UNIVERSIDADE ESTADUAL DO MARANHÃO
PRO-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO

Programa de Mestrado Profissional em Matemática em Rede Nacional

Roberto Amorim Silva

Congruência Modular no desenvolvimento da aprendizagem de Matemática nos anos finais do Ensino Fundamental

São Luís-MA
2022

Roberto Amorim Silva

Congruência Modular no desenvolvimento da aprendizagem de Matemática nos anos finais do Ensino Fundamental

Dissertação apresentada a Comissão Acadêmica Institucional do PROFMAT-UEMA como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. João Coelho Silva Filho

São Luís-MA
2022

Silva, Roberto Amorim.
Congruência modular no desenvolvimento da aprendizagem de matemática nos anos finais do ensino fundamental / Roberto Amorim Silva. – São Luís, 2022.
85 f

Dissertação (Mestrado Profissional) - Programa de Pós-Graduação em Matemática em Rede Nacional, Universidade Estadual do Maranhão, 2022.

Orientador: Prof. Dr. João Coelho Silva Filho.

1.Congruência modular. 2.Aplicações de congruência. 3.Congruência no ensino fundamental.

CDU: 51:373.3

Elaborado por Giselle Frazão Tavares - CRB 13/665

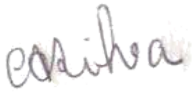
Roberto Amorim Silva

Congruência Modular no desenvolvimento da aprendizagem de Matemática nos anos finais do Ensino Fundamental

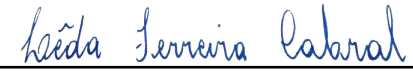
Aprovada em: 19/05/2022

Comissão Examinadora

Prof. Dr. João Coelho Silva Filho
UEMA
(Orientador)



Prof. Dra. Celina Amélia da Silva
UEMA



Prof. Dra. Leda Ferreira Cabral
IFMA

À Kedma e Mariana, minhas melhores companhias.

Agradecimentos

– Agradecer é um dos gestos mais sublimes que conheço e neste trabalho este momento mostra-se paradoxal, pois devemos fazer com que a nossa vivência caiba nessas laudas. É como se as peculiaridades de nossas relações com amigos e familiares pudessem ser compactadas. Não caberiam aqui, os ensinamentos de meus pais, a batalha de minha mãe, o carinho de meus tios e irmãos, o companheirismo de minha esposa, a felicidade proporcionada por minha filha, etc. é impossível mensurar. Ainda que insuficientes, estas palavras são uma tentativa de falar de como me sinto agradecido por todos conviverem comigo e da importância que todos têm em minha vida.

– À Deus, que me guia na trajetória da vida abençoando minha existência. Que mostrou-me que um novo começo é possível e que nunca estou só, que a vida é seu conhecido mistério e todos somos irmãos incumbidos de cativar e alimentar sentimentos bons, em especial o amor.

– À meu pai, que embora tenha nos deixado cedo, construiu conosco comportamentos e valores que impregnam nosso cotidiano. Mesmo pequeno, pude ver que ele era do bem e bom, que as dificuldades não o desencorajavam e, principalmente, sempre fazia o impossível quando o assunto era educação. Sou muito grato, sei que Deus preparou um lugar especial para ele.

– Em vista dessa difícil perda, minha mãe assumiu um posto que a exigiu muito, obrigando-a a ser enérgica quando necessário. Mas isto de forma alguma a desencorajou, pois em nenhum momento ela nos deixou sem rumo ou descuidados. A vida a obrigou a ser forte e ela é muito mais, é chefe e amiga, é conselheira e carinhosa, é perseverante, é motivadora etc. agradeço pelos incentivos e cobranças, pela educação reta, respeitosa, pela parceria em todos os momentos de minha vida. Minha mãe é prova de que não é preciso muito para ser do bem e praticá-lo, é uma evidência do fato de mãe ser tudo acima de tudo. Não há palavras que possam agradecer o ato de educar e amar e isto ela faz muito bem.

– Aos meus queridos irmãos Daniele, Paulo e Roger pelo apoio incondicional em todas as fases de minha vida. O Roger sempre demonstrou-me muito carinho sendo simultaneamente o irmão mais velho e mais agitado e brincalhão. Sempre esteve presente ainda que em determinada fase não estivesse próximo. É notória sua inteligência possibilitando sempre uma visão ou interpretação coerente diante dos mais diversos assuntos. Hoje é formado em direito e exerce a profissão no interior do estado. A Daniele é mestre em desenvolvimento socioeconômico pela UFMA e, doutoranda em economia pela UNESP, despertando um orgulho que não é só meu. A admiro por sua persistência diante das dificuldades existentes e pela responsabilidade mediante os estudos mostrando-se uma

profissional aluna; por ser carinhosa, compreensiva, respeitosa, e por ser minha irmã. O Paulo foi com quem tive convivência mais frequente, sempre estávamos juntos e até nos confundiram muitas vezes. Descobrimos muitas coisas juntos e pudemos conhecer e conviver com os sonhos do outro. É um prazer tê-lo em minha vida. Ele é Gestor Público pelo Instituto Federal e Contabilista pela UFMA.

- À minha esposa Kedma, a quem dispenso profunda admiração e carinho. É impossível agradecer nestas palavras o quanto és importante em minha vida. Vivemos muitas situações, inclusive algumas bem adversas, mas que não abalaram a nossa relação construída de forma simples e sólida, com amor, respeito, carinho e companheirismo. Sem falar que nossa princesa Mariana deixa as nossas vidas repletas de Luz.
- Aos meus tios Cecília e Ferreira, que me acolheram quando cheguei à São Luís e por quem tenho muito carinho e admiração.
- Ao meu orientador Prof. Dr. João Coelho Silva Filho por oportunizar a liberdade de criação para a realização deste trabalho, mas principalmente por compartilhar seu conhecimento e experiência, dando as contribuições, as sugestões e as críticas que lapidaram esta pesquisa.
- Aos professores Lélia, Lusitônia, Sandra, Félix, Sérgio, Roberto e Brandão pelas contribuições ao longo do curso.
- À professora Celina pela parceria e disponibilidade durante todo o curso, inclusive neste momento de conclusão.
- Aos amigos que fiz aqui: Camila, Daniel, Eliabe, Fábio, Gilberto, Israel, Ivao, Jandherson, Jardel, Jociel, Joel, Leonardo, Luciano, Marlon, Olegário, Paul, Ricardo, Sérgio e Vitor. Todos foram importantíssimos nesse processo.
- Aos amigos do IFMA campus Barra do Corda, nas pessoas dos professores Marinete Moura, Carlos Eduardo e Antonio Vitor, que me apoiaram para a concretização deste sonho.
- Aos amigos do departamento de engenharia da reitoria do IFMA na pessoa do professor Berto de Tácio, pelo incetivo durante essa jornada.
- E as pessoas que contribuíam direta ou indiretamente para que mais um degrau fosse ultrapassado.

"A alegria não chega apenas no encontro do achado, mas faz parte do processo da busca. E ensinar e aprender não pode dar-se fora da procura, fora da boniteza e da alegria." - *Paulo Freire*

Resumo

A pesquisa objeto deste trabalho enfatiza a teoria de Congruências, expondo seus fundamentos e diversidade de aplicações no cotidiano e propondo o ensino desse conteúdo nos anos finais do ensino fundamental por sua relevância teórico-prática para o desenvolvimento do ensino de matemática. A pesquisa aborda tópicos fundamentais à teoria de congruências. São apresentadas aplicações de Congruências modulares em calendários, sistemas de identificação e criptografia bem como as propriedades que auxiliam na resolução mais célere de problemas. E realiza-se aplicação com alunos da rede pública de São Luís para verificar as hipóteses acerca das contribuições da teoria de congruências para essa etapa do ensino.

Palavras-chave: Congruência modular. Aplicações de congruência. Congruência no ensino fundamental.

Abstract

The research object of this work emphasizes the theory of Congruences, exposing its foundations and diversity of applications in everyday life and proposing the teaching of this content in the final years of elementary school due to its theoretical-practical relevance for the development of mathematics teaching. The research addresses fundamental topics to the theory of congruences. Applications of modular Congruences in calendars, identification and cryptography systems are presented, as well as the properties that help in the faster resolution of problems. And an application is carried out with students from the public network of São Luís to verify the hypotheses about the contributions of the theory of congruences to this stage of teaching.

Keywords: Modular congruence. Congruence applications. Congruence in elementary education.

Lista de figuras

Lista de tabelas

Lista de abreviaturas e siglas

BNCC	Base Nacional Comum Curricular
CPF	Cadastro de Pessoas Físicas
CNPJ	Cadastro Nacional de Pessoas Jurídicas
GTIN	Global Trade Item Number
ISBN	International Standard Book Number
PISA	Programa Internacional de Avaliação de Estudantes
PIC	Programa de Iniciação Científica Jr.
POTI	Programas Polo Olímpico de Treinamento Intensivo
PROFMAT	Programa de Mestrado Profissional em Matemática em Rede Nacional
RPM	Revista do Professor de Matemática
UEMA	Universidade Estadual do Maranhão

Lista de símbolos

α	Letra grega Gama
λ	Lambda
$\in$	Pertence
$\mathbb{N}$	Conjunto dos números naturais
$\mathbb{Z}$	Conjunto dos números inteiros

Sumário

1 Introdução

A Teoria dos números é um ramo da Matemática utilizada como sinônimo de Aritmética e estuda os números inteiros com suas propriedades e operações. É a matemática utilizada frequentemente em tarefas do cotidiano, em cálculos científicos e negócios.

O estudo da Aritmética faz parte do currículo obrigatório do ensino fundamental brasileiro onde são trabalhadas as quatro operações básicas, objetivando embasamento teórico e o desenvolvimento de habilidades para a vida social e escolar. Neste trabalho, é concedida atenção especial à divisão de números inteiros e seus respectivos restos, visando destacar uma das vertentes da Teoria dos números conhecida como Aritmética Modular. Esta por sua vez, só é vista em programas de iniciação científica, projetos de pesquisas e pós-graduações das ciências exatas.

São diversas as contribuições da Aritmética para o desenvolvimento dos alunos da educação básica, porém a sua aprendizagem ainda não alcançou níveis satisfatórios conforme alertam as pesquisas e avaliações nacionais de desempenho escolar. Como exemplo, cita-se o resultado do Índice de Desenvolvimento da Educação Básica – IDEB 2019.

> Em 2019, o Brasil bateu a meta para os primeiros anos de aprendizagem (até o 5ª ano) pela sétima vez seguida, desde que o índice foi criado em 2005, com edição a cada dois anos. Mas não atingiu o mínimo proposto para a avaliação dos anos finais do ensino fundamental (6º ao 9º ano) pela quarta vez consecutiva. (OLIVEIRA, 2020)

Os dados mostram declínio no desenvolvimento do ensino e aprendizagem de Matemática nessa etapa de ensino, visto que os alunos pertencentes aos anos finais não têm alcançado as metas estabelecidas, diferentemente dos alunos dos anos iniciais. Pode-se tentar justificar tais resultados pelo nível de complexidade e aumento do repertório de conteúdos nos anos finais, convergindo para o enfoque dessa pesquisa quanto à proposição de ferramentas que auxiliem no desempenho dos alunos. Oportunamente pretende-se suprir a necessidade de um ensino mais eficaz em que os conceitos importantes de matemática sejam compreendidos pelos alunos proporcionando avanço no estudo e aprendizagem da disciplina.

Em pesquisa encomendada pelo movimento Todos Pela Educação e divulgada no Jornal Opinião Estadão, revela-se que apenas 65% dos alunos que ingressam no ensino fundamental concluem o ensino médio e com o agravante de apenas 7% possuírem aprendizagem adequada em Matemática (CRUZ, 2018). Significando que a grande maioria dos alunos não compreende os conceitos básicos de matemática em sua formação inicial e alerta para a necessidade de melhoria de eficácia do ensino de matemática, pois os conhecimentos da base, em particular os de aritmética, são indispensáveis para a aprendizagem

de outros conteúdos e desenvolvimento na disciplina.

Outra evidência da situação delicada em que se encontra a educação brasileira ocorreu no Programa Internacional de Avaliação de Estudantes - PISA, conforme trecho extraído do Relatório Brasil no Pisa 2018.

> A maioria dos estudantes brasileiros que participaram do Pisa 2018 se encontra no Nível 1 ou abaixo dele (68,1%). Todos os países e economias participantes do Pisa têm estudantes que se encontram nesses níveis, mas as maiores proporções de estudantes nessa situação são encontradas nos países com menor desempenho. (BRASIL, 2020, p.114)

O Pisa é um programa realizado a cada três anos pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e consiste num estudo comparativo internacional para fornecer informações sobre o desempenho de estudantes na faixa etária de 15 anos, idade em que se pressupõe o término do Ensino Fundamental que corresponde a segunda etapa da Educação Básica brasileira e fim da escolaridade obrigatória em alguns países. O objetivo do programa é que os países participantes possam avaliar os conhecimentos e habilidades de seus estudantes em comparação com outros países e assim formular políticas e programas educacionais visando melhoria da qualidade e equidade da aprendizagem. O resultado do Pisa avalia estudantes que já concluíram o ensino fundamental e o fator preocupante corresponde aos alunos que, por algum motivo, não desenvolveram as habilidades e, consequentemente, não atingiram as competências previstas para essa etapa de ensino.

É imprescindível uma educação de qualidade a todos os cidadãos, pois isso permite viver em um país mais justo socialmente, economicamente mais competitivo, inovador e ético. Sabe-se atualmente que o domínio de competências básicas como as proporcionadas pelo ensino de matemática oportuniza sobrevivência digna e a busca por equidade, porém isso não se verifica no panorama atual da educação brasileira.

Aponta-se o aspecto de dependência acumulada dos conteúdos de matemática no qual não é possível dissociar os conhecimentos ou conceitos mais básicos como os vistos na aritmética do ensino fundamental de outros mais complexos do mesmo nível ou níveis subsequentes de ensino.

Isso leva a escolha do tema deste trabalho, pois os conceitos de congruência modular têm muitas contribuições para o ensino e aprendizagem de matemática, com diversas aplicações e contextualizações no cotidiano sem falar que estão presentes no uso de tecnologias. Destaca-se ainda a celeridade na resolução de problemas de repetições periódicas, os quais às vezes tornam-se inviáveis com a utilização dos conteúdos pertencentes ao currículo do ensino fundamental.

Neste trabalho, são tratados os conceitos e propriedades da aritmética modular

evidenciando a pertinência que o conhecimento do tema possui nos anos finais do ensino fundamental e na dinâmica da vida moderna. Tal fato é consolidado no objetivo de investigar na teoria de congruência modular ferramentas para o desenvolvimento do ensino de matemática nos anos finais do ensino fundamental.

Destaca-se as aplicações da Congruência nos sistemas de identificação como o standard book number - ISBN, códigos de barras, cadastro das pessoas físicas - CPF, cadastro nacional da pessoa jurídica – CNPJ, em criptografia, relógios, calendários etc.

Em virtude do estudo e aplicabilidade das congruências modulares, propõe-se seu ensino a partir dos anos finais do ensino fundamental pois é quando se inicia o estudo do conteúdo de divisão euclidiana conforme a Base Nacional Comum Curricular - BNCC. O conhecimento da teoria permitiria à matemática se aproximar de alguns dos objetivos previstos para essa fase escolar nas leis e diretrizes que regem a educação no Brasil.

Dessa forma, são abordados neste tranalho de pesquisa os seguintes objetivos específicos: a) Pesquisar teoremas relativos à teoria de Congruência Modular que auxiliem na resolução de problemas que envolvem repetições periódicas; b) Identificar aplicações da teoria de Congruência Modular no cotidiano; c) Elencar contribuições da teoria das Congruências Modulares para o ensino-aprendizagem da Aritmética nos anos finais do ensino fundamental.

Considerando que esta pesquisa propõe a inserção do conteúdo de congruências modulares na grade curricular do ensino fundamental-anos finais, optou-se, a princípio, por uma metodologia de pesquisa bibliográfica seguida de pesquisa de campo do tipo experimental com alunos da Unidade de Educação Básica Bandeira Tribuzzi, escola do município de São Luís.

No que concerne a estrutura deste trabalho, apresenta-se na primeira seção a motivação para realização desta pesquisa considerando a situação em que se encontra a educação brasileira e também alguns conceitos e teorias que são requisitos para tratar do conteúdo de congruências modulares. Em seguida, a teoria principal é apresentada embasada em autores renomados da área da Aritmética, abragendo aplicações em situações do nosso cotidiano. Após, detalhou-se a experiência de trabalhar a teoria de congruências modulares com alunos de uma escola da rede pública municipal de São Luís - MA. Na sequência, apresentou-se as considerações a respeito do trabalho, apontando as situações mais relevantes.

2 Fundamentos Básicos de Teoria dos Números

A Aritmética é uma área abrangente da matemática e compõe a base curricular do ensino fundamental sob a forma dos conteúdos de números naturais e inteiros com suas propriedades e operações, múltiplos e divisores, números primos e compostos, regras de divisibilidade, máximo e mínimo divisor comum. Além disso, na Aritmética existem os conceitos de Congruência Modular que fazem parte de sua parte mais complexa. Tais conceitos foram introduzidos por Carl Friedrich Gauss em 1801, como segue

> 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)

As ideias contidas no Disquisiotiones Arithmeticae serviram de embasamento para o desenvolvimento da teoria dos números e, até as notações da teoria de congruência modular introduzidas por Gauss se mantiveram até os dias atuais (SANTOS, 1998). Isso mostra a grande importância de Gauss para a Matemática, deixando conhecimentos e conceitos fecundos para estudos posteriores. Para embasar o estudo da Aritmética modular serão apresentados conceitos mais básicos mas fundamentais da teoria dos números.

2.1 Números Inteiros e suas propriedades

A Aritmética dos restos, teoria abordada neste capítulo, foi construída sobre o conjunto dos números inteiros e, considerando que este conjunto também é parte do currículo do Ensino Fundamental, o estudo inicia-se com a definição desse conjunto numérico.

De uma forma geral, os números inteiros surgem da impossibilidade de representar a diferença $a - b$ quando a $<$ b no conjunto dos números Naturais. Segue definição formal do conjunto dos números inteiros.

As definições apresentadas a seguir podem ser encontradas em Filho (1981), Domingues (1991), Hefez (2016), Iezzi (2013) e Oliveira (2012).

O conjunto dos números inteiros cujo símbolo é $\mathbb{Z}$, pode ser representado por

$$\mathbb{Z} = \{ ..., -3, -2, -1, 0, 1, 2, 3, ...\}.$$

Destacam-se os seguintes subconjuntos de $\mathbb{Z}$:

(a) Conjunto $\mathbb{Z}^*$ dos inteiros não nulos:

$$\mathbb{Z}^* = \{x \in \mathbb{Z} \ ; \ x \neq 0\} = \{..., -2, -1, +1, +2, ...\}.$$

(b) Conjunto $\mathbb{Z}_+$ dos inteiros não negativos:

$$\mathbb{Z}_+ = \{x \in \mathbb{Z} \ ; x \geq 0\} = \{0, +1, +2, +3, ...\}.$$

(c) Conjunto $\mathbb{Z}_-$ dos inteiros não positivos:

$$\mathbb{Z}_- = \{x \in \mathbb{Z} \ ; \ x \leq 0\} = \{ \ 0, -1, -2, -3, ...\}.$$

(d) Conjunto $\mathbb{Z}_+^*$ dos inteiros positivos:

$$\mathbb{Z}_+^* = \{x \in \mathbb{Z}; x > 0\} = \{+1, +2, +3, +4, ...\}.$$

(e) Conjunto $\mathbb{Z}_-^*$ dos inteiros negativos:

$$\mathbb{Z}_+^* = \{x \in \mathbb{Z}; x < 0\} = \{..., -4, -3, -2, -1\}.$$

O conjunto $\mathbb{Z}$ é munido das operações de adição e multiplicação e, estas operações possuem as seguintes propriedades:

1. A adição e a multiplicação são bem definidas:

   Para todos $a, b, a', b' \in \mathbb{Z}$, se $a = a'$ e $b = b'$, então $a + b = a' + b'$ e $a \cdot b = a' \cdot b'$;

2. A adição e a multiplicação são comutativas:

   Para todos $a, b, \in \mathbb{Z}$, $a + b = b + a$ e $a \cdot b = b \cdot a$;

3. A adição e a multiplicação são associativas:

   Para todos $a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$ e $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

4. A adição e a multiplicação possuem elementos neutros:

   Para todo $a \in \mathbb{Z}$, $a + 0 = a$, e $a \cdot 1 = a$;

5. A adição possui elementos simétricos:

   Para todo $a \in \mathbb{Z}$, existe $b(= -a)$ tal que $a + b = 0$;

6. A multiplicação é distributiva em relação à adição:

   Para todos $a, b, c \in \mathbb{Z}$, tem-se $a \cdot (b + c) = a \cdot b + a \cdot c$;

7. O conjunto $\mathbb{N}$ é fechado para adição e para a multiplicação, ou seja, para todos $a, b \in \mathbb{N}$, tem-se que $a + b \in \mathbb{N}$ e $a \,.\, b \in \mathbb{N}$;

8. Tricotomia: Dados $a, b \in \mathbb{Z}$. Uma, e somente uma, das seguintes possibilidades é verificada:

   $$\text{i) } a = b; \qquad \text{ii) } b - a \in \mathbb{N}; \qquad \text{iii) } -(b - a) \in \mathbb{N}.$$

A propriedade 1 significa que é possível somar um dado número a ambos os lados de um igualdade, assim como pode-se multiplicar ambos os lados por um mesmo número.

Sempre que um conjunto numérico, munido das operações de adição e multiplicação possuir as propriedades 1 a 6 acima, diz-se que os elementos desse conjunto bem como suas operações estão sujeitos às leis básicas da Aritmética. Devido a existência de muitos conjuntos nessa condição, é necessário melhor caracterizar o conjunto dos números

inteiros.

As propriedades 7 e 8 nos ajudarão a discorrer sobre a ordenação no conjunto dos números inteiros.

Observe que o conjuntodos números inteiros é particionado em três subconjuntos:

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup (-\mathbb{N})$$

em que o conjunto $-\mathbb{N}$ é o simétrico dos elementos de $\mathbb{N}$.

Seguem consequências dos axiomas apresentados nas propriedades acima.

Proposição 2.1. $a \cdot 0 = 0$ para todo $a \in \mathbb{Z}$.

Demonstração: segue das propriedades 4 e 6 que

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0.$$

Somando $-(a \,.\, 0)$ aos membros extremos da igualdade, pelas proriedades 5, 2, 3 e 4, obtem-se:

$$\begin{aligned} 0 &= -(a \cdot 0) + (a \cdot 0) \\ &= -(a \cdot 0) + (a \cdot 0 + a \cdot 0) \\ &= (-(a \cdot 0 + a \cdot 0) + a \cdot 0 = 0 + a \cdot 0 \\ &= a \cdot 0. \end{aligned}$$

Proposição 2.2. A adição é compatível e cancelativa com respeito à igualdade:

$$\text{Para todos } a, b, c \in \mathbb{Z},\ a = b \Longleftrightarrow a + b = b + c.$$

Demonstração: A implicação $a = b \Rightarrow a + c = b + c$ é consequência da adição ser bem definida conforme a propriedade 1.

Suponha agora que $a + c = b + c$. Somando $(-c)$ a ambos os lados, consegue-se o resultado.

A operação de adição permite definir uma nova operação chamada de subtração conforme segue

$$b - a = b + (-a).$$

Diz-se que $b - a$ é o resultado da subtração de a e de b. É comum dizer também que a operação de subtração é somar com o simétrico, no caso em questão, somou-se b com o simétrico de a.

Visando auxiliar nosso estudo em Teoria dos Números, será apresentada a relação de ordem existente no conjunto dos números inteiros.

Embasados nas propriedades mencionadas, em particular nas propriedades 7 e 8, em que a primeira fala do fechamento do conjunto $\mathbb{N}$, isto é, a soma e o produto de números naturais são sempre números naturais e a segunda da tricotomia, em que dados dois números inteiros pode ocorrer somente uma das possibilidades para esses números, ou eles são iguais, ou um é menor do que o outro. A relação de ordem em $\mathbb{Z}$ será melhor caracterizada adiante.

Diz-se que a é menor do que b, e representa-se por $a < b$ toda vez que a propriedade 8-ii) for verificada. Assim, a propriedade 8-iii) significa que $b < a$. E pode-se reescrever o enunciado de 8, como segue:

8-1) Dados $a, b \in \mathbb{Z}$, uma e somente uma, das seguintes condições é verificada:

$$\text{i) } a = b; \qquad \text{ii) } a < b; \qquad \text{iii) } b < a.$$

Proposição 2.3. A relação "menor do que" é transitiva:

$$\forall\, a, b, c \in \mathbb{Z}, a < b \text{ e } b < c \Rightarrow a < c.$$

Demonstração: Supondo $a < b$ e $b < c$, tem-se $b - a \in \mathbb{N}$ e $c - b \in \mathbb{N}$. Como $\mathbb{N}$ é fechado para a adição, tem-se

$$c - a = (b - a) + (c - b)$$

logo, $a < c$.

Proposição 2.4. A adição é compatível e cancelativa com respeito à relação"menor do que" :

$$\forall\, a, b, c \in \mathbb{Z}, a < b \iff a + c < b + c.$$

Demonstração: Suponha que $a < b$. Logo, $b - a \in \mathbb{N}$. Portanto,

$$(b + c) - (a + c) = (b - a) \in \mathbb{N}$$

o que implica que, $a+c < b+c$. Reciprocamente, suponha que $a+c < b+c$. Pela primeira parte da proposição, pode-se somar $(-c)$ a ambos os lados sa desigualdade, o que nos conduz ao resultado.

Proposição 2.5. A multiplicação por elementos de $\mathbb{N}$ é compatível e cancelativa com respeito à relação"menor do que" :

$$\forall\, a, b, c \in \mathbb{Z}, a < b \iff a \,.\, c < b \,.\, c.$$

Demonstração: Suponha que $a < b$. Logo, $b - a \in \mathbb{N}$. Assim, se $c \in \mathbb{N}$, pelo fato de $\mathbb{N}$ ser multiplicativamente fechado, tem-se

$$bc - ac = (b - a)c \in \mathbb{N},$$

logo, $ac < bc$. Reciprocamente, suponha que $ac < bc$, com $c \in \mathbb{N}$. Pela tricotomia, temo-se três possibilidades a analisar:

(i) $a = b$. Isso acarretaria $ac = bc$, o que é falso. (ii) $b < a$. Isso acarretaria, pela primeira parte da demonstração, que $bc < ac$, o que também é falso. (iii) $a < b$. Esta é a única possibilidade válida.

Definição 2.1. Seja $a \in \mathbb{Z}$, definimos

$$|a| = \begin{cases} a, \; se\, a \geq 0 \\ -a, se\, a < 0. \end{cases}$$

Note que para todo $a \in \mathbb{Z}$, tem-se que $|a| \geq 0$ e $|a| = 0$ se, e somente se, $a = 0$. O número inteiro $|a|$ é chamado de módulo ou valor absoluto de a. Seguem enunciados das propriedades básicas do módulo.

Proposição 2.6. Para $a, b, c \in \mathbb{Z}$, tem-se

1. $|ab| = |a||b|$;
2. $|a| \leq r$ se, e somente se, $-r \leq a \leq r$;
3. $-|a| \leq a \leq |a|$;
4. $||a| - |b|| \leq |a \pm b| \leq |a| + |b|$.

As propriedades enunciadas até aqui não bastam para caracterizar o conjunto dos números inteiros, pois, por exemplo, os conjuntos dos números racionais e reais possuem todas as propriedades acima. Entretanto, somente os inteiros possuem o Princípio da Boa Ordenação, cujo enunicado é o seguinte: se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então S possui um menor elemento. Com este axioma é possível distinguir os números inteiros dos números racionais e reais e, compõe com os oito axiomas acima enunciados a caracterização do conjunto dos números inteiros, de onde pode-se deduzir qualquer propriedade nesse conjunto. Além disso, com a utilização do Princípio da Boa Ordenação podem ser demonstradas mais algumas propriedades de $\mathbb{Z}$ necessárias ao nosso estudo.

Proposição 2.7. Não existe nenhum número inteiro n tal que $0 < n < 1$.

Demonstração: Suponha por absurdo que exista n com essa propriedade. Logo, o conjunto $S = \{x \in \mathbb{Z}; 0 < x < 1\}$ é não vazio, além de ser limitado infeirormente. Portanto, S possui um menor elemento a, com $0 < a < 1$. Multiplicando esta última desigualdade por a, obtém-se $0 < a^2 < a < 1$, logo $a^2 \in S$ e $a^2 < a$, uma contradição. Poranto, $S = \emptyset$.

Corolário 2.1. Dado um número inteiro n qualquer, não existe nehum número inteiro m tal que $n < m < n + 1$.

Demonstração: Suponha, por absurdo, que exista um número inteiro m que satisfaça as desigualdades $n < m < n+1$. Subtraindo n nessas desigualdades, obtém-se $0 < m-n < 1$, o que contradiz a Proposição 2.7.

Corolário 2.2. Seja $a, b \in \mathbb{Z}$. Se $ab = 1$, então $a = b = \pm 1$.

Demonstração: Incialmente, note que $a \neq 0$ e $b \neq 0$, pois caso contrário, $ab = 0$. Suponha $a > 0$. Como $ab = 1 > 0$, segue que $b > 0$. Segue-se da proposição 2.7 que $a \geq 1$ e $b \geq 1$. Logo, $1 = ab \geq b \geq 1$, o que implica $b = 1$. E como $ab = 1$, isso acarreta que $a = 1$.

Corolário 2.3. Se $a, b \in \mathbb{Z}$, com $b \neq 0$, então $|ab| \geq |a|$.

Demonstração: De fato, como $b \neq 0$, pela proposição 2.7, tem-se que $|b| \geq 1$. Logo,

$$|ab| = |a||b| \geq |a|.$$

Corolário 2.4. Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Então existe $n \in \mathbb{Z}$ tal que $nb > a$.

Demonstração: Como $b \neq 0$, segue da proposição 2.7 que $|b| \geq 1$, logo

$$(|a| + 1)|b| \geq |a| + 1 > |a| \geq a.$$

2.2 Divisibilidade

Inicialmente deve-se observar que as operações de adição, subtração e multiplicação de números inteiros sempre resultam em números inteiros, porém o quociente de números inteiros pode ser um inteiro ou não.

Definição 2.2. Sejam a e b inteiros. Diz-se que a divide b, e escreve-se $a \mid b$, se existe um inteiro q, tal que

$$b = a \cdot q.$$

Nesse caso, diz-se que a é um divisor de b, que b é múltiplo de a, que a é um fator de b, ou ainda que b é divisível por a. Escreve-se $a \nmid b$ para indicar que a não divide b, significando que não existe um inteiro q que satisfaça a equação $b = a \cdot q$.

Exemplo 2.1. $3 \mid 15$ pois $15 = 3\dot{5}$. Por outro lado, $5 \nmid 32$ pois não existe $q \in \mathbb{Z}$ tal que $32 = 5 \cdot q$.

Teorema 2.1. Sejam a, b, c e d números inteiros. Então,

(a) $a \mid 0$, $1 \mid a$ e $a \mid a$;

(b) Se $a \mid 1$, então $a = \pm 1$;

(c) Se $a \mid b$ e $b \mid c$ então $a \mid c$;

(d) Se $a \mid b$ e $c \mid d$ então $ac \mid bd$;

(e) Se a e b são positivos e $a \mid b$ então $0 < a \leq b$;

(f) Se $a \mid b$ e $b \mid a$ então $a = b$ ou $a = -b$;

(g) Se $a \mid b$ e $a \mid c$, então $a \mid (bx + cy)$, para todos x e y inteiros.

(h) Se $a \mid (b \pm c)$, então $a \mid b \iff a \mid c$.

Demonstração:
(a) Por definição, se $a \mid 0$ então existe $q_1 \in \mathbb{Z}$ tal que $0 = a \cdot q_1$. Assim, basta tomar $q_1 = 0$, pois $0 = a \cdot 0$; se $1 \mid a$, então existe $q_2 \in \mathbb{Z}$ tal que $a = 1 \cdot q_2$, assim $q_2 = a$ e $a = 1 \cdot a$; se $a \mid a$ então existe $q_3 \in \mathbb{Z}$ tal que $a = a \cdot q_3$, assim $q_3 = 1$ e $a = a \cdot 1$.

Agora será demonstrado o item (b). Se $a \mid 1$, então existe $q \in \mathbb{Z}$ tal que $1 = a \cdot q$, implicando nas seguintes possiblidades $a = 1$ e $q = 1$ ou $a = -1$ e $q = -1$. Logo, $a = \pm 1$.

Segue-se com a demonstração de (c). Se $a \mid b$ e $b \mid c$ então

$$b = a \cdot q_1,\ q_1 \in \mathbb{Z} \tag{1}$$
$$c = b \cdot q_2,\ q_2 \in \mathbb{Z}. \tag{2}$$

Multiplicando as equações (1) e (2), obtém-se

$$b \cdot c = (a \cdot b) \cdot q_1 \cdot q_2 \Rightarrow a \mid c.$$

Provando a afirmação (c).

Agora apresenta-se a demonstração do item (d). De fato, se $a \mid b$ e $b \mid c$ valem as igualdades

$$b = a \cdot q_1,\ q_1 \in \mathbb{Z} \tag{3}$$
$$c = b \cdot q_2,\ q_2 \in \mathbb{Z}. \tag{4}$$

Multiplicando membro a menbro (3) e (4) obtém-se

$$b \cdot c = (a \cdot b)(q_1 \cdot q_2) \Rightarrow ac \mid bc.$$

Prosseguindo com a prova de (e). Com efeito, se $a \mid b$ sendo ambos positivos, então $b = aq$ com

$$q \geq 1. \tag{5}$$

Logo, multiplicando por a ambos os lados de (5) tem-se (como a é positivo) que

$$b = aq \geq a > 0,$$

conforme desejava-se demonstrar.

A prova de (f) pode ser realizada como segue. Observe que se $a \mid b$ e $b \mid a$ então $|a|$ divide b e b divide $|a|$. Portanto, pelo item c) segue que $|a| \leq |b|$ e $|b| \leq |a|$, ou seja, $|a| \leq |b| \leq |a|$. Logo, $|a| = |b|$ e consequentemente $a = b$ ou $a = -b$.

Será apresentada a prova de (g). Se $a \mid b$ e $a \mid c$, então

$$b = a \cdot q_1,\ q_1 \in \mathbb{Z} c = a \cdot q_2,\ q_2 \in \mathbb{Z}. \tag{6}$$

Portanto, quaisquer que sejam os inteiros x e y, multiplicando (6) por x e (7) por y e somando membro a membro obtem–se:

$$bx + cy = aq_1x + aq_2y = a(q_1x + q_2y), \tag{7}$$

e, portanto, $a \,|\, (bx + cy)$ para quaiquer x e y inteiros.

Finalmente, será demostrado o item (h). Supondo que $a \,|\, (b+c)$. Logo, existe $f \in \mathbb{Z}$ tal que $b + c = fa$. Agora, se $a \,|\, b$ segue que existe $g \in \mathbb{Z}$ tal que $b = ga$. Juntando as duas igualdades acima, tem-se

$$ga + c = fa,$$

donde segue que, $c = a(f - g)$, logo $c \,|\, a$. A prova da implicação contrária é análoga. Por outro lado, se $a \,|\, (b-c)$ e $a \,|\, b$, pelo caso anterior, tem-se que $a \,|\, -c$, o que implica que $a \,|\, c$.

Exemplo 2.2. Prove que o número $N = 5^{45362} - 7$ não é divisível por 5.

Solução: Essa demonstração será feita por contradição. Supondo, por contradição, que N seja divisível por 5, então $5^{45362} - 7 = 5q$. Logo, $7 = 5^{45362} - 5q$, ou seja, 7 seria divisível por 5, o que é uma contradição.

Definição 2.3. Sejam a e b dois números inteiros e $d \neq 0$, chama-se de divisor comum dos inteiros a e b um inteiro d tal que $d \,|\, a$ e $d \,|\, b$.

Ao afirmar que que d é divisor comum dos inteiros a e b significa dizer que d pertence, simultaneamente, aos conjuntos dos divisores de a e de b, indicando por $D(a, b)$ esse conjunto e, denota-se por

$$D(a, b) = \{x \in \mathbb{Z}^*; x \in D(a) \text{ e } x \in D(b)\}.$$

Dois inteiros a e b quaisquer admitem sempre -1 e 1 como divisores comuns, dessa forma segue–se que o conjunto $D(a, b)$ dos divisores comuns de a e b nunca é vazio, ou seja, $D(a, b) \neq \emptyset$. Em particular, se $a = b = 0$, então todo inteiro não nulo é um divisor comum de a e b, isto é, $D(a, b) = \mathbb{Z}^*$.

Exemplo 2.3. Determine todos os divisores comuns dos inteiros $a = -12$ e $b = 8$.

Solução: *Tem-se que* $D(-12) = \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm12\}$ *e* $D(8) = \{\pm1, \pm2, \pm4, \pm8\}$. *Logo,*

$$D(-12, 8) = \{\pm1, \pm2, \pm4\}.$$

2.2.1 Algoritmo da Divisão

Teorema 2.2. (Divisão Euclidiana). Dados dois inteiros a e b, sendo a positivo, existem únicos inteiros q e r tais que

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

Se $a \nmid b$, então r satisfaz a desigualdade estrita $0 < r < a$.

Demonstração: Sem perda de generalidade, pode-se supor que b é positivo. Se $b < a$, basta tomar $q = 0$ e $r = b$. Se $b = a$, então toma-se $q = 1$ e $r = 0$. Assim, assumi-se que $b > a > 0$. Considerando o conjunto

$$R = \{b - aq \in \mathbb{Z}; b - aq \geq 0\} \subseteq \mathbb{N} \cup \{0\}. \tag{8}$$

Note que o conjunto R é não vazio, pois $b - a \in R$, já que $b - a > 0$. Assim, pelo Princípio da Boa Ordenação tem-se que R admite um menor elemento, denotado por r. Claramente $r = b - a \geq 0$. Além disso, $r < a$, pois caso contrário

$$r = b - a \geq a \Rightarrow b - a(q + 1) \geq 0. \tag{9}$$

Por outro lado,

$$a > 0 \Rightarrow b - a(q + 1) < b - aq. \tag{10}$$

Das desigualdades (9) e (10) segue que

$$0 \leq b - a(q + 1) < b - aq,$$

contradizendo o fato de que $r = b - aq$ é o menor elemento não negativo de R. Agora será provado que de fato r e q, escolhidos desta forma, são únicos. Com efeito, supondo que existam outros inteiros r_1 e q_1 tais que

$$b = aq_1 + r_1,\ 0 \leq r_1 < a.$$

Resultando que $aq + r = aq_1 + r_1$. Logo,

$$(r - r_1) = (q - q_1)\, a; \tag{11}$$

assim $r - r_1$ é múltiplo de a. Mas, em virtude de $-a < r - r_1 < a$, o único valor que $r - r_1$ pode tomar, sendo este múltiplo de a, é $r - r_1 = 0$. Portanto, $r = r_1$, de onde se deduz diretamente de (1.9) que $q = q_1$.

Corolário 2.5. Dados dois números a e b com $1 < a \leq b$, existe um número natural n tal que

$$na \leq b < (n + 1)a.$$

Demonstração: Pela divisão euclidiana, existem únicos $q, r \in \mathbb{N}$ com $0 \leq r < a$ tais que $b = aq + r$. Assim,

$$aq \leq b = aq + r < aq + a = a(q + 1).$$

Agora resta tomar $q = n$ para obter o resultado.

Exemplo 2.4. Se a é um número natural com $a \geq 3$, então a^2 deixa resto 1 na divisão por $a - 1$. Consequentemente, $a - 1$ divide $a^2 - 1$.

Solução: *Usando a identidade* $a^2 - 1 = (a - 1)(a + 1)$ *segue que* $a^2 = (a - 1)(a + 1) + 1$ *com* $1 < a - 1$*, de onde segue o resultado.*

Teorema 2.3. (Teorema dos Restos). A soma e o produto de quaisquer dois números naturais deixa o mesmo resto que a soma e o produto dos seus restos, na divisão por um inteiro positivo a.

Demonstração: Considere $n_1, n_2 \in \mathbb{Z}$. Fazendo a divisão com resto de ambos os números por a tem-se que

$$n_1 = aq_1 + r_1 \text{ e } n_2 = aq_2 + r_2,$$

com $0 \leq r_1, r_2 < a$. Então,

$$\begin{aligned} n_1 n_2 &= (aq_1 + r_1)(aq_2 + r_2) \\ &= a^2 q_1 q_2 + aq_1 r_2 + aq_2 r_1 + r_1 r_2 \\ &= a(q_1 q_2 + q_1 r_2 + q_2 r_1) + r_1 r_2 \\ &= aq + r_1 r_2, \end{aligned} \tag{12}$$

onde $q = aq_1 q_2 + q_1 r_2 + q_2 r_1$. Dividindo $r_1 r_2$ por a obtém-se

$$r_1 r_2 = ap + r, p \in \mathbb{Z}, 0 \leq r < a. \tag{13}$$

Das igualdades (12) e (13) segue que

$$n_1 n_2 = aq + ap + r = a(q + p) + r, 0 \leq r < a. \tag{14}$$

Portanto, de (13) e (14) concluimos que os restos que deixam $n_1 n_2$ e $r_1 r_2$ na divisão por a são iguais. Provando o resultado para o produto. Agora isso será mostrado para a soma. Note que

$$\begin{aligned} n_1 + n_2 &= (aq_1 + r_1) + (aq_2 + r_2) \\ &= aq_1 + aq_2 + r_1 + r_2 \\ &= a(q_1 + q_2) + r_1 + r_2 \\ &= aq + r_1 + r_2, \end{aligned} \tag{15}$$

onde $q = q_1 + q_2$. Dividindo $r_1 + r_2$ por a para obtém-se

$$r_1 + r_2 = as + r, s \in \mathbb{Z}, 0 \leq r < a. \tag{16}$$

Das igualdades (15) e (16) segue que

$$n_1 + n_2 = aq + as + r = a(q + s) + r, 0 \leq r < a. \tag{17}$$

Logo, de (16) e (17) conclui-se que os restos que deixam $n_1 + n_2$ e $r_1 + r_2$ na divisão por a são iguais.

A vantagem do Teorema 2.3 é que em certos problemas que envolvem números muito grandes é possível substituir estes por números muito menores e mais confortáveis para se trabalhar.

Apresenta-se a seguir algumas aplicações do Teorema dos restos com a finalidade de deixar mais evidente as propriedades apresentadas anteriormente.

Exemplo 2.5. Encontre o resto da divisão de $1989 \cdot 1990 \cdot 1991 + 1992^3$ por 7.

Solução: *Observe que* $1989, 1990, 1991$ *e* 1992 *deixam, respectivamente, restos* $1, 2, 3$ *e* 4 *na divisão por* 7. *Assim, pelo Teorema 2.3, pode-se reescrever o problema* $1989 \cdot 1990 \cdot 1991 + 1992^3$ *como* $1 \cdot 2 \cdot 3 + 4^3 = 6 + 64 = 70$ *que é múltiplo de* 7 *e, portanto, deixa resto* 0 *na divisão por* 7.

Exemplo 2.6. Prove que em qualquer triângulo retângulo com lados inteiros, pelo menos um deles é múltiplo de 3.

Solução: *Inicialmente serão analisados quais são os restos possíveis de um número quadrado na divisão por* 3. *De acordo com o Teorema dos restos, tem-se as possibilidades seguintes para* n *e* n^2 *na divisão por* 3:

Tabela 1 – Restos de um quadrado por 3

n	n^2
0	0
1	1
2	1

Fonte: OLIVEIRA, 2012, p. 99.

Em síntese, se um número não é múltiplo de 3 *então o resto da divisão de seu quadrado por* 3 *deve ser igual a* 1. *Denotando por* a *e* b *os catetos e por* c *a hipotenusa, suponha, por absurdo, que nenhum deles seja múltiplo de* 3. *Assim,* a^2 *e* b^2 *deixam resto* 1 *na divisão por* 3. *Logo,* $a^2 + b^2$ *deixa resto* $1^2 + 1^2 = 2$ *na divisão por* 3*; o que é uma contradição, pois, pelo Teorema de Pitágoras,* $a^2 + b^2 = c^2$ *e* c^2 *deixa resto* 1 *na divisão por* 3.

2.2.2 Máximo Divisor Comum

Definição 2.4. (Máximo Divisor Comum). Sejam a e b inteiros diferentes de zero. Chama-se de máximo divisor comum de a e b, o inteiro positivo d que satisfaz as seguintes propriedades:

(a) d é um divisor comum de a e b, isto é, $d \mid a$ e $d \mid b$;

(b) Se $c \mid a$ e $c \mid b$, então $c \leq d$.

O máximo divisor comum de a e b é indicado por $d = mdc\,(a, b)$. E como o $mdc\,(a, b)$ não depende da ordem que são tomados, é imediato que $mdc\,(a, b) = mdc\,(b, a)$. Os casos seguintes também são imediatos:

1. O $mdc\,(0, 0)$ não existe;
2. O $mdc\,(1, a) = 1$;
3. Se $a \neq 0$, então o $mdc\,(a, 0) = |a|$;
4. Se $a \neq a$, então o $mdc\,(a, a) = |a|$;

Além disso, note que dados $a, b \in \mathbb{Z}$, se existir o $mdc\,(a, b)$, então

$$(a, b) = (-a, b) = (a, -b) = (-a, -b).$$

Dessa forma, o mdc de dois números, é sempre um número positivo.

Teorema 2.4. Sejam a e b dois inteiros. Então valem as seguintes afirmações:

(a) Se a é múltiplo de b, então o $mdc\,(a, b) = b$;

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

Demonstração: Inicia-se com a prova de (a). Com efeito, todo divisor comum dos números a e b é um divisor de b. Reciprocamente, como a é múltiplo de b, todo divisor de b também é um divisor de a, isto é, um divisor comum dos números a e b. Portanto, o conjunto dos divisores comuns dos números a e b é igual ao conjunto dos divisores de b. Como o maior divisor de b é ele mesmo, resulta que $mdc\,(a, b) = b$.

A demonstração de (b) é apresentada a seguir. Usando o item (g) do teorema 2.1 tem-se que o divisor comum de a e b também divide c e, consequentemente, é um divisor de b e c. Pela mesma razão todo divisor comum de b e c também divide a e , consequentemente, é um divisor de a e b. Portanto, os divisores comuns de a e b são os mesmos que os divisores comuns de b e c. Particularmente, também coincidem com os maiores divisores comuns, ou seja, $mdc\,(a, b) = mdc\,(b, c)$.

Teorema 2.5 (Teorema de Bachet-Bézout). Se d é o $mdc\,(a, b)$, então existem números inteiros x_0 e y_0 tais que $d = ax_0 + by_0$.

Demonstração: Considere a combinação linear $ax + by$, onde x e y percorrem todos os inteiros. Este conjunto de inteiros denotado por

$$M_{a,b} = \{ax + by; x, y \in \mathbb{Z}\},$$

inclui valores positivos e negativos. Além disso, escolhendo $x = y = 0$, vê-se que $M_{a,b}$ também contém o zero.

Pelo princípio da boa ordenação, basta escolher x_0 e y_0 tais que $\lambda = ax_0 + by_0$ seja o menor número inteiro positivo contido no conjunto $M_{a,b}$.

Agora será mostrado que $\lambda \,|\, a$ e $\lambda \,|\, b$. Suponha, por contradição, que $\lambda \nmid a$, então existem $q, r \in +Z$ tais que $a = \lambda q + r$ com $0 < r < \lambda$. Portanto,

$$r = a - \lambda q = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0)$$

e assim r está contido no conjunto $M_{a,b}$, o que é uma contradição com a hipótese de λ ser o menor elemento positivo contido em $M_{a,b}$.

Uma vez que λ divide a e b só resta provar que $\lambda = d$. Com efeito, desde que $d = mdc(a, b)$, pode-se escrever $a = da_1, ba = db_1$ e

$$\lambda = ax_0 + by_0 = d(a_1x_0 + b_1y_0).$$

Assim $d \,|\, \lambda$. Logo, pela parte (e) do Teorema 2.5, conclui-se que $d \leq \lambda$. Agora $d < \lambda$ é impossível pois $d = mdc\,(a, b)$ e portanto $d = \lambda = ax_0 + by_0$. O caso $\lambda \,|\, b$ é análogo.

A demonstração do Teorema 2.5 acima evidencia que o $mdc\,(a, b)$ é o menor inteiro positivo da forma $ax + by$, ou seja, que pode ser expresso como combinação linear de a e b. Mas esta representação não é única, pois

$$mdc\,(a, b) = d = a\,(x + bt) + b\,(y - at),$$

qualquer que seja o inteiro t.

Além disso, note que, se

$$d = ax_0 + by_0 \tag{18}$$

para algum par de inteiros x_0 e y_0. Então d não é necessariamente o $mdc\,(a, b)$. Assim, por exemplo, se

$$mdc\,(a, b) = ax + by,$$

então

$$t \cdot mdc\,(a,b) = atx + bty$$

para todo inteiro t, em que $d = t \cdot mdc\,(a,b), x_0 = tx$ e $y_0 = ty$ em (18).

Exemplo 2.7. Sejam os inteiros a = 6 e b = 15, tem-se que

$$mdc\,(15,6) = 3 \Rightarrow 15x + 6y = 3.$$

e, portanto:

$$mdc\,(a,b) = 3 = 15\,(1+6t) + 6\,(-2-15t)$$

qualquer que seja o inteiro t.

Há resultados importantes ao nosso estudo, correspondentes ao âmbito de números primos entre si, que são números cujo máximo divisor comum é 1. Assim, dois números inteiros a e b serão ditos primos entre si, se $mdc\,(a,b) = 1$.

Teorema 2.6. Considere $a, b \in \mathbb{Z}^*$. Então a e b são primos entre si se, e somente se, existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$.

Demonstração: Suponha que existam $x, y \in \mathbb{Z}$ tais que $ax + by = 1$ e seja $d = mdc(a,b)$. Então, segue do item (g) do Teorema 2.1, que $d \,|\, 1$ e, portanto, $d = 1$. A recíproca é imediata.

Lema 2.1 (Lema de Gauss). Sejam a, b e c números inteiros. Se $a \,|\, bc$ e $mdc\,(a,b) = 1$, então $a \,|\, c$.

Demonstração: Como $mdc\,(a,b) = 1$, tem-se que existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$. Multiplicando essa última igualdade por c, obtém-se $acx + bcy = c$. Por hipótese, $a \,|\, bc$ e $a \,|\, a$, assim, pelo item (g) do Teorema 2.1, segue que $a \,|\, (acx + bcy)$ e, portanto, $a \,|\, c$.

2.2.3 Algoritmo de Euclides

Embora sejam conhecidas propriedades teóricas do *mdc* entre dois inteiros, encontrá-lo nem sempre é tarefa fácil, ainda mais se não forem utilizadas as ferramentas adequadas. Pelo significado, é natural pensar em calcular todos os divisores de a, todos os divisores

de b e descobrir qual é o maior elemento comum aos dois conjuntos. Para achar o mdc se faz uso de um importante método denominado *Algoritmo Euclides*, um primor do ponto de vista computacional e pouco conseguiu-se aperfeiçoa-lo em pouco mais de dois milênios.

Teorema 2.6. (Algoritmo de Euclides). Dados dois inteiros positivos, a e b, aplica-se sucessivamente a divisão euclidiana para obter a seguinte sequência de igualdades

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

até algum r_n dividir r_{n-1}. Assim, o $mdc\,(a, b) = r_n$, ou seja, é o último resto não-nulo no processo de divisão anterior.

Demonstração: Note que o processo de divisão acima é finito. Com efeito a sequência de números inteiros r_k é estritamente decrescente e está contida no conjunto $\{r \in \mathbb{Z}, 0 \leq r < a\}$, portanto não pode conter mais do que a inteiros positivos. Examinando as igualdades e utilizando a teorema 2.4 tem-se

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

Exemplo 2.8. Achar o mdc($\underbrace{111...111}_{80vezes}, \underbrace{111...111}_{50vezes}$).

Solução: *Primeiro escreve-se os números na base decimal, ou seja,*

$$\underbrace{111...111}_{80vezes} = 10^{79} + 10^{78} + \cdots + 1,$$

$$\underbrace{111...111}_{50vezes} = 10^{49} + 10^{48} + \cdots + 1.$$

Aplica-se agora o algoritmo de Euclides para obter as seguintes igualdades

$$\underbrace{111...111}_{80vezes} = (10^{49} + 10^{48} + \cdots + 1)10^{30} + 10^{29} + 10^{28} + \cdots + 1,$$

$$\underbrace{111...111}_{50vezes} = (10^{39} + 10^{38} + \cdots + 1)10^{10} + 10^{9} + 10^{8} + \cdots + 1,$$

$$10^{29} + 10^{28} + \cdots + 1 = (10^{19} + 10^{18} + \cdots + 1)10^{10} + 10^{9} + 10^{8} + \cdots + 1.$$

Disso resulta que

$$\begin{aligned} mdc\,(\underbrace{111...111}_{80vezes}, \underbrace{111...111}_{50vezes}) &= 10^{9} + 10^{8} + \cdots + 1, \\ &= (\underbrace{111...111}_{10vezes}). \end{aligned}$$

Conclusão: o número de vez que o 1 aparece, que são 10 vezes, é o mdc(50,80) = 10.

Exemplo 2.9. Utilize o algoritmo de Euclides para encontrar o $mdc\,(748, 517)$.

Solução: *Para resolver o problema, será utilizado um dispositivo cujo processo prático se traduz como segue: para se encontrar o mdc de dois números inteiros positivos, divide-se maior dos números pelo menor, este pelo primeiro resto obtido, o segundo resto pelo primeiro resto obtido e assim sucessivamente até se encontrar resto nulo. Então*

	1	2	4	5
748	517	231	55	11
231	55	11	0	

Portanto o $mdc\,(748, 517) = 11$. *Além disso, pode-se encontrar a expressão do* $mdc\,(748, 517) = 11$ *como combinação linear de* 748 *e* 517, *conforme segue:*

$$\begin{aligned} 748 &= 517 \cdot 1 + 231 \\ 517 &= 231 \cdot 2 + 55 \\ 231 &= 55 \cdot 4 + 11 \\ 55 &= 11 \cdot 5 + 0. \end{aligned} \tag{19}$$

Pode-se isolar 11 *em (21), depois substituir adequadamente as informações de (19) e (20) para obter*

$$\begin{aligned} 11 &= 231 - 4 \cdot 55 \\ &= 231 - 4 \cdot (517 - 231 \cdot 2) \\ &= 231 - 4 \cdot 517 + 8 \cdot 231 \\ &= 9 \cdot 231 - 4 \cdot 517 \\ &= 9 \cdot (748 - 1 \cdot 517) - 4 \cdot 517 \\ &= 9 \cdot 748 - 9 \cdot 517 - 4 \cdot 517 \\ &= 748 \cdot 9 + 517 \cdot (-13). \end{aligned} \tag{20}$$

Logo,

$$11 = mdc\,(748, 517) = 748x + 517y,$$

em que $x = 9$ e $y = -13$. *Essa combinação linear não é única.*

3 Fundamentos Básicos de Congruências

Nesta seção é apresentada uma das noções mais fecundas da aritmética, introduzida por Gauss em seu livro *DisquisiotionesArithmeticae*, de 1801. Consiste na realização de uma aritmética com restos da divisão euclidiana por um número fixado, conforme já tratou-se ao falar em divisibilidade. Todas essas definições e resultados apresentados posteriormente aqui podem ser encontrados em Filho (1981), Fomin (2019), Hefez (2016) e Santos (1998).

Definição 3.1. Seja m um número natural. Diz-se que dois números a e b são congruentes módulo m e, escreve-se $a \equiv b \mod m$, se os restos de sua divisão por m são iguais. Caso contrário, diz-se que a e b são incongruentes e, denota-se $a \not\equiv b \mod m$.

Exemplo 3.1. $25 \equiv 11 \mod 7$*, pois os restos da divisão de* 25 *e* 11 *por* 7 *são iguais a* 4*.*

Exemplo 3.2. $13 \not\equiv 8 \mod 6$*, pois os restos da divisão de* 13 *e* 8 *por* 6*, são* 1 *e* 2*, respectivamente.*

Considerando a definição 3.1, para verificar se dois números são congruentes módulo m, não é necessário efetuar a divisão euclidiana de ambos por m para depois comparar seus restos. É suficiente a aplicação do resultado apresentado na proposição 3.1 a seguir.

Proposição 3.1. Suponha que $a, b, m \in \mathbb{Z}$, com $m > 1$. Então $a \equiv b \mod m$ 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 $a \equiv b \mod m$. Segue, da definição, que, $r = r'$ e daí $b - a = m(q' - q) + r' - r = m(q' - q)$, portanto, $m \mid b - a$.

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 $m \in \mathbb{N}$. Para todos $a, b, c \in \mathbb{Z}$, tem-se que

(a) *Reflexiva*: $a \equiv a \mod m$;

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

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

Demonstração: (a) Como $m \mid 0$, então, $m \mid (a-a)$ o que implica que $a \equiv a \mod m$. (b) Se $a \equiv b \mod m$, então $a = b + k_1 m$, $k_1 \in \mathbb{Z}$. Logo, $b = a - k_1 m$, o que implica pela proposição 3.1, que $b \equiv a \mod m$. (c) Se $a \equiv b \mod m$ e $b \equiv c \mod m$, 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 $a - c \equiv m(k_1 + k_2) \mod m$, de onde segue que, $a \equiv c \mod m$.

Reciprocamente, suponha que $m \mid b - a$. Como $r' - r = b - a - m(q' - q)$ e $m \mid b - a$, concluimos que $m \mid r' - r$. Sendo $0 \leq r', r < m$, tem-se que $|r' - r| < m$, logo $r' = r$. Portanto, $a \equiv b \mod m$.

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

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

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

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

(d) Se $a \equiv b \mod m$, então $ka \equiv kb \mod m$, $\forall k \in \mathbb{Z}$;

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

Demonstração:

(a) De $a \equiv b \mod m$ e $c \equiv d \mod m$, segue que existem $k_1, k_2 \in \mathbb{Z}$ 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 $a + c \equiv b + d \mod m$.

(b) Basta subtrair membro a membro as equações $a - b = mk_1$ e $c - d = mk_2$, que implica em $(a - c) - (b - d) = m(k_1 - k_2)$, acarretando $a - b \equiv c - d \mod m$.

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

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

(e) Será utilizada indução sobre k. Para $k = 1$ a proposição é verdadeira, pois, $a^1 \equiv b^1 \mod m$ conforme hipótese. Supondo a propriedade verdadeira para k, isto é, que $a^k \equiv b^k$

mod m, deve-se mostrar que isso implica na validade para $k+1$, ou seja, $a^{k+1} \equiv b^{k+1}$ mod m. De fato, como $a \equiv b \mod m$ e, por hipótese de indução, $a^k \equiv b^k \mod m$, basta multiplicar, membro a membro as congruências, para obter, $a \cdot a^k \equiv b \cdot b^k \mod m$, o que acarreta $a^{k+1} \equiv b^{k+1} \mod m$.

Exemplo 3.3. Mostrar que $2.222^{5.555} + 5.555^{2.222}$ é divisível por 3.

Solução: *Como* $2.222 = 740 \cdot 3 + 2$ *e* $5.555 = 1851 \cdot 3 + 2$ *tem-se que*

$$2.222 \equiv 2 \mod 3 \text{ e } 5.555 \equiv 2 \mod 3.$$

Sendo $2 \equiv -1 \mod 3$, *pelo item (c) da proposição 3.2 tem-se que*

$$2.222 \equiv -1 \mod 3 \text{ e } 5.555 \equiv -1 \mod 3.$$

Assim pelo item (e) da proposição 3.3,

$$2.222^{5.555} \equiv -1 \mod 3 \text{ e } 5.555^{2.222} \equiv 1 \mod 3.$$

Logo, pelo item (a) da proposição 3.3,

$$2.222^{5.555} + 5.555^{2.222} \equiv 0 \mod 3.$$

A proposição 3.3, em seu item (a), nos diz que, para as congruências, vale o cancelamento com respeito à adição. No entanto, em geral, isto não é válido para a multiplicação como se pode verificar no exemplo a seguir.

Exemplo 3.4. *Como* $4 \cdot 9 - 4 \cdot 5 = 16$ *e* $8 \mid 16$, *tem-se que* $4 \cdot 9 \equiv 4 \cdot 5 \mod 8$, *entretanto,* $9 \not\equiv 5 \mod 8$.

Mas pode-se realizar o cancelamento multiplicativo desde que atendida a condição apresentada no seguinte resuldado.

Proposição 3.4. Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$ e $mdc(c, m) = 1$. Então

$$ac \equiv bc \mod m \iff a \equiv b \mod m.$$

Demonstração: Se $ac \equiv bc \mod m$, então $m \mid (a-b)c$. Como $mdc\,(c, m) = 1$, tem-se pelo Lema de Gauss, que $m \mid (a-b)$. Portanto, $a \equiv b \mod m$.

3.1 O Pequeno Teorema de Fermat

Estima-se que antes de 500 anos A. C., os chineses sabiam que, se p é um número primo, então $p \mid (2^p - 2)$. Mas foi Pierre Fermat quem generalizou esse resultado, enunciando O Pequeno Teorema de Fermat apresentado a seguir. Antes, será apresentado o Lema 3.1, necessário à sua demonstração .

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

Demonstração: O resultado vale trivialmente para $i = 1$. Pode-se, supor $0 < i < p$. Nesse caso, $i! \mid p(p-1)\cdots(p-i+1)$. Como $mdc(i!, p) = 1$, decorre que $i! \mid (p-1)\cdots(p-i+1)$, e o resultado se segue, pois

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

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

Demonstração: Se $p = 2$, então $a^2 - a = a(a-1)$ é par e assim 2 divide $a^2 - a$. Suponha p ímpar. Nesse caso, como

$$(-a)^p - (-a) = -(a^p - a),$$

basta provar o resultado para $a \geq 0$. Para isso, será utilizada indução sobre a. O resultado vale para $a = 0$, pois p divide 0. Supondo o resultado válido para a, deve-se prová-lo para $a + 1$. Pelo Binômio de Newton,

$$(a+1)^p - (a+1) = a^p - a + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a. \tag{21}$$

Pela hipótese de indução e o fato de que $\binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a$ é divisível por p conforme Lema 3.1, conclui-se que p divide $(a+1)^p - (a+1)$.

Exemplo 3.5. Determine os números primos tais que p divide $3^p + 382$.

Solução: *Como p é primo, pelo Teorema de Fermat, tem-se que $p \mid 3^p - 3$. Escreve-se*

$$3^p + 382 = 3^p - 3 + 385$$

e, conclui-se pelo item (h) do Teorema 2.1 que $p \mid 3^p + 382$ *se, e somente se,* p *divide* $385 = 5 \cdot 7 \cdot 11$. *Portanto,* $p = 5, 7$ *ou* 11.

O Pequeno Teorema de Fermat é muito útil na resolução dos problemas abordados neste trabalho 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 3.6. Encontre o resto da divisão de 237^{28} por 13.

Solução: *Inicialmente, note que* $237 \equiv 3 \mod 13$ *pois o resto da divisão de* 237 *por* 13 *é* 3. *Pelo Pequeno Teorema de Fermat, segue que* $237^{12} \equiv 1 \mod 13$. *Logo, pelo item (e) da proposição 3.3, segue que*

$$237^{24} = (237^{12})^2 \equiv 1 \mod 13. \tag{22}$$

Analogamente, tem-se que

$$237^4 \equiv 3^4 \equiv 81 \equiv 3 \mod 13. \tag{23}$$

Usando (25), (26) e o item (c) da proposição 3.3, obtem-se que $237^{28} \equiv 3 \mod 13$. *Portanto, o resto da divisão de* 237^{28} *por* 13 *é* 3.

Exemplo 3.7. Determine o resto da divisão por 19 do número

$$S = 1^{18} + 2^{18} + 3^{18} + \cdots + 95^{18}.$$

Solução: *Encontrar o resto da divisão de* S *por* 19 *equivale a resolver a congruência*

$$S \equiv x \mod 19,$$

onde $S = 1^{18} + 2^{18} + 3^{18} + \cdots + 95^{18}$.

De 1 *a* 95 *há* 5 *múltiplos de* 19*, a saber:* $19, 38, 57, 76$ *e* 95*. Isso signifca que esses números são congruentes a* 0 *módulo* 19*, ou seja:*

$$19, 38, 57, 76, 95 \equiv 0 \mod 19$$

assim,

$$19^{18}, 38^{18}, 57^{18}, 76^{18}, 95^{18} \equiv 0 \mod 19. \tag{24}$$

Basta então calcular a soma dos restos dos demais números por 19*. Como* 19 *não divide nenhum deles e, além disso é primo, segue do Pequeno Teorema de Fermat que*

$$\begin{aligned} 1^{18} &\equiv 1 \mod 19 \\ 2^{18} &\equiv 1 \mod 19 \\ 3^{18} &\equiv 1 \mod 19 \\ &\cdots \\ 93^{18} &\equiv 1 \mod 19 \\ 94^{18} &\equiv 1 \mod 19. \end{aligned} \tag{25}$$

Somando membro a membro as equações em (28), obtem-se

$$\begin{aligned} S = 1^{18} + 2^{18} + 3^{18} + \cdots + 95^{18} &\equiv 1 + 1 + 1 + \cdots + 1 \mod 19, \\ &\equiv \underbrace{1 + 1 + 1 + \cdots + 1}_{90\, vezes} \mod 19, \\ &\equiv 90 \mod 19, \\ &\equiv 14 \mod 19. \end{aligned} \tag{26}$$

Logo, o resto da divisão de S *por* 19 *é 14.*

3.2 Critérios de divisibilidade

Os critérios de divisibilidade permitem determinar se um número $n \in \mathbb{N}$ é divisível ou não por outro, a um custo menor que efetuar a divisão. A teoria de congruências é

ferramenta poderosa para evidenciar tais critérios, conforme apresenta-se a seguir.

Exemplo 3.8. Critérios de divisibilidade por $2, 5$ e 10.

Um número inteiro é divisível por 2 quando o último algarismo é par ou é zero. Note que todo número $n \in \mathbb{N}$ pode ser escrito como $n = a_n a_{n-1} \cdots a_1 a_0$, ou equivalentemente, $n = a_r 10^r + a_{r-1} 10^{r-1} + \cdots + a_1 10 + a_0$. Utilizando essa última representação de n e a noção de congruência, tem-se que

$$\begin{aligned} 10^0 \equiv 1 \mod 2 &\implies a_0 10^0 \equiv a_0 \mod 2 \\ 10^1 \equiv 0 \mod 2 &\implies a_1 10^1 \equiv 0 \mod 2 \\ 10^2 \equiv 0 \mod 2 &\implies a_2 10^2 \equiv 0 \mod 2 \\ &\cdots \\ 10^r \equiv 0 \mod 2 &\implies a_r 10^r \equiv 0 \mod 2. \end{aligned} \tag{27}$$

Pelo item (a) da proposição 3.3 pode-se somar membro a membro as equações de congruências em (27), para obter

$$n = a_r 10^r + a_{r-1} 10^{r-1} + \cdots + a_1 10 + a_0 \equiv a_0 \mod 2, \tag{28}$$

o que nos diz que o resto da divisão de um número natural n na base 10 por 2 depende somente de a_0 que é o último algarismo da direita. Assim, Portanto, n é divisível por 2 se $a_0 = 0, 2, 4, 6, 8$.

De modo análogo, conseguimos evidenciar os critérios de divisiblidade por 5 e por 10. Portanto, n é divisível por 5 se $a_0 = 0$ ou $a_0 = 5$ e n é divisível por 10, se é divisível por 2 e por 5, simultaneamente. Logo, $a_0 = 0$.

Exemplo 3.9. Critério de divisibilidade por 3 e 9.

Um número natural é divisível por 3 se, e somente se, a soma de seus algarismos for um número divisível por 3. Utilizando a noção de congruências segue que

$$\begin{aligned}
10^0 \equiv 1 \mod 3 &\implies a_0 10^0 \equiv a_0 \mod 3 \\
10^1 \equiv 1 \mod 3 &\implies a_1 10^1 \equiv a_1 \mod 3 \\
10^2 \equiv 1 \mod 3 &\implies a_2 10^2 \equiv a_2 \mod 3 \\
&\cdots \\
10^r \equiv 1 \mod 3 &\implies a_r 10^r \equiv a_r \mod 3.
\end{aligned} \tag{29}$$

Pelo item (a) da proposição 3.3 pode-se somar membro a membro as equações de congruências em (29), para obter

$$n = a_r 10^r + a_{r-1} 10^{r-1} + \cdots + a_1 10 + a_0 \equiv a_r + \cdots + a_1 + a_0 \mod 3, \tag{30}$$

o que nos diz que o resto da divisão de um número por 3 *só depende da soma dos seus algarismos. Portanto, um número é divisível por* 3 *se* $a_r + \cdots + a_1 + a_0$ *é múltiplo de* 3.

A divisibilidade por 9 *segue a mesma estrutura da divisibilidade por* 3*, pois*

$$\begin{aligned}
10^0 \equiv 1 \mod 9 &\implies a_0 10^0 \equiv a_0 \mod 9 \\
10^1 \equiv 1 \mod 9 &\implies a_1 10^1 \equiv a_1 \mod 9 \\
10^2 \equiv 1 \mod 9 &\implies a_2 10^2 \equiv a_2 \mod 9 \\
&\cdots \\
10^r \equiv 1 \mod 9 &\implies a_r 10^r \equiv a_r \mod 9.
\end{aligned} \tag{31}$$

Somando membro a membro tem-se que

$$a_r 10^r + a_{r-1} 10^{r-1} + \cdots + a_1 10 + a_0 \equiv (a_r + \cdots + a_1 + a_0) \mod 9. \tag{32}$$

Assim, o resto da divisão de um número por 9 *depende somente da soma dos seus algarismos. Portanto,* n *é divisível por* 9 *se* $a_r + \cdots + a_1 + a_0$ *for múltiplo de* 9.

Exemplo 3.10. Critério de divisibilidade por 4 e 8.

Um número natural é divisível por 4 *quando o número formado pelos dois últimos algarismos da direita for divisível por 4. Note que,*

$$\begin{aligned}
10^0 \equiv 1 \mod 4 &\implies a_0 10^0 \equiv a_0 \mod 4 \\
10^1 \equiv 2 \mod 4 &\implies a_1 10^1 \equiv 2a_1 \mod 4 \\
10^2 \equiv 0 \mod 4 &\implies a_2 10^2 \equiv 0 \mod 4 \\
&\cdots \\
10^r \equiv 0 \mod 4 &\implies a_r 10^r \equiv 0 \mod 4.
\end{aligned} \tag{33}$$

Somando membro a membro as equações em (36), tem-se

$$a_r 10^r + a_{r-1} 10^{r-1} + \cdots + a_1 10 + a_0 \equiv 2a_1 + a_0 \mod 4. \tag{34}$$

Assim, $n = a_r 10^r + a_{r-1} 10^{r-1} + \cdots + a_1 10 + a_0 \equiv 2a_1 + a_0 \mod 4$*, isto é, o resto da divisão de um número por* 4 *depende somente da soma do dobro do penúltimo algarimo com o último algarismo. Logo,* n *é divisível por* 4 *se* $2a_1 + a_0$ *é múltiplo de* 4*.*

De modo análogo, evidencia-se a divisibilidade por 8*, pois,*

$$n = a_r 10^r + a_{r-1} 10^{r-1} + \cdots + a_1 10 + a_0 \equiv 4a_2 + 2a_1 + a_0 \mod 8 \tag{35}$$

Portanto, n *é divisível por* 8 *se* $4a_2 + 2a_1 + a_0$ *é múltiplo de* 8*.*

Exemplo 3.11. Critério de divisibilidade por 6.

Um número é divisível por 6, se é divisível por 2 e por 3, simultaneamente.

Exemplo 3.12. Critério de divisibilidade por 7.

Para verificar se um número natural é divisível por 7, multiplica-se por 2 o último algarismo do número dado, depois subtraia este valor do número inicial excluindo o último algarismo, se o resultado for múltiplo de 7 então o número inicial também será. Utilizando congruência modular, note que

$$\begin{aligned}
10^0 \equiv 1 \mod 7 &\implies a_0 10^0 \equiv a_0 \mod 7 \\
10^1 \equiv 3 \mod 7 &\implies a_1 10^1 \equiv 3a_1 \mod 7 \\
10^2 \equiv 2 \mod 7 &\implies a_2 10^2 \equiv 2a_2 \mod 7 \\
10^3 \equiv -1 \mod 7 &\implies a_3 10^3 \equiv -a_3 \mod 7 \\
10^4 \equiv -3 \mod 7 &\implies a_4 10^4 \equiv -3a_4 \mod 7 \\
10^5 \equiv -2 \mod 7 &\implies a_5 10^5 \equiv -2a_5 \mod 7 \\
10^6 \equiv 1 \mod 4 &\implies a_6 10^6 \equiv a_6 \mod 7 \\
&\cdots
\end{aligned} \tag{36}$$

Somando membro a membro as equações em (36), obtem-se

$$\cdots + a_3 10^3 + a_2 10^2 + a_1 10^1 + a_0 \equiv \cdots - (a_3 + 3a_4 + 2a_5) + (a_0 + 3a_1 + 2a_2) \mod 7. \tag{37}$$

Assim, pode-se efetuar as operações que aparecem do lado direito da equação de congruência para verificar se determinado número n é divisível ou não por 7.

Exemplo 3.13. Critério de divisibilidade por 11.

Considere n na sua forma decimal, $n = a_r 10^r + a_{r-1} 10^{r-1} + \cdots + a_1 10 + a_0$. Como $10 \equiv -1 mod 11$ segue que

$$\begin{aligned}
a_0 &\equiv a_0 \mod 11 \\
a_1 10 &\equiv -a_1 \mod 11 \\
a_2 10^2 &\equiv a_2 \mod 11 \\
a_3 10^3 &\equiv -a_3 \mod 11 \\
&\cdots \\
a_r 10^r &\equiv a_r \mod 11
\end{aligned} \tag{38}$$

somando as equações em (38) membro a membro, conforme item (a), da Proposição 3.3, obtem-se

$$n = a_0 + a_1 10 + \cdots + a_{r-1} 10^{r-1} + a_r 10^r \equiv a_0 - a_1 + \cdots - a_{r-1} 10^{r-1} + a_r 10^r \mod 11, \tag{39}$$

de onde conclui-se que n é divisível por 11 se, e somente se, o número $a_0 - a_1 + a_2 - a_3 + a_4 + \cdots - a_{r-1} + a_r$ for divisíel por 11.

3.2.1 Outros critérios de divisibilidade

Apresenta-se nesta seção critérios de divisibilidade fáceis, porém menos usuais denominados não mnemônicos. Corrobora-se com Táboas e Ribeiro (RPM 6, p.21) quando afirmam que um critério de divisibilidade só é útil quando for mais simples que a própria divisão. Isso porque é possível conseguir diversas regras ou uma infinidade de critérios de divisbilidade e, portanto, a aplicabilidade dos mesmos se dará se o esforço dispensado ao utilizá-los for menor do que efetuar a divisão. Para fins de síntese apresenta-se os critérios não mnemônicos para os números 7 e 11 com suas respectivas justificativas e uma tabela com os critérios para os números primos de 7 a 100.

Considere n na sua forma decimal

$$\begin{aligned} n &= b_r 10^r + b_{r-1}10^{r-1} + \cdots + b_1 10 + b_0, \\ &= (b_{r-1}10^{r-1} + b_{r-2}10^{r-2} + \cdots + b_1)10 + b_0. \end{aligned} \tag{40}$$

Observe em (40) que pode-se reescrever n como

$$n = 10a + b_0. \tag{41}$$

A equação em (41) é utilizada para apresentar os critérios não mnemônicos pelos números 7 e 11 nos exemplos a seguir.

Exemplo 3.14. Critério de divisibilidade não mnemônico por 7.

Observe que $10 \equiv 3 \mod 7$. *Então, por (41), segue*

$$n \equiv 10a + b_0 \equiv 3a + b_0 \mod 7. \tag{42}$$

Multiplicando (42) por -2 e, considerando que $6 \equiv -1 \mod 7$, *obtém-se*

$$-2n \equiv a - 2b_0 \mod 7. \tag{43}$$

Assim, se n é divisível por 7 tem-se $0 \equiv a - 2b_0$.

Conclui-se, por esse critério, que um número é divisível por 7 se, e somente se, o dobro do algarismo das unidades subtraído da soma dos demais algarismos resultar em um número divisíve por 7.

Alternativamente, pode-se multiplicar (42) por 5 e, considerando que $15 \equiv 1 \mod 7$, *obtém-se*

$$5n \equiv a + 5b_0. \tag{44}$$

Por (44) se n é divisível por 7, então $0 \equiv a + 5b_0$. De onde conclui-se que um número é divisível por 7, se e somente se, a soma do quíntuplo do algarismo das unidades com os demais algarismos for um múltiplo de 7.

As equações apresentadas em (43) e (44) representam os critérios de divisibilidade não mnemônicos por 7 nas suas formas subtrativa e aditiva respectivamente.

Exemplo 3.15. Critério de divisibilidade não mnemônico por 11.

Note que $10 \equiv -1 \mod 11$, *então pode-se escrever (41) como,*

$$n \equiv 10a + b_0 \equiv -a + b_0 \mod 11. \tag{45}$$

Multiplicando (45) por 10, obtém-se

$$\begin{aligned} n &\equiv a + 10b_0 && (46)\\ &\equiv a - b_0. && (47) \end{aligned}$$

Por (46) e (47) se n é divisível por 11, então $0 \equiv a + 10b_0 \mod 11$ e $0 \equiv a - b_0$, respectivamente. Conclui-se, pelo critério aditivo, que um número é divisível por 11 se, e somente se, a soma do decúplo do algarismo das unidades com os demais algarismos resultar em um número divisível por 11. Pelo critério subtrativo, um número é divisível por 11 se, e somente se, o algarismo das unidades subtraído da soma dos demais algarismos resultar em um número divisível por 11.

Na Tabela 2 são apresentados critérios de divisibilidade não mnemônicos que possibilitam ao leitor verificar, com facilidade, se um dado número é, ou não, divsível por um número primo entre 7 e 100.

Tabela 2 – Critérios não mnemônicos primos de 7 a 100

n.º	**aditiva**	**subtrativa**	**n.º**	**aditiva**	**subtrativa**
7	*a + 5b*	*a - 2b*	47	*a + 80b**	*a - 14b*
11	*a + 10b*	*a - b*	53	*a + 16b*	*a - 90b**
13	*a + 4b*	*a - 9b*	59	*a + 6b*	*a - 53b*
17	*a + 12b*	*a - 5b*	61	*a + 55b*	*a - 6b*
19	*a + 2b*	*a - 17b*	67	*a + 47b*	*a - 20b*
23	*a + 7b*	*a - 16b*	71	*a + 64b*	*a - 7b*
29	*a + 3b*	*a - 26b*	73	*a + 22b*	*a - 51b*
31	*a + 90b**	*a - 3b*	79	*a + 8b*	*a - 71b*
37	*a + 26b*	*a - 11b*	83	*a + 25b*	*a - 58b*
41	*a + 37b*	*a - 4b*	89	*a + 9b*	*a - 80b*
43	*a + 13b*	*a - 30b*	97	*a + 68b*	*a - 29b*

*90, 80 e 90 foram colocados na tabela no lugar dos números 28, 33 e 37, respectivamente, porque dão mais agilidade no processo.

Fonte: GUEDES, RPM 12, p. 24.

A tabela contém os números primos de 7 a 100 com critérios na forma aditiva e na forma subtrativa, ratificando o fato mencionado anteriormente sobre a diversidade de regras que pode-se obter justificadamente usando a teoria de congruência modular.

3.3 Aplicações de congruência modular no cotidiano

Nesta seção são apresentadas algumas aplicações de congruência modular no cotidiano, apresentando as potencialidades da teoria bem como esta se revela na sociedade, em particular, na tecnologia. Será dado enfoque em sistemas de identificação e criptografia.

3.3.1 Sistemas de identificação

De maneira geral, é simples perceber um erro de ortografia em um texto, pois há somente duas possibilidades: a palavra não existe no idioma ou não faz sentido no contexto. Mas se ocorre a troca de algarismos de um número ou mesmo de um código de identificação, a verificação do erro não é uma tarefa tão fácil. Com o objetivo de evitar fraudes, foram criados os dígios de controle ou de verificação que são baseados na noção de congruência.

Exemplo 3.14. O código de barras EAN-13 está presente em nosso cotidiano em uma diversidade considerável de produtos. Consiste numa sequência de 13 dígitos traduzidos para barras de cores preta ou branca de espessuras variadas. Na verdade, são quatro as espessuras possíveis para as barras: finas, médias, grossas ou muito grossas.

Figura 1 – Código de barras

Fonte: GS1

Conforme mencionado, observa-se que na Figura 1, o código de barras representa uma série de números aos quais são firmados espaços de espessura fixa, que corresponde sempre a uma sequência de 7 dígitos iguais a 0 ou 1. 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. Para mais detalhes, sugerimos consulta a Milies (2009). No que concerne ao particionamento do código, os três primeiros números indicam o país que o produto foi cadastrado, o segundo bloco de números identifica a empresa que fabricou o produto (varia de 4 a 7 dígitos), o terceiro bloco identifica o produto (considera tipo, quantidade, embalagem, peso, tamanho) e por fim tem-se o dígito verificador obtido com operações sobre os números anteriores.

Para verificar se ocorreu algum erro de digitação no código EAN-13, exemplificar-se-á como é atribuído o dígito de verificação, o qual será denotado por x . Considere o código $a_1a_2 \cdots a_{12}x$ de um produto cadastrado no EAN-13. Como os 12 primeiros dígitos contêm informações sobre país de cadastro, empresa fabricante e produto, eles são naturalmente determinados por um método padrão pertencente a autoridade classficadora do país. Denote-se por $\alpha = (a_1, a_2, \cdots, a_{12}, x)$ e, considere um vetor fixo w utilizado pelo sistema EAN-13, tal que

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

Calculando o produto dos vetores α e w, obtém-se:

$$\begin{aligned}\alpha \cdot w &= (a_1, a_2, \cdots, a_{12}, x) \cdot (1,3,1,3,1,3,1,3,1,3,1,3,1) \\ &= a_1 \cdot 1 + a_2 \cdot 3 + a_4 \cdot 1 + a_5 \cdot 3 + \cdots + a_{10} + a_{11} + a_{12} \cdot 3 + x \cdot 1 \qquad (48) \\ &= a_1 + 3a_2 + a_3 + 3a_3 + a_5 + 3a_6 + a_7 + 3a_8 + a_9 + 3a_{10} + a_{11} + 3a_{12} + x\end{aligned}$$

Então escolhe-se x de forma que a soma em (48) seja um número múltiplo de 10, isto é, que

$$\alpha \cdot w \equiv 0 \mod 10, \qquad (49)$$

caso a equação em (49) não se verifique, o computador informa que existe algum erro no código.

Tomando como exemplo o código de barras da Figura 1. Os dígitos conhecidos serão representados por

$$\alpha = (7,8,9,8,3,5,7,4,1,0,0,1,x)$$

e deseja-se descobrir o dígito verificador x. Para isso deve-se multiplicar α por w em que

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

obtendo

$$\begin{aligned}\alpha \cdot w &= 7 + 8 \cdot 3 + 9 + 8 \cdot 3 + 3 + 5 \cdot 3 + 7 + 4 \cdot 3 + 1 + 1 \cdot 3 + x \\ &= 105 + x \qquad (50)\end{aligned}$$

Assim, para que a soma em (50) seja um número múltiplo de 10, ou seja, $105 + x \equiv 0 \mod 10$, deve-se ter $x = 5$, ratificando o código de barras do exemplo.

Exemplo 3.15. O International Standard Book Number - ISBN foi criado em 1969 devido a necessidade das editoras catalogarem livros e informatizarem o sistema de encomendas. É utilizado para catalogação de publicações monográficas como livros, artigos, apostilas, CD-Roms, publicações em braile etc. A criação desse padrão representou um marco do no mercado editorial, otimizando os processos de produção, distribuição, análise de vendas a armazenamento de dados bibliográficos. Uma vantagem de sua utilização reside no fato de superar as barreiras idiomáticas, pois o código consiste na identificação de publicações através de um código de 13 algarismos. Nesse código, o último dígito é calculado através de

arimética modular envolvendo os outros doze dígitos e, estes sempre são fracionados em 4 partes, de tamanhos diversos, contendo informações do país, editora e livro ou publicação.

A distribuição dos números no código ISBN ocorre da seguinte forma: a primeira seção de algarismos corresponde ao código Global Trade Item Number - GTIN (um identificador para itens comerciais desenvolvido e controlado pela GS1), a segunda indica o país ou grupo registrante, a terceira a editora, a quarta a publicação no âmbito de controle da editora e o último é o de verificação. Se houver algum dígito errado ou mesmo troca de dígitos adjacentes, os erros serão detectados pelo método de verificação ISBN, de outro modo o código ISBN será inválido. Para calcular o dígito verificador no sistema ISBN, pode-se realizar as seguintes etapas:

1) Multiplicar os 12 primeiros dígitos mais o 13° pela base $\{1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1\}$;

2) Calcular a soma dos produtos de 1) e, verificar qual valor a_{13} pode assumir para que essa soma seja um número múltiplo de 10.

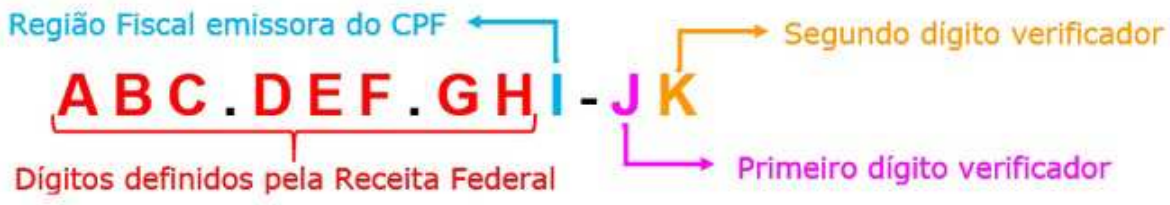
Tomando , como exemplo, o livro de Aritmética do PROFMAT tem ISBN 978-85-8337-105-2. O dígito de verificação é 2 pois

$$9\cdot 1+7\cdot 3+8\cdot 1+8\cdot 3+5\cdot 1+8\cdot 3+3\cdot 1+3\cdot 3+7\cdot 1+1\cdot 3+0\cdot 1+5\cdot 3+2 \equiv 0 \mod 10. \quad (51)$$

Por (51) conclui-se que a verificação feita pelo computador é uma congruência módulo 10.

Exemplo 3.16. O cadastro de pessoas físicas - CPF no Brasil é constituído de 11 dígitos, em que os dois últimos, assim como nos códigos de barras e ISBN, são dígitos de controle ou verificação determinados com aplicação da noção de congruência.

Figura 2 – Cadastro de pessoas físicas.

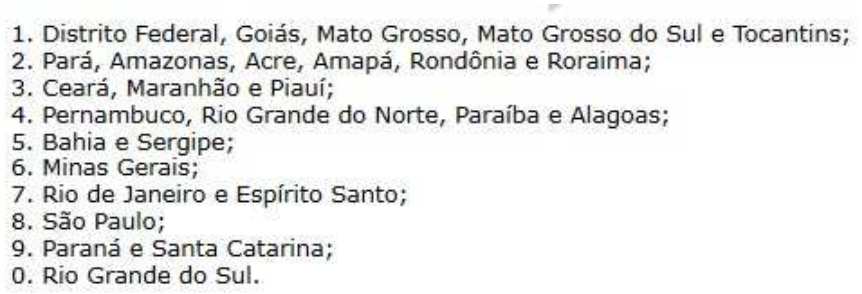


Fonte: Clubes de Matemática da Obmep

A Figura 2 apresenta o significado dos dígitos que compõem o CPF no Brasil: os oito primeiros dígitos formam um número-base definido pela Receita Federal no ato da

inscrição; o nono dígito define a Região Fiscal responsável pela emissão conforme a Figura 3; o penúltimo dígito representado pela letra J é o dígito verificador dos nove primeiros; o último dígito, representado por K, é o dígito verificador dos outros nove anteriores a ele.

Figura 3 – Região Fiscal de emissão de CPF.



Fonte: Receita Federal

A Fgura 3 apresenta os dígitos associados a cada Região Fiscal de onde o CPF é emitido. Observa-se que o nono dígito dos CPFs emitidos nos estados do Maranhão, Piauí e Ceará será 3.

Uma forma de encontrar os dígitos verificadores de um CPF é exempliicada a seguir. Considere $a_1a_2a_3a_4a_5a_6a_7a_8a_9$ a sequência formada pelos nove primeiros dígitos, os quais devem ser multiplicados, nessa ordem, pela base $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ e, efetuar-se-á a soma dos produtos obtidos. O décimo dígito, a_{10}, deve ser subtraído daquela soma, tal que o resultado seja um número múltiplo de 11. Em outras palavras, denotando a soma dos podutos obtidos por S, $S - a_{10} \equiv 0 \mod 11$, ou seja, a_{10} é o resto da divisão de S por 11. O décimo primeiro dígito é calculado de modo análogo, considerando o décimo dígito encontrado e uma base de 0 a 9. Por exemplo, se o CPF de uma pessoa tem os seguintes nove primeiros dígitos 053 213 743, o primeiro dígito de controle pode ser obtido como segue:

(1) Escreve-se os nove primeiros dígitos e abaixo a base de 1 a 9;

$$\begin{array}{ccccccccc} 0 & 5 & 3 & 2 & 1 & 3 & 7 & 4 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array}$$

(2) Efetua-se as multiplicações correspondentes e soma-se os podutos obtidos;

$$0 \cdot 1 + 5 \cdot 2 + 3 \cdot 3 + 2 \cdot 4 + 1 \cdot 5 + 3 \cdot 6 + 7 \cdot 7 + 4 \cdot 8 + 3 \cdot 9 = 158$$

(3) Dividi-se o resultado obtido em (2) por 11 e toma-se o resto.

$$158 = 14 \cdot 11 + 4.$$

Pelos passos (1), (2) e (3) realizados, tem-se que o décimo dígito (ou 1º dígito de controle) é 4. Resta descobrir o décimo primeiro dígito e, para isso, serão realizadas etapas análogas às anteriores, como segue

(1') Escreve-se os dez dígitos e abaixo a base de 0 a 9;

0	5	3	2	1	3	7	4	3	4
0	1	2	3	4	5	6	7	8	9

(2') Efetua-se as multiplicações correspondentes, somando os podutos obtidos;

$$0 \cdot 0 + 5 \cdot 1 + 3 \cdot 2 + 2 \cdot 3 + 1 \cdot 4 + 3 \cdot 5 + 7 \cdot 6 + 4 \cdot 7 + 3 \cdot 8 + 4 \cdot 9 = 166$$

(3') Dividi-se o resultado obtido em (2) por 11 e toma-se o resto.

$$166 = 15 \cdot 11 + 1.$$

Pelos passos realizados em (1'), (2') e (3') conclui-se que o 11º dígito (ou 2º dígito de controle é 1). E portanto, o CPF procurado corresponde a $053 \,.\, 213 \,.\, 743 - 41$.

3.3.2 Criptografia

De um modo geral, a criptografia corresponde a uma escrita em código, de modo que somente pessoas autorizadas possam compreendê-la. Essa palavra é de origem grega em que $krypto = escondido, oculto$ e $grapho = grafia, escrita$. Há registros de sua utilização no sistema de escrita hieroglífica egípcio e em comunicações sobre planos de batalha romanos.

> Contudo, desde aquele tempo, seu princípio básico continua o mesmo: encontrar uma transformação (função) injetiva f entre um conjunto de mensagens escritas em um determinado alfabeto (de letras, números ou outros símbolos) para um conjunto de mensagens codificadas. O fato de f ser inversível é a garantia de o processo ser reversível e as mensagens poderem ser reveladas pelos receptores. O grande desafio de um processo criptográfico, portanto, está em ocultar eficientemente os mecanismos (chaves) para a inversão de f, de modo que estranhos não possam fazê-lo. (TAMAROZZI, 2001, p.41)

Pode-se afirmar que, de forma simplificada, há um combinado entre o emissor e o receptor da mensagem de modo que somente esse último deve conseguir decifrar a mensagem criptografada. Como exemplo, cita-se o código do imperador Julio César, que

enviava mensagens aos seus generais utilizando uma espécie de chave “pule três"ou chave 3, em que o receptor deveria tomar sempre a 3 letra em vez daquela escrita no código. Abaixo um exemplo de como funcionava essa chave.

Tabela 3 – Chave 3 de Julio César

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

Fonte: SÁ, 2015, p.9.

Utilizando a chave 3 de Julio César conforme a Tabela 3, a mensagem criptografa **CBIFW XKL KLSL** corresponde a **FELIZ ANO NOVO**. Observe que se designarmos x a letra original e por y a letra que substituirá no código, então pode-se escrever $y = x+3$.

A seguir será abordado um exemplo mais completo envolvendo congruência modular. Considere a Tabela 4 em que cada letra ficará associada a um número que representa sua posição no alfabeto.

Tabela 4 – Chave: somar 5

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Fonte: Elaborada pelo autor.

Nesse exemplo, será usada a chave **somar 5**. Assim, o número associado a cada letra deverá ser aumentado de 5 para a correta decodificação da mensagem. Caso o número obtido após a soma seja superior a 26, será utilizado apenas o resto de sua divisão por 26, retornado assim ao início do alfabeto. Por exemplo, 29 corresponde a letra C, pois $29 = 26 \cdot 1 + 3$ ou de forma equivalente $29 \equiv 3 \mod 26$. Outra forma de representar essa chave seria $y = x + 5$ em que x é a letra original e obtém-se y somando 5 ao número associado a letra x. Assim, para enviar a mensagem **ILHA DO AMOR**, a criptografia a ser utilizada seria **NQMF IT FRTW**.

4 Cogruência Modular no Ensino Fundamental

Os resultados apresentados nas seções anteriores constituem uma síntese considerável para a formação do professor que intencionar trabalhar esse conteúdo. 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. "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)

O conhecimento da teoria de Congruências modulares pode contribuir de forma significativa para o processo de ensino e aprendizagem em matemática nos anos finais do ensino fundamental (6° ao 9º anos) possibilitando a aproximação de um dos objetivos previstos nos Parâmetros Curriculares Nacionais: "saber utilizar diferentes fontes de informação e recursos tecnológicos para adquirir e construir conhecimentos." (BRASIL, 1998).

Agora serão abordadas algumas possiblidades da teoria de congruência modular para o desenvolvimento do ensino de matemática no Ensino Fundamental. Sabe-se que a teoria de congruências abrange propriedades e teoremas dos números inteiros que estendem-se de níveis mais elementares aos mais avançados. Entretanto, serão enfatizados os resultados que possibilitem resolver problemas mais básicos como os abordados no ensino fundamental. A proposta desta pesquisa é o ensino de congruências modulares a partir do 6º ano do ensino fundamental, visto que, conforme a BNCC, a divisão euclidiana, ponto fulcro do estudo de congruência, é estudada a partir desse ano. Esse conhecimento, tende a fortalecer o estudo de divisibilidade sendo tratado sob nova abordagem e tornar mais vultoso o conjunto de ferramentas necessárias a resolução de problemas haja vista a diversidade de aplicações de congruências em problemas de nosso cotidiano e em avaliações de desempenho bem como a celeridade para resolvê-los.

4.1 Suporte metodológico da Pesquisa

Considerando o objeto desta pesquisa, optou-se por uma metodologia de pesquisa bibliográfica seguida de pesquisa de campo do tipo experimental. A pesquisa bibliográfica é a obtenção de uma perspectiva geral e/ou todas as informações sobre as teorias existentes acerca de um tema. E assim, foram selecionados os conteúdos da teoria de congruência modular de literatura pertinente ao ensino de matemática no ensino fundamental. Além disso, realizou-se um experimento com alunos de uma escola da rede pública do município de São Luís conforme descrição no parágrafo seguinte, em conformidade com (LAKATOS;

MARCONI, 2021) que definem a pesquisa de campo como um meio pelo qual é possível comprovar hipóteses ou ratificar informações sobre determinado problema.

Conforme mencionado, foi realizada uma aplicação com os alunos do ensino fundamental dos anos finais da UEB Bandeira Tribuzzi, como forma de experimentar o objetivo proposto nesse trabalho. A escola situa-se no centro de São Luís e, como a maioria das escolas da rede, contém alunos carentes que residem em seu entorno, correspondente, neste caso, aos bairros Areinha, Centro, Jaracaty e Liberdade.

Nesse sentido, pode-se ainda classificar esta pesquisa de campo como experimental, consonante definição seguinte: "Experimentais - consistem em investigações de pesquisa empírica cujo objetivo principal é o teste de hipóteses que dizem respeito a relações de tipo causa-efeito." (LAKATOS; MARCONI, 2021, p.189). Deseja-se verificar se a teoria de congruências modulares fornece celeridade na resolução de problemas de repetição periódica, contribuindo para o processo de ensino e aprendizagem de Matemática nos anos finais do ensino fundamental.

A escolha da escola deve-se ao fato do autor deste trabalho exercer suas atividades na mesma. A princípio, o projeto consistia na aplicação da proposta, de forma presencial, ainda que as aulas voltassem de forma híbrida, em todas as turmas do ensino fundamental anos finais, para comparar as formas de resolução de problemas com e sem a utilização da teoria de congruências, verificar a receptividade com relação ao novo conteúdo e, de uma forma geral, investigar as contribuições desse novo conhecimento para essa etapa de ensino. Porém as aulas continuaram remotas por todo o segundo semestre de 2021, com baixa participação de alunos nas aulas regulares. Ainda assim, houve grande quantidade de aulas com o objetivo de compensar a carga horária deficitária do ano letivo de 2020 que se encerrara antecipadamente para unificação de calendários da rede municipal.

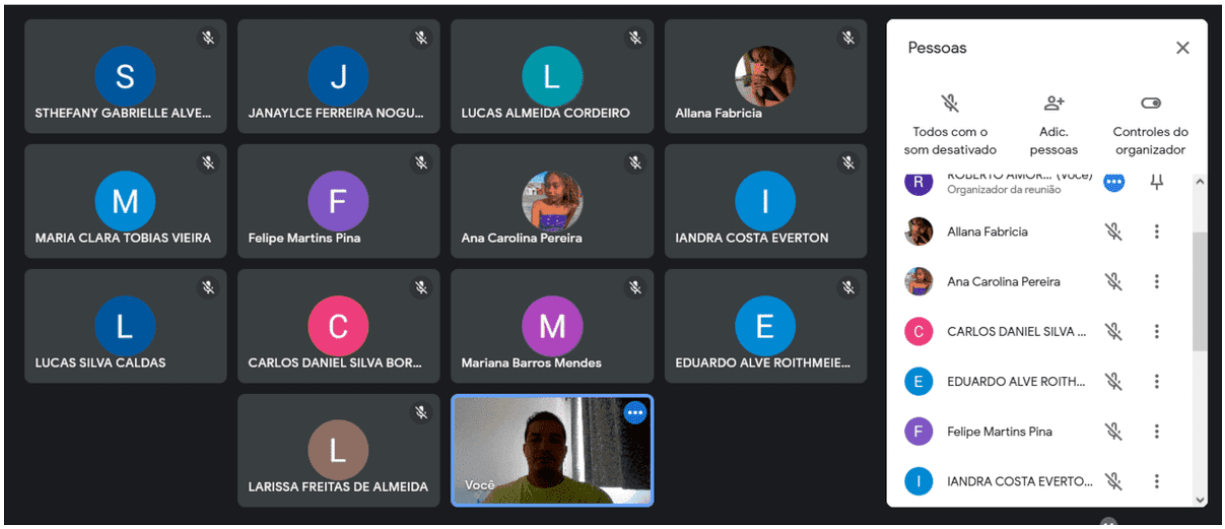
Assim, optei por fazer a aplicação somente nas turmas do 7º e 8º anos, que eram as turmas que trabalhava. O convite estendeu-se a todos os alunos dessas turmas, mas pela dificuldade de acesso à internet muitos não conseguiram participar, situação que ocorria nas aulas regulares também. Havia a expectativa de suporte da Secretaria de educação para desenvolvimento das atividades letivas, mas isso ocorreu tardiamente nas proximidades do fim do ano letivo.

Dessa forma, os encontros aconteceram de forma remota. As turmas do 7º e 8º anos contém 37 e 38 alunos respectivamente, mas somente cerca de 20 alunos participaram do projeto, sendo 11 meninas e 9 meninos. Esse quantitativo é praticamente o mesmo das aulas regulares, pois a maioria dos alunos não têm acesso à internet e a estes são destinadas atividades impressas. Como o projeto carecia de iteração instantânea, não foi utilizado esse recurso.

Os encontros aconteceram no período de outubro a dezembro do corrente ano,

às sextas-feiras, em horários compatíveis com a disponilidade das duas turmas. Foram utilizados planos de estudos embasados em Fomin (2019), Iezzi (2013), Hefez (2016), Jurkiewicz (2017) e apostilas do Polo de Treinamento Intensivo - POTI. A seguir na Figura 4 apresenta-se um registro de um dos encontros com as turmas.

Figura 4 – Alunos presentes na aula



Fonte: Próprio autor

A teoria de congruências modulares tem como pré-requisitio o conteúdo de divisibilidade, presente no currículo do ensino fundamental a partir do 6º ano. Nesse trabalho, desenvolveu-se um plano de estudos para nivelar os conhecimentos matemáticos das turmas acerca de conteúdos básicos e habilidades necessárias à superação dos problemas propostos.

Na aplicação, houve um total de 6 encontros de 80 minutos em que foram trabalhados inicialmente conteúdos de nivelamento matemáticos relacionados à pesquisa. Após foram estudados conteúdos relativos à divisibilidade, reafirmando conceitos conhecidos pelos alunos, porém com nova abordagem e aplicadas a situações-problema mais elaboradas presentes em provas de desempenho escolar e olimpíadas. Na sequência, introduzimos o conceito de congruência, relacionando-o com o conteúdo de divisiblidade e apresentando suas propriedades.

Em todos os encontros instigou-se os alunos a pensar nos problemas utilizando os conhecimentos prévios adquiridos durante a trajetória escolar, para assim, obtermos um comparativo quanto à celeridade ou mesmo desempenho quando o fizessem conhecendo a teoria de congruências. Os materiais utilizados nas aulas estão nos anexos I, II e III.

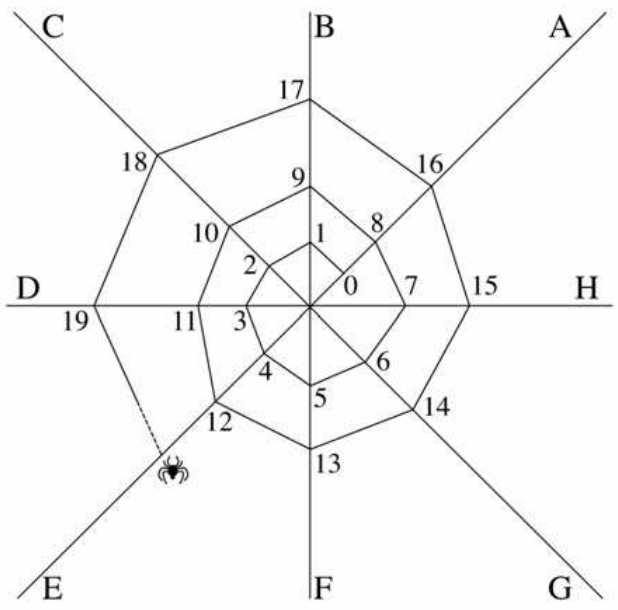
No primeiro e segundo encontros, consonante o material constante no apêndice I,

trabalhou-se conteúdos de revisão buscando nivelamento matemático das turmas com os conteúdos de potenciação, radiciação, fatoração, dízimas periódicas e notação científica. Observou-se que a maioria dos alunos apresentaram dificuldades nesses conteúdos, ainda mais considerando que alguns os tinham visto no ano letivo de 2021.

No terceiro e quarto encontros, conforme plano de estudo no apêndice II, foi desenvolvido o conteúdo relativo à divisibilidade. Iniciou-se com um problema do banco de questões da OBMEP do ano de 2006, a fim de verificar os conhecimentos que os alunos detinham a respeito desse conteúdo.

Problema proposto. A, B, C, D, E, F, G e H são os fios de apoio que uma aranha usa para construir sua teia, conforme mostra a Figura 5. A aranha continua seu trabalho. Sobre qual fio de apoio estará o número 118?

Figura 5 – Teia de aranha



Solução: Note que são 8 fios de apoio que a aranha utiliza, numerados a partir do fio A iniciando com 0. Assim,

- sobre o fio A aparecem os múltiplos de 8;
- sobre o fio B aparecem os (múltiplos de 8) + 1;
- sobre o fio C aparecem os (múltiplos de 8) + 2;
- sobre o fio D aparecem os números (múltiplos de 8) + 3;
- sobre o fio E aparecem os números (múltiplos de 8) + 4;
- sobre o fio F aparecem os números múltiplos de 8) + 5;

- sobre o fio G aparecem os números (múltiplo de 8) + 6;
- sobre o fio H aparecem os números (múltiplos de 8) + 7.

Na divisão de 118 por 8 encontrou-se resto 6, o que significa que $118 = 14 \cdot 8 + 6$. Portanto, 118 está sobre o fio G.

Solução utilizando congruência: Pode-se resolver o problema por congruência. Para isso, utiliza-se congruência módulo 8. Ou seja, basta fazer $118 \equiv 6 \mod 8$, o que significa que o número 118 estará no mesmo fio que os números que deixam resto 6 na divisão por 8, portanto, no fio G.

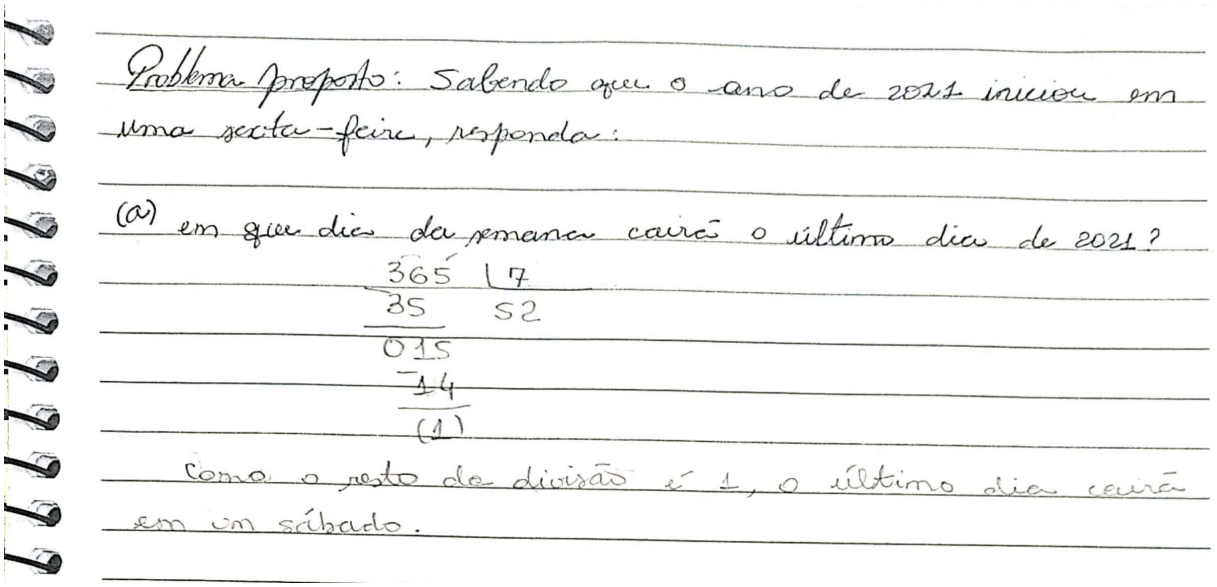
Problema proposto. Sabendo que o ano de 2021 iniciou em uma sexta-feira, responda

(a) em que dia da semana cairá o último dia de 2021?

(b) em que dia da semanda cairá o 1º dia de 2024? E o último dia?

O aluno A conseguiu pensar no problema e, inclusive explicou e efetuou corretamente os cálculos necessários à sua resolução como pode-se ver na Figura 6. Entretanto, o aluno A equivocou-se na conclusão de sua solução ao interpretar o significado do resto da divisão efetuada. Conforme será apresentada na solução esperada abaixo, o resto 1 indica o início da semana pois no problema em questão as semanas são iniciadas às sextas-feiras e encerram-se às quintas-feiras. Logo, não será sábado o último dia de 2021, mas sim sexta-feira. Os encontros objetivam o sanamento de dúvidas como essas e o desenvolvimento de habilidades que permitam utilizar o conteúdo de divisibilidade de forma adequada na resolução de problemas e assim apropiar-se desse conhecimento para fortalecer a base para novos conteúdos, em particular daqueles que tomam esse como pré-requisito.

Figura 6 – Solução do aluno A



Fonte: Próprio autor

Solução: (a) Na Tabela 5 a seguir, forma listados os primeiros 16 dias de 2021.

Tabela 5 – Primeiros 16 dias de 2021

dom	seg	ter	qua	qui	sex	sab
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16

Fonte: Próprio autor

Analisando a tabela, observa-se que os múltiplos de 7 sempre estão na quinta-feira, os números que deixam resto 1 quando divididos por 7 estão na sexta-feira, os que deixam resto 2 no sábado, e restos 3, 4, 5 e 6, domingo, segunda, terça e quarta, respectivamente. Como o ano de 2021 têm 365 dias, ao dividir 365 por 7, obtem-se quociente 52 e resto 1 ($365 = 52 \cdot 7 + 1$). De onde conclui-se que o último dia de 2021 cairá numa sexta-feira.

(b) Pelo item (a), o ano de 2021 encerrará numa sexta-feira. Então o ano de 2022 iniciará num sábado e, como têm 365 dias, terminará num sábado. Assim, o ano de 2023 iniciará e teminará num domingo, pois têm 365 dias também. Desse modo, o ano de 2024 iniciará numa segunda-feira, mas têm 366 dias. Então, será utilizada a Tabela 6 para auxiliar na solução do problema.

Tabela 6 – Primeiros 20 dias de 2024

dom	seg	ter	qua	qui	sex	sab
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20

Fonte: Próprio autor

Observa-se na tabela que os múltiplos de 7 estão no domingo e os números que deixam restos 1, 2, 3, 4, 5 e 6 quando divididos por 7, estão na segunda, terça, quarta, quinta e sexta, respectivamente. Efetuando a divisão de 366 por 7 obtem-se quociente 52 e resto 2 ($366 = 52 \cdot 7 + 2$). Portanto, o último dia de 2024 cairá numa terça-feira.

Solução utilizando congruência: O problema pode ser resolvido utilizando-se congruência. Para isso utiliza-se congruência *mod* 7 devido a semana têm 7 dias. Assim, no item (a) pode-se escrever

$$365 \equiv 1 \mod 7,$$

evidenciando que o último dia de 2021 cairá no mesmo dia da semana que o primeiro dia. E no item (b), pode-se escrever

$$365 \equiv 2 \mod 7,$$

significando que o último dia de 2024 cairá no mesmo dia da semana do segundo dia, ou em outros termos, no dia da semana seguinte ao dia da semana do primeiro dia.

Esse problema foi oportuno para apresentar alguns resultados aos alunos. Isto é, se um ano é comum, com 365 dias, então termina no mesmo dia da semana que iniciou. Se for bissexto, com um dia a mais acrescentado no mês de fevereiro, termina no dia da semana seguinte ao dia da semana que iniciou. Assim, comentou-se que descobrir o dia da semana, fato que muitas vezes é entendido como uma espécie de mágica, deve-se a utilização de algum algoritmo.

Além disso, fez-se a caracterização do ano bissexto devido a sua identificação não ser tão simples. Aparentemente, os anos bissextos ocorrem sempre de 4 em 4 anos, porém isso não é verdade conforme encontra-se em Boczko (1984),

> A Reforma Gregoriana ao calendário Juliano, que deu início ao Calendário Gregoriano, sob orientação do astrônomo Lélio, e sob o pontificado de Gregório XIII, imposta em 1582 da era Cristã, consistiu no seguinte:
>
> b) - os anos da era Cristã que fossem múltiplos 100 (anos centenários) deixariam de ser bissextos, exceto quando fossem também múltiplos de 400 (com isso retirava-se 1 dia a cada 100 anos, e adicionava-se 1 a cada 400 anos); (BOCZKO, 1984, p. 23)

Pode-se então explicar a regra para anos bissextos como segue: se um ano for múltiplo de 4, então ele é bissexto. Por exemplo, 2020 é bissexto pois seus dois últimos algarismos formam um número múltiplo de 4 e, portanto, 2020 é divisível por 4. No entanto, se um ano for, simultaneamente, múltiplo de 4 e de 100, então ele deixa de ser bissexto. Isso ficará mais evidente no ano de 2100, pois 2100 é múltiplo de 4 e de 100. As pessoas se supreenderão, pois estão acostumadas a anos bissextos ocorrerem sempre a cada 4 anos, mas 2100 não será. Só então aprenderão essa regra ou mesmo outra que se desenvolva. Mas a regra não acabou, pois se um ano for múltiplo de 4, de 100 e de 400, então é bissexto. Isso ocorreu no ano de 2000, mas passou naturalmente porque obedeceu a regra conhecida, ou seja, 4 anos após 1996 que também foi bissexto.

A explicação para a regra de anos bissextos apresentada é que a Terra leva 365 dias e aproximadamente 6 horas (5 horas 49 minutos e 12 segundos) para realizar seu movimento de translação. Conforme verifica-se em (BOCZKO, 1984, p.23), a seguinte expressão equivale a duração do Ano Gregoriano

$$365,2425 = 365 + \tfrac{1}{4} - \tfrac{1}{100} + \tfrac{1}{400}.$$

Assim, a cada 4 anos, um dia a mais é acrescentado em fevereiro, no dia 29, como forma de compensar as horas “perdidas". Entretanto, cria-se uma defasagem ao contrário, pois ao acrescentar-se um dia a mais a cada 4 anos, há um excesso que terá relevância a cada 100 anos e, portanto, nessa oportunidade não se deve acrescentar um dia. Ao não se acrescentar um dia a cada 100 anos, com a correção anterior, novamente comete-se um erro que a cada 400 anos acumulam-se em aproximadamente um dia e, portanto, outra vez um dia deve ser acrescentado.

Nos dois últimos encontros desenvolveu-se o conteúdo de congruência, tendo como base o plano de estudos e material constantes no apêndice III e anexo III, apresentando suas propriedades na resolução de problemas. Explorou-se inicialmente o conceito de congruência associado aos relógios analógicos, como forma de aproximar o conteúdo do cotidiano e mesmo facilitar sua compreensão. Os alunos disseram que nunca tinham visto o conteúdo, mas acharam simples sua definição principalmente pela relação intríseca com a divisibilidade. Os problemas trabalhados nos primeiros encontros foram novamente abordados para comparar esse conteúdo em termos de celeridade e mesmo sintetização da solução.

Problema proposto. Ache o resto da divisão de $13^{16} - 2^{25}3^{15}$ por 3.

Solução: De maneira mais simples, pode-se analisar cada parcela módulo 3 e depois aplicar as propriedades de congruência modular para obter o resultado. Assim,

$$13 \equiv 1 \mod 3 \implies 13^{16} \equiv 1 \mod 3, \tag{52}$$
$$2 \equiv -1 \mod 3 \implies 2^{25} \equiv -1 \mod 3, \tag{53}$$
$$3 \equiv 0 \mod 3 \implies 3^{15} \equiv 0 \mod 3. \tag{54}$$

De (52), (53), (54) e pelos itens (b), (c) e (e) da proposição 3.3, segue que

$$13^{16} - 2^{25}3^{15} \equiv 1 - (-1) \cdot 0 \equiv 1 \mod 3 \tag{55}$$

Logo, conforme (55), o resto da divisão de $13^{16} - 2^{25}3^{15}$ por 3 é 1.

Problema proposto. Prove que n^2+1 não é divisível por 3 qualquer que seja o inteiro n.

Solução: Todo inteiro n é congruente módulo 3 a 0, 1 ou 2. Assim, pelo item (e) da proposição 3.3, tem-se

$$n \equiv 0 \mod 3 \implies n^2 \equiv 0 \mod 3, \tag{56}$$
$$n \equiv 1 \mod 3 \implies n^2 \equiv 1 \mod 3, \tag{57}$$
$$n \equiv 2 \mod 3 \implies n^2 \equiv 1 \mod 3. \tag{58}$$

Somando 1 em ambos os membros das equações em (56), (57) e (58), nunca tem-se $n^2 + 1 \equiv 0 \mod 3$.

No decorrer do processo algumas situações ocorreram, a saber:

- A maioria dos alunos entrava na aula, mas não interagia;
- A participação era irregular, com baixa devolutiva de atividades;
- Os alunos apresentaram dificuldades em conteúdos básicos.

Dessa forma,vimos que a decisão de encontros de nivelamento matemático foi acertada, principalmente pelo fato da aplicação do projeto ocorrer em meio à pandemia de coronavírus causadora de grandes prejuízos à educação nos dois últimos anos. Sabe-se da imprescindibilidade do domínio de conceitos ou conhecimentos básicos em Matemática

conforme ratificado pelo professor Elon Lages Lima em entrevista à Revista Professor de Matemática que

> O conhecimento matemático é, por natureza, encadeado e cumulativo. Um aluno pode, por exemplo, saber praticamente tudo sobre a proclamação da república brasileira e ignorar completamente as capitanias hereditárias. Mas não será capaz de estudar Trigonometria se não conhecer os fundamentos da Álgebra, nem entenderá essa última se não souber as operações aritméticas, etc. Esse aspecto de dependência acumulada dos assuntos matemáticos leva a uma sequência necessária, que torna difícil pegar o bonde andando. (LIMA, 1994, p. 1)

O conhecimento e domínio das propriedades e operações com números inteiros objeto de estudo da Aritmética prepara os alunos para os conteúdos subsequentes da disciplina e também para o aprendizado de conteúdos pertencentes a outros ramos da Matemática.

Vale destacar a dificuldade apresentada pelos discentes em contextualização dos conteúdos, evidenciada na necessidade de relacionar os conteúdos de Matemática com as situações cotidianas objeto das aplicações matemáticas. Isso significa que os objetivos previstos para essa etapa de ensino não estão sendo atingidos, como por exemplo, os Parâmetros Curriculares Nacionais - PCN estabelecem que os alunos sejam capazes de

> utilizar as diferentes linguagens verbal, musical, matemática,gráfica, plástica e corporal como meio para produzir, expressar e comunicar suas idéias, interpretar e usufruir das produções culturais, em contextos públicos e privados,atendendo a diferentes intenções e situações de comunicação". (BRASIL, 1998, p. 7)

Assim, pode-se dizer que falta o letramento matemático em alguns alunos, pois há dificuldade em formular, empregar ou interpretar a matemática em diversos contextos e utilizar conceitos e ferramentas matemáticas para descrever, explicar ou mesmo prevê fenômenos. Situação essa, que corrobora com o resultado verificado no PISA 2018, em que cerca de 70% dos estudantes brasileiros encontram-se no nível I ou abaixo dele e cujas habilidades desenvolvidades são

> No Nível 1, os estudantes são capazes de responder a questões que envolvem contextos familiares, nas quais todas as informações relevantes estão presentes e as questões estão claramente definidas. Conseguem identificar informações e executar procedimentos rotineiros, de acordo com instruções diretas, em situações explícitas. Conseguem realizar ações que são, quase sempre, óbvias e que decorrem diretamente dos estímulos dados. (BRASIL, 2020, p.114)

Há necessidade de diferentes abordagens de conteúdos básicos contemplando con-

textualizações e aproximação das vivências dos discentes, visando aprendizagem significativa de conteúdos essenciais. Encontra-se na proposta desse trabalho algumas possibilidades.

Os problemas apresentados foram importantes para o desenvolvimento do conteúdo em aula, principalmente quando abordados utilizando congruência modular. Observou-se que os alunos que já apresentam um bom desempenho na disciplina de Matemática destacaram-se nos encontros aplicando corretamente a teoria para a resolução de problemas ao passo que a maioria dos alunos, infelizmente, ficou mais inibida, dificultando um diagnóstico mais preciso em sala. Dessa forma, complementarmente, foram utilizados questionários via formulários do Google com duas finalidades:

- Verificar a aprendizagem dos alunos do conteúdo de congruências de forma mais abrangente;
- Avaliação das aulas e professor na perspectiva dos alunos.

A Tabela 7 ilustra os resultados do teste em que elencou-se 6 questões relacionadas ao conteúdo de congruência modular, conforme apêndice IV, aplicado via formulário eletrônico. Para fazer a análise do resultado utilizou-se a frequência acumulada haja vista sua utilidade na obtenção de quantidade de dados que estão abaixo ou acima de um valor determinado.

Tabela 7 – Resultado do Teste

Número de acertos	**Frequência absoluta**	**Frequência acumulada**
0	0	0
1	1	1
2	6	7
3	1	8
4	5	13
5	1	14
6	6	20
Somatório	20	-

Fonte: Próprio autor

Observando a Tabela 7, nota-se que a menor quantidade de acertos foi 1 questão. É, também, fácil identificar que 8 alunos acertaram 3 ou menos questões. E consequentemente, pela diferença, 12 alunos acertaram mais que 3 questões.

Utilizou-se formulário eletrônico também para aplicação de questionário de cunho mais subjetivo cuja finalidade é obter a percepção dos estudantes com relação a teoria abordada com todas as suas especificidades e sobre a metodologia utilizada pelo professor para desenvolvimento dos conceitos. Assim, foram utilizadas as 4 perguntas a seguir:

(1) Você considera possível o entendimento do conteúdo de Congruência Modular por alunos do ensino fundamental?

(2) A quantidade de encontros destinados ao projeto foi suficiente para apreender o conteúdo de Congruência Modular?

(3) Você acredita que o conteúdo de Congruência Modular torna a resolução de questões mais rápida?

(4) Como você avalia os recursos utilizados pelo professor durante os encontros (escrita na lousa digital, videochamada, etc.).

Os vinte alunos responderam ao questionário acima. Com relação a primeira pergunta, 95% dos alunos concordaram ser possível a apreensão do conteúdo de Congruência modular nas especificidades que lhes foi apresentada e 5% disseram que isso não era possível mas não especificaram o motivo. Para a segunda pergunta, 90% dos alunos consideraram suficiente a quantidade de encontros ainda que virtuais para apreensão e desenvolvimento do conteúdo, incluso o tempo utilizado com os conteúdos que eram pré-requisito; 5% consideraram insuficiente e não especificaram o motivo e os outros 5% responderam:

- Aluno B: Bom para quem se esforçou para aprender, acredito que sim. Já pra quem estava presente mas não se importou muito acredito que não foi suficiente.

Na terceira pergunta, 95% dos alunos responderam acreditar na celeridade de resolução de problemas oportunizada pela teoria de congruênicas modulares e os outros 5% responderam:

- Aluno C: Não sei todas, mas algumas sim.

Na quarta e última pergunta, 85% dos alunos responderam que os recursos utilizados pelo professor nos encontros foram suficientes para desenvolvimento dos conteúdos e os outros 15% responderam:

- Aluno D: Eu acredito que que foi suficiente para quem quiz aprender, pois foram ótimas explicações.

- Aluno E: Foram bem usados.

- Aluno F: Se fosse presencial poderíamos aproveitar melhor.

4.2 Uma sequência didádica de congruências

Nesta seção, propõe-se uma sequência didática sobre o ensino de Congruências Modulares no Ensino Fundamental, oportunizando uma possibilidade aos professores que tiverem interesse em trabalhar a teoria nessa etapa de ensino.

Apoia-se teoricamente em Zabala (1998, p.18) , que estabele as "sequências didáticas como um conjunto de atividades ordenadas, estruturadas e articuladas para a realização de certos objetivos educacionais, que têm um princípio e um fim, conhecidos tanto pelos professores como pelos alunos".

Além disso, as sequências didáticas consistem numa forma de organização das aulas antongonista ao modelo tradicional de ensino, pois "[...] é uma maneira de encadear e articular as diferentes atividades ao longo de uma unidade didática" (ZABALA, 1998, p. 20). Sendo, portanto, uma metodologia adequada à proposta apresentada nesse trabalho.

SEQUÊNCIA DIDÁTICA CONGRUÊNCIA MODULAR

ÁREA: CIÊNCIAS EXATAS
DISCIPLINA: MATEMÁTICA
SÉRIE: 7º/8º ANOS
CONTEÚDOS

- Caracterização de números inteiros congruentes;
- Aplicações de Congruência modular no cotidiano.

OBJETIVOS

- Utilizar as propriedades de congruências na resolução de problemas;
- Aplicar a teoria de congruências na resolução de problemas.

DESCRITORES

- D18, D19 e D20.

TEMPO ESTIMADO

- 3 aulas

MATERIAL NECESSÁRIO

- Texto sobre códigos de barras, caneta, Papelel A4, calculadora e embalagens de produtos (café, açucar, creme dental, chocolate em pó, leite, etc.).

APRESENTAÇÃO DO PROJETO

Professor, embora este não seja um conteúdo da grade curricular desta etapa de ensino, esta aplicação ressignifica o processo de ensino-aprendizagem de divisão, contribuindo para a aprendizagem adequada desse conteúdo essencial da Matemática.

As pesquisas apontam as dificuldades dos alunos em conteúdos essenciais da Matemática, particularmente das operações básicas. Em vista da impossibilidade de dissociar conteúdos básicos de outros mais avançados, encontra-se na contextualização e nas aplicações de conteúdos de Matemática ou ainda na introdução de uma nova teoria que permita abordagem diferente ao que já é trabalhado, alternativas eficientes para enfrentamento dessas adversidades.

Essa sequência consistirá na verificação de códigos de barras de produtos, situação que está associada ao conceito de congruência modular e divisão.

DESENVOLVIMENTO

- **1ª Etapa**

  1. Distribua as embalagens de produto, de forma que cada aluno fique com uma (o professor pode solicitar que os alunos tragam as embalagens de casa);
  2. Distribua material embasado em Milles (2021) contendo a história dos códigos de barras e detalhamento de sua composição. Pode ser interessante fazer uma leitura conjunta do material visando sanar as dúvidas emergidas;

- **2ª Etapa**

  1. Demonstre como é calculado o dígito de verificação, fazendo uma combinação dos dígitos previamente determinados em um código de barras genérico;
  2. Solicite aos alunos que verifiquem se o dígito de verificação dos códigos de barras de suas embalagens está correto (A folha de papel A4 será utilizada para fazer os registros). Alternativamente, pode-se usar a calculadora para fazer a verificação dos cálculos.

  Nota importante

  – Nessa etapa é possível verificar se os alunos apresentam dificuldades nas operações básicas. A calculadora deve ser utilizada somente como fonte de verificação dos resultados.

- **3ª Etapa**

    1. Relacione o cálculo do dígito de verificação de um código de barras com o conceito de congruência modular;
    2. Solicite aos alunos que refaçam os cálculos de verificação do dígito de verificação dos códigos de barras utilizando congruência modular.

    Faça os seguintes questionamentos

    – Há dificuldade em efetuar os cálculos utilizando congruência?

    – Há alguma vantagem em efetuar os cáculos utilizando congruência?

AVALIAÇÃO

Os alunos serão avaliados pelos registros em papel A4 relativos ao cálculo do dígito de verificação do código de barras da embalagem de sua posse.

5 Considerações Finais

Descreveu-se neste trabalho experimento realizado com turmas de 7° e 8° anos do ensino fundamental, desenvolvendo conceitos importantes da Teoria dos Números, com destaque às congruências modulares, como forma de reforçar os conteúdos trabalhados nessa etapa de ensino utilizando nova abordagem e simultaneamente apresentar novas ferramentas importantes no estudo da matemática. Aconteceram apenas encontros virtuais devido às restrições impostas pela pandemia causada pelo corononavírus, dificultando tanto a participação das turmas em sua totalidade quanto uma avaliação dos alunos participantes de forma mais precisa e, tentou-se superar isso com indagações em aula e utilizando questionários por meio de formulários eletrônicos.

Embora a proposta seja o trabalho com alunos muito jovens, a teoria abordada é de fácil compreensão e a base é o conteúdo de divisibilidade estudado a partir do 6º ano do ensino fundamental conforme verifica-se na BNCC. A teoria de congruências modulares têm diversos benefícios a oferecer seja no âmbito escolar ou para o cotidiano dos alunos, pois possibilita a aquisição de competências e habilidades necessárias e auxilia no cálculo, reflexão e comparação, fatores importantes para a tomada de decisões. Além disso, é possível justificar alguns resultados que são apenas apresentados nessa etapa de ensino, como por exemplo, os critérios de divisibilidade. E também, a atualidade do conteúdo pela suas aplicações no campo tecnológico, evidenciadas no cálculo de dígitos verificadores de códigos de barras, CPF e ISBN.

No cenário atual, conforme apresentou-se em entrevistas e resultados de avaliações aplicadas em nível nacional, em que estão evidentes as fragilidades da educação brasileira, abordagens diferentes de conteúdos fundamentais para o estudo da matemática tornam-se essenciais para êxito no desempenho escolar, contribuindo para que os alunos desempenhem seus papéis como cidadãos. Sabe-se que mais fatores devem entrar nessa conta, como por exemplo, a valorização dos professores que atualmente têm lutado por reajuste salarial que deveria ser automático conforme previsão legal.

Avalia-se positivamente a experiência realizada, pois há o resgate de conteúdos trabalhados nos anos finais do ensino fundamental e oportuniza novas experiências aos alunos. Buscou-se utilizar materiais e conteúdos já conhecidos no ensino de Matemática, contextualizando os problemas abordados. Em relação aos resultados dos questionários, também foi obtido um resultado motivador, pois apesar das adversidades impostas pela pandemia, no questionário/teste objetivo mais da metade dos alunos acertaram mais de 50% das questões. A aplicação do questionário subjetivo trouxe resultados interessantes, visto que as perspectivas dos discentes com relação a teoria de congruências e metodologias utilizadas pelo professor foram publicizadas e, mostraram-se favoráveis ao

desenvolvimento do experimento com alunos nessa etapa de ensino.

Além disso, apresentou-se proposta de sequência didática aos professores que intencionarem trabalhar a teoria de congruências modulares nos anos finais do ensino fundamental. A sequência trata da aplicação de congruência modular relacionada aos códigos de barras, utilizando embalagens de produtos presentes em nosso dia a dia. Constitui-se em uma forma de apresentar a teoria de congruência para o ensino fundamental por meio de suas aplicações e contextualizações.

Por todo o exposto, têm-se na proposta deste trabalho constribuições importantes e alternativa eficiente para o desenvolvimento do processo de ensino-aprendizagem de Matemática nos anos finais do Ensino Fundamental, a saber: a) há nova abordagem ao conteúdo de divisão já presente no currículo; b) há muitas possibilidades de contextualizações e aplicações pela cotidianidade da teoria; c) a teoria de congruências está presente em tecnologias em processos de verificação de sistemas de identificação; d) é possível justificar os critérios de divisibilidade que geralmente são apenas apresentados aos alunos; e) possibilita maior celeridade na resolução de problemas e prepara os alunos para conteúdos mais avançados em Matemática.

Ressalta-se ainda que não foram aqui esgotadas todas as possibilidades da teoria de congruências com respeito às contribuições para o ensino fundamental ou mesmo para o Ensino Básico. Foram destacadas aplicações próximas ao cotidiano, visando destacar a presença da Matemática na vida dos discentes e com isso, dando significado ao processo de ensino-aprendizagem. Almeja-se, portanto, que a teoria de congruências atinja os alunos do Ensino Fundamental seja através de projetos, sequências didáticas ou com a introdução do conteúdo nos Anos Finais, para que consiga-se desenvolver as competências e habilidades previstas para essa etapa de ensino.

Referências

BOYER, C. B.; MERZBACH U. C. **História da Matemática**. Tradução de Helena de Castro. São Paulo: Blucher, 2012.

BOCZKO, Roberto. **Conceitos de astronomia** / R. Boczko - São Paulo, Edgard Blücher, 1984.

BRASIL. Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira. **Brasil no Pisa 2018 [recurso eletrônico]**. – Brasília : Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira, 2020.

BRASIL. Ministério da Educação. **Base Nacional Comum Curricular**. Brasília, 2018.

BRASIL. Secretaria de Educação Fundamental. **Parâmetros Curriculares Nacionais: Matemática**. Brasília: MEC/SEF, 1998.

CRUZ, Priscila. **O brasileiro quer educação pra já**. Estadão de São Paulo, 10 de março de 2018. Disponível em: opiniao.estadao.com.br. Acesso em 05 de outubro de 2021.

DOMINGUES, H. H. **Fundamentos de aritmética**. São Paulo: Atual, 1991.

FILHO, E. de A. **Teoria elementar dos números**. - São Paulo: Nobel, 1981.

FOMIN, D.; GENKIN, S.; ITENBERG, I. **Círculos Matemáticos/A experiência Russa**. Tradução de Valéria de Magalhães Iório - 1. ed. - Rio de Janeiro: IMPA 2019.

GUEDES, M. G. P. **Outros Critérios de Divisibilidade**. Revista do Professor de Matemática. Niterói - RJ. Sociedade Brasileira de Matemática. Volume 12, p. 24 - 27, 1° semestre de 1988.

HEFEZ, A. **Aritmética**. Rio de Janeiro: SBM, 2016.

IEZZI, G.; MURAKAMI, C. **Fundamentos de matemática elementar, 1**. - 9. ed. - São Paulo: Atual, 2013.

JURKIEWICZ, Samuel. **Divisibilidade e números inteiros**. Apostila do PIC. OBMEP. IMPA 2017.

LAKATOS, E. M.;MARCONI, M. A. **Fundamentos de Metodologia Científica**. 9ª edição. São Paulo: atlas, 2021.

MILIES, Francisco César Polcino Milies. **A matemática dos Códigos de Barras**. PIC. OBMEP. 2009. Disponível em; <http://obmep.org.br/docs/apostila6.pdf>. Acesso em 02 de agosto de 2021.

OLIVEIRA, E. **Ideb: Brasil atinge outra vez meta nas séries iniciais do ensino fundamental, mas ainda falha nos anos finais**. https://g1.com.br, 2020. Disponível

em: <https://g1.- globo.com/educacao/noticia/2020/09/15/ideb-brasil-atinge-outra-vez-meta-nas-series-ini- ciais-do-ensino-fundamental-mas-ainda-falha-nos-anos-finais.ghtml>. - Acesso em, 08 de outubro de 2021.

LIMA, E. L. **Sobre o ensino da matemática**. Revista do Professor de Matemática. Rio de Janeiro. Sociedade Brasileira de Matemática. Volume 28, p. 1 - 5, maio/agosto 1995.

OLIVEIRA, K. I. M.; Fernández, A. J. C. **Iniciação à Matemática: um curso com problemas e soluções**. 2ª ed. Rio de Janeiro: SBM, 2012.

PROFMAT. – **Provas e Soluções**. Disponível em <http://www.profmat-sbm.org.br/>. Acesso em 14 dez. 2021.

SÁ, Ilydio Pereira de. **Aritmética modular e algumas de suas aplicações**. Disponível em: http://www.magiadamatematica/diversos/eventos/20-congruência.pdf. Acesso em 18 de novembro de 2020.

SANTOS, José Plínio de O. **Introdução à teoria dos números**. Instituto de Matemática Pura e Aplicada, 1998.

TÁBOAS, C. M. G.; RIBEIRO, H. S. **Sobre Critérios de Divisibilidade**. Revista do Professor de Matemática. São Carlos - SP. Sociedade Brasileira de Matemática. Volume 06. Disponível em <https://www.rpm.org.br/cdrpm/6/5.htm>. Acesso em 02 de fevereiro de 2022.

ZABALA, Antoni. **A prática educativa: como ensinar**/Antoni Zabala;trad. Ernani F. da F. Rosa. Porto Alegre: ArtMed, 1998.

Apêndices

APÊNDICE I

PLANO DE ESTUDOS			
ALINHAMENTO MATEMÁTICO - Aulas 01 e 02			
TURMA: 7° e 8° anos	COMPONENTE CURRICULAR: MATEMÁTICA		
DATA: 05 e 12/11/2021	TEMPO PREVISTO : 02 ENCONTROS		
PROFESSOR: ROBERTO AMORIM SILVA			
CONTEÚDOS	HABILIDADES BNCC	METODOLOGIA	AVALIAÇÃO
-Potenciação e suas propriedades; -Notação científica e dízimas periódicas; -Fatoração.	(EF08MA02) Resolver e elaborar problemas usando a relação entre potenciação e radiciação, para representar uma raiz como potência de expoente fracionário; (EF08MA01) Efetuar cálculos com potências de expoentes inteiros e aplicar esse conhecimento na representação de números em notação científica; (EF09MA09) Compreender os processos de fatoração de expressões algébricas, com base em suas relações com os produtos notáveis.	-Aulas expositivas; -Diálogo e troca de ideias entre os alunos e entre eles e o professor; -Sessões de resoluções de problemas;	-Participação nos encontros; -Resolução de lista de exercícios.
Dúvidas	Podem ser postadas no mural do Google Classroom ou via Google meet no horário da aula.		
Devolutiva	Via Google classroom ou Whatsapp		

APÊNDICE II

PLANO DE ESTUDOS			
DIVISIBILIDADE - Aulas 03 e 04			
TURMA: 7° e 8° anos	COMPONENTE CURRICULAR: MATEMÁTICA		
DATA: 19 e 26/11/2021	TEMPO PREVISTO : 02 ENCONTROS		
PROFESSOR: ROBERTO AMORIM SILVA			
CONTEÚDOS	HABILIDADES BNCC	METODOLOGIA	AVALIAÇÃO
-Algoritmo da divisão; -Múltiplos e divisores de um número inteiro; -Teorema dos restos; -Critérios de divisibilidade.	(EF06MA06) Resolver e elaborar problemas que envolvam as ideias de múltiplo e divisor; (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 ao conteúdo.	-Participação nos encontros; -Resolução de lista de exercícios. -Resolução de teste individual.
Dúvidas	Podem ser postadas no mural do Google Classroom ou via Google meet no horário da aula		
Devolutiva	Via Google classroom ou Whatsapp		

APÊNDICE III

PLANO DE ESTUDOS			
CONGRUÊNCIAS - Aulas 05 e 06			
TURMA: 7° e 8° anos	COMPONENTE CURRICULAR: MATEMÁTICA		
DATA: 03 e 10/12/2021	TEMPO PREVISTO : 02 ENCONTROS		
PROFESSOR: ROBERTO AMORIM SILVA			
CONTEÚDOS	HABILIDADES BNCC	METODOLOGIA	AVALIAÇÃO
-Inteiros congruentes; -Caracterização de inteiros congruentes; -Propriedades das congruências; -Aplicações de congruências.	(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; Associação da teoria com situações do cotidiano: relógios, calendários, etc. Nova abordagem de problemas já vistos; Discussão e resolução de problemas com a turma;	Participação nos encontros; Resolução de lista de exercícios. Resolução de teste individual.
Dúvidas	Podem ser postadas no mural do Google Classroom ou via Google meet no horário da aula		
Devolutiva	Via Google classroom ou Whatsapp		

APÊNDICE IV

Questionário Projeto: Congruência Modular como ferramenta para o desenvolvimento da educação no ensino fundamental

UNIVERSIDADE ESTADUAL DO MARANHÃO
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL
PROFESSOR: ROBERTO AMORIM SILVA
TURMAS: 7° E 8° ANOS - UEB BANDEIRA TRIBUZZI
NOME DO ALUNO:

Exercício 1. Considerando a tabela abaixo, responda em que coluna aparecem os números 128 e 535.

0	1	2	3	4
5	6	7	8	9
10	11	12	13	14
15	16	17	18	19
20	21	22	23	24
25	26	27	28	29
30	31	32	33	34
35	36	37	38	39
40	41	42	43	44
45	46	47	48	49
50	51	52	53	54
55	56	57	58	59
60	61	62	63	64
65	66	67	68	69

Exercício 2. Para descobrir o resto da divisão do número $1000 \cdot 1001 \cdot 1002$ na divisão por 9, podemos ver o resto da divisão de cada número em separado por 9 e multiplicar os resultados como segue: $1000 \cdot 1001 \cdot 1002 \equiv 1 \cdot 2 \cdot 3 \mod 9$. Assim, $1000 \cdot 1001 \cdot 1002 \equiv 6 \mod 9$. Isso significa que o resto da divisão de $1000 \cdot 1001 \cdot 1002$ por 9 é 6.

(a) A resolução está correta

(b) A resolução NÂO está correta

Exercício 3. Qual o resto da divisão do número $1000^2 \cdot 1001^2 \cdot 1002^2$ por 9?

(a) 0

(b) 1

(c) 2

(d) 3

Exercício 4. Encontre o algarismo das unidades do número 2^{34}.

Exercício 5. Considere a imagem do cartão de CPF abaixo e responda: Qual o estado brasileiro responsável pela emissão do CPF? O primeiro dígito verificador está correto? E o segundo?

Fonte:clubes.obmep.org.br

Anexos

ANEXO I

Módulo Potenciação e Dízimas periódicas

(Material Adaptado Módulo Potenciação e Dízimas periódicas – Portal da OBMEP)

- Potenciação

Definição: Se $\boldsymbol{a}$ é um número racional e $\boldsymbol{n}$ é um número inteiro positivo, a potência de base $\boldsymbol{a}$ e expoente $\boldsymbol{n}$ é definida por

$$a^1 = a$$
$$a^n = \underbrace{a \cdot a \cdots a}_{n\,vezes}$$

Propriedades:

1. $a^m \cdot a^n = a^{m+n}$
2. $a^m : a^n = a^{m-n}$
3. $(a^m)^n = a^{m \cdot n}$
4. $(a \cdot b)^n = a^n \cdot b^n$
5. $a^0 = 1$
6. $a^{-n} = \frac{1}{a^n}$
7. $a^{\frac{m}{n}} = \sqrt[n]{a^m}$

Observação: As propriedades 5, 6 e 7, correspondem aos respectivos casos específicos, expoente zero, expoente negativo e expoente racional.

- Dízimas periódicas

Definição: Dizemos que um inteiro positivo x está escrito em notação científica se é da forma $x = m \cdot 10^k$ onde k é um número inteiro e m satisfaz $1 \leq |m| < 10$.

Exercício 1. Calcule o valor das expressões:

(a) 5^3

(b) $2^2 + 5^2$

(c) 5^4

(d) $4^3 + 3^3$

(e) $\frac{1}{3} \cdot 3^2 \cdot 10$

Exercício 2. Calcule o valor das expressões:

(a) $(0,02)^2$

(b) $100 \cdot \frac{1}{5^2}$

(c) $40 \cdot (\frac{1}{4})^3$

(d) $\frac{1}{4} \cdot (0,1)^2$

(e) $50 \cdot (0,02)^3$

Exercício 3. Escreva os seguintes números na notação científica:

(a) 123456

(b) $0,0085964$

(c) -778

(d) $0,097$

Exercício 4. Encontre a fração geratriz de:

(a) $0,555\ldots$

(b) $0,121212\ldots$

(c) $6,11111\ldots.$

(d) $-0,3333\ldots$

Exercício 5. Fatore as expressões:

(a) $5x + bx$

(b) $ax + ay$

(c) $ya + yb + yc$

(d) $bx + b$

(e) $mn + no + mno$

Exercício 6. Simplifique as frações fatorando o denominador e o numerador.

(a) $\frac{3x+5y}{6x+10y}$

(b) $\frac{5m+5n}{7m+7n}$

(c) $\frac{3p^2+5p}{6p+10}$

(d) $\frac{x(a+b)+y(a+b)}{(x-y)a+(x-y)b}$

(e) $\frac{x^4+x^3}{x^2+x}$

ANEXO II

Módulo Divisibilidade

(Material Adaptado - Módulo Divisibilidade POTI, Oliveira (2012) e Fomin (2019))

Teorema 1 (Algoritmo da Divisão). Para quaisquer inteiros a e b com $a \neq 0$, existe um único par de inteiros $(q,\ r)$ tais que $b = aq + r$ e $0 \leq r < |a|$. Os números q e r são chamados de quociente e resto, respectivamente, da divisão de a por b.

Exemplo: $7 \,|\, 21$ pois $21 = 7 \cdot 3$. Por outro lado $3 \not| \ 8$, pois 8 não pertence ao conjunto dos múltiplos de 3.

Exercício 1. Verifique se o número $2^9 \cdot 3$ é divisível por 2, 3, 5, 8 ou 9.

Exercício 2. É verdade que se um número inteiro for divisível por 4 e por 3, então ele será divisível por 12?

Exercício 3. O número **A** não é divisível por 3. É possível que o número **2A** seja divisível por 3?

Exercício 4. O número **A** é par. É verdade que o número **3A** tem que ser divisível por 6?

Teorema 2 (Teorema dos Restos). Se b_1 e b_2 deixam restos r_1 e r_2 na divisão por a, respectivamente, então:

(i) $b_1 + b2$ deixa o mesmo resto que $r_1 + r_2$ na divisão por a;

(ii) $b_1 \cdot b_2$ deixa o mesmo resto que $r_1 \cdot r_2$ na divisão por a.

Exercício 5. Qual o resto que o número $1002 \cdot 1003 \cdot 1004$ deixa quando dividido por 7?

Exercício 6. Qual o resto que o número 4^{5000} deixa quando dividido por 3?

Exercício 7. Qual o resto que o número 2^{2k+1} deixa quando dividido por 3?

Exercício 8. Sabendo que o ano de 2021 iniciou em um sexta-feira, responda: Em que dia da semana cairá o último dia desse ano? Em que dia da semana cairá o 1º dia de 2024? E o último dia?

Exercício 9. Qual o resto de $n^3 + 2$ na divisão por 3?

Exercício 10. Prove que $n^2 + 1$ não é divisível por3qualquer que seja o inteiro n.

ANEXO III

Módulo Congruências

(Material Adaptado - Módulo Congruências POTI, Oliveira (2012) e Fomin (2019))

Definição 1: Dizemos que os inteiros a e b são congruentes módulo m se eles deixam o mesmo resto quando divididos por m. Denotaremos por $a \equiv b \mod m$.

E podemos estabelecer as seguintes propriedades em relação a congruência:

Teorema 1. Se $a \equiv b \mod m$ e $c \equiv d \mod m$, então:

(i) $a + b \equiv c + d \mod m$;

(ii) $a - b \equiv c - d \mod m$;

(iii) $ka \equiv kb \mod m$;

(iv) $ac \equiv bd \mod m$;

(v) $a^k \equiv b^k \mod m$.

Teorema 2. Se p é um número primo e $a, b \in \mathbb{Z}, ento$

$$a^p \equiv a \mod p$$

Além disso, se p não divide a

$$a^{p-1} \equiv 1 \mod p$$

Exercício 1. Calcule o resto de 4^{100} por 3, 5 e 7.

Exercício 2. Ache o resto da divisão de:

a) 7^{10} por 51.

b) 2^{100} por 11.

c) 14^{256} por 17.

Exercício 3. Qual o resto da divisão de 237^{28} por 13?

Exercício 4. Qual o resto de $36^{36} + 41^{41}$ na divisão por 77?

Exercício 5. Determine o resto da divisão por 7 do número:

a) $1^7 + 2^7 + 3^7 + ... + 100^7$.

b) $1^6 + 2^6 + 3^6 + ... + 100^6$.

Exercício 6. Ache o resto da divisão de $13^{16} - 2^{25}3^{15}$ por 3.