtem-se $(a + c) - (b + d) = m(k_1 + k_2)$, acarretando que $a + c \equiv b + d \bmod m$.

(b) Basta subtrair membro a membro as equações $a - b = mk_1$ e $c - d = mk_2$, que implica em $(a - c) - (b - d) = m(k1 - k2)$, acarretando $a - c \equiv b - d \bmod m$.

(c) Como $a \equiv b \bmod m$ e $c \equiv d \bmod m$, existem $k_3, k_4 \in Z$, tais que $a-b = k_3m$ e $c-d = k_4m$. Multiplicando $a-b = k_3m$ por c e $c-d = k_4$ por b, obtem-se $ac-bc = ck_3m$ e $bc - bd = ck_4m$. Somando membro a membro essas últimas igualdades, segue que $ac-bd-bc+bc = ck_3m+ck_4m$, acarretando $ac-bd = m(ck_3+ck_4)$ e, portanto, $ac \equiv bd \bmod m$.

(d) De $a \equiv b \bmod m$, segue que existe algum t inteiro, tal que $a - b = tm$. Multiplicando ambos os membros dessa equação por k, obtem-se, $ka - kb = ktm$ e, portanto, $ka = kb \bmod m$, $\forall k \in Z$.

(e) Será utilizada indução sobre k. Para $k = 1$ a proposição é verdadeira, pois, $a^1 \equiv b^1 \bmod m$ conforme hipótese. Supondo a propriedade verdadeira para k, isto é, que $a^k \equiv b^k \bmod m$, deve-se mostrar que isso implica na validade para $k+1$, ou seja, $a^{k+1} \equiv b^{k+1} \bmod m$. De fato, como $a \equiv b \bmod m$ e, por hipótese de indução, $a^k \equiv b^k \bmod m$, basta multiplicar, membro a membro as congruências, para obter, $a.a^k \equiv b.b^k \bmod m$, o que implica em $a^{k+1} \equiv b^{k+1} \bmod m$.

■

Exemplo 3.3. Determinar o resto da divisão de 2^{100} por 11.

Solução: Note que calcular a potência de 2^{100} para tentar dividir por 11 não parece ser viavél. Observe como fica a solução por congruência modular.

$$2^5 = 32 \equiv -1 \bmod 11$$

pelo item (e) da proposição 3.3 temos: $(2^5)^{20} \equiv (-1)^{20} \bmod 11$

$$2^{100} \equiv 1 \bmod 11$$

Portanto, 2^{100} deixa resto 1 na divisão por 11.

Exemplo 3.4. Determinar o resto da divisão de $2222^{5555} + 5555^{2222}$ por 3.

Solução: : Observe que $2222 = 740 \,.\, 3 + 2$ e $5555 = 1851 \,.\, 3 + 2$. Dessa forma temos:

$2222 \equiv 2 \bmod 3$ e $5555 \equiv 2 \bmod 3$.

Como $2 \equiv -1 \bmod 3$, pelo item (c) da proposiçaõ 3.2 temos:

$2222 \equiv -1 \bmod 3$ e $5555 \equiv -1 \bmod 3$.

Assim pelo item (e) da proposição 3.3 temos:

$2222^{5555} \equiv -1 \bmod 3$ e $5555^{2222} \equiv 1 \bmod 3$

Usando o item (a) da proposição 3.3 temos:

$2222^{5555} + 5555^{2222} \equiv -1 + 1 \equiv 0 \bmod 3$

Portanto, $2222^{5555} + 5555^{2222}$ deixa resto 0 na divisão por 3.

3.1 Pequeno Teorema de Fermat

Acredita-se que há pelo menos, 500 anos antes de Cristo, os chineses sabiam que, se p é um número primo, então, $p|2^p-2$. Mas coube a Pierre de Fermat, meados do século XVII, generalizar esse resultado, enunciando assim o "Pequeno Teorema de Fermat"como é conhecido nos dias atuais.

Para demonstrar o esse teorema de Fermat precisaremos do lema a seguir.

Lema 3.1: Seja p um número primo. os números $\binom{p}{i}$, onde $0 < i < p$, são todos divisíveis por p.

Demonstração: O resultado vale trivialmente para $i = 1$.

Podemos, então supor $1 < i < p$. Nesse caso, $i!|p(p-1)...(p-i+1)$.

Como $(i!, p) = 1$, decorre que $i!|(p-1)...(p-i+1)$, e o resultado se segue, pois

$$\binom{p}{i} = p\frac{(p-1)...(p-i+1)}{i!}.$$

Teorema 3.1: (Pequeno Teorema de Fermat): Dado um número primo p, tem-se que p divide o número $a^p - a$, para todo $a \in \mathbb{Z}$.

Se $p = 2$, o resultado é trivial já que $a^2 - a = a(a-1)$ é par. Suponhamos p ímpar. Nesse caso claramente basta mostrar o resultado para $a \geq 0$. Vamos provar o resultado por indução sobre a.

O resultado vale claramente para $a = 0$, pois $p|0$.

Supondo o resultado valido para a, iremos prová-lo para $a + 1$. Pela fórmula do Binômio de Newton,

$$(a+1)^p - (a+1) = a^p - a + \binom{p}{1}a^{p-1} + ... + \binom{p}{p-1}a.$$

Como, pelo lema 3.1 e pela hipótese de indução, o segundo membro da igualdade acima é divisível por p, conclui-se que p divide $(a+1)^p - (a+1)$.

O Pequeno Teorema de Fermat é muito eficiente na resolução dos problemas sobre congruência modular por dar celeridade à resolução dos mesmos. Em notação de congruências, o teorema de Fermat enuncia-se assim:

Se p é um número primo e $a \in \mathbb{Z}$, então $a^p \equiv a \mod p$. Além disso, se $p \nmid a$, então,

$$a^{(p-1)} \equiv 1 \mod p.$$

A seguir serão apresentadas algumas aplicações do Pequeno Teorema de Fermat.

Exemplo 3.1.1: Calcule o resto da divisão de 2^{257} por 7.

Solução: Note que 7 é primo e além disso $7 \nmid 2$. Assim temos que $257 = 6 \cdot 42 + 5$. Pelo Pequeno Teorema de Fermat temos que $2^6 \equiv 1 \mod 7$. Dessa forma $R \equiv 2^{(642+5)} \mod 7$, $R \equiv 1^{42}.2^5 \mod 7$, portanto $R \equiv 32 \mod 7$, Logo $R \equiv 4 \mod 7$

$$2^{257} \equiv 4 \mod 7.$$

Exemplo 3.1.2: Calcule o resto da divisão de 3^{23451} por 13.

Solução: Note que 13 é primo e além disso $13 \nmid 3$. Assim temos que $23451 = 12 \cdot 1954 + 3$. Pelo Pequeno Teorema de Fermat temos que $13^{12} \equiv 1 \bmod 13$. Dessa forma $R \equiv 3^{(121954+3)} \bmod 13$, $R \equiv 1^{1954} \cdot 3^3 \bmod 13$, portanto $R \equiv 27 \bmod 13$, Logo $R \equiv 1 \bmod 13$

$$3^{23451} \equiv 1 \bmod 13.$$

3.2 Critérios de divisibilidade

Nessa seção é apresentado alguns critérios de divisibilidade, usando os conceitos, definições e propriedades de congruência modular. A ideia principal é mostrar os critérios de divisibilidade e estabelecer condições que nos permitam determinar se um dado número inteiro $a > 0$ é ou não divisível por outro número inteiro $b > 1$, a um custo menor do que efetuar a divisão.

Um número inteiro na base 10, Será apresentado da seguinte forma:

$$a = r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + ... + r_1 \cdot 10 + r_0.$$

3.2.1 Divisibilidade por 2

Um número inteiro $a > 0$ é divisível por 2 quando o último algarismo é par ou é zero. Utilizando a noção de congruência, note que: $10 \equiv 0 \bmod 2$, assim $10^i \equiv 0 \bmod 2$.Assim,

$$r_i \cdot 10^i \equiv 0 \bmod 2, \text{ para } i > 1.$$

Portanto, dado um número n, tem–se que:

$a = r_n \cdot 10n + r_{n-1} \cdot 10_{n-1} + ... + r_1 \cdot 10 + r_0 \equiv 0 + 0 + ... + 0 + r_0 = n_0 \bmod 2$, assim $n \equiv n_0 \bmod 2$. E a é divisível por 2 se, e somente se, r_0 é divisível por 2, ou seja, se r_0 é par ou zero.

Exemplo 3.2.1.1: Verifique se o número 3416 é divisível por 2.

Solução:

$5678 = 5 \cdot 10^3 + 6 \cdot 10^2 + 7 \cdot 10 + 8 \equiv 0 + 0 + 0 + 8 \equiv 8 \bmod 2$,

mas, $8 \equiv 0 \bmod 2$, por transitividade $3416 \equiv 0 \bmod 2$. O que confirma que 5678 é divisível por 2 já que 8 é um número par e é divisível por 2.

Exemplo 3.2.1.2: Verifique se o número 6543 é divisível por 2.

Solução:

$6543 = 6 \cdot 10^3 + 5 \cdot 10^2 + 4 \cdot 10 + 3 \equiv 0 + 0 + 0 + 3 \equiv 3 \bmod 2$,

mas, $3 \equiv 1 \bmod 2$, por transitividade $6543 \equiv 1 \bmod 2$. portanto o número 6543 não é divisível por 2, já que 3 é um número ímpar e não é divisível por 2.

3.2.2 Divisibilidade por 3

Um número inteiro $a > 0$ é divisível por 3 se, e somente se, a soma de seus algarismos for um número divisível por 3. Utilizando a noção de congruência e a proposição 3.2, note que: $10 \equiv 1 \bmod 3$, por outro lado, $10^2 \equiv 10 \cdot 10 \equiv 1 \cdot 1 \equiv 1 \bmod 3$, ou ainda, $10^3 \equiv 10^2 \cdot 10 \equiv 1 \cdot 1 \equiv 1 \bmod 3$, assim, $10^i \equiv 1 \bmod 3$. Daí,

$$r_i \cdot 10^i \equiv 1 \bmod 3, \text{ para } i \geq 1.$$

Assim,

$$\begin{aligned} r_0 &\equiv n_0 \bmod 3 \\ r_1 \cdot 10 &\equiv n_1 \bmod 3 \\ r_2 \cdot 10^2 &\equiv n_2 \bmod 3 \\ &\vdots \\ r_{n-1} \cdot 10^{n-1} &\equiv r_{n-1} \bmod 3 \\ r_n \cdot 10^n &\equiv r_n \bmod 3 \end{aligned}$$

Somando membro a membro tem-se que:

$$(r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + \cdots + r_1 \cdot 10 + r_0) \equiv (r_n + r_{n-1} + \cdots + r_1 + r_0) \bmod 3,$$

dessa forma temos que $a \equiv (r_n + r_{n-1} + ... + r_1 + r_0) \bmod 3$. Assim a é divisível por 3 se, e somente se, $(r_n + r_{n-1} + \cdots + r_1 + r_0)$ é divisível por 3, ou seja, se a soma de todos os algarismo for divisível por 3, em congruência a é divisível por 3 se:

$$(r_n + r_{n-1} + \cdots + r_1 + r_0) \equiv 0 \bmod 3.$$

Exemplo 3.2.2.1: Verifique se o número 7455 é divisível por 3.

Solução:

$7455 = 7 \cdot 10^3 + 4 \cdot 10^2 + 5 \cdot 10 + 5 \equiv 7 + 4 + 5 + 5 \equiv 21 \bmod 3$,

como $21 \equiv 0 \bmod 3$, tem-se por transitividade que $7455 \equiv 0 \bmod 3$, portanto o número 7455 é divisível por 3. pois a soma dos seus algarismos é divisível por 3.

Exemplo 3.2.2.2: Verifique se o número 4589 é divisível por 3.

Solução:

$4589 = 4 \cdot 10^3 + 5 \cdot 10^2 + 8 \cdot 10 + 9 \equiv 4 + 5 + 8 + 9 \equiv 26 \bmod 3$,

como $26 \equiv 2 \bmod 3$, tem-se por transitividade que $4589 \equiv 2 \bmod 3$, portanto o número 4589 não é divisível por 3, pois a soma dos seus algarismos não é divisível por 3.

3.2.3 Divisibilidade por 4

Um número inteiro $a > 0$ é divisível por 4 se, e somente se, quando termina em 00 ou quando os dois últimos algarismos da direita for divisível por 4. Como $10 \equiv 2 \bmod 4$, por outro lado, $10^2 = 10 \cdot 10 \equiv 2 \cdot 2 = 0 \bmod 4$. Daí

$$r_i.10^i \equiv 0 \bmod 4, \text{ para } i > 1.$$

Assim,

$$\begin{aligned} a &\equiv r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + \cdots + r_1 \cdot 10 + r_0 \bmod 4 \\ a &\equiv 0 + 0 + \cdots + r_1 \cdot 10 + r_0 \bmod 4 \\ a &\equiv r_1 \cdot 10 + r_0 \bmod 4 \end{aligned}$$

Portanto, a é divisível por 4 se, e somente se, $r_1 r_0$ for divisível por 4.

Exemplo 3.2.3.1: Verifique se o número 8732 é divisível por 4.

Solução:

$8732 = 8 \cdot 10^3 + 7 \cdot 10^2 + 3 \cdot 10 + 2 \equiv 0 + 0 + 30 + 2 \equiv 32 \bmod 4$,

como $32 \equiv 0 \bmod 4$, tem-se por transitividade que $8732 \equiv 0 \bmod 4$, portanto o número 8732 é divisível por 4. pois $n_1 n_0$ é 32 que é divisível por 4.

Exemplo 3.2.3.2: Verifique se o número 9813 é divisível por 4.

Solução:

$9813 = 9 \cdot 10^3 + 8 \cdot 10^2 + 1 \cdot 10 + 3 \equiv 0 + 0 + 10 + 3 \equiv 13 \bmod 4$,

como $13 \equiv 1 \bmod 4$, tem-se por transitividade que $9813 \equiv 1 \bmod 4$, portanto o número 9813 não é divisível por 4. pois $n_1 n_0$ é 13 que não é divisível por 4.

3.2.4 Divisibilidade por 5

Um número inteiro $a > 0$ é divisível por 5 quando o último algarismo for 0 ou 5. Utilizando a noção de congruência, note que: $10 \equiv 0 \bmod 5$, dessa forma $10^i \equiv 0 \bmod 5$. Dessa forma temos;

$$r_i \cdot 10^i \equiv 0 \bmod 5, \text{ para } i \geq 1.$$

Assim,

$a \equiv r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + \cdots + r_1 \cdot 10 + r_0 \equiv 0 + 0 + \cdots + 0 + r_0 \equiv r_0 \bmod 5$,

assim $a \equiv r_0 \bmod 5$. Assim, a é divisível por 5 se, e somente se, r_0 é divisível por 5, ou seja, se r_0 for divisível por 0 ou 5.

Exemplo 3.2.4.1: Verifique se o número 3754 é divisível por 5.

Solução:

$3754 = 3 \cdot 10^3 + 7 \cdot 10^2 + 5 \cdot 10 + 4 \equiv 0 + 0 + 0 + 4 \equiv 4 \bmod 5$,

como $4 \equiv 4 \bmod 5$, tem-se por transitividade que $3754 \equiv 4 \bmod 5$, portanto o número 3754 não é divisível por 5, pois seu algarismo da unidade não é 0 ou 5.

Exemplo 3.2.4.2: Verifique se o número 2025 é divisível por 5.

Solução:

$2025 = 2 \cdot 10^3 + 0 \cdot 10^2 + 2 \cdot 10 + 5 \equiv 0 + 0 + 0 + 5 \equiv 5 \bmod 5$,

como $5 \equiv 0 \bmod 5$, tem-se por transitividade que $2025 \equiv 0 \bmod 5$, portanto o número 2025 é divisível por 5, pois seu algarismo da unidade é 5.

Exemplo 3.2.4.3: Verifique se o número 3450 é divisível por 5.

Solução:

$3450 = 3 \cdot 10^3 + 4 \cdot 10^2 + 4 \cdot 10 + 0 \equiv 0 + 0 + 0 + 0 \equiv 0 \bmod 5$,

como $0 \equiv 0 \bmod 5$, tem-se por transitividade que $3450 \equiv 0 \bmod 5$, portanto o número 3450 é divisível por 5, pois seu algarismo da unidade é 0.

3.2.5 Divisibilidade por 6

Um número $a > 0$ é divisível por 6 se, e somente se, a é divisível por 2 e 3. Uma justificativa desse critério vem do Teorema Fundamental da Aritmética - TFA, de fato pode-se notar que a decomposição em fatores primos do 6 é $6 = 2 \cdot 3$.

Demonstração: Seja a um número natural, tomando $a = 6 \cdot t = 2 \cdot (3 \cdot t)$, se fizermos $x = 3 \cdot t$, então $a = 2 \cdot x$, com $x \in N$, daí a é divisível por 2. Analogamente $a = 6 \cdot t = 3 \cdot (2 \cdot t)$, se fizermos $z = 2 \cdot t$, então $a = 3 \cdot z$, com $z \in N$, assim a é divisivel por 3, logo se a é divisível por 6, então a é divisível por 2 e 3.

Por outro lado, suponhamos, que a seja divisível por 2 e 3, como $2|a$, então existe $k \in N$ tal que $a = 2 \cdot k$, notemos que $3 - 2 = 1$, multiplicando essa igualdade por k, obtemos $3 \cdot k - 2 \cdot k = k \Rightarrow 3 \cdot k - a = k$ (i), por outro lado, existe também $t \in N$ tal que $a = 3 \cdot t$, pois $3|a$ (ii), logo, por (i) e (ii) temos que $k = 3 \cdot k - a = 3 \cdot k - 3 \cdot t = 3(k - t)$.

Exemplo 3.2.5.1: Verifique se o número 6654 é divisível por 6.

Solução:

Nesse caso da divisão por 6, vamos dividir em duas partes que é verificar se o número é divisível por 2 e caso seja, verificar se também é divisível por 3.

Parte 1: (verificar se 6654 é divisível por 2)

$6654 \equiv 0 + 0 + 0 + 4 \bmod 2$,

$6654 \equiv 4 \bmod 2$

Temos então que 6654 é divisível por 2 já que 4 é um número par e é divisível por 2.

Parte 2: (verificar se 6654 também é divisível por 3)

$6654 \equiv 6 + 6 + 5 + 4 \bmod 3$,
$6654 \equiv 21 \bmod 3$

Portanto o número 6654 é divisível por 3. pois a soma dos seus algarismos é divisível por 3.

3.2.6 Divisibilidade por 8

Um número inteiro $a > 0$ é divisível por 8 se, e somente se, quando termina em 000 ou quando os três últimos algarismos da direita for divisível por 8. Como $10 \equiv 2 \bmod 8$, por outro lado, $10^3 = 10 \cdot 10 \cdot 10 \equiv 2 \cdot 2 \cdot 2 = 0 \bmod 8$. Daí

$$r_i.10^i \equiv 0 \bmod 8, \text{ para } i > 2.$$

Assim,

$$a \equiv r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + \cdots + r_2 \cdot 10^2 + r_1 \cdot 10 + r_0 \bmod 8$$
$$a \equiv 0 + 0 + \cdots + r_2 \cdot 10^2 + r_1 \cdot 10 + r_0 \bmod 8$$
$$a \equiv r_2 \cdot 10^2 + r_1 \cdot 10 + r_0 \bmod 8$$

Portanto, a é divisível por 8 se, e somente se, $r_2r_1r_0$ for divisível por 8.

Exemplo 3.2.6.1: Verifique se o número 9832 é divisível por 8.

Solução:

$9832 = 9 \cdot 10^3 + 8 \cdot 10^2 + 3 \cdot 10 + 2 \equiv 0 + 800 + 30 + 2 \equiv 832 \bmod 8$,

como $832 \equiv 0 \bmod 8$, tem-se por transitividade que $9832 \equiv 0 \bmod 8$, portanto o número 9832 é divisível por 8. pois $r_2r_1r_0$ é 832 que é divisível por 8.

Exemplo 3.2.6.2: Verifique se o número 1985 é divisível por 8.

Solução:

$1985 = 1 \cdot 10^3 + 9 \cdot 10^2 + 8 \cdot 10 + 5 \equiv 0 + 900 + 80 + 5 \equiv 985 \bmod 8$,

como $985 \equiv 1 \bmod 8$, tem-se por transitividade que $1985 \equiv 1 \bmod 8$, portanto o número 1985 não é divisível por 8. pois $r_2r_1r_0$ é 985 que não é divisível por 8.

3.2.7 Divisibilidade por 9

Um número inteiro $a > 0$ é divisível por 9 se, e somente se, a soma de seus algarismos for um número divisível por 9. Utilizando a noção de congruência e a proposição 3.2, note que: $10 \equiv 1 \bmod 9$, por outro lado, $10^2 \equiv 10 \cdot 10 \equiv 1 \cdot 1 \equiv 1 \bmod 9$, ou ainda, $10^3 \equiv 10^2 \cdot 10 \equiv 1 \cdot 1 \equiv 1 \bmod 9$, assim, $10^i \equiv 1 \bmod 9$. Daí,

$$r_i.10^i \equiv 1 \bmod 9, \text{ para } i \geq 1.$$

Assim,

$$r_0 \equiv r_0 \bmod 9$$

$$r_1 \cdot 10 \equiv r_1 \bmod 9$$

$$r_2 \cdot 10^2 \equiv r_2 \bmod 9$$

$$\vdots$$

$$r_{n-1} \cdot 10^{n-1} \equiv r_{n-1} \bmod 9$$

$$r_n \cdot 10^n \equiv r_n \bmod 9$$

Somando membro a membro tem-se que:

$$(r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + \cdots + r_1 \cdot 10 + r_0) \equiv (r_n + r_{n-1} + \cdots + r_1 + r_0) \bmod 9,$$

dessa forma temos que $a \equiv (r_n + r_{n-1} + ... + r_1 + r_0) \bmod 9$. Assim a é divisível por 9 se, e somente se, $(r_n + r_{n-1} + \cdots + r_1 + r_0)$ é divisível por 9, ou seja, se a soma de todos os algarismo for divisível por 9, em congruência a é divisível por 9 se, e somente se:

$$(r_n + r_{n-1} + \cdots + r_1 + r_0) \equiv 0 \bmod 9.$$

Exemplo 3.2.7.1: Verifique se o número 8451 é divisível por 9.

Solução:

$8451 = 8 \cdot 10^3 + 4 \cdot 10^2 + 5 \cdot 10 + 1 \equiv 8 + 4 + 5 + 1 \equiv 18 \bmod 9,$

como $18 \equiv 0 \bmod 9$, tem-se por transitividade que $8451 \equiv 0 \bmod 9$, portanto, o número 8451 é divisível por 9. pois a soma dos seus algarismos é divisível por 9.

Exemplo 3.2.7.2: Verifique se o número 2317 é divisível por 9.

Solução:

$2317 = 2 \cdot 10^3 + 3 \cdot 10^2 + 1 \cdot 10 + 7 \equiv 2 + 3 + 1 + 7 \equiv 13 \bmod 9,$

como $13 \equiv 4 \bmod 9$, tem-se por transitividade que $2317 \equiv 4 \bmod 9$, portanto, o número 2317 não é divisível por 9, pois a soma dos seus algarismos não é divisível por 9.

3.2.8 Divisibilidade por 10

Um número inteiro $a > 0$ é divisível por 10 quando o último algarismo é zero.Utilizando a noção de congruência, note que: $10 \equiv 0 \bmod 10$, assim $10^i \equiv 0 \bmod 10$.Assim,

$$r_i \cdot 10^i \equiv 0 \bmod 10, \text{ para } i > 1.$$

Portanto, dado um número $a > 0$, tem–se que:

$a = r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + ... + r_1 \cdot 10 + r_0$
$a \equiv 0 + 0 + ... + 0 + r_0 \bmod 10$
$a \equiv r_0 \bmod 10.$

Assim $a \equiv r_0 \bmod 10$. E a é divisível por 10 se, e somente se, r_0 é divisível por 10, ou seja, se r_0 é zero.

Exemplo 3.2.8.1: Verifique se o número 3540 é divisível por 10.

Solução:

$3540 = 3 \cdot 10^3 + 5 \cdot 10^2 + 4 \cdot 10 + 0$
$3540 \equiv 0 + 0 + 0 + 0 \bmod 10$
$3540 \equiv 0 \bmod 10,$

Mas, $0 \equiv 0 \bmod 10$, por transitividade $3540 \equiv 0 \bmod 10$. O que confirma que 3540 é divisível por 10 já que termina em 0.

Exemplo 3.2.8.2: Verifique se o número 7589 é divisível por 10.

Solução:

$7589 = 7 \cdot 10^3 + 5 \cdot 10^2 + 8 \cdot 10 + 9$
$7589 \equiv 0 + 0 + 0 + 9 \bmod 10$
$7589 \equiv 9 \bmod 10,$

Mas, $9 \equiv 9 \bmod 10$, por transitividade $7589 \equiv 9 \bmod 10$. Portanto, o número 7589 não é divisível por 10, já que o mesmo é um número que não termina em zero.

Exemplo 3.2.8.3: Verifique se o número 78560 é divisível por 10.

Solução:

$78560 = 7 \cdot 10^4 + 8 \cdot 10^3 + 5 \cdot 10^2 + 6 \cdot 10 + 0$
$78560 \equiv 0 + 0 + 0 + 0 + 0 \bmod 10$
$78560 \equiv 0 \bmod 10,$

Mas, $0 \equiv 0 \bmod 10$, por transitividade $78560 \equiv 0 \bmod 10$. O que confirma que 78560 é divisível por 10 já que termina em 0.

3.2.9 Divisibilidade por 11

Um número inteiro $a = r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + ... + r_1 \cdot 10 + r_0$ é divisível por 11 quando $r_0 - r_1 + r_2 - r_3 + ... - r_{n-1} + r_n$.Utilizando a noção de congruência, note que: $10 \equiv -1 \bmod 11$ e que $10^2 \equiv 1 \bmod 11$.Assim temos:

$$r_0 \equiv r_0 \bmod 11$$

$$r_1 \cdot 10 \equiv -r_1 \bmod 11$$

$$r_2 \cdot 10^2 \equiv r_2 \bmod 11$$

$$r_3 \cdot 10^3 \equiv -r_3 \bmod 11$$

$$.$$

$$.$$

$$.$$

$$r_{n-1} \cdot 10^{n-1} \equiv -r_{n-1} \bmod 11$$

$$r_n \cdot 10^n \equiv r_n \bmod 11$$

Somando membro a membro tem-se que:

$(r_0 + r_1 \cdot 10 + r_2 \cdot 10^2 + r_3 \cdot 10^3 + \cdots + r_{n-1} \cdot 10^{n-1} + r_n \cdot 10^n) \equiv (r_0 - r_1 + r_2 - r_3 + ... - r_{n-1} + r_n) \bmod 11$,

Dessa forma temos que $a \equiv (r_0 - r_1 + r_2 - r_3 + ... - r_{n-1} + r_n) \bmod 11$. Assim a é divisível por 11 se, e somente se, $(r_0 - r_1 + r_2 - r_3 + ... - r_{n-1} + r_n)$ é divisível por 11, em congruência a é divisível por 11 se, e somente se:

$$(r_0 - r_1 + r_2 - r_3 + ... - r_{n-1} + r_n) \equiv 0 \bmod 11.$$

Exemplo 3.2.9.1: Verifique se o número 4567 é divisível por 11.

Solução:

$4567 \equiv 7 - 6 + 5 - 4 \bmod 11$
$4567 \equiv 2 \bmod 11$

Como 2 não é divisível por 11,temos que 4567 não é divisível por 11 .

Exemplo 3.2.9.2: Verifique se o número 482713 é divisível por 11.

Solução:

$482713 \equiv 3 - 1 + 7 - 2 + 8 - 4 \bmod 11$
$482713 \equiv 11 \bmod 11$

Como 11 é divisível por 11,temos que 482713 é divisível por 11 .

4 Aplicações de Congruência Modular no Cotidiano

Nesta seção são apresentadas algumas das possíveis aplicações de congruência modular no cotidiano nos quais iremos mostrar também aos alunos, apresentando as potencialidades desta teoria, bem como ela se mostra bem útil na sociedade, em particular, na tecnologia. Nesse trabalho foi dado enfoque em criptografia e sistemas de identificação

4.1 Criptografia

A origem da criptografia (do grego kryptós = escondido e gráphien = escrita) vem dentre outras utilidades, da insegurança que havia no tráfego de mensagens entre o remetente e destinatário, segundo Montanher. Na época das batalhas romanas, a mensagem tinha que ser recebida em sua integralidade, não havendo espaço para erros, dúvidas ou inconsistências, pois o remetente enviava informações valiosas e secretas, que o emissor teria de receber e colocá-las em prática, sendo este muitas vezes o único que sabia decifrá-las, e usar como estratégias nas batalhas.

Há datações de códigos criptografados desde o último século antes de Cristo, no sistema de escrita hieroglífica egípcio e em comunicações sobre planos de batalha romanos, conforme Silva. Inclusive, o mais completo exemplo sobre isso é a Criptografia do Imperador Júlio César.

O imperador romano precisava transmitir informações secretas ao seu general nos campos de batalhas, pois, naquela época, as mensagens escritas poderiam ser facilmente violadas, e sendo estas decodificadas, somente o emitente e o receptor teriam as chaves que possibilitariam a decodificações das informações.

Oliveira, 2016, resume em seu trabalho como era basicamente o modelo de Criptografia de Julio Cézar:

> 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. (Oliveira, 2016, p. 30)

Portanto, nesse processo de pré-codificação as letras são transformadas em números, e na codificação eram transformadas em outros números, então uma mensagem havia duas fases de codificações, para somente assim chegar ao código da mensagem.

Exemplificando melhor essa criptografia, vamos usar o exemplo da Chave 3 ou "pule 3", usada por Júlio Cézar ao transmitir informações à sua equipe, que nesse caso, se na mensagem constava a letra K, isso correspondia a N, ou seja, $K = L + 2$. Assim, a decodificação da mensagem era feita pela simples substituição da letra escrita pela terceira letra depois dela. O quadro a seguir (Quadro 1) apresenta a transposição da criptografia de César.

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

HVFROD

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	o	p	12
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, 2017, p. 31

Partindo do processo de pré-codificação, estas letras precisariam ser pré-codificadas em números, e depois, na codificação, precisariam ser codificadas em outros números, seguindo o seguinte quadro com a mesma Criptografia de César - Chave 3:

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, 2017, p. 31

Usando o mesmo exemplo, agora para pré-decodificar a palavra ESCOLA no sistema numérico ficaria assim:

$$04 - 18 - 02 - 14 - 11 - 00$$

Na codificação, usando a Chave 3, assumiria a seguinte forma:

$$07 - 21 - 05 - 17 - 14 - 03$$

Ao observarmos o quadro 2, percebemos que esta é uma criptografia formada por 26 símbolos – 00 à 25 – que quando tratada nos termos da congruência modular, um importante recurso para aprimoramento, poderia ser estabelecido além de uma chave c, com a aplicação de mod 26, ou seja, todos os restos de uma divisão onde o divisor é 26, tal que $0 \leq c < 26$.

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".

A Pré-codificação segundo o quadro 2: $12 - 00 - 17 - 08 - 10$.

A Codificação:

$$\begin{aligned} 12 + 15 &= 27 \equiv 01 \bmod 26 \\ 00 + 15 &= 15 \equiv 15 \bmod 26 \\ 17 + 15 &= 32 \equiv 06 \bmod 26 \\ 08 + 15 &= 23 \equiv 23 \bmod 26 \\ 00 + 15 &= 15 \equiv 15 \bmod 26 \end{aligned}$$

Logo, a codificação utilizando a congruência modular será:

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

Desse modo, pode-se afirmar:

$$\mathrm{B}\ (a) \equiv a + c \bmod 26$$

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

$$\mathrm{E}\ (a) \equiv d - c \bmod 26$$

Onde E (a) = número decodificado e d = B (a).

A Criptografia têm sido fundamental no uso das tecnologias, sendo esta cada vez mais desenvolvida e buscada por grandes empresas, pois hoje em dia, os smartphones contêm diversos documentos que antes eram só papeis na carteira física, como por exemplo, a carteira digital de trânsito, que basta usar uma senha que será autenticado o sistema, dando acesso a diversas informações do motorista, inclusive sendo usado Qrcode, para verificar autenticidade do documento.

Outro exemplo que vislumbramos muito na prática é o uso dos bancos digitais, que antigamente era praticamente impossível resolver algo sem a assinatura física, sem ter que ir ao banco ou destinar a um procurador tal função, hoje basta a autenticação digital para obter vários serviços, em qualquer lugar, qualquer momento, sendo possível realizar transações apenas com a criptografia dos dados, tornando este um sistema que facilita e demonstra segurança até certo ponto, aos usuários. Portanto, a Criptografia deve ser segura a quem usa, e secreta, como próprio nome diz:

> "Os serviços básicos de segurança que um sistema criptográfico deve fornecer são, Confidencialidade, Integridade, Autenticação e Não Repudiação. A Confidencialidade consiste em manter a informação secreta para todos os que não estão autorizados ao contato com essa informação. Integridade garante que a informação não foi alterada por entidades desconhecidas ou não autorizadas. Autenticação garante a identidade de uma entidade envolvida na comunicação. Por último, a Não Repudiação previne a negação de ações e compromissos previamente realizados." (SILVEIRA, 2013)

Para garantir todos esses pilares, as empresas de tecnologia são responsáveis por cruzar várias informações que garantem a segurança das senhas fornecidas e permitir o acesso do usuário aos recursos tecnológicos desejados, pois como podemos perceber, a criptografia em meios digitais tornou-se essencial aos usuários.

4.2 Sistemas de Identificação - Código de barras com 13 dígitos

O código de barras é utilizado universalmente em diferentes áreas, como no comércio, nas indústrias, em bibliotecas, em bancos, dentre outros. Foi criado por Joseph Woodland e Bernard Silver em 1952, inicialmente com 12 dígitos, conforme Montanher nos diz, e acabou sendo nomeado como Universal Product Code (UPC), conforme foi disposto na figura 1 abaixo.

Figura 1: Ilustração do Código de barras UPC (12 dígitos)

Fonte: Google imagens

George J. Laurer aprimorou o método, e em meados da década de 70, foi acrescido mais um dígito, servindo com identificação do país de origem, esse código recebeu o nome de European Article Numbering system (EAN-13) – figura 2 -, adotado até os dias atuais.

Figura 2: Ilustração Código de Barras EAN-13

Fonte: Google imagens

Conforme Oliveira, o nome código de barras surgiu devido à existência da sequência de barras que são identificadas pela largura de sua impressão e correspondem a um código numérico, para o qual foi utilizado congruência modular. Sendo que, estas barras, sejam elas brancas ou pretas, possuem espessuras possíveis: finas, médias, grossas ou muito grossas.

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).

O código de barras do tipo EAN-13 é usado em diversos produtos, e é formado por 13 algarismos sendo este o mais utilizado 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.

Sá (2020) discrimina o EAN-13 da seguinte forma:

> [...] 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, 2020, p. 7).

A compreensão dessa estrutura nos permite, mais uma vez, entender a importância da aritmética modular para a construção desses mecanismos de controle, visto que, a interpretação dos padrões e sequências de barras, cujas as leitoras eletrônicas decodificam até chegar a algarismos, que por fim, ainda chegarão a uma sequência lógica matemática que identifica produto a produto, é fruto do aprimoramento desses estudos.

Para que seja realizada a leitura de um código de barras, o leitor óptico afere a espessura e cor de uma sequência de quatro barras associando-as a uma sequência de sete dígitos binários. Há três blocos de barras um pouco maiores que não são lidos pelo aparelho óptico e possuem a finalidade de dividir os campos do código de barras, e são denominados como lado esquerdo e lado direito.

Cada dígito de 0 a 9 possui uma sequência referente aos sete dígitos binários. Especificamente, o lado esquerdo possui duas representações diferentes dependendo da quantidade par ou ímpar de algarismos "uns". Isso tornou-se necessário para que um mesmo leitor óptico conseguisse realizar leituras nos sistemas UPC e EAN-13, visto que, o primeiro usa 12 dígitos e o segundo usa 13.

Pode-se estabelecer que o símbolo 0 represente uma listra branca fina, o símbolo 00 uma listra branca média, 000 uma listra grossa e 0000 uma listra muito grossa. Do mesmo modo, o símbolo 1 representaria uma listra preta fina e, 11, 111 e 1111, listras média, grossa e muito grossa. Essas sequências de 0 e 1 podem ser convertidas em números de 0 a 9. Como por exemplo, o número 7, o primeiro do código na Figura 1 é representado pela sequência 0101011.

Conforme Oliveira (2017) reforça:

> 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.

O código de barras do tipo EAN-13 é formado por 13 algarismos e é universalmente utilizado. Este código usa a congruência de 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, sendo o 13º algarismo chamado de algarismo de controle. Segue abaixo – quadro 3 – ilustração de tabela da sequência binária de dígitos no sistema EAN-13:

Os números do lado esquerdo são dependentes da quantidade par ou ímpar de algarismos "uns" para serem identificados, e partindo dessa classificação é gerado o primeiro algarismo do código de barras, seguindo a sequência, conforme o quadro abaixo ilustrado – quadro 4:

QUADRO 3: Ilustração da sequência binária de dígitos no sistema EAN-13

Dígito	Lado Esquerdo (Ímpar)	Lado Esquerdo (Par)	Lado Direito
0	0001101	0100111	1110010
1	0011001	0110011	1100110
2	0010011	0011011	1101100
3	0111101	0100001	1000010
4	0100011	0011101	1011100
5	0110001	0111001	1001110
6	0101111	0000101	1010000
7	0111011	0010001	1000100
8	0110111	0001001	1001000
9	0001011	0010111	1110100

Fonte: (ESQUINCA, 2013)

QUADRO 4: Ilustração da sequência geradora do primeiro dígito no sistema EAN-13

Dígito Inicial	1º	2º	3º	4º	5º	6º
0	Ímpar	Ímpar	Ímpar	Ímpar	Ímpar	Ímpar
1	Ímpar	Ímpar	Par	Ímpar	Par	Par
2	Ímpar	Ímpar	Par	Par	Ímpar	Par
3	Ímpar	Ímpar	Par	Par	Par	Ímpar
4	Ímpar	Par	Ímpar	Ímpar	Par	Par
5	Ímpar	Par	Par	Ímpar	Ímpar	Par
6	Ímpar	Par	Par	Par	Ímpar	Ímpar
7	Ímpar	Par	Ímpar	Par	Ímpar	Par
8	Ímpar	Par	Ímpar	Par	Par	Ímpar
9	Ímpar	Par	Par	Ímpar	Par	Ímpar

Fonte: (ESQUINCA, 2013)

Partindo desta breve explicação, nos parágrafos seguintes será apresentada uma demonstração de como o código EAN-13 é constituído e os passos para a obtenção do algarismo de controle.

Seja a sequência $(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13})$ a representação dos 13 dígitos de um código EAN-13. onde $(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13})$ são os doze primeiros dígitos e a_{13}) o dígito de verificação do código EAN-13. para encontrar o dígito de verificação basta seguir os seguintes passos:

1º Passo: Montar a sequência com os 12 algarismos do código respeitando a seguinte ordem.

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

2º Passo: Multiplicar os termos de posições respectivas da sequência do passo anterior pela seguinte sequência:

$(1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3)$

3º Passo: Determinar a soma S somando os produtos do passo anterior.

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

4º Passo: Encontrar a_{13} usando congruência modular, $S + a_{13} \equiv 0 \mod 10$ Note que a_{13} é um algarismo que somado a S é um múltiplo de 10.

Exemplo 4.2.1: Observe na prática.

Figura 3: Código EAN-13 sem o último algarismo

Fonte: Google imagens (modificado para o exemplo)

Solução:

1º Passo: Montar a sequência com os 12 algarismos do código respeitando a seguinte ordem.

$(7, 8, 0, 9, 8, 3, 4, 2, 3, 4, 5, 6)$

2º Passo: Multiplicar os termos de posições respectivas das sequências:

$(7, 8, 0, 9, 8, 3, 4, 2, 3, 4, 5, 6) \cdot (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3)$

$(7 \cdot 1 + 8 \cdot 3 + 0 \cdot 1 + 9 \cdot 3 + 8 \cdot 1 + 3 \cdot 3 + 4 \cdot 1 + 2 \cdot 3 + 3 \cdot 1 + 4 \cdot 3 + 5 \cdot 1 + 6 \cdot 3)$

3º Passo: Determinar a soma S somando os produtos do passo anterior.

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

$S = 123$

4º Passo: Encontrar a_{13} usando congruência modular, $S + a_{13} \equiv 0 \mod 10$.

Sabendo que $S = 123$ tem-se: $123 + a_{13} \equiv 0 \mod 10$.

Logo, $a_{13} = 7$, pois $130 \equiv 0 \mod 10$.

De fato como pode-se notar no código EAN-13 completo abaixo o dígito de veificação é o algarismo 7.

Atualmente, códigos de barras são utilizados não só em produtos, como também em crachás de identificação ou pulseiras, permitindo o controle do fluxo de pessoas em determinados ambientes, além de existir outros diversos outros modelos de códigos de barras, presente em vários seguimentos. Dessa maneira, concluímos que, o uso desse recurso acelera processos físicos por meio dos recursos computacionais e de cálculos numéricos.

Figura 4: Código EAN-13 (completo)

Fonte: Google imagens

4.3 Cadastro de Pessoa Física - CPF

O Cadastro de Pessoa Física – CPF – no Brasil é constituído por 11 dígitos, sendo os dois últimos separados por hífen e com características de dígitos de controle, ou verificação determinados com aplicação da noção de congruência. Para ilustrar, a figura 7 nos mostra um esquema que organiza o que cada combinação numérica representa:

Figura 5: Descrição dos Dígitos do CPF

Fonte: Clube de Matemática da OBMEP

Na ilustração acima percebemos que os 8 primeiros dígitos são números bases já definidos pela Receita Federal, o nono número faz referência a região que foi emitida a documentação – números de 0 à 9, ficando alguns estados brasileiros com números iguais, já que possuímos 27 estados já somando com o Distrito Federal – DF , ainda ficando os dois últimos números como dígitos de verificação contra fraudes.

Na figura 8 temos o mapa do CPF por região fiscal onde o 9º dígito do CPF indica o estado em que o documento foi emitido e tem as seguintes identificações:

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

Figura 6: Região Fiscal Emissora do CPF

Fonte: Google imagens

Seja a sequência $(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 - a_{10}, a_{11})$ a representação dos 11 dígitos de um C.P.F. onde $(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9)$ são os noves primeiros dígitos e $a_{10}, a_{11})$ os dígitos de verificação do C.P.F. para encontrar os dígitos de verificação vamos dividir em duas etapas:

1º Etapa: Calculando o a_{10}, penúltimo dígito:

Multiplique a sequência $(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9)$ respectivamente pelos números $(1, 2, 3, 4, 5, 6, 7, 8, 9)$, depois some os noves produtos obtendo $S1$, isto é, $S1 = a_1 \cdot 1 + a_2 \cdot 2 + a_3 \cdot 3 + a_4 \cdot 4 + a_5 \cdot 5 + a_6 \cdot 6 + a_7 \cdot 7 + a_8 \cdot 8 + a_9 \cdot 9$, Daí a_{10} será o resto da divisão de $S1$ por 11 (caso seja 10, adote $a_{10} = 0$).

2º Etapa: Calculando o a_{11}, último dígito:

Agora com 10 dígitos conhecidos da sequência: $(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10})$ de forma análoga, multiplique os termos $(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10})$ respectivamente pelos números $(0, 1, 2, 3, 4, 5, 6, 7, 8, 9)$ e some todos produtos obtendo $S2 = a_1 \cdot 0 + a_2 \cdot 1 + a_3 \cdot 2 + a_4 \cdot 3 + a_5 \cdot 4 + a_6 \cdot 5 + a_7 \cdot 6 + a_8 \cdot 7 + a_9 \cdot 8 + a_{10} \cdot 9$, Assim a_{11} será o resto da divisão de $S2$ por 11. Utilizando a congruência modular podemos denotar os dígitos de controle da seguinte forma:

$$S1 - a_{10} \equiv 0 \bmod 11 \text{ e } S2 - a_{11} \equiv 0 \bmod 11$$

Exemplo 4.3.1: Considerando o C.P.F. 041.530.823−XW, calcule os dígitos de verificação X e W.

Solução: Dividindo o problema em duas etapas tem-se:

1º Etapa: Calcular o penúltimo dígito a_{10} que é o primeiro dígito de verificação, o a_{10} =X:

Multiplicando a sequência $(0, 4, 1, 5, 3, 0, 8, 2, 3)$ respectivamente pelos números

$(1, 2, 3, 4, 5, 6, 7, 8, 9)$ e depois somando os noves produtos obtemos $S1$,ou seja $S1 = 0 \cdot 1 + 4 \cdot 2 + 1 \cdot 3 + 5 \cdot 4 + 3 \cdot 5 + 0 \cdot 6 + 8 \cdot 7 + 2 \cdot 8 + 3 \cdot 9$. conclui-se assim que $S1 = 145$. como a_{10} é o resto da divisão de 145 por 11 tem-se que $145 \equiv 2 \bmod 11$. portanto $a_{10} = 2$ ou seja X= 2

2º Etapa: Calculando o último dígito a_{11} que é o úlltimo dígito verificador o $a_{11=}$W:

Agora com 10 dígitos conhecidos da sequência tem-se: $(0, 4, 1, 5, 3, 0, 8, 2, 3, 2)$ de forma análoga, multiplique os termos $(0, 4, 1, 5, 3, 0, 8, 2, 3, 2)$ respectivamente pelos números $(0, 1, 2, 3, 4, 5, 6, 7, 8, 9)$ e some todos produtos obtendo $S2 = 0 \cdot 0 + 4 \cdot 1 + 1 \cdot 2 + 5 \cdot 3 + 3 \cdot 4 + 0 \cdot 5 + 8 \cdot 6 + 2 \cdot 7 + 3 \cdot 8 + 2 \cdot 9$, conclui-se assim que $S2 = 137$. como a_{11} é o resto da divisão de 137 por 11 tem-se que $137 \equiv 5 \bmod 11$. portanto $a_{11} = 2$ ou seja W= 5

Logo, os dígitos de verificação procurados são: 2 e 5, completando assim a numeração do C.P.F. de dígitos $041.530.823 - 25$.

Exemplo 4.3.2: Considerando o C.P.F. 068.047.675−XW, calcule os dígitos de verificação X e W.

Solução: Dividindo o problema em duas etapas tem-se:

1º Etapa: Calcular o penúltimo dígito a_{10} que é o primeiro dígito de verificação, o a_{10} =X:

Multiplicando a sequência $(0, 6, 8, 0, 4, 7, 6, 7, 5)$ respectivamente pelos números $(1, 2, 3, 4, 5, 6, 7, 8, 9)$ e depois somando os noves produtos obtemos $S1$,ou seja $S1 = 0 \cdot 1 + 6 \cdot 2 + 8 \cdot 3 + 0 \cdot 4 + 4 \cdot 5 + 7 \cdot 6 + \cdot 7 + 7 \cdot 8 + 5 \cdot 9$. conclui-se assim que $S1 = 241$. como a_{10} é o resto da divisão de 241 por 11 tem-se que $241 \equiv 10 \bmod 11$. Nesse caso vale a observação feita na explicação acima e portanto $a_{10} = 0$ ou seja X= 0

2º Etapa: Calculando o último dígito a_{11} que é o úlltimo dígito verificador o $a_{11=}$W:

Agora com 10 dígitos conhecidos da sequência tem-se: $(0, 6, 8, 0, 4, 7, 6, 7, 5, 0)$ de forma análoga, multiplica-se os termos $(0, 6, 8, 0, 4, 7, 6, 7, 5, 0)$ respectivamente pelos números $(0, 1, 2, 3, 4, 5, 6, 7, 8, 9)$ e some todos produtos obtendo $S2 = 0 \cdot 0 + 6 \cdot 1 + 8 \cdot 2 + 0 \cdot 3 + 4 \cdot 4 + 7 \cdot 5 + 6 \cdot 6 + 7 \cdot 7 + 5 \cdot 8 + 0 \cdot 9$, conclui-se assim que $S2 = 182$. como a_{11} é o resto da divisão de 182 por 11 tem-se que $182 \equiv 6 \bmod 11$. portanto $a_{11} = 6$ ou seja W= 6

Logo, os dígitos de verificação procurados são: 0 e 6, completando assim a numeração do C.P.F. de dígitos $068.047.675 - 06$.

4.4 Congruência Modular no Ensino Fundamental

Uma das grandes preocupações dos professores de matemática da educação básica está relacionado a aceitação dos conteúdos estudados. É muito comum o professor ser questionado sobre qual a utilidade daquele conteúdo, por isso existe uma grande preocupação em existir sempre uma contextualização. A ausência de metodológias que aproximem os conteúdos com aplicações no cotidiano acaba desmotivando grande parte dos alunos.

A congruência modular é um conceito matemático fascinante que pode ser introduzido com sucesso no ensino fundamental, enriquecendo a compreensão dos alunos sobre números e operações aritméticas. Esta abordagem pedagógica permite explorar de forma prática e interessante propriedades dos números inteiros, além de fornecer uma base sólida para o desenvolvimento de habilidades matemáticas mais avançadas. Neste contexto, exploraremos a importância da congruência modular no ensino fundamental anos finais, suas aplicações práticas e como pode ser integrada de forma eficaz no currículo escolar.

A introdução da congruência modular no ensino fundamental pode ser feita de forma gradual e acessível aos alunos, começando com conceitos básicos e avançando conforme o desenvolvimento cognitivo de cada grupo. Os alunos podem começar explorando a congruência com módulos pequenos, como 2, 3 ou 4, e gradualmente progredir para módulos maiores à medida que adquirem mais familiaridade com o conceito. Isso permite que os alunos desenvolvam uma compreensão sólida dos fundamentos da congruência modular antes de se aventurarem em aplicações mais avançadas. (GROSS et al., 2020)

Um dos aspectos mais empolgantes da congruência modular é suas aplicações práticas em diversas áreas, desde a matemática pura até a criptografia e a teoria dos jogos. Por exemplo, na matemática pura, a congruência modular é amplamente utilizada para estudar padrões e propriedades dos números inteiros, como o Teorema de Euler ou o Pequeno Teorema de Fermat. Na criptografia, a congruência modular desempenha um papel fundamental na garantia da segurança das comunicações digitais, sendo a base de algoritmos como o RSA, amplamente utilizados na proteção de dados sensíveis. (COUTINHO et al., 2021)

Além disso, a congruência modular pode ser explorada de forma interdisciplinar, integrando-se com outras disciplinas, como ciência da computação, física e até mesmo música. Por exemplo, na ciência da computação, a congruência modular é usada em algoritmos de hash para garantir a integridade de dados e em algoritmos de geração de números pseudoaleatórios. Na física, é usada para modelar fenômenos periódicos, como as órbitas dos planetas ao redor do sol. E na música, é usada para criar escalas musicais e padrões rítmicos. (SILVA, 2021)

A introdução da congruência modular no ensino fundamental não apenas enriquece a compreensão dos alunos sobre matemática, mas também promove o desenvolvimento de habilidades cognitivas essenciais, como pensamento crítico, resolução de problemas e raciocínio lógico. Ao explorar padrões numéricos e propriedades dos números inteiros, os alunos são desafiados a pensar de forma abstrata e a aplicar conceitos matemáticos em contextos do mundo real.

Ao apresentar aos alunos um conteúdo com várias possibilidades de aplicações, servirá como estímulo para aceitação do mesmo e a desmistificação de que a matemática, além de difícil, tem pouca aplicabilidade.

A curiosidade dos alunos é um fator positivo e poder ser visto como vantagem, pois a partir dela que surge a motivação para a aprendizagem, conforme Lorenço preceitua e ainda 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).

O conhecimento da teoria de congruência modulares apresenta uma vasta possibilidade de aplicações de problemas por meio do conteúdo em varias áreas. Podemos relacionar o tema com aplicações envolvendo: criptográfia, código de barras, CPF, RG,cartão de crédito, calendários, relógios, etc. "É um tema bastante atual e que pode ser trabalhado já nas classes do Ensino Fundamental e gerador de excelentes oportunidades de contextualização no processo de ensino-aprendizagem de matemática." (SÁ, 2015, p.8)

Em verdade, a matemática sempre estará presente em diversos pontos do cotidiano, seja as pessoas sabendo o básico ou não, ela sempre está em diversos aspectos. A sala de aula em si é um espaço de crescimento e discussão de diversos temas, e geram expectativas diferentes em cada aluno, pois cada um carrega uma particularidade dentro do seu próprio processo de aprendizagem. Portanto, a depender de como temas considerados mais difíceis são tratados, estes além de uma melhor aceitação, podem gerar curiosidade, que é outro aspecto muito importante para o entendimento e aprofundamento.

4.5 Utilização de Tecnologia na Educação Matemática

A utilização de tecnologia na educação matemática tem se tornado cada vez mais relevante e difundida nos últimos anos. Com o avanço tecnológico e a crescente integração da tecnologia na vida cotidiana, é natural que seu uso também se expanda no contexto educacional, incluindo o ensino e aprendizagem da matemática. (RODRIGUES; GONZAGA, 2022)

Nesse sentido, a tecnologia oferece uma série de recursos e ferramentas que podem enriquecer o processo de ensino e aprendizagem, tornando-o mais dinâmico, interativo e acessível. Desde softwares específicos até aplicativos para dispositivos móveis, há uma ampla gama de opções disponíveis para auxiliar os educadores no ensino da matemática.

Uma das principais vantagens da utilização da tecnologia na educação matemática é a possibilidade de tornar os conceitos abstratos mais concretos e visuais. Por meio de softwares de geometria dinâmica, por exemplo, os alunos podem explorar figuras geométricas, realizar construções e visualizar propriedades de forma interativa, o que facilita a compreensão e a internalização dos conceitos. (NUNES, 2020)

Além disso, a tecnologia permite uma maior personalização do ensino, adaptando-se às necessidades individuais de cada aluno. Com o uso de softwares educacionais, é possível oferecer exercícios e atividades que se adequem ao nível de conhecimento e ao ritmo de aprendizagem de cada estudante, proporcionando uma experiência de ensino mais personalizada e eficaz. (KASAHARA; DE SÁ, 2023)

Outro aspecto relevante da utilização da tecnologia na educação matemática é a promoção da colaboração e do trabalho em equipe. Através de plataformas online e ferramentas de comunicação, os alunos podem compartilhar ideias, discutir soluções para problemas e colaborar em projetos matemáticos, o que estimula o desenvolvimento de habilidades sociais e cognitivas. (RUSSO et al., 2024)

Além disso, a tecnologia oferece a oportunidade de diversificar as estratégias de ensino, tornando-o mais atrativo e envolvente para os alunos. Jogos educacionais, simulações interativas e vídeos explicativos são apenas algumas das formas pelas quais a tecnologia pode ser incorporada às aulas de matemática, tornando o aprendizado mais lúdico e interessante. (IDEM, 2022)

No entanto, é importante ressaltar que a utilização da tecnologia na educação matemática deve ser feita de forma consciente e planejada. É fundamental que os educadores compreendam as potencialidades e limitações das ferramentas tecnológicas disponíveis, bem como saibam como integrá-las de maneira eficaz ao currículo escolar. (RODRIGUES; GONZAGA, 2022)

Cabe ao professor orientar os alunos na utilização das tecnologias, estimular o pensamento crítico e a reflexão sobre os conteúdos estudados, e promover atividades que explorem tanto os recursos tecnológicos quanto os métodos tradicionais de ensino. (NUNES, 2020)

A integração de tecnologias digitais na educação matemática tem ganhado destaque, especialmente no que se refere ao uso de ferramentas como calculadora de resto para melhorar a compreensão de conceitos complexos como a congruência modular. Ferramentas tecnológicas, como a calculadora de resto, podem simplificar o aprendizado de conceitos matemáticos avançados.

Elas permitem aos estudantes explorar e visualizar esses conceitos de maneira interativa, o que pode melhorar a compreensão e o engajamento (Borba; Penteado, 2019). Os autores argumentam que o uso de tecnologia na educação matemática transforma o processo de aprendizagem, tornando-o mais dinâmico e acessível, especialmente para

conceitos abstratos como a congruência modular.

Estudos têm mostrado que a integração de ferramentas digitais na matemática escolar pode levar a melhorias significativas no desempenho acadêmico dos alunos. A tecnologia facilita a experimentação e a resolução de problemas de forma mais eficiente e intuitiva (Heid; Blume, 2008). Os autores destacam que a tecnologia não apenas auxilia no entendimento de conceitos matemáticos, mas também contribui positivamente para o desempenho geral dos alunos, uma vez que estimula formas de pensamento mais críticas e analíticas (RODRIGUES; GONZAGA, 2022)

A integração da tecnologia na educação matemática, especialmente através do uso de ferramentas como a calculadora de restos, representa um avanço significativo na forma como os conceitos matemáticos são ensinados e aprendidos. A congruência modular, um tópico complexo e abstrato, é um exemplo de como a tecnologia pode facilitar o aprendizado, tornando-o mais acessível e compreensível para os estudantes (NUNES, 2020).

O uso de calculadoras de restos no estudo da congruência modular permite que os alunos visualizem e manipulem os números de maneira mais eficaz. Esta abordagem prática ajuda a desmistificar um conceito que, de outra forma, poderia parecer distante e teórico. O uso de tecnologias informáticas é discutido no âmbito na matemática desde a década de 80, conforme Borba (2023) nos diz:

> Nos anos 1980 o uso de calculadoras simples e científicas e de computadores já era discutido em educação matemática. Durante essa fase, expressões como "tecnologias informáticas"(TI) ou tecnologias computacionais começaram a ser utilizadas pelas pessoas para se referirem ao computador ou software, por exemplo. BORBA, 2023, p. 26

Borba e Penteado (2019) destacam inclusive esse aspecto metodológico como "Zona de Conforto e Zona de Risco", pois as atividades investigativas propostas em sala de aula como uso de TI - tecnologias informáticas – possuem caráter aberto, buscando visualizar diversas soluções para um mesmo problema, mesmo isso não se encaixando com a já formada "imagem da Matemática", colocada como ciência exata, de maneira absoluta.

Inclusive as TI podem apresentar funcionamento bom ou ruim, a depender do operador, pois os alunos podem saber utilizar algumas funcionalidades de maneira mais aprimorada se comparar ao professor, a depender da geração e nível de atualização em que o profissional se encontra, colocando o professor em zona de risco, exigindo de certa forma uma dinamização do "poder" em sala de aula.

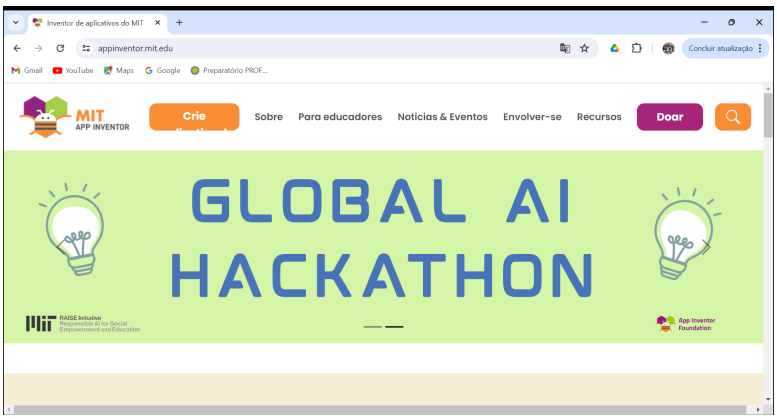
Além disso, a tecnologia oferece uma ponte entre o conteúdo matemático e suas aplicações práticas, mostrando aos alunos como a matemática está integrada em diversos aspectos do mundo real, desde a criptografia até a resolução de problemas cotidianos.

O professor que se encontra na sua zona de conforto, trabalhando com métodos de uma matemática exata, de uma única solução para cada problema, e não fazendo uso de TI, de certa maneira não busca entrar na sua zona de risco, já que este não deseja mudar sua metodologia tradicional de ensino de matemática, e precisar lidar com métodos tecnológicos que talvez os alunos estejam mais familiarizados, por exemplo.

A adoção de ferramentas tecnológicas no ensino de matemática também reflete uma mudança no papel do educador, que passa a ser um facilitador do processo de aprendizagem. Isso incentiva uma abordagem mais colaborativa e exploratória na sala de aula, onde os alunos são encorajados a investigar e descobrir por si mesmos, construindo assim uma compreensão mais profunda e duradoura dos conceitos.

4.6 MIT App Inventor

Figura 7: Página Inicial do Site



Fonte: Pesquisa 2024

O MIT App Inventor é uma plataforma de programação visual e intuitivo que permite a todos – até mesmo crianças – criar aplicativos totalmente funcionais para telefones Android, iPhones e tablets Android/iOS. Aqueles que são novos no MIT App Inventor podem ter um primeiro aplicativo simples instalado e funcionando em menos de 30 minutos. E mais, nossa ferramenta baseada em blocos facilita a criação de aplicativos complexos e de alto impacto em um tempo significativamente menor do que os ambientes de programação tradicionais. O projeto MIT App Inventor busca democratizar o desenvolvimento de software, capacitando todas as pessoas, especialmente os jovens, a passarem do consumo de tecnologia para a criação de tecnologia.

Uma pequena equipe de funcionários e estudantes do MIT CSAIL, liderada pelo professor Hal Abelson, forma o núcleo de um movimento internacional de inventores. Além de liderar a divulgação educacional em torno do MIT App Inventor e de realizar pesquisas sobre seus impactos, essa equipe principal mantém o ambiente de desenvolvimento de aplicativos on-line gratuito que atende a mais de 6 milhões de usuários registrados.

Os programas de codificação baseados em blocos inspiram o empoderamento intelectual e criativo. O MIT App Inventor vai além disso para fornecer capacitação real para que as crianças façam a diferença – uma maneira de alcançar um impacto social de valor imensurável para suas comunidades. Na verdade, os inventores de aplicativos na escola e fora dos ambientes educacionais tradicionais se uniram e fizeram exatamente isso.

De acordo com o CSAIL (Computer Science and Artificial Intelligence Laboratory), laboratório de criação do Instituto de Tecnologia de Massachusetts (MIT), a ferramenta já apresenta mais de atualmente o site conta com mais de um milhão de visitantes únicos mensais de 195 países criando coletivamente quase 30 milhões de aplicativos, o MIT App Inventor está mudando a forma como o mundo cria aplicativos e a forma como as crianças aprendem sobre computação.

Uma das principais características do MIT App Inventor é sua interface gráfica de arrastar e soltar, que permite aos usuários construir aplicativos visualmente, montando blocos de código em vez de escrever linhas de código tradicionais. Esses blocos representam funcionalidades como botões, textos, sensores, operações lógicas e muito mais, facilitando a construção e compreensão do aplicativo.

O MIT App Inventor oferece uma variedade de componentes e recursos prontos para uso, incluindo integração com sensores do dispositivo, acesso à internet, banco de

dados local, multimídia, entre outros. Isso permite aos usuários criar uma ampla gama de aplicativos, desde jogos simples até aplicativos educacionais e utilitários.

Além disso, o App Inventor oferece suporte a recursos avançados, como conectividade com dispositivos externos, integração com APIs web e publicação de aplicativos na Google Play Store.

Uma das grandes vantagens do MIT App Inventor é seu foco na educação. Ele é frequentemente utilizado em escolas e cursos introdutórios de programação para ensinar conceitos básicos de desenvolvimento de aplicativos de uma forma prática e envolvente.

Em resumo, o MIT App Inventor é uma ferramenta poderosa que torna a criação de aplicativos móveis acessível a uma ampla audiência, promovendo a aprendizagem e a criatividade na área da tecnologia.

5 RESULTADOS E DISCUSSÕES

As próximas seções apresentam os resultados obtidos na etapa de intervenção pedagógica da pesquisa. São tratados os resultados obtidos do questionário diagnóstico, da integração tecnológica na realização das atividades propostas e no questionário final.

5.1 Questionário diagnóstico

O objetivo do questionário diagnóstico foi verificar se os 32 estudantes selecionados para participar da pesquisa tinham acesso à internet, se usavam o celular como principal ferramenta de acesso a internet, se usavam o celular para fins pedagógicos, investigar com que frequência eles usam ferramentas tecnológicas em sala de aula, questionar se nos últimos anos foi usado a calculadora como ferramenta educacional na escola e a dificuldade dos mesmo em aprender matemática.

Quando questionados sobre o acesso à internet em casa e quais dispositivos são usados com mais frequência. 100% dos entrevistados disseram usar internet em casa e o dispositivo mais utilizado é o smartphone. Isto confirma a expansão e popularidade dos serviços digitais com a difusão da Internet , cada casa tem um telefone e é mais comum utilizá-lo para acesso à internet do que qualquer outro dispositivo eletrônico.

A grande maioria dos alunos passam em média 3 horas ou mais conectados na internet e na sua maioria usam esse tempo diário pra navegar nas redes sociais e jogos *onlines*. Vale ressaltar que apesar de terem disponíveis gratuitamente vários meios educacionais e informativos os alunos quase não usam a internet para essa finalidade.

Ao serem questionados sobre o uso de dispositivos móveis 100% dos alunos responderam que nos últimos 4 anos não usaram o celular como ferramenta educacional na escola e grande maioria respondeu que nenhuma vez fez uso da calculadora em sala de aula a pedido do professor. Esse resultado comprova que a tecnologia para o ensino de matemática não está sendo aproveitada de maneira eficiente, uma vez que os alunos têm acesso a ela pelo celular, mas, em sala de aula, não é usada com o propósito educacional.

A BNCC propõe que os estudantes utilizem tecnologias, como calculadoras e planilhas eletrônicas, desde os anos iniciais do Ensino Fundamental, aumentando assim a possibilidade do uso de dispositivos móveis em sala de aula.

Sobre a aprendizagem em matemática cerca de mais 75% dos alunos afirmaram ter alguma dificuldades em aprender conteúdos de matemática. Isso é um alerta para refletirmos sobre as práticas docentes nos dias atuais.

Quando questionados sobre a ideia do uso de aplicativos em dispositivos móveis como ferramenta educacional dos 32 alunos entrevistados a grande maioria tem um pensamento positivo sobre essa prática. 16 alunos acharam a ideia boa, 8 acharam a ideia ótima, 7 acharam a ideia regular e 1 achou a ideia ruim.

Vejamos algumas justificativas de alunos sobre a ideia do uso de aplicativos em dispositivos móveis:

Aluno C: "É uma ideia boa, pois torna a aula mais atrativa."

Aluno D: "É uma ótima ideia porque foge um pouco das aulas tradicionais."

Aluno E: "Eu acho muito boa, pois pode ser o algo a mais pra deixar a matemática interessante."

Aluno F: "É uma boa ideia, porém se não for bem administrada pode prejudicar a aprendizagem."

Aluno G: "Gostei da ideia, achei boa, pois todos nós temos celular, daí ninguém vai ficar de fora do estudo."

Aluno H: "Eu acho regular, pode ser bom mas alguns alunos podem usar o celular pra outras finalidades."

5.2 O Aplicativo

Nesta seção apresentamos a ferramenta educacional, um software para dispositivos movéis, desenvolvida no intuito de auxiliar alunos da educação básica durante as aplicações do conteúdo de congruência modular.

Em um contexto histórico, as calculadoras gráficas revolucionaram a época em que se tornaram populares, pois já não era necessário o auxílio de um computador (algo imóvel), já que em vez dos alunos se deslocarem a um laboratório de informática, as calculadoras que eram levadas até as salas de aula, como nos informa Borba, Silva e Gadanidis, ainda concluindo que:

> Uma sala de aula, feita para trabalho em grupo, pode ter a lousa e as calculadoras gráficas como atores que facilitam a comunicação[...]Tal perspectiva permitia que os alunos associassem o movimento corporal às interfaces gráficas das calculadoras, rompendo com a tradição de imobilidade física na sala de aula. Dava um passo a mais na possibilidade de termos um "ambiente de aprendizagem multimodal"com gráficos, lousa, cadernos e movimentos compondo as possibilidades de expressão multimodal. (Borba; Silva; Gadanidis, 2023. p. 84.)

Portanto, um ambiente de aprendizagem multimodal quando criado, ele abre ainda mais portas. Sendo os comentários acima tecidos a respeito de calculadoras gráficas, porém, na nossa atualidade já tem algo ainda mais ao alcance de cada aluno e docente, que é o uso do celular e da rede mundial de computadores, e aproveitando desse recurso que frequentemente já está inserido em sala de aula, vem a busca por desenvolver um aplicativo que trata exclusivamente sobre a Divisão Euclidiana, ponto forte desse trabalho.

Com a ideia de propor uma dinâmica mais atrativa, interessante e que possa atrair a interação dos alunos nas aulas de matématica, desenvolvel-se um aplicativo movél uma calculadora modular. Está calculadora difere das demais pois a mesma apresenta o resto inteiro da divisão entre dois inteiros, o que torna ela bem útil para o objeto de estudo desse trabalho.

> A utilização de tecnologias móveis como laptops, telefones celulares ou tablets tem se popularizado consideravelmente nos últimos anos em todos os setores da sociedade. Muitos de nossos estudantes, por exemplo, utilizam a internet em sala de aula a partir de seus telefones para acessar plataformas como o Google. Eles também utilizam as câmeras fotográficas ou de vídeo para registrar momentos das aulas. Os usos dessas tecnologias já moldam a sala de aula, criando novas dinâmicas, e transformam a inteligência coletiva, as relações de poder (de Matemática) e as normas a serem seguidas nessa mesma sala de aula. (Borba; Silva; Gadanidis, 2023. p. 83.)

Dito isso, percebemos o quanto as tecnologias vieram para somar no ramo da matemática e em outras ciências, pois tudo está interligado. O aplicativo em si possui uma interface simples, de rápido entendimento, e apesar de parecer redundante – visto que praticamente todos os celulares possuem calculadora como uma ferramenta – este apresenta-se aos alunos de uma maneira diferente, já que antes de usar, precisa baixar na sessão de aplicativos, após o uso, ainda é perceptível o nome de cada elemento envolvido na divisão, reforçando o entendimento sobre alguns termos muito presentes na matemática.

De modo geral o objetivo principal é usar a calculadora de forma a relembrar a divisão Euclidiana e dos conceitos de congruência modular, afim de facilitar e agilizar as aplicações de problemas relacionados a criptográfia e dígitos de verificações.

O aplicativo foi batisado como **calculadora modular** o mesmo foi desenvolvido durante objeto de estudo desse trabalho no site do MIT inventor, é gratuito e de código

aberto, está disponivel pra cópia e *download* em:
https://gallery.appinventor.mit.edu/?galleryid=b9899702-2066-4776-86d3-02d20da821ce

Figura 8: Interface da calculadora modular

Fonte: Desenvolvido pelo autor 2023

Apesar de ter ficado evidente pelo o que foi exposto nas seções anteriores, vale ressaltar aqui a importância dos restos inteiros das divisões para a compreensão de congruência modular. Por esse motivo e pelas fortes tendências do uso de tecnológias em sala de aula, foi essencial o desenvolvimento de uma calculadora que apresentasse esses restos de forma clara e mais direta.

A calculadora apresenta na sua interface 2 botões que são os de **Calcular** e **Limpar**. Além de 4 campos em branco que representam: **Dividendo, Divisor/Módulo, Quociente e Resto**. Ao preencher os campos do dividendo e do módulo deve-se apretar o botão calcular para obter de forma automática o quociente e o resto dessa divisão. Ápos anotar as informações recomenda-se apertar o botão de limpar para recomeçar o processo limpando todos os campos.

Exemplo 5.1 Ao colocarmos no Dividendo 358, no Divisor 11 e apertar o botão **CALCULAR** teremos como resposta o Quociente 32 e o resto 6.

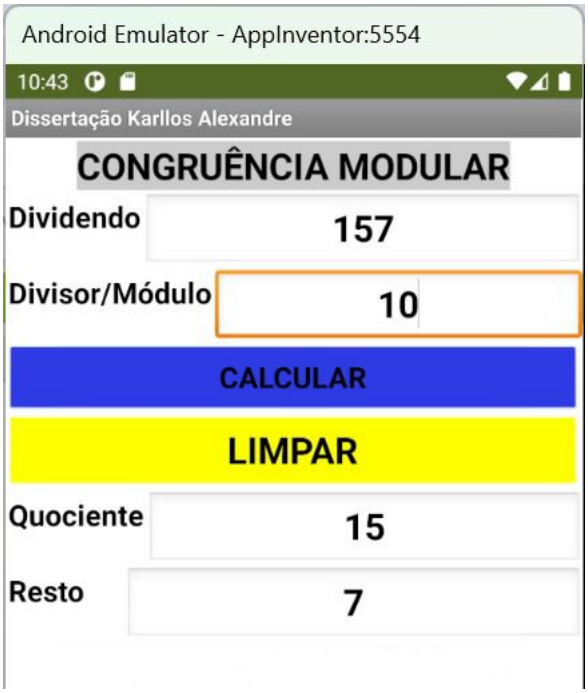
Com isso, essa função da calculadora modular facilita a compreensão tanto pra divisão Euclidiana quanto para congruência modular, Pois com os dados do Exemplo 5.1 temos:

Na divisão Euclidiana; $358 = 32 \cdot 11 + 6$
Na congruência modular; $358 \equiv 6 \mod 11$

Exemplo 5.2 Ao colocarmos no Dividendo 157, no Divisor 10 e apertar o botão **CALCULAR** teremos como resposta o Quociente 15 e o resto 7.

Veja o Exemplo 5.2 direto na tela:

Figura 9: Exemplo 5.2



Fonte: Desenvolvido pelo autor 2023

Com isso, essa função da calculadora modular facilita a compreensão tanto pra divisão Euclidiana quanto para congruência modular, Pois com os dados da imagem temos:

Na divisão Euclidiana; $157 = 10 \cdot 15 + 7$
Na congruência modular; $157 \equiv 7 \mod 10$

5.3 A Integração da Ferramenta Tecnológica

Nessa seção é relatado o uso da calculadora modular como a ferramenta digital que irá auxiliar os alunos na resolução de problemas envolvendo congruência modular durante os encontros realizados para essa pesquisa. Esta calculadora, conforme apresentada anteriormente, trata-se de um aplicativo desenvolvido para esse trabalho. O aplicativo calculadora modular foi disponibilizado via *link* no WhatsApp para os alunos, que rapidamente fizeram a instalação do mesmo.

Os encontros tiveram duração de 90 minutos cada e foram no total 7 encontros por turma, os mesmos aconteceram nos meses de setembro, outubro, novembro e dezembro de 2023, sempre as segundas-feiras no turno vespertino. Os seis primeiros encontros aconteceram em cada turma de forma separada e foram usados os planos de aulas elaborados pelo autor com base na BNCC e adaptado pois congruência modular não faz parte da grade curricular. No sétimo e último encontro, foi realizado uma atividade com as duas turmas juntas na mesma sala e por fim, foi aplicado o questionário final.

A congruência modular torna o conteúdo de divisibilidade como principal pré-requisito, conteúdo esse que faz parte do currículo a partir do $6^{\underline{o}}$ ano do ensino fundamental. Devido a dificuldade de alguns alunos em conceitos básicos, tornou-se necessário iniciar os encontros com aulas de nivelamento das turmas sobre os conceitos básicos e necessários para uma melhor compreensão do objeto de estudo, em seguida foi disponibilizado o aplicativo calculadora modular via *WhatsApp* para todos os alunos onde cada um facilmente realizou a instalação do mesmo em seus respectivos *smartphones*.

Após encerrar o nivelamento sobre divisibilidade e ensinar aos alunos como usar a calculadora modular, deu-se seguimento aos planos de estudos, no **primeiro e segundo** encontro foram estudados os seguintes conteúdos: Múltiplos e divisores de um número inteiro; Critérios de divisibilidade e Divisão Euclidiana. Os conteúdos foram abordados sempre na tentativa de instigar os conhecimentos já adquiridos pelos alunos.

Os principais objetivos nos dois primeiros encontros foram melhorar de forma geral o desempenho de cada turma na parte de divisibilidade dando ênfase na divisão Euclidiana e a apresentação da ferramenta tecnológica, pois esses dois tópicos são essenciais para o desenvolvimento desse trabalho. Os materiais utilizados nos encontros estão disponíveis nos apêndices D, E e F.

Problema proposto: Realize a seguinte divisão: $337 : 8$ e reescreva na forma Euclidiana, onde o dividendo = divisor $\cdot$ quociente + resto.

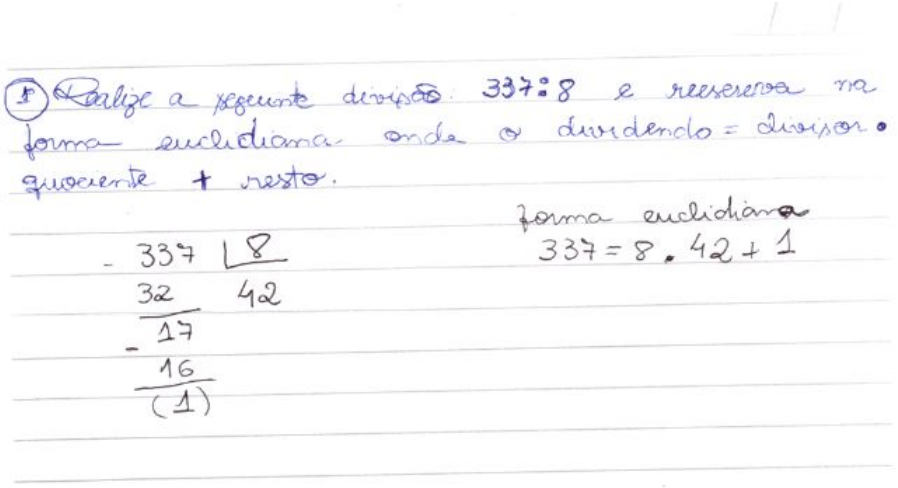
Comentário geral sobre o primeiro e o segundo encontro:

Nesse início do projeto, usou-se o quadro acrílico com principal método para nivelamento dos alunos, visto que, vários assuntos foram abordados afim de buscar a revisão dos mesmos. Feito isso e explanado de uma maneira Geral os focos principais desse projeto, deu-se início a metologia ativa, que busca a participação dos alunos, justamente com o uso do aplicativo da Calculadora Modular.

Fora observado que, grande parte dos alunos mostrou interesse justamente nesse tópico, pois a interação teve um aumento significativo por conta desse tipo de metodologia aliada ao uso da tecnologia por meio dos celulares pessoais, já que cada um podia ter individualmente o uso de uma calculadora eficiente para auxiliar na resolução dos problemas que seriam apresentados.

No **terceiro e no quarto** encontro foi introduzido os conceitos iniciais de congruência modular. Nessas aulas foram abordados os seguintes conteúdos: Inteiros congru-

Figura 10: Solução aluno A



Fonte: Pesquisa, 2023

Figura 11: Registro do primeiro encontro

Fonte: Pesquisa 2023

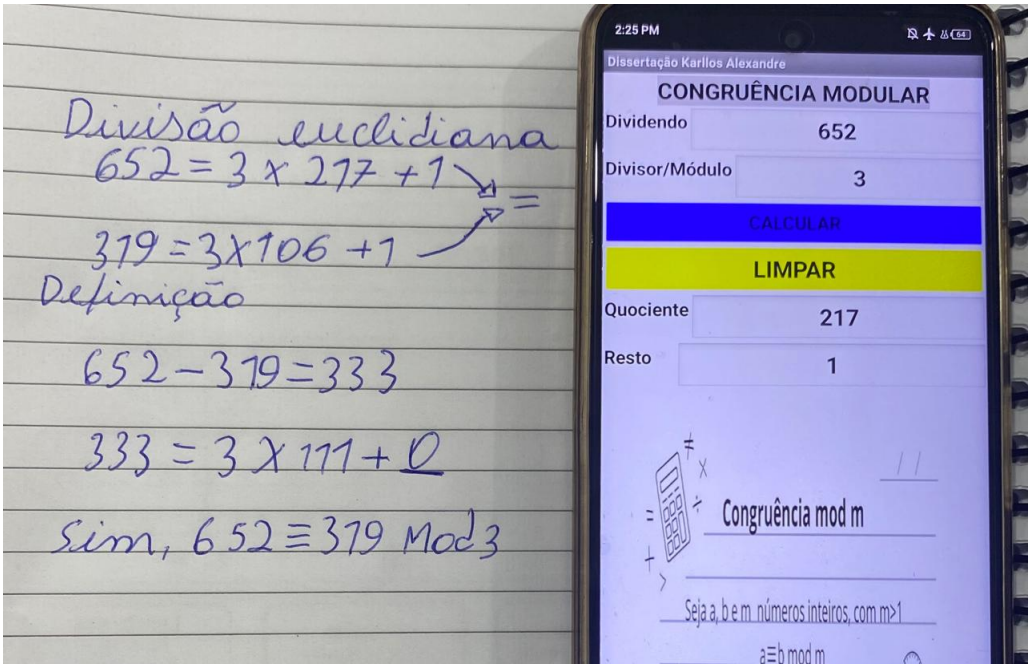
entes; Caracterização de inteiros congruentes; Propriedades das congruências e Aplicações iniciais de congruências. Durante essas aulas foi mostrada a definição de congruência modular, foi feita a comparação do uso da definição e o uso da divisão Euclidiana em problemas e durante a resolução dos problemas foi utilizado a calculadora modular.

Nesses encontros, também fora mostrado aos alunos a exemplificação do uso do conteúdo de congruência modular relacionado ao relógio, tornando o tema mais atraente uma vez que muitos alunos criam uma certa resistência aos conteúdos onde não conseguem ver aplicações.

Problema proposto: Com o auxílio da calculadora modular verifique se os números 652 e 319 são congruentes mod 3. Para fazer essa verificação use a divisão Euclidiana e a definição, em seguida faça uma comparação de qual método acha mais

eficiente para esse tipo de verificação.

Figura 12: Solução aluno B



Fonte: Pesquisa, 2023

Comentário geral sobre o terceiro e o quarto encontro:

Durante esses encontros foi apresentado aos alunos o conteúdo de congruência modular, conteúdo este nunca visto pelos mesmos, o que gerou várias dúvidas e questinamentos o que é completamente normal por se tratar de algo novo pra eles. No entanto todos estavam atentos pois precisavam compreender o assunto em questão para usar a calculadora modular de forma correta.

No final da aula foi possivél observar um bom desenvolvimento e interação das turmas durante a resolução de problemas. Cerca de 60% dos alunos estavam conseguindo resolver os problemas com o auxilio da calculadora modular, já os demais apresentaram em primeiro momento dificuldades em como relacionar o uso da calculadora com o conteúdo e alguns afirmaram que essa dificuldade se deu por não terem compreendido completamente o conteúdo.

Já no **quinto e no sexto** encontro foram trabalhados algumas das aplicações de congruência com o auxilio da calculadora modular. Nessas aulas foram abordados os seguintes assuntos: criptográfia atraves da cifra de César, a importância e como encontrar o dígito verificador do código de barras EAN-13, a importância e o como encontrar os dígitos verificadores no CPF. Para melhorar a contemplação dos assuntos após a explanação dos mesmos, os alunos focaram na resolução dos problemas usando o aplicativo em questão.

Durante esses encontros após a resolução das atividades os alunos formaram duplas, onde foi entregue a cada dupla um código de barras EAN - 13 e uma cédula de CPF cada um sem seus correscondentes dígitos de verificação, onde cada dupla deveria determinar corretamente os dígitos de verificação com o auxílio da calculadora modular.

Problema proposto: 1. Após as aulas de criptografia, João decidiu criptografar

Figura 13: Dígitos de verificação no CPF

Fonte: Pesquisa, 2023

uma frase usando a chave 10 e mandar para seu professor. Analise o quadro 5 abaixo e com o auxilio da calculadora modular decifre a frase que João mandou ao seu professor.

A frase: (14 - 04 10 - 22 - 24 14 - 02 - 03 - 04 - 13 - 10 - 01)

QUADRO 5: Problema proposto:1

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

Problema proposto: 2. Com o auxílio da calculadora modular, Encontrar os dígitos verificadores X e W no CPF cujo os números são:

123.456.789-XW

Comentário geral sobre o quinto e o sexto encontro:

O quinto encontro destinou-se inteiramente ao tema de criptografia, nessa aula foi destacado a importância da criptografia nos dias atuais e usamos a cifra de César combinada com diferentes chaves sempre relacionando a congruência para codificar e decodificar: palavras, frases e até mesmos textos. Tudo isso com o auxílio da calculadora modular.

Figura 14: Registro do uso da calculadora modular

Fonte: Pesquisa 2023

Nesse encontro foi possivél notar um grande interesse por parte dos alunos para conseguir decodificar as palavras. A utilização da cifra de César é frequentemente usada com a chave 3 o que não dificulta tanto os cálculos mas ao combinarmos com a chave 5 ou um pouco maior o uso da calculadora modular se mostrou essencial para auxíliar os alunos e agilizar o processo de decodificação.

Já o sexto encontro ficou reservado para ser abordado a questão dos dígitos de verificação. Nesse encontro foi explicado aos alunos a importância do dígito de verificaçao no código de barras e os dígitos de verificação no CPF, além disso foi mostrado aos alunos como encontrar esses dígitos usando congruência e fazendo o uso da calculadora modular.

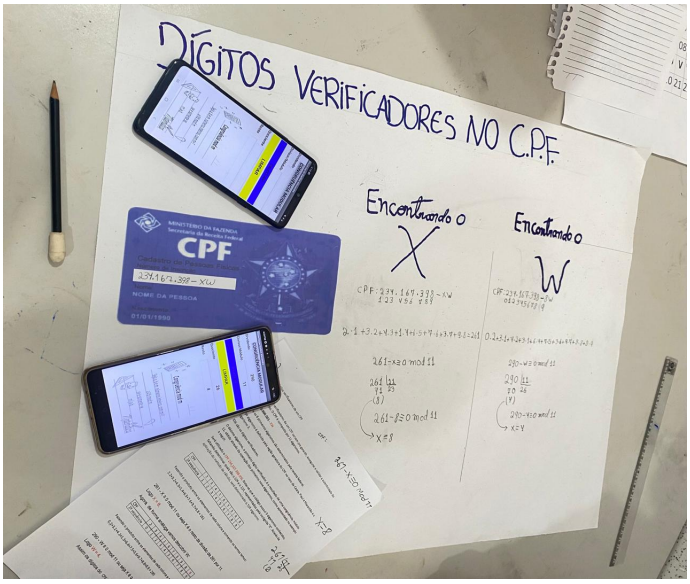
No **sétimo** e último encontro foi realizado uma Atividade com as duas turmas juntas 8º e 9º ano, o objetivo dessa última era analisar as aplicações de congruência modular sobre os dígitos de verificação no código de barras EAN-13 e C.P.F. com o auxílio da calculadora modular. Nesse encontro foi utilizado embalagens de produtos que fazem parte do nosso cotidiano (leite, café, açucar, sal, arroz e feijão) esses produtos tiveram o seu dígito de verificação que fica no seu código de barras ocultados para que os alunos encontrassem.

Decorrido uma parte do último encontro foi distribuido a cada aluno(a) uma cédula de CPF com exatamente 9 dígitos faltando assim justamente os dígitos vererificadores para que os alunos encontrassem individualmente. Na reta final do encontro os alunos foram separados em grupos para a produção de cartazes sobre o objeto de estudo e por fim foi entrege o questionário final.

Figura 15: Registro da Atividade Sobre Código de Barras

Fonte: Pesquisa, 2023

Figura 16: Registro da Atividade Sobre CPF



Fonte: Pesquisa, 2023

5.4 Questionário Final

No questionário final o objetivo foi a avaliar a oficina realizada, analisar o uso da calculadora modular, verificar se o estudo contribui para a aprendizagem dos alunos e o pensamento dos mesmos sobre a intregração de tecnologia através de aplicativos em dispositivos móveis.

01 – Como você avalia a oficina?

Em resultado dessa questão nenhum aluno avaliou a oficina como ruim ou péssima. Isso nos faz entender que a oficina foi relevante no ponto de vista dos participantes.

Além disso a maioria avaliou como ótima sendo 59% dos alunos, 25% dos alunos acharam boa e 16% dos alunos acharam regular.

O resultado indica que a oficina foi bem avaliada pelos alunos que participaram, já que nenhum aluno a avaliou como ruim ou péssimo. A maioria dos alunos avaliou a mesma como ótima, o que sugere que a oficina foi bem atrativa, interessante e proveitosa para a maioria deles. Além disso, um percentual significativo avaliou como boa, o que indica que alguns alunos tiveram uma experiência positiva. Já o percentual de alunos que avaliaram como regular pode indicar que alguns tiveram uma experiência mediana, mas ainda assim, não consideraram a oficina ruim. No geral, o resultado é foi positivo e sugere que a oficina foi bem aceita pelos alunos.

02 – Em relação a calculadora modular no celular, você acha que o uso da mesma é:

Sobre como usar o aplicativo calculadora modular os alunos por grande maioria tiveram facilidade em usar o mesmo. Cerca de 80% achou fácil o uso da calculadora e 20% achou regular. Isso mostra a facilidade dos alunos em aprender novidades tecnológicas.

03 - Com base na oficina, o uso da calculadora modular contribuiu para sua aprendizagem? Justifique.

Em resposta todos os alunos entrevistados afirmaram que sim. Sendo assim mais um ponto positivo para nosso objeto de estudo. O que nos mostra que podemos trazer propostas inovadoras para sala de aula.

Vejamos algumas justificativas para essa pergunta:

Aluno I: "Sim, ajudou a compreender a divisão com resto diferente de zero."

Aluno J: "Sim, facilitou bastante o entendimento sobre divisibilidade."

Aluno K: "Sim, ajudou a entender e ver quem é o resto da divisão."

04 – O que mais lhe chamou atenção ao usar a calculadora modular durante a oficina?

Aluno L: "A facilidade em reescrever a divisão na forma Euclidiana."

Aluno M: "O quociente da divisão sempre inteiro."

Aluno N: "Em encontrar o resto da divisão."

05 – Como você analisa a ideia de usar aplicativos em dispositivos móveis (smartphones, tablets, etc) como ferramenta de aprendizagem matemática? Justifique sua resposta.

A título de comparação a última questão desse questionário tinha o intuito de comparar o que já havia sido coletado antes da realização da oficina. De fato, repetir essa indagação no questionário final reforçou o entendimento de que os alunos são conscientes da importância que o uso da tecnologia traz para o ensino de matemática.

Nos primeiros resultados, antes da realização da oficina que inseriu a tecnologia com o aplicativo calculadora modular, os dados se mostraram distribuídos entre as opiniões ruim, regular, boa e ótima: 3% disseram que achavam ruim a ideia de utilizar dispositivos móveis nas aulas de Matemática para fins educativos, outros 22% achavam regular, 25% opinaram que a ideia era boa e 50% achavam ótima. Após ter passado

pela experiência de usar o aplicativo calculadora modular no smartphone nas aulas, esses números tiveram mudanças significativas, nenhum aluno permaneceu com a ideia de que utilizar dispositivos móveis em salas de aula para a aprendizagem dos conteúdos matemáticos era ruim ou regular, suas opiniões mudaram para boa ou ótima. Sendo que 65% responderam ótimo e os outros 35% boa.

Esses resultados indicam que muitos alunos estão interessados em usar ferramentas tecnológicas à sua disposição, especialmente os smartphones. Portanto , é viável e é importante que os professores utilizem essas ferramentas para contribuir com seu ensino. Compreender e aproveitar o conhecimento prévio dos alunos.

vejamos algumas justificativas para essa pergunta:

Aluno O: "É uma boa ideia, pois podemos usar o celular pra nos auxiliar na aprendizagem."

Aluno P: "É ótima, porque consigo me concentrar melhor com novidades."

Aluno Q: "É ótima, pois estamos com os celulares sempre a disposição e aprender algo novo é sempre bom."

Aluno R: "Ótima, porque torna a aula mais atrativa e inclui todos os alunos."

Diante dos dados colhidos nesse questionário, podemos compreender que a utilização do celular em sala de aula com responsabilidade e mediada pelo professor para fins pedagógicos é muito bem-vinda, uma vez que ele deixa de ser apenas um instrumento de distração e torna-se uma potencial ferramenta de aprendizagem. Também é possivel perceber com base nas resposta que os alunos enxergam a inserção de tecnologia nas aulas é como fugir do tradicional.

Uma das principais constatações da pesquisa foi o aumento do interesse dos alunos pela matemática após a integração de tecnologia sobre a teoria da congruência modular no ensino fundamental. Muitos alunos relataram que a abordagem prática e interativa da congruência modular os ajudou a compreender conceitos matemáticos complexos de forma mais clara e acessível. Além disso, os alunos demonstraram maior motivação para participar das atividades de matemática e estavam mais engajados durante as aulas.

6 CONSIDERAÇÕES FINAIS

Dada a situação atual da educação brasileira, observamos que os alunos carecem de motivação e que há insatisfação devido à incapacidade de conectar a teoria à prática. Os professores estão insatisfeitos com as diversas dificuldades que encontram em suas carreiras, a pesquisa mostra que a intregração entre os métodos tradicionais de sala de aula e o uso de tecnologia pode proporcionar aos alunos uma aprendizagem mais envolvente e eficaz.

Utilizar o aplicativo calculadora modular como ferramenta tecnologica em sala de aula teve uma grande relevância, pois o mesmo permitiu que os alunos usassem o aplicativo em seus *smartphones* para auxiliar no desenvolvimento das atividades matemáticas.

Durante a realização da pesquisa, foi possível perceber o aumento do interesse de vários estudantes durante os encontros. Também ficou claro que aumentou o número de alunos a participarem durante as aulas. Outro fator importante que se pode destacar é a inclusão de todos os alunos, pois até mesmo aqueles alunos que apresentam dificuldades em matemática se mostram ativos e participativos durante a realizaçao das atividades.

Por todo o exposto, têm-se na proposta deste trabalho constribuições significativas para um bom desenvolvimento do processo de ensino-aprendizagem de matemática nos anos finais do Ensino Fundamental, a saber: a) nova abordagem ao conteúdo de divisão já presente no currículo; b) uso de tecnologia aliada ao ensino; c) a teoria de congruências presente em praticamente todas as partes da pesquisa; d) a prática e aplicabilidade de um assunto que antes era visto só teoricamente; e) demonstração de outros modos resolução de problemas e preparação dos alunos para conteúdos mais avançados em Matemática.

Outrossim, deixamos claro que aqui não foram esgotadas todas as possibilidades de ensino da teoria de congruências ligada a integração de tecnologia com respeito às contribuições para o ensino fundamental ou mesmo para o Ensino Básico. Porém, foram destacadas aplicações relacionadas ao cotidiano e de maneira mais didática, visando destacar a presença da Matemática na vida dos discentes e com isso, instigar o interesse por conteúdos que são vistos como muitos dificeis.

Dado que as tecnologias de informação e comunicação estão cada vez mais presentes nos ambientes escolares e intimamente relacionados com a matemática, este estudo envolve a integração de software na prática docente. Contudo na parte pratica desse trabalho a calculadora modular contribuiu significativamente para auxiliar os alunos tanto na resolução das atividades quanto para a compreensão das aplicações de congruência modular.

Portanto, o ensino de congruência modular nos anos finais do ensino fundamental com a integração de tecnologia através do aplicativo calculadora modular, se mostrou eficiente, pois trouxe uma série de benefícios a realidade dos alunos que fizeram o uso do mesmo diretamente de seus *smartphones* como ferramenta educacional. Fazendo assim a ligação entre a participação ativa da grande maioria dos alunos e a inclusão de todos os alunos que com a integração da tecnologia responderam todas as atividades. Diante todo exposto podemos concluir que o uso da calculadora modular como ferramenta educaional mostrou impactos positivos, trazendo assim resultados satisfatórios.

Referências

ANDREWS, G. E. *Number theory*. [S.l.]: Courier Corporation, 1994.

BORBA, M. D. C.; PENTEADO, M. G. *Informática e educação matemática*. [S.l.]: Autêntica Editora, 2019.

BORBA, M. de C.; SILVA, R. S. R. da; GADANIDIS, G. *Fases das tecnologias digitais em Educação Matemática: sala de aula e internet em movimento*. [S.l.]: Autêntica Editora, 2023.

BOYER, C. B.; MERZBACH, U. C. *História da matemática*. [S.l.]: Editora Blucher, 2012.

BURN, R. P. Números e funções: Passos para análise. 2005.

CARVALHO, J. Z. d. S. et al. A aplicabilidade da criptografia no ensino de matemática no contexto da educação profissional. 2020.

COUTINHO, D. S. et al. , educação matemática e inclusão escolar: um olhar sobre as perspectivas e necessidades o aluno com deficiência intelectual. Universidade Federal Rural do Rio de Janeiro, 2021.

DENZIN, N. K.; LINCOLN, Y. S. *O planejamento da pesquisa qualitativa: teorias e abordagens*. [S.l.]: Artmed, 2006.

ESQUINCA, J. C. P. Aritmética: códigos de barras e outras aplicações de congruências. 2013.

FRAZ, J. N. Mil e uma cenas do processo de ensino e aprendizagem da matemática na modalidade a distância: representações sociais de professores de matemática envolvidos na trama da formação inicial. 2023.

FREITAS, C. L. d. et al. Formação de professores com software de geometria dinâmica: conhecimentos para a docência mediados por tecnologia. Universidade Federal do Pará, 2023.

GAUSS, C. F. *Disquisitiones arithmeticae auctore d. Carolo Friderico Gauss*. [S.l.]: in commissis apud Gerh. Fleischer, jun., 1801.

GODOY, A. S. Introdução à pesquisa qualitativa e suas possibilidades. *Revista de administração de empresas*, SciELO Brasil, v. 35, p. 57–63, 1995.

GROSS, G. F. S. et al. *Cultura digital frente às demandas das escolas do campo: a robótica educacional como possibilidade para o ensino de matemática*. Dissertação (Mestrado) — Universidade Tecnológica Federal do Paraná, 2020.

HEATH, T. L. e. o. Os treze livros dos elementos, vol. 3: Livros 10-13. 1908.

HUF, S. F. et al. Potencialidades da aprendizagem significativa por meio das tendências metodológicas em educação matemática: possíveis caminhos para o ensino e aprendizagem de matemática no 6º ano do ensino fundamental. Universidade Tecnológica Federal do Paraná, 2021.

IDEM, R. d. C. Compreensões sobre a resolução de problemas com tecnologias digitais na construção de padrões dinâmicos no scratch por estudantes do ensino fundamental. Universidade Estadual Paulista (Unesp), 2022.

KASAHARA, R. F. R.; SÁ, P. F. de. Estudos brasileiros sobre o ensino de vetores com experimentação em sala de aula no período de 2010-2021. *Revista Exitus*, v. 13, p. e023013–e023013, 2023.

LOURENÇO, P. *Aplicações da aritmética modular*. Tese (Doutorado) — Dissertação de mestrado. Universidade de Coimbra, 2011.

MELO, C. B. d. A matemática dos restos e o calendário gregoriano. 2014.

MONTANHER, J. F. Introdução da criptografia no ensino básico sob a óptica da aritmética modular. Universidade Estadual Paulista (Unesp), 2022.

NUNES, B. L. Uma proposta de utilização de exercícios de autocorreção com construções geométricas por meio da integração geogebra. 2020.

OLIVEIRA, C. Congruência modular e aplicações. 2017.

PISA, P. I. d. A. d. E. Divulgados os resultados do pisa 2022. disponível em: https://www.gov.br/inep/pt-br/assuntos/noticias/acoes-internacionais/divulgados-os-resultados-do-pisa-2022. acesso em: 27 de janeiro de 2024.

PONTES, E. A. S. A práxis do professor de matemática por intermédio dos processos básicos e das dimensões da aprendizagem de knud illeris. *Rebena-Revista Brasileira de Ensino e Aprendizagem*, v. 2, p. 78–88, 2021.

REIS, A. M. S. dos et al. *EDUCAÇÃO MATEMÁTICA ESCOLAR: Múltiplos Contextos & Abordagens de Ensino*. [S.l.]: Editora BAGAI, 2021.

RODRIGUES, M.; GONZAGA, S. Software geogebra nos processos formativos dos professores de matemática: estado do conhecimento das dissertações e teses no brasil. *Revista do Instituto GeoGebra Internacional de São Paulo*, v. 11, n. 2, p. 92–118, 2022.

RUSSO, A. M. et al. Propriedades da geometria plana exploradas por alunos do ensino fundamental com o uso do geogebra discovery. Pontifícia Universidade Católica de São Paulo, 2024.

SÁ, I. P. d. Aritmética modular e algumas de suas aplicações. 2020.

SANTOS, P. S. d. A. et al. Congruência e equações diofantinas: uma proposta para o ensino básico. Universidade Federal de Alagoas, 2013.

SILVA, R. A. Congruência modular no desenvolvimento da aprendizagem de matemática nos anos finais do ensino fundamental. UEMA, 2022.

SILVA, R. B. d. Educação matemática na perspectiva da educação inclusiva: vivências de professores do ensino fundamental. Universidade Federal de São Carlos, 2021.

SILVEIRA, J. P. C. *Aplicações de Criptografia Baseada em Identidade com Cartões de Identificação Eletrónica*. Tese (Doutorado) — Universidade da Beira Interior (Portugal), 2013.

VILAÇA, M. d. O. Robótica educacional de baixo custo no ensino e aprendizagem em uma perspectiva interdisciplinar: interfaces com a educação matemática. 2023.

ZAZKIS RINA E CAMPBELL, S. Divisibilidade e estrutura multiplicativa de números naturais: compreensão dos professores de formação inicial. 1996.

Apêndice A - Termo de consentimento livre e esclarecido

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO- (TCLE)

Prezados participantes,

Sou mestrando do Programa PROFMAT- UEMA e estou solicitando por meio deste TCLE sua autorização para o uso das respostas efetuadas no questionário a seguir , para produção dos dados que nortearão a elaboração do relatório da pesquisa "Congruência Modular Nos Anos Finais Do Ensino Fundamental Integração De Tecnologia Na Educação Matemática", desenvolvida por Karllos Alexandre Sousa Pereira sob orientação do professor Dr. Sergio Nolêto Turibus. Os dados obtidos poderão ser usados na dissertação como também, poderá constituir artigos científicos que serão apresentados em congressos e publicados em anais e periódicos científicos. O consentimento para a participação é uma escolha livre e voluntária, poderá ser interrompida a qualquer momento, caso você precise ou deseje. Para a garantia de sua privacidade, será mantido o sigilo em relação a quaisquer informações que possam vir a identificá-lo (a) e a instituição na qual desempenha sua atividade profissional. Em caso de dúvidas sobre os procedimentos aqui relacionados, você pode esclarecê-los com o pesquisador responsável: KARLLOS ALEXANDRE SOUSA PEREIRA. Em caso de concordância ou discordância, solicitamos que informe a seguir: Concordo ( ) ou Discordo ( ).

_____

Nome do Participante da Pesquisa

_____

Assinatura do Responsável pelo Participante da Pesquisa

_____

Pesquisador: Karllos Alexandre Sousa Pereira

Apêndice B – Questionário diagnóstico

Questionário diagnóstico

01 – Você tem acesso à internet em casa?

a) Não.
b) Sim.

02 – Qual dispositivo você costuma usar pra acessar a internet com maior frequência?

a) *Smartphone.*
b) *Tablet.*
c) Computador.
d) TV.
e) Não uso.

03 – Diariamente quanto tempo você usa internet?

a) 1 hora.
b) 2 horas.
c) 3 horas.
d) 4 horas.
e) Mais de 4 horas.

04 – Quais conteúdos você mais costuma acessar na internet?

a) Redes sociais.
b) Jogos.
c) Pesquisas escolares.
d) Trabalho.
e) Outro._____

05 – Sobre sua experiência com o uso de calculadoras na educação, quantas vezes você fez uso dessa ferramenta nas aulas:

a) Uma vez.
b) Duas vezes.
c) Três vezes.
d) Quatro vezes.
e) Nenhuma vez.

06 – Durantes suas aulas de matemática nos últimos 4 anos. Alguma vez foi solicitado o uso do *smartphone* em sala de aula como ferramenta educacional? (Calculadora, tradutor, pesquisas, aplicativos, etc)

a) Uma vez.
b) Duas vezes.
c) Três vezes.
d) Várias vezes.
e) Nenhuma vez.

07 – Você sente dificuldade na aprendizagem de conteúdos de matemática?

a) Sim.
b) Não.
c) Parcialmente.

08 – Como você analisa a ideia de usar aplicativos em dispositivos móveis (*smartphones, tablets*, etc) como ferramenta de aprendizagem matemática? Justifique sua resposta.

a) Ruim.
b) Regular.
c) Boa.
d) Ótima.

Apêndice C – Questionário final

Questionário final

01 – Como você avalia a oficina?

a) Péssima.
b) Ruim.
c) Regular.
d) Boa.
e) Ótima.

02 – Em relação a calculadora modular no celular, você acha que o uso da mesma é:

a) Fácil.
b) Regular.
c) Difícil.

03 – Com base na oficina, o uso da calculadora modular contribuiu para sua aprendizagem? Justifique.

a) Sim.
b) Não.

04 – O que mais lhe chamou atenção ao usar a calculadora modular durante a oficina?

05 – Como você analisa a ideia de usar aplicativos em dispositivos móveis (*smartphones, tablets*, etc) como ferramenta de aprendizagem matemática? Justifique sua resposta.

a) Ruim.
b) Regular.
c) Boa.
d) Ótima.

Apêndice D – Plano de aula (primeiro e segundo encontro)

PLANO DE ESTUDOS 1			
ALINHAMENTO MATEMÁTICO – Primeiro e Segundo Encontro			
TURMA: 8° e 9° ano	COMPONENTE CURRICULAR: MATEMÁTICA		
DATA:	TEMPO PREVISTO: 90 minutos cada encontro		
PROFESSOR: KARLLOS ALEXANDRE SOUSA PEREIRA			
CONTEÚDOS	**HABILIDADES**	**METODOLOGIA**	**AVALIAÇÃO**
-Algoritmo da divisão; -Múltiplos e divisores de um número inteiro; -Critérios de divisibilidade. -Divisão Euclidiana; -Teorema dos restos;	(EF07MA01) Resolver e elaborar problemas, de diversos contextos, com números naturais, envolvendo as noções de divisor e de múltiplo, podendo incluir máximo divisor comum ou mínimo múltiplo comum, por meio de estratégias diversas, sem a aplicação de algoritmos. (EF07MA11) Compreender e utilizar a multiplicação e a divisão de números inteiros, a relação entre eles e suas propriedades operatórias; (EF06MA05) Classificar números em primos e compostos e estabelecer por meio de investigação os critérios de divisibilidade.	-Aulas expositivas; -Discussão e resolução de problemas com a turma; -Perguntas sobre conhecimentos prévios relativos a o conteúdo. -Integração de tecnologia.	-Participação durante as aulas; -Resolução de lista de exercícios. -Resolução de teste individual.

Apêndice E – Plano de aula (Terceiro e Quarto encontro)

<table>
<tr><td colspan="4">PLANO DE ESTUDOS</td></tr>
<tr><td colspan="4">ALINHAMENTO MATEMÁTICO – Terceiro e Quarto Encontro</td></tr>
<tr><td>TURMA: 8° e 9° ano</td><td colspan="3">COMPONENTE CURRICULAR: MATEMÁTICA</td></tr>
<tr><td>DATA:</td><td colspan="3">TEMPO PREVISTO: 90 minutos cada encontro</td></tr>
<tr><td colspan="4">PROFESSOR: KARLLOS ALEXANDRE SOUSA PEREIRA</td></tr>
<tr><td>CONTEÚDOS</td><td>HABILIDADES</td><td>METODOLOGIA</td><td>AVALIAÇÃO</td></tr>
<tr><td>-Inteiros congruentes;
-Caracterização de inteiros congruentes;
-Propriedades das congruências;
-Aplicações de congruências</td><td>(EF07MA12) Resolver e elaborar problemas, de diversos contextos, que envolvam as operações fundamentais com números racionais, utilizando-se de diversos procedimentos, com ou sem o uso de calculadora.
(EF07MA11) Compreender e utilizar a multiplicação e a divisão de números inteiros, a relação entre eles e suas propriedades operatórias;
(EF06MA05) Classificar números em primos e compostos e estabelecer por meio de investigação os critérios de divisibilidade.</td><td>-Aulas expositivas;
-Discussão e resolução de problemas com a turma;
-Perguntas sobre conhecimentos prévios relativos ao conteúdo.
-Integração de tecnologia.</td><td>-Participação durante as aulas;
-Resolução de lista de exercícios.
-Resolução de teste individual.</td></tr>
</table>

Apêndice F – Plano de aula (Quinto e Sexto encontro)

<table>
<tr><td colspan="4">PLANO DE ESTUDOS</td></tr>
<tr><td colspan="4">ALINHAMENTO MATEMÁTICO – Quinto e Sexto Encontro</td></tr>
<tr><td>TURMA: 8° e 9° ano</td><td colspan="3">COMPONENTE CURRICULAR: MATEMÁTICA</td></tr>
<tr><td>DATA:</td><td colspan="3">TEMPO PREVISTO: 90 minutos cada encontro</td></tr>
<tr><td colspan="4">PROFESSOR: KARLLOS ALEXANDRE SOUSA PEREIRA</td></tr>
<tr><td>CONTEÚDOS</td><td>HABILIDADES</td><td>METODOLOGIA</td><td>AVALIAÇÃO</td></tr>
<tr><td>-Aplicações de congruências:
*Criptografia.
*Dígito verificador no código AEN-13.
*Dígitos Verificadores no C.P.F.</td><td>(EF07MA12) Resolver e elaborar problemas, de diversos contextos, que envolvam as operações fundamentais com números racionais, utilizando-se de diversos procedimentos, com ou sem o uso de calculadora.
(EF07MA11) Compreender e utilizar a multiplicação e a divisão de números inteiros, a relação entre eles e suas propriedades operatórias;</td><td>-Aulas expositiva;
-Associação da teoria com situações do cotidiano: relógios, calendários, etc.
-Nova abordagem de problemas já vistos;
- Discussão e resolução de problemas com a turma;
-Integração de tecnologia.</td><td>-Participação durante as aulas;
-Resolução de lista de exercícios.
-Resolução de teste individual.</td></tr>
</table>