UNIVERSIDADE FEDERAL RURAL DO SEMIÁRIDO (UFERSA)
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
CENTRO DE CIÊNCIAS EXATAS E NATURAIS
MESTRADO PROFISSIONAL EM MATEMÁTICA (PROFMAT)

FRANCISCO JOSÉ DE SOUZA SILVA

CONGRUÊNCIAS MODULARES: A APLICABILIDADE DA TEORIA DOS NÚMEROS NO SUPORTE À RESOLUÇÃO DE PROBLEMAS

MOSSORÓ – RN
2023

FRANCISCO JOSÉ DE SOUZA SILVA

CONGRUÊNCIAS MODULARES: A APLICABILIDADE DA TEORIA DOS NÚMEROS NO SUPORTE À RESOLUÇÃO DE PROBLEMAS

Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática – Centro de Ciências Exatas e Naturais - UFERSA, na modalidade Mestrado Profissional, como requisito parcial para obtenção do título de Mestre em Matemática

Orientador: Dr. Walter Martins Rodrigues

MOSSORÓ – RN

2023

S586c SILVA, FRANCISCO JOSÉ DE SOUZA SILVA.
CONGRUÊNCIAS MODULARES: A APLICABILIDADE DA TEORIA DOS NÚMEROS NO SUPORTE À RESOLUÇÃO DE PROBLEMAS / FRANCISCO JOSÉ DE SOUZA SILVA SILVA. - 2023.
101 f. : il.

Orientador: WALTER MARTINS RODRIGUES RODRIGUES.
Dissertação (Mestrado) - Universidade Federal Rural do Semi-árido, Programa de Pós-graduação em Matemática, 2023.

1. CONGRUÊNCIA MODULAR. 2. MATEMÁTICA. 3. TEORIA DOS NÚMEROS. I. RODRIGUES, WALTER MARTINS RODRIGUES, orient. II. Título.

Ficha catalográfica elaborada por sistema gerador automáto em conformidade com AACR2 e os dados fornecidos pelo) autor(a).
Biblioteca Campus Mossoró / Setor de Informação e Referência
Bibliotecária: Keina Cristina Santos Sousa e Silva
CRB: 15/120

FRANCISCO JOSÉ DE SOUZA SILVA

CONGRUÊNCIAS MODULARES: A APLICABILIDADE DA TEORIA DOS NÚMEROS NO SUPORTE À RESOLUÇÃO DE PROBLEMAS

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional-PROFMAT da Universidade Federal Rural do Semi-Árido-UFERSA, como requisito para obtenção do título de Mestre em Matemática.

Linha de Pesquisa: Ensino de Matemática

Defendida em: 28 /06 / 2023.

BANCA EXAMINADORA

Assinado de forma digital por WALTER MARTINS RODRIGUES:10304206881
Dados: 2023.08.31 16:50:30 -03'00'

Prof. Dr. Walter Martins Rodrigues. (Orientador) UFERSA

Documento assinado digitalmente
gov.br
ODIRLEI SILVA JESUS
Data: 01/09/2023 09:01:39-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Odirlei Silva Jesus (UFRN)

Elmer Rolando Llanos Villarreal
Assinado de forma digital por Elmer Rolando Llanos Villarreal
Dados: 2023.08.31 18:12:31 -03'00'

Prof. Dr. Elmer Rolando LIanos Villarreal (UFERSA)

Dedicatória:

Dedico esse trabalho à minha família

AGRADECIMENTOS

Agradeço, primeiramente a Deus, pelo dom da vida e a força magistral que tem me proporcionado todos os dias e, as pessoas do meu convívio que acreditaram e contribuíram, ainda que indiretamente, para a conclusão deste curso.

Aos meus pais José Airton da Silva e Maria Zenilde de Souza Silva, pelo amor e pela paciência que têm me doado todo esse tempo. Por terem feito o possível e o impossível para me oferecer a oportunidade de estudar, acreditando e respeitando minhas decisões e nunca deixando que as dificuldades acabassem com os meus sonhos.

À minha esposa Aline Maria Da Silveira Medeiros Silva, por ter sentido junto comigo, todas as angústias, dificuldades e felicidades associadas no transcorrer do curso, acompanhando cada passo de perto; pelo amor, paciência e carinho depositados, além da companhia por todos esses 34 anos de convivência. Agradeço ao meu orientador, Professor Dr. Walter Martins Rodrigues, pela paciência, dedicação, compromisso e ensinamentos magistrais que possibilitaram a realização deste trabalho.

À esta universidade e todo corpo docente do curso, que realizam seu trabalho com tanto amor e dedicação, trabalhando incansavelmente para que nós, alunos, possamos contar com um ensino de extrema qualidade. Em especial ao coordenador Professor Dr. Walter Martins Rodrigues, que por feliz coincidência é também meu orientador.

Agradeço à todos os meus amigos da turma PROFMAT- UFERSA 2021, por confiarem em mim e estarem ao meu lado em todos os momentos, em especial aos colegas Kaio Lamaison, Djalma Júnior, Paulo Rodrigues e Davidson Estanislau, contribuindo com a minha aprendizagem e com palavras de incentivo no suporte à minimização das angústias e dificuldades enfrentadas.

Por fim, agradeço à Sociedade Brasileira da Matemática - SBM pelo oferecimento deste Curso em Rede Nacional.

RESUMO

Este trabalho de pesquisa discorre sobre a evolução da Teoria dos Números, fazendo referência à fundamentação teórica de seus principais tópicos, mais especificamente relacionada às congruências modulares e a contribuição trazida por esta ferramenta como suporte na resolução de problemas, com exemplos de aplicações cotidianas; para isso, faz-se uma intervenção pedagógica sobre a "Congruência Modular no Ensino Médio", em turmas de uma Escola Estadual de Ensino Médio em Tempo Integral de Fortaleza – Ceará. Metodologicamente, aborda-se a pesquisa qualitativa e pesquisa ação, objetivando, principalmente, utilizar a Congruência como uma metodologia para o desenvolvimento do raciocínio lógico ou letramento matemático no suporte à boa prática da capacidade de resolução de problemas e, consequentemente a elevação da auto estima do estudante, a confiança em sua própria capacidade. À partir daí, espera-se que os(as) alunos(as) percebam a importância do amparo que a temática entrega como ferramenta que produz solução. Como consequência natural, é esperado que soluções sejam conseguidas e, paralelo à tal conquista, venha o interesse e a motivação no estudo geral da Matemática. A exposição tem esteio pedagógico e legal na observação cuidadosa que foi feita na Base Nacional Comum Curricular (BNCC, 2017). Pensamos que, se há noção e motivação em relação ao que está sendo abordado, os objetivos em relação à aprendizagem serão alcançados e haverá uma consequente melhora nos resultados de avaliações tanto internas quanto externas, ingresso ao ensino superior e demais objetivos alcançados.

Palavras Chaves: Congruência modular. Matemática. Teoria dos Números.

ABSTRACT

This research work discusses the evolution of Number Theory, referring to the theoretical foundation of its main topics, more specifically related to modular congruences and the contribution brought by this tool as a support in solving problems, with examples of everyday applications; for this, a pedagogical intervention on "Congruence in Secondary Education" is carried out in classes at a State High School in Full Time in Fortaleza-Ceará. Methodologically, qualitative research and action research are approached, aiming, mainly, to use Congruence as a methodology for the development of logical reasoning or mathematical literacy in support of good practice in problem solving capacity and, consequently, the elevation of self-esteem of the student, confidence in his own ability. From there, it is expected that the students realize the importance of the support that the theme delivers as a tool that produces a solution. As a natural consequence, it is expected that solutions will be achieved and, parallel to this achievement, interest and motivation in the general study of Mathematics will come. The exhibition has a pedagogical and legal basis in the careful observation that was made in the National Curricuar Base (BNCC, 2017). We think that, if there is an awareness and motivation in relation to what is being addressed, the objectives in relation to learning will be achieved and there will be a consequent improvement in the results of both internal and external evaluations, admission to higher education and other objectives.

Keywords: Modular congruence. Math. Number Theory.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

De acordo com a necessidade natural ao longo do tempo e o consequente surgimento da Teoria dos Números, considerando-se ainda suas evidentes aplicações práticas, fruto do trabalho de grandes estudiosos que foram relevantes para o reconhecimento dessa parte da Matemática, tal temática tornou-se de muita relevância e alvo de muitos debates acadêmicos; sendo assim, o presente trabalho de dissertação pretende fazer um breve histórico sobre a evolução da Teoria dos Números, fazendo referência à fundamentação teórica dos principais tópicos de tal conteúdo, sobretudo as congruências modulares e, o suporte que o tema dará à execução da resolução de problemas; para isso terá destaque os teoremas com exemplos de aplicações na área da Matemática bem relacionados principalmente às congruências modulares e a consequente utilidade dessa ferramenta. Ainda como justificativa da ideia central do presente trabalho, some-se o fato da temática dar suporte na facilitação e compreensão do aluno sobre diversos conceitos. Para finalizar, são apresentados relatos do resultado de atividades realizadas com alunos do Ensino Médio numa Escola de Ensino Médio em Tempo Integral em Fortaleza que está nos primeiros lugares quando nos referimos aos índices pedagógicos da Rede Pública Estadual do Estado do Ceará; com a ação, objetivamos incrementar dentre outros conteúdos da Base Comum, exatamente o que está sendo proposto, visando ressaltar a importância de entender a aplicabilidade da teoria dos números, sobretudo enfatizando as congruências modulares na sala de aula contemporânea num cenário de pós pandemia em que as redes de ensino mobilizam a recomposição de aprendizagem.

Diante dos números extremamente insatisfatórios que pairam sobre a aprendizagem matemática de um modo geral e que foram acentuados em virtude do período de pandemia, temos a incumbência e objetivação geral de introduzir naturalmente as nuances do tema afim de discorrer sobre a evolução da Teoria dos Números e onde tal proposta tem o poder de produzir efeitos positivos na motivação através da resolução de problemas e o estudo da matemática como um todo; fazendo referência à fundamentação teórica dos principais tópicos da Teoria dos Números, principalmente as congruências modulares, destacando os teoremas com exemplos de aplicações na área da Matemática de modo que se esclareça o quão é importante a utilização de seus conceitos como amparo à resolução de problemas.

Como objetivo específico, temos a intenção de desenvolver um estudo a respeito da teoria dos números, especificamente relacionado à congruência modular, fazendo referência a evolução de tal conteúdo e a fundamentação teórica dos principais tópicos com o objetivo de facilitar a compreensão do aluno desde o conceito de divisibilidade até conseguir o consequente suporte para

adquirir a boa habilidade na resolução de problemas.

A metodologia adotada foi qualitativa utilizando-se a pesquisa ação, em conformidade com (BARBIER, 2007) e (BOGDAN; BIKLEN, 1994). Em relação a estrutura, esta se dá na divisão em seis capítulos.

No primeiro capítulo, abordo a introdução com o objetivo geral e o objetivo específico do trabalho, bem como a relevância da pesquisa para o ensino e aprendizagem de qualidade na Matemática no Ensino Médio.

No segundo capítulo apresento o contexto histórico enfatizando a origem da matemática, desde a necessidade do simples registro de quantidades para controles gerais até o conceito bem amplo de número e deste aos números reais; em seguida, levanto um breve histórico acerca de alguns matemáticos e algumas de suas contribuições presentes na educação básica da atualidade, o que de certa forma mostra que as "ferramentas" matemáticas não surgem com o intuito de criar angústias; muito pelo contrário, surgem paralelas às necessidades das sociedades ao longo do tempo e com o intuito de contribuir com suas evoluções.

No terceiro e quarto capítulos, discorro sobre os principais fundamentos da teoria dos números com definições, proposições, demonstrações e as consequentes utilidades, incluindo a divisibilidade e as congruências com suas respectivas e possíveis aplicações em sala de aula no que se refere ao suporte à resolução de problemas;

No quinto capítulo, mostramos os registros de explanações em sala de aula, o processo de resolução das questões por parte dos alunos, seguida do nosso acompanhamento e as consequentes impressões coletadas.

Por fim, no sexto capítulo, dedico-me a descrever as considerações finais, com nuances produzidas desde a proposta do trabalho, a contribuição para a temática dos principais matemáticos ao longo dos tempos e, relatos e discussões das análises e impressões da aplicação e intervenção pedagógica "Congruência no Ensino Médio" na Escola de Ensino Médio em Tempo Integral Visconde do Rio Branco, em Fortaleza Ceará.

2 FUNDAMENTAÇÃO HISTÓRICA

Reconhece-se, antes de evidenciar a história da Teoria dos Números que, os documentos oficiais que regulam o ensino no Brasil, desde a constituição de 1988, a instituição da Lei de Diretrizes e Bases da Educação e a própria Base Nacional Comum ,norteiam e validam legalmente o tema proposto. Mas, sabemos que os documentos norteadores construídos exigem naturalmente muito trabalho e, muita energia demandada no momento de pôr em execução; pois, são notórias as deficiências do ensino-aprendizagem em álgebra e na matemática no cômputo geral , evidenciadas principalmente nas avaliações externas geradas pelo poder público e que estão elencadas na Base Nacional Comum Curricular (BNCC, 2017) que é um documento normatizador muito importante em relação a estrutura curricular; dentre outros fins, apresenta em sua estrutura para o componente curricular Matemática a Unidade Temática Álgebra, e recomenda que esta seja desenvolvida desdeos anos iniciais do Ensino Fundamental. Na álgebra, especificamente, a linguagem apresentada deve prevê generalizações relacionadas à dependência entre grandezas e que produza suporte à resolução de problemas.

Mergulharemos um pouco na história da matemática, vendo o sentido e de certa forma mostrando como a importância do tema proposto se evidenciou na humanidade e que há documentos legais no ordenamento jurídico que o validam como explicita os supracitados e mostram o quão é necessário que os alunos aprendam a identificar regularidade e padrões em sequência numérica; criem leis matemáticas que representam a relação de interdependência entre grandezas eutilizem e interpretem as diversas representações gráficas e simbólicas, necessárias à resolução de problemas, que fazem uso de equações e inequações.

Tal realidade contida no texto legal apresenta déficit evidenciado ao longo do tempo e poderá ser simplesmente uma consequência de se trabalhar muito a fundamentação teórica (que é necessária), porém, sem situar tal conteúdo no mundo real do aluno, onde ele possa ver na prática, a importância do mesmo, mostrando um sentido de execução prática.

Dito isto, este capítulo apresenta a história da teoria dos números, os principais conceitos da evolução da teoria dos números e os matemáticos, conceitos e contribuições já como uma justificativa da necessidade de se mostrar em sala de aula devido entre outros motivos da existência de conexões com situações reais e cotidianas.

Pode-se destacar que os números inteiros, que faz parte da Teoria dos Números, é um tema que domina a maior parte dos conteúdos nos currículos do Ensino Fundamental. Encontramos

muitos pesquisadores explorando a temática, como por exemplo Campbell e Zaskis (2002).

Por outro lado, estes autores questionam a falta de estudos neste campo e ressaltam a necessidade de mais pesquisas com esta temática. Além disso, o estudo dos números inteiros propicia o desenvolvimento de ideias matemáticas importantes, como a divisibilidade, os números primos e outros temas relacionados.

Nunca é demais enfatizar aos estudantes que a evolução dos números naturais, chegando aos inteiros não acontece através de uma pessoa que busca criar algo a mais pra complicar e colaborar para que se entenda cada vez mais a matemática como uma ciência complicada; muito pelo contrário, deve se fazer um retrospecto de como a evolução dos números acontece de forma gradual, natural e sempre à medida da evolução dos povos e das sociedades e paralela às suas necessidades, para o bom viver, e para que a otimização das relações diárias possa sempre ocorrer, é necessária a busca de ferramentas que possam e devam ser usadas nessa construção.

Como podemos notar na abordagem , ao longo da história podemos observar o avanço da Matemática, a necessidade de contar e relacionar quantidades fez com que o homem desenvolvesse símbolos no intuito de expressar inúmeras situações. Diversos sistemas de numeração foram criados em todo o mundo no decorrer dos tempos, sendo os mais antigos, originários do Egito, Suméria e Babilônia. Podemos também citar outros sistemas de numeração bastante conhecidos, como o Chinês, os Maias, o Grego, o Romano, o Indiano e o Arábico. Acrescenta-se ainda que o homem criava situações interessantes na contagem de seus objetos, animais, etc; ao levar seu rebanho para a pastagem ele relacionava uma pedra a cada animal, no momento em que ele recolhia os animais fazia a relação inversa, no caso de sobrar alguma pedra poderia constatar a falta de algum animal; era uma criação primitiva de símbolo a partir da necessidade de controle do pasto; ou seja, a criação como consequência da necessidade.

No entanto, o homem buscava algo mais concreto, que representasse de uma forma mais simples tais situações. O surgimento dos números naturais (0, 1, 2, 3, 4...) revolucionou o método de contagem, pois relacionava símbolos (números) à determinadas quantidades.

Com o início do Renascimento surgiu a expansão comercial, que aumentou a circulação de dinheiro, obrigando os comerciantes a expressarem situações envolvendo lucros e prejuízos. A maneira que eles encontraram de resolver tais situações problema consistia no uso dos símbolos + e –. Suponha que um comerciante tenha três sacas de arroz de 10 kg cada em seu armazém; se ele

vendesse 5 Kg de arroz, escreveria o número 5 acompanhado do sinal –; se ele comprasse 7 Kg de arroz, escreveria o numeral 7 acompanhado do sinal +.

Utilizando essa nova simbologia, os Matemáticos da época desenvolveram técnicas operatórias capazes de expressar qualquer situação envolvendo números positivos e negativos. Surgia um novo conjunto numérico representado pela letra Z (significa: Zahlen: número em alemão), sendo formado pelos números positivos ou nulo (Naturais) e seus respectivos opostos, podendo ser escrito da seguinte forma: Z = {...,–3, –2, –1, 0, 1, 2, 3,...}."

2.1 História da Teoria dos Números

A ciência matemática, reconhecida contemporaneamente, é resultado de mais de 4.000 anos de progressão, pesquisa e estudo que apresenta um nível de complexidade alto como também exige performance no pensamento lógico e abstrato. Tendo em vista estas considerações, é consenso, muitas vezes, que ensinar, aplicar e aprender torna-se difícil. Por isso, pretendemos reconstruir um recorte dessa história e conectar fatos com a Matemática no Ensino Médio, com a intenção de mostrar a conexão íntima da ciência matemática com o mundo e fazer com que os alunos entendam que o enfrentamento da matemática pode se tornar natural e necessário, tudo dependerá da forma de olhar.

Há indícios de que os primeiros povos viviam nos espaços abertos das matas e sobreviviam da caça, da pesca de animais, da colheita de frutos como também havia a necessidade de frequente mudanças, logo eram nômades, sendo assim, não há um marco temporal com certeza de quando iniciou e finalizou a idade da pedra como também não se sabe quando a matemática iniciou.

Embora nesse período a matemática fizesse parte da sociedade já que os habitantes faziam trocas de mantimentos entre tribos, conviviam com o sistema da divisão do que se caçava entre as comunidades e familiares, logo precisavam contar e dividir igualmente; esses indícios já utilizavam formas de senso numérico.

Historicamente, há o desenvolvimento da agricultura e do comércio que necessitava do sistema de contagem bem como de se expressar de alguma forma por meio do que se dispunha de

concreto como, por exemplo, nós em corda, marcação em madeira, ossos ou barro, amontoado de pedras empilhadas. Alguns povos, inclusive, preferiram usar partes do corpo para reproduzir a contagem como os dedos das mãos, dos pés de animais como cabras, bois e carneiros, utilizando a correspondência biunívoca entre os animais e um amontoado de pedras, visto que era assim possível verificar que os animais haviam saído pela manhã e voltaram à noite. A contagem dos dias, dos anos, a enumeração familiar tanto do nascimento quanto da morte eram necessidades; a questão de concluir transações comerciais, o escambo e para tal necessidade tinham que saber se tinham condições de trocar ou adquirir mercadorias.

Em conclusão, é a história da humanidade, que devido às circunstâncias empíricas levam a enumerar os acontecimentos e utilizarem materiais concretos.

Para Aristóteles a base numérica usada atualmente prevaleceu devido aos dez dedos nas mãos que possuímos e que foram usados como belíssima referência na contagem, além do amontoamento de pedras em grupos de cinco, dez e vinte assemelhando-se a contagem dos dedos. Assim, a origem da matemática também é discutida, numa perspectiva antropológica, que apontam que a contagem surgiu em rituais religiosos primitivos. Sendo assim, há muitas suposições não respondidas em relação à origem da matemática, conforme discute-se:

> Além disso, há um grande número de perguntas não respondidas com relação à origem da matemática. Imagina-se que surge a partir das necessidades gerais do ser humano enquanto ser que evolui na terra desde sua aparição._Foi sugerido que a arte de contar surgiu em conexão de rituais religiosos primitivos e que o aspecto ordinal precedeu o conceito quantitativo. Em ritos cerimoniais representando mitos da criação era necessário chamar os participantes à cena segundo uma ordem específica, e talvez a contagem tenha sido inventada para resolver esse problema. BOYER (1996, p. 04)

Sendo assim, no próximo tópico discutiremos mais sobre os principais conceitos da evolução da teoria dos números. É importante salientar que tais conceitos vão surgindo paralelo às necessidades que aparecem, de forma muito natural e em meio às tentativas de solução deproblemas; é bem importante salientar que, de acordo com a necessidade emergente num dado momento, gera automaticamente como consequência uma ação que busque a resolução da situaçãosurgida; notemos que a ferramenta nova que aparece não foi em função de criar mais uma estratégiae acabar deixando mais complexo tal tema mas, muito ao contrário disso, tal incremento aparece

como opção à situações fáticas que aparecem junto à evolução das sociedades e suas respectivas necessidades.

Percebe-se que as ideias iniciais e bem primitivas no surgimento dos números e de dois tipos de subconjuntos, categorias ou classificação, nos números naturais a saber: números pares (feminino) e números ímpares (masculino) que é um marco na matemática está na criação ou utilização do símbolo para o nada, o zero. Sendo assim, sobrepondo-se a toda justificativa que possa surgir, nasce a necessidade natural de contar, dentre outros fins, o de controlar de um modo geral os pertences de cada povo, de cada comunidade; some se a isso o fato de que entendemos e percebemos nas literaturas diversas que o ato de contar possui uma origem que é fruto de um produto natural. Essa percepção carece de prova, ela apenas é produção do pensamento enquanto observador de como as pessoas se desenvolvem ao longo do tempo e, hoje está em sintonia com o que realmente está ocorrendo.

Os hindus no final do século VI também realizaram constatação disto, conforme COSTA e SANTOS (2008, p. 11). Após a criação do zero, cria-se o sistema de posicionamento da base dez, utilizando a casa das unidades, dezenas, centenas e ademais subsequentes, livrando-se, dessa forma, dos problemas gerados pela ausência deste, como, por exemplo, distinguir o número 15 do 105. A ideia de produção de uma simbologia para representar o nulo, vazio é um ato valoroso da ação racional humana e relativamente recente, considerando ali o marco inicial da era cristã.

Uma coisa que nem toda a gente repara é que essa numeração constitui uma autêntica maravilha que permite, não só escrever muito simplesmente os números, como também efetuar as operações. CARAÇA (2003, p. 06)

O que se percebe é que a contagem e os números surgiram devido a necessidade diária da população mediante as situações sociais, ou seja, o homem pensava e viabilizava maneiras que facilitassem e agilizassem os cálculos. Sendo assim, criaram para utilizar vários instrumentos de contagem, como, por exemplo o ábaco, instrumento que ofereceu um valoroso suporte às operações iniciais com números inteiros. Muito prático, desobrigou o homem do esforço de acumulações, porém, exigiu o conhecimento das combinações resultantes da posição de cada conta. Não é, pois, um instrumento de cálculo, mas, apenas, indica os números adicionados e subtraídos. COSTA (1996, p. 175-178)

Destacamos também o complexo sistema de numeração romano e conforme IFRAH (1985, p. 396), que é um sistema não favorecedor de operações, ele apenas fornece símbolos que servem para abreviações e controles gerais dos números inteiros. O ábaco deu esteio à execução de muitos cálculos, apesar de que hoje, o sistema hindu-arábico prevalece nas nossas execuções de operações atuais. Nesse contexto em que tenta se relatar o histórico de surgimento, manipulação e aperfeiçoamento dos números, é prudente lembrarmos do ábaco, lançado em 1614 por Jonh Napier, enquanto instrumento lançado como suporte às execuções mais facilitadas das operações aritméticas, substituindo as multiplicações por adições e as divisões por subtrações; neste aparelho, ele generalizou o procedimento tabular dos árabes e construiu um dispositivo simples e barato; constituído de bastões de ossos, facilitando os cálculos com números grandes. Esta foi a primeira máquina de calcular, base para as que conhecemos hoje e para os modernos computadores, já com dispositivos eletrônicos. COSTA (1996, p. 175-178)

Destacamos também o complexo sistema de numeração romano e conforme IFRAH (1985, p. 396) “os algarismos romanos não permitiram a seus utilizadores fazerem cálculos(...) na verdade, os algarismos romanos não são sinais que servem para efetuar operações aritméticas, mas abreviações destinadas a notificar e reter os números”. Então,

P_5: Se uma coleção S de números naturais para efetuar cálculos, os romanos recorriam à invenção grega: o ábaco. No entanto, de acordo COSTA (1996, p. 175-176), o atual sistema em uso é produto da civilização hindu-arábica e pauta-se numa mescla entre as mesmas operações que realizamos e o sistema tabular, inspirado no sistema decimal posicional. Registramos ainda a invenção de um instrumento ou aparelho que serviu de base para a construção dos atuais computadores, tal qual conhecemos hoje.

Assim percebemos que a contagem foi produzida através dos acontecimentos empíricos até tornar-se um processo abstrato e aperfeiçoado como conhecemos hoje, tal invenção ou utilização trouxe também as operações de adição e multiplicação e as relações de diferença, divisão e ordem, designado por números naturais e representado pela sequência

$1, 2, 3, \cdots, n, n+1, \cdots.$

Apesar de tal apresentação, apenas no século XIX foi que o italiano Giuseppe Peano (1858−1932) produziu formalmente os números naturais e os respectivos conceitos primitivos, que

hoje dão suporte às demonstrações por indução em n; e, para caracterizá-los, formulou os seguintesaxiomas, conhecidos como Axiomas de Peano, conforme Domingues (1991, p. 80-81):

> P_1: Zero é um número natural.
> P_2: Se a é um número natural, então a tem um único sucessor que também é um número natural.
> P_3: Zero não é sucessor de nenhum número natural.
> P_4: Dois números naturais que têm sucessores iguais são, eles próprios, iguais.
> P_5: Contém o zero e, também, o sucessor de todo elemento de um conjunto S, então S é o conjunto de todos os números naturais.

Devemos então lembrar que os naturais são hoje assim representados:N = {0, 1, 2, 3, ⋯ , n, n+ 1, ⋯ }.

As reticências depois do número 3 nos informa que entre 1 e n existem números que não estão escritos nesta sequência, números estes obtidos através da ideia de sucessor de 1, do sucessor do sucessor de 1 etc. Já, as reticências depois no n + 1 o sucessor de n, indicam que não existe um número natural maior que todos os outros naturais, isto é, um número natural por maior que seja, sempre existe o sucessor deste, ou seja, um outro número maior. Logo, essa ideia nos remete ao ilimitado, em outras palavras, que o conjunto dos números naturais são infinitos. O conjunto dos números naturais é fechado em relação a adição e multiplicação, isto é, dados a, b naturais, tem que $a + b$ é natural; assim como $a \times b$ é natural.

Com a já citada evolução do ser humano e a crescente complexidade entre suas relações, surge a ideia de diferença, pois, o conjunto dos números naturais não era suficiente para abranger tais situações. Apenas o conjunto dos naturais sozinho não resolvia questões que envolvessem certas diferenças, como por exemplo: dados x, y números naturais, com x < y, a diferença x − y nãoé natural. Então, para resolver questões como 1 − 4 de modo a tornar o conjunto fechado em relaçãoa subtração, houve a necessidade de determinar outros símbolos. Estes novos símbolos são os números negativos cuja união com os naturais formam o conjunto de números inteiros que são representados por Z = {⋯ , −n, −(n+ 1), ⋯ , −3, −2, −1, 0, 1, 2, 3,⋯ , n, n+ 1, ⋯ }.

Notemos que a ideia de número inteiro precede a dos naturais e até mesmo sua utilização para registrar vantagens ou desvantagens nas trocas, ou outras situações, porém, não havia ainda uma aceitação formal para os mesmos, como destaca (HEFEZ, 2016).

O conceito de número inteiro originou - se do conceito bem mais antigo de número natural, cuja criação objetivava resolver problemas de contagem. Os números negativos têm sido considerados esporadicamente desde a antiguidade, mas sempre com muita desconfiança por parte dos matemáticos até que, a partir do desenvolvimento das atividades mercantis que ocorriam na Europa no final da Idade Média, sentiu-se a necessidade de considerar os inteiros relativos e com eles efetuar operações.

> (...) A evolução da noção intuitiva de número inteiro para um conceito mais elaborado foi muito lenta. Apenas em meados do século XX, onde o mundo respirava ideais iluministas, renascentistas é que a ideia de número inteiro passou a ser aceita e baseada na teoria dos conjuntos, HEFEZ (2016, p. 02).

O conjunto Z é fechado em relação às operações de adição, subtração e multiplicação. No entanto, o conjunto dos números inteiros agora formado, não é fechado em relação a divisão, isto é, dados a, $b \in$ Z, nem sempre é possível dividir a por b em Z. Como exemplo temos 2 não divide 1.

As necessidades advindas das natalidades eminentes e as consequentes complexidades de problemas que naturalmente vão surgindo, como pesagens, medições, etc, e estas com a probabilidade muito pequena de serem expressas por números inteiros. Diante disso, houve a necessidade de utilizar um novo símbolo para representar partes ou fração do todo, indicado por a / b, uma parte a do todo b obtendo dessa forma um conjunto fechado em relação a divisão designado de números racionais e denotado por Q. De um modo geral adotamos como sendo uma fração (irredutível) representado por a / b sendo a, b inteiros com b não-nulo. Ademais, exigimos que a e b não tenham divisores comuns. O conjunto de todas as frações (irredutíveis) será indicado pelo conjunto Q = $\{a / b: a, b \in Z, b \neq 0\}$, e a / b é chamado de número racional não nulo se $a \neq 0$. Por fim, registramos que o conjunto dos números racionais é fechado para as operações de adição, multiplicação, subtração e divisão.

De acordo com COSTA (1997, p. 196), em linhas gerais tudo pode ser traduzido e interpretado em números, ou seja, a essência de todas as coisas seriam os números. Logo, os Pitagóricos exaltavam os números inteiros e pensaram serem estes suficientes para explicar os

fenômenos do universo e ao descobrirem a incomensurabilidade da medida da diagonal de um quadrado de lado um, entraram em crise.

A descoberta da existência de números irracionais foi surpreendente e perturbadora para os pitagóricos. Em primeiro lugar porque parecia desferir um golpe mortal na filosofia pitagórica segundo a qual tudo dependia dos números inteiros. Além disso, parecia contrária ao senso comum, pois intuitivamente havia o sentimento de que toda grandeza poderia ser expressa por algum número racional. A contrapartida geométrica era igualmente espantosa, pois quem poderia duvidar que, dados dois segmentos de reta, sempre seria possível encontrar um terceiro segmento de reta, talvez muito, mas exageradamente pequeno, mas que coubesse um número inteiro de vezes dentro dos segmentos destacados, EVES (2004, p. 106).

Estes e outros fatos levaram os matemáticos a considerarem outros tipos de números, como exemplo, o conjunto dos números irracionais denotado por I. A união do Q com I forma o conjunto dos números reais e é designado por R, e estes formam uma correspondência biunívoca com a reta real. Importante destacar que no Brasil, mesmo com várias reformas educacionais, novas diretrizes e orientações propostas para o sistema educacional no ensino de Álgebra, permaneceu com poucas alterações na Educação Básica. Veja que o trabalho com congruência explora uma parte da matemática que os estudantes dominam com certa facilidade, e que a ideia de congruência tem forte apelo para ideia algébrica, trazendo uma nova oportunidade de fortalecer o fundamento de aprendizado de álgebra partindo de algo que eles dominam melhor. Há um elemento a favor do professor na tentativa de demonstrar leveza, praticidade e consequentemente conquistar o foco dos estudantes no assunto, já que se trata de algo com boa familiarização com o mundo real e que parte de conhecimento prévio muito simples como é o caso da divisão.

Fortificando a ideia de que a teoria dos números é uma ferramenta algébrica que deve ser mais pesquisada, explorada e, consequentemente, executada; principalmente, a partir de um sobrevoo histórico que devamos fazer ao abordar tal matéria e, em linhas gerais, é a ênfase que tentamos evidenciar, estudamos e, cada vez, mais solidifica nosso entendimento da importância do assunto em tela, o trabalho de RESENDE (2007 , p.68-72). Por exemplo, sobre *"*o surgimento dos números naturais, devido à necessidade de contar, está nas raízes da história da Teoria dos Números e presente nas civilizações mais antigas". Sendo assim, podemos observar que a matéria prima dessa importante área da matemática está posta desde épocas remotas, e o estudo das propriedades e das

relações envolvendo os números inteiros foi sendo realizado, mesmo que ainda de modo não-formal e não-sistematizado, ao longo da história dascivilizações.

Os povos egípcios e os babilônios buscaram formas de representar os números naturais e modos de operar com eles. Registraram relações, como se pôde observar na tábua Plimpton 322, escrita pelos babilônios por volta de 1900 a 1600 a.C. e descoberta recentemente. Nela, estão registradas triplas de números, que mais tarde foram denominados números pitagóricos, pois satisfazem o teorema conhecido como de Pitágoras. Essa tabela tem um importante significado na Teoria dos Números, pois os ternos pitagóricos primitivos são soluções para as equações do tipo $x^2 + y^2 = z^2$, mais tarde chamadas de equações diofantinas.

Foi na Grécia, no entanto, que o estudo dos inteiros positivos ganhou caráter mais formal, atrelado a um forte misticismo, em especial na escola pitagórica. A filosofia desta escola baseava-se no pressuposto de que a causa última das coisas são os números naturais. Isto levava consequentemente à uma exaltação e ao estudo das propriedades dos números e da aritmética (no sentido da teoria dos números), junto com a geometria, a música e a astronomia; percebam a extensão e conexão dos números com grandes ramos do mundo real.

Os pitagóricos levaram ao extremo a admiração aos números, baseando neles a sua filosofia e seu modo de viver. O número um, diziam eles, é o gerador dos números, o número da razão; o dois é o primeiro número par ou feminino, o número da opinião; o três, o primeiro número masculino verdadeiro, o da harmonia; o quatro é o número da justiça; o cinco é o número do casamento, união do masculino e do feminino; o seis é o número da criação; e o dez é o mais sagrado,pois representava a soma de todas as dimensões geométricas".

No próximo tópico discutiremos sobre os matemáticos, conceitos e suas contribuições ao longo da história, na manipulação desses números e como uma efetiva estratégia didática na inserção de uma cultura de importância do letramento matemático.

2.2 Matemáticos, conceitos e contribuições

Um dos primeiros pensadores a ser referendado como matemático é Tales. Tales de Mileto, assim chamado porque nasceu na cidade comercial de Mileto na Ásia Menor, fundou a escola

Ioniana e nesta estudava a geometria, astronomia e teoria dos números. No entanto, não se sabe ao certo as obras provindas de Tales e tampouco com precisão sobre sua vida. Sabemos que Tales de Mileto era considerado muito inteligente, sendo, portanto, designado o primeiro dos Sete Sábios da Antiguidade.

Tales de Mileto era comerciante de profissão, conseguiu tornar-se rico e, no final de sua vida, pode dedicar-se aos estudos e viagens. Tales viajava muito em virtude de sua profissão e, em uma dessas viagens deparou-se no Egito e Mesopotâmia adquirindo base matemática devido seu contato com a matemática desenvolvida naquelas localidades, fato este que o fez tornar se matemático. E, em virtude de sua passagem pelo Egito, calculou a altura de uma pirâmide, usando para tal a sombra da referida pirâmide.

Porém Eves destaca que,

> Com relação ao modo como Tales de Mileto calculou e explorou as dimensões gigantes das pirâmides egípcias, simplesmente usando a sombra, que eram medidas acessíveis. O relato mais antigo, dado por Hierônimos, um discípulo de Aristóteles, diz que Tales anotou o comprimento da sombra no momento em que esta era igual à altura da pirâmide que a projetava. A versão posterior, dada por Plutarco, diz que ele fincou verticalmente uma vara e fez uso da semelhança de triângulos. Ambas as versões pecam ao não mencionar a dificuldade de obter, nos dois casos, o comprimento da sombra da pirâmide. EVES (2004, p. 115).

De acordo com BOYER (1996, p. 34), o que hoje é conhecido como teorema de Tales pode ter sido fruto de conhecimentos adquiridos por ele em suas viagens à Babilônia. É atribuído a Tales a criação da geometria dedutiva, e algumas das primeiras demonstrações matemáticas. E ainda conforme Boyer credita a Tales a prova dos seguintes Teoremas:

> 1) Um círculo é bissectado por um diâmetro.
> 2) Os ângulos da base de um triângulo isósceles são iguais.
> 3) Os pares de ângulos opostos pelo vértice, originados por duas retas concorrentes, possuem medidas iguais.
> 4) Dois triângulos são tais que dois ângulos e um lado de um são iguais respectivamente a dois ângulos e um lado de outro, então os triângulos são congruentes. BOYER (1996, p. 34).

Dessa forma, coube a Tales diante de raciocínio lógico grandes descobertas matemáticas em particular na geometria, descobertas essas que estão presentes no ensino acadêmico de hoje, conforme a Base Nacional Comum Curricular – BNCC, No Ensino Fundamental (...) devem ser enfatizadas também as tarefas que analisam e produzem transformações e ampliações ou reduções de figuras geométricas planas, identificando seus elementos e todos os seus elementos quer sejam variáveis ou fixos, com o fim de desenvolver as ideias de congruência e semelhança. Esses conceitos devem ter destaque no Ensino Fundamental, de modo que os alunos sejam capazes de reconhecer as condições necessárias e suficientes para obter triângulos congruentes ou semelhantes e que saibam aplicar esse conhecimento para realizar demonstrações simples, contribuindo para a formação de um tipo de raciocínio importante para a Matemática, o raciocínio hipotético-dedutivo. BRASIL (2017, p. 272).

Para o Ensino Médio, a Base Nacional Comum Curricular – BNCC, sobre o raciocínio lógico em particular na geometria, destaca que:

> O trabalho de representar as diferentes figuras planas e espaciais, presentes na natureza ou imaginadas, deve ser aprofundado e sistematizado a partir de alguns conceitos estudados no ensino fundamental devem ser consolidados, como, por exemplo, as ideias de congruência, semelhança e proporcionalidade, o Teorema de Tales e suas aplicações, as relações métricas e trigonométricas nos triângulos (retângulos e quaisquer). BNCC MEC (2006, p. 75-76).

A Escola que exalava os ideais de Tales foi perdendo consistência diante da eminente escola de Pitágoras, situada no sul da Itália, fundada por Pitágoras, uma unidade munida de rituais e cerimônias, além de estudar matemática (aritmética e geometria), música, astronomia, filosofia e ciências. Segundo EVES (2004, p. 97), “é possível que Pitágoras tenha sido discípulo de Tales, pois era cinquenta anos mais novo do que este e morava perto de Mileto, onde vivia Tales”.

No entanto, BOYER (1996, p. 35) afirma que essa diferença de idade era bem maior, o que resta bem improvável que um fosse discípulo do outro.

Algumas semelhanças de seus interesses podem ser explicadas graças a viagens em que Pitágoras também tenha realizado, como Egito e Babilônia”. Para Pitágoras, todo o universo era matemática como destaca Costa, Pitágoras de Samos (580/78 − 497/6 a.C.) fundou uma espécie de associação de caráter mais religioso que filosófico, cujas doutrinas eram mantidas em segredo, os

ensinamentos não eram escritos, eram transmitidos oralmente e guardados em segredo pelos iniciados.

Segundo seus ensinamentos, o sagrado mistério da ciência tem o seu centro nas matemáticas, no estudo do número, cuja lei domina em todas as coisas: nos astros, cujas distâncias, grandezas e movimentos são regulados por meio de relações matemáticas (geométricas e numéricas); nos sons, cujas relações de harmonia obedecem a leis numéricas fixas; na vida e na saúde, que são proporções numéricas e harmônicas de elementos; nos fatos morais entre os quais também a justiça é proporção etc. Assim, imaginam que os números falam e representam as próprias figuras geométricas, coisas e resumem tudo à uma unidade e a ideia primitiva de ponto. Concluem eles que os números são entes geométricos e reduzem todas as coisas à unidade e ao ponto, bem como destaca Boyer, Misticismo sobre números não é criação dos pitagóricos. O número sete, por exemplo, era objeto de especial respeito, presumivelmente por causa das sete estrelas errantes, ou planetas, das quais a semana derivou todas as coisas. COSTA (1997, p. 196).

Percebemos então que Pitágoras exaltava os números. Místico e profeta da natureza, para ele os números eram entes de devoção. Bem como relata Boyer, o Misticismo que envolve os números não é fruto do pensamento pitagórico; haviam números com especial respeito por representarem situações relacionadas à natureza, ao sistema planetário, as estrelas, enfim, respeito especial. Os pitagóricos não eram os únicos a imaginar que os números ímpares tinham atributos masculinos e femininos os pares – com a concomitante crença (não destituída de preconceito), encontrada ainda em Shakespeare, de que “há divindade nos números ímpares”.

Muitas civilizações primitivas partilharam de vários aspectos da numerologia, mas os pitagóricos levaram a extremos a adoração dos números, baseando neles sua filosofia e modo de viver. Cada número representava alguma coisa importante quer seja na matemática, quer seja nas relações do dia a dia como razão, harmonia, justiça, opinião, ajuste de contas, casamento, criação, etc.

Cada número tinha, por sua vez, seus atributos peculiares. O mais sagrado era o dez ou o tetractys, pois 21 representava o número do universo, inclusive a soma de todas as possíveis dimensões geométricas. Um ponto gera as dimensões, dois pontos determinam uma reta de dimensão um, três pontos não alinhados determinam um triângulo com área de dimensão dois, e quatro pontos não coplanares determinam um tetraedro com volume de dimensão três; a soma dos

números que representam todas as dimensões é, portanto, o adorado número dez. A abstração da matemática pitagórica atribui ao número 10 uma série de convicções positivas ao considerá-lo; notemos que ainda hoje a ideia é disseminada tanto no futebol como numa nota máxima pedagógica atribuída a um aluno, enfim essa veneração ao número 10 é comentada em, BOYER (1996, p. 39).

O costume da época era dar ao fundador da escola o mérito de todas as descobertas realizadas pela escola, então, não se sabe ao certo se as descobertas atribuídas a Pitágoras necessariamente tenham sido produzidas por ele; é fato que a escola tem o mérito, porém, é possível que outros seguidores tenham feito uma produção ou outra. Grandes feitos na Teoria dos números são atribuídos a Pitágoras, por exemplo, a classificação em par e ímpar. A definição de número primo, entre outras. Além da descoberta do teorema que leva seu nome, a saber: "Em um triângulo retângulo, o quadrado da hipotenusa é igual à soma dos quadrados dos catetos".

Dentre as contribuições de Pitágoras na matemática presente hoje em dia no ensino básico, podemos destacar: Relações métricas no triângulo retângulo Teorema de Pitágoras: verificações experimentais e demonstração retas paralelas cortadas por transversais: teoremas de proporcionalidade e verificações experimentais.(...) Demonstrar relações métricas do triângulo retângulo, entre elas o teorema de Pitágoras, utilizando, inclusive, a semelhança de triângulos. O teorema é muito amplo e consegue ser ferramenta e guia de solução mesmo considerando outros conteúdos que não sejam diretamente o triângulo retângulo; até mesmo em outra disciplina como na física, a contribuição ao entendimento e suporte na resolução de problemas é algo fenomenal. Tal abrangência é comentada por, BRASIL (2017, p. 318-319).

Destacamos ainda conforme o Sistema de Avaliação da Educação Básica – SAEB - MEC Inep (2017, p. 65), o aluno deve ganhar autonomia para perceber as relações entre figuras semelhantes; também é provável que seja capaz de determinar: uma das medidas de uma figura tridimensional, utilizando o teorema de Pitágoras". Com o fim da escola Pitagórica que conforme MOL (2013, p. 35) "Após um levante popular, o templo de Pitágoras em Crotona foi destruído e sua irmandade deixou de existir como um grupo ativo e organizado", Platão, influenciado pelas ideias do também filósofo Pitágoras, fundou em Atenas a sua escola: Academia, lugar destinado ao estudo da filosofia e ciência. Platão dava muita importância ao estudo da matemática, especificamente geometria, acreditava que está dominava o universo e a considerava indispensável para a formação racional das pessoas. E, na entrada de sua escola, estava escrito conforme afirma

BOYER (1996, p. 63) “Que ninguém que ignore a geometria entre aqui”. Evidenciando dessa forma o quão importante era a matemática para Platão. E ainda conforme BOYER (1996, p. 63) “os poliedros regulares (...) foram chamados (...) sólidos platônicos devido a maneira pela qual Platão (...) os aplicou à explicação de fenômenos científicos”. No entanto, não existem contribuições matemáticas apontadas a Platão.

Assim destaca Eves,

> “A importância de Platão na matemática não se deve a nenhuma das descobertas que fez mas, isto sim, à sua convicção entusiástica de que o estudo da matemática fornecia o mais refinado treinamento do espírito e que, portanto, era essencial que fosse cultivado pelos filósofos e pelos que deveriam governar seu Estado ideal.(...) A matemática parecia da mais alta importância a Platão devido ao seu componente lógico e à atitude espiritual abstrata gerada por seu estudo; por essa razão ela ocupava um lugar de destaque no currículo da Academia. Alguns veem nos diálogos de Platão o que poderia ser considerada a primeira tentativa séria de uma filosofia da matemática.” EVES (2004, p. 131-132).

Percebemos então que apesar da matemática ser de suma importância para Platão, este não se tornou um matemático, todavia, em sua escola (Academia) formava matemáticos. E de acordo com Boyer, Platão é importante na história da matemática principalmente por seu papel como inspirador e guia de outros, e talvez a ele se deva a distinção clara que se fez na Grécia antiga entre aritmética (no sentido de teoria dos números) e logística (a técnica de computação). Platão considerava a logística adequada para negociantes e guerreiros, que precisam aprender a arte dos números, ou não saberão dispor suas tropas. De fato, o filósofo, demonstra conhecer a aritmética porque um ser pensante sem dúvida será capaz de conquistas até mesmo fora de sua área habitual, ele é convidado a raciocinar sobre o número do abstrato. Mostrando dessa forma, que suas contribuições vão além da geometria, e, por exemplo, o estudo da aritmética. BOYER (1996, p. 64)

Reforcemos também que se deve a Platão a montagem de alguns conceitos matemáticos, assim afirma Roque e Carvalho; ele prega críticas duras aos geômetras por não empregarem critérios de rigor desejáveis nas práticas matemáticas.

> (...) Sendo assim, ainda que não possamos dizer que a transformação dos fundamentos da Matemática grega é devida a Platão, ele expressa o descontentamento dos filósofos com os métodos empregados e articula o trabalho dos pensadores à sua volta para que se dediquem

> a formalizar os conceitos e técnicas utilizadas indiscriminadamente na Matemática da época. ROQUE e CARVALHO (2012, p. 52)

Inclusive podemos enumerar algumas contribuições de Platão na matemática acadêmica da atualidade como:

> Desenvolver o raciocínio lógico, o espírito de investigação e a capacidade de produzir argumentos convincentes, recorrendo aos conhecimentos matemáticos para compreender e atuar no mundo. Compreender as relações entre conceitos e procedimentos dos diferentes campos da Matemática (Aritmética, Álgebra, Geometria, Estatística e Probabilidade) e de outras áreas do conhecimento, sentindo segurança quanto à própria capacidade de construir e aplicar conhecimentos matemáticos, desenvolvendo a autoestima e a perseverança na busca de soluções. Fazer observações sistemáticas de aspectos quantitativos e qualitativos presentes nas práticas sociais e culturais, de modo a investigar, organizar, representar e comunicar informações relevantes, para interpretá-las e avaliá-las crítica e eticamente, produzindo argumentos convincentes. BRASIL (2017, p. 267).

Alexandre, o Grande, fundou a cidade de Alexandria e está, no lugar de Atenas, tornou o centro de saberes culturais, filosóficos e matemáticos. Ali, construiu uma escola conhecida como Museu, muito bem equipada e que possuía ampla biblioteca. E tiveram que recorrer a alguns intelectuais "estrangeiros" para desenvolver os vários campos de estudos, em particular foram atrás de Euclides. Pouco se sabe da vida de Euclides, acredita que sua formação matemática é proveniente da escola de Platão. Euclides escreveu a obra "Os elementos", volumes que até hoje inspiram vários assuntos matemáticos e expõem um leque de opções para resolução de problemas diversos, com linguagem clara e precisa, conhecimentos matemáticos elementares acumulados ou conhecidos até então. A saber: Teoria dos números, Geometria (pontos, retas, círculos e esferas) e Álgebra, sendo este depois da bíblia, o livro mais lido e editado em toda história. E conforme Roque e Carvalho, Com Euclides, a Matemática na Grécia parece ter adquirido uma configuração particular, passando a empregar enunciados geométricos gerais, que não envolvem somente procedimentos de medida. Os Elementos de Euclides representam, neste contexto, o resultado dos esforços deformalização da Matemática para apresentar uma geometria consistente e unificada que valesse para grandezas quaisquer, fossem elas comensuráveis ou incomensuráveis.

> (...). O papel desta obra na Matemática não pode ser superestimado. Em primeiro lugar, ela expõe, de maneira organizada, a Matemática elementar que os gregos da época clássica

> tinham criado e desenvolvido. Assim, muito do que sabemos da Matemática grega deve-se a esta obra de Euclides. Em segundo lugar, como os Elementos constituem a mais antiga exposição organizada de Matemática que nos chegou, eles muito influenciaram seu desenvolvimento posterior. (...) Os Elementos se dividem em três grandes partes: 1. Geometria plana – Livros I-VI; 2. Aritmética – Livros VII-IX; 3. Geometria espacial – Livros XI-XIII. ROQUE e CARVALHO (2012, p. 53-67).

Acredita que os Elementos não é obra exclusiva de Euclides, e que os matemáticos coordenados por ele, colaboraram com a escrita da tão importante e suntuosa obra da matemática, que infelizmente metade se perdeu. Esse fenomenal trabalho foi usado conforme MOL (2013, p. 45) "como livros-textos para o ensino da matemática até o final do século XIX e início do século XX". No entanto, não existem evidências de descobertas matemáticas atribuídas a Euclides, e sua contribuição a matemática se dá na organização, sistematização, demonstração e exposição da matemática através dos Elementos. Além dos Elementos, Euclides escreveu vários outros livros, e que alguns se perderam. Dentre as várias contribuições de Euclides ainda presentes no ensino da matemática da atualidade, destacamos:

> Compreender as relações entre conceitos e procedimentos dos diferentes campos da Matemática (Aritmética, Álgebra, Geometria, Estatística e Probabilidade) e de outras áreas do conhecimento, sentindo segurança quanto à própria capacidade de construir e aplicar conhecimentos matemáticos, desenvolvendo a autoestima e a perseverança na busca de soluções. BRASIL (2017, p. 267).

Destacamos ainda os elementos de conhecimentos contidos em séries bem iniciais que conforme a BNCC BRASIL (2017, p. 300), elenca as quatro operações básicas e mais a potenciação envolvendo números naturais.

O mais recente matemático da escola de Alexandria foi Diofanto, que escreveu uma coleção composta por treze livros intitulada Aritmética; no teor, explicita técnicas que dão suporte à resoluções de problemas sem o uso de técnicas geométricas, até então presente em toda matemática, e assim sendo, sua obra se assemelha muito da álgebra da atualidade, pois introduziu símbolos, notações e abreviaturas matemáticas.

Segundo ROQUE e CARVALHO (2012, p. 131) "Uma de suas principais contribuições está em ter introduzido uma forma de representar o valor desconhecido em um problema, designando o como arithme, de onde vem o nome aritmética". Foi pela obra de Diofanto que surgiu a álgebra moderna. No entanto, muitos desses livros foram perdidos.

Conforme EVES (2004, p. 207) o italiano Diofanto escreveu alguns trabalhos de Aritmética, entendendo que em geral contribuiriam sobremaneira à independência da álgebra em relação à geometria, dando força à álgebra e produzindo adesão no mundo.

Dentre os vários assuntos estudados por Diofanto destacamos: equações indeterminadas cuja soluções empregava artifícios nos cálculos indicando dessa forma seu vasto conhecimento das propriedades dos números naturais, sendo portando considerado conforme MOL (2013, p. 58): Diofanto é sem dúvida um dos principais nomes da álgebra moderna; foi quem a deixou de certa forma mais independente e um tanto quanto desgarrada da geometria.

> A unidade temática Álgebra, por sua vez, tem como finalidade o desenvolvimento de um tipo especial de pensamento – pensamento algébrico – que é essencial para utilizar modelos matemáticos na compreensão, representação e análise de relações quantitativas de grandezas e, também, de situações e estruturas matemáticas, fazendo uso de letras e outros símbolos. Para esse desenvolvimento, é necessário que os alunos identifiquem regularidades e padrões de sequências numéricas e não numéricas, estabeleçam leis matemáticas que expressem a relação de interdependência entre grandezas em diferentes contextos, bem como criar, interpretar e transitar entre as diversas representações gráficas e simbólicas, para resolver problemas por meio de equações e inequações, com compreensão dos procedimentos utilizados. As ideias matemáticas fundamentais vinculadas a essa unidade são: equivalência, variação, interdependência e proporcionalidade. Em síntese, essa unidade temática deve enfatizar o desenvolvimento de uma linguagem, o estabelecimento de generalizações, a análise da interdependência de grandezas e a resolução de problemas por meio de equações ou inequações. BRASIL (2017, p. 270).

A contribuição de Diofanto deve ter chegado à muitas pessoas que vislumbraram um modo diferente de tratá-la, nessas influências está o advogado francês Pierre de Fermat. Este, dedicava as suas horas de lazer ao estudo da matemática, mas, pouco publicou a respeito. Contudo, manteve correspondência com os principais matemáticos de sua época, exercendo dessa forma vasta influência na área, sendo assim considerado o maior matemático francês do século XVII.

Conforme EVES (2004, p. 390) dentre as variadas contribuições de Fermat à matemática, a mais importante é a fundação da moderna teoria dos números. E em se tratando da Teoria dos números, Fermat foi um monstro e um dos inspiradores destes trabalhos diversos no campo da álgebra.

Como se constata em MOL (2013, p. 97), dentre outros interesses no campo da aritmética estavam os números primos, a propriedades de divisibilidade e várias outras situações muito

importantes, porém, apesar das imensas contribuições deixadas por Fermat, não houve assim uma obra efetivada; seus escritos e descobertas estavam de modo bem informal apesar de bem claras, juntadas de seus amigos ou colaboradores. Dentre as várias descobertas atribuídas a Fermat destacamos conforme Mol, o pequeno Teorema de Fermat que afirma que:

> Se p é primo e a é um número não divisível por p o número a^{p-1} é divisível por p(...) O último Teorema de Fermat: Para $n > 2$, não existem números inteiros positivos x,y e z satisfazendo a identidade $x^n + y^n = z^n$. MOL (2013, p. 97-98).

Os Teoremas acima enunciados foram demonstrados pelos seus seguidores e de acordo com EVES (2004, p. 392) "o último teorema de Fermat ganhou a distinção de ser o problema matemático com maior número de demonstrações incorretas publicadas".

Eis aqui algumas contribuições de Fermat no ensino atual: Construir algoritmo em linguagem natural e representá-lo por fluxograma que indique a resolução de um problema simples (por exemplo, se um número natural qualquer é par). Classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos "é múltiplo de", "é divisor de", "é fator de", e estabelecer, por meio de investigações, critérios de divisibilidade por 2,3,4,5,6,8,9,10,100 e 1000. Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor. BRASIL (2017, p. 301).

Observamos ainda nos Parâmetros Curriculares Nacionais - PCN'S, conceitos como os de "múltiplo" e "divisor" de um número natural ou o conceito de "número primo" podem ser abordados neste ciclo como tópicos práticos que permitem ao aluno encontrar, mecanicamente, o mínimo múltiplo comum e máximo divisor comum sem compreender as situações-problema que esses conceitos permitem resolver. Os números inteiros podem surgir como uma ampliação do campo aditivo, pela análise de diferentes situações em que esses números estejam presentes. Eles podem representar diferença, "falta", orientação e posições relativas. As primeiras abordagens dos inteiros podem apoiar-se nas ideias intuitivas que os alunos já têm sobre esses números por vivenciarem situações de perdas e ganhos num jogo, débitos e créditos bancários ou outras situações. BRASIL (1998, p. 66).

Deve-se ao teólogo e matemático suíço Leonhard Euler a prova do Pequeno Teorema de Fermat e contribuição na demonstração do último Teorema de Fermat. Euler é considerado um dos grandes gênios responsáveis pela matemática da atualidade.

No considerado pensamento de MOL (2013, p. 118) Leonard Euler foi um dos, senão o mais ilustre e produtivo matemático de seu tempo, e porque não dizer de toda sua era. Publicou diversos livros e artigos totalizando 866 trabalhos. Não existe na matemática qualquer ramo que não tenha contribuição de Euler. No entanto, em toda sua vida Euler não ocupou cargo de professor. Morreu subitamente aos 76 anos totalmente cego, deficiência esta que não o fez parar de produzir.

Parece ser uma convicção que ao perder um sentido, há de forma natural o aprimoramento dos outros, pois, com a perda da visão, Euler conseguiu manter uma extraordinária atividade produtiva matemática. Ajudado por uma memória fenomenal e por um poder de concentração incomum e imperturbável, Euler continuou seu trabalho criativo com a ajuda de um secretário que anotava suas ideias, expressas verbalmente ou escritas com giz numa lousa grande. EVES (2004, p. 472).

Algumas notações usadas atualmente na álgebra, geometria e análise devem a Euler, e conforme a BNCC, analisar funções definidas por uma ou mais sentenças (tabela do Imposto de Renda, contas de um modo geral), são representadas pela álgebra, encontram um significado simbólico, gráfico, na álgebra de Euler, sobretudo em representações de crescimento e decrescimento e hoje principalmente nas tecnologias digitais, segundo percebemos em, BRASIL (2017, p. 539).

Destacamos ainda nos Parâmetros Curriculares nacionais do Ensino Médio - PCNEM, que ler e interpretar textos de Matemática. Ler, interpretar e utilizar representações matemáticas (tabelas, gráficos, expressões etc). Transcrever mensagens matemáticas da linguagem corrente para linguagem simbólica (equações, gráficos, diagramas, fórmulas, tabelas etc.) e vice-versa. Exprimir-se com correção e clareza, tanto na língua materna, como na linguagem matemática, usando a terminologia correta. Produzir textos matemáticos adequados. BRASIL (2000, p. 46).

Ainda sobre fenomenais nomes que tanto contribuíram para o surgimento, desenvolvimento e aprimoramento da matemática ao longo do tempo, citamos o matemático Carl Friedrich Gauss (1777−1855), que desde cedo demonstrou sua tendência para a matemática, Carl foi uma das mais

notáveis crianças-prodígio, dessas que aparecem de raro em raro. Diz-se que com a idade de três anos detectou um erro aritmético no borrador de seu pai. Há uma história segundo o qual o professor de Carl na escola pública, quando ele tinha dez anos de idade, um professor teria passado à classe, para mantê-la ocupada, a tarefa de somar os números de 1 a 100. Quase que imediatamente Carl colocou sua lousa sobre a escrivaninha do irritado professor. Quando as lousas foram finalmente viradas, o professor surpreso verificou que Carl tinha sido o único a acertar a resposta, 5050, mas sem fazê-la acompanhar de nenhum cálculo. Carl havia mentalmente calculado a soma da progressão aritmética $1+2+\cdots+100$ observando que $100+1 = 101, 99+2 = 101, 98+3 = 101$ e assim por diante com os cinquenta pares possíveis dessa maneira, sendo a soma portanto $50\times101 = 5050$. Mais tarde, quando adulto, Gauss costumava jactar-se de ter aprendido a contar antes de aprender a falar. EVES (2004, p. 519).

Apesar de tamanha inteligência matemática, Gauss chegou a questionar se tornaria um filósofo ou um matemático, e a queda pela matemática prevaleceu, tornando um dos grandes nomes da área, ficando mais tarde conhecido como “o Príncipe dos Matemáticos”.

Conforme EVES (2004, p. 521), “É famosa a afirmação de Gauss de que a matemática é a rainha das ciências, e a teoria dos números é a rainha da matemática. Já se descreveu Gauss como o gigante matemático que do alto de sua magnitude abarca num relance as estrelas e os abismos”.

Gauss aos vinte e três anos de idade, na sua tese de doutorado apresentou a demonstração do Teorema Fundamental da Álgebra, a saber: “todo polinômio não constante com coeficientes complexos possui pelo menos uma raiz complexa”, sendo que ele apresentou durante toda sua vida quatro demonstrações desse Teorema. Gauss possuía um diário matemático no qual anotava todas as suas descobertas, e, como era muito perfeccionista, só divulgava suas teorias quando estas estivesse totalmente acabadas; Gauss adotou como lema segundo EVES (2004, p. 521): “Pouca sed matura (Poucos, porém maduros)”.

E, diante deste paradigma, muitas obras ficaram por publicar, dentre os quais destacamos a geometria não-euclidiana, tornando dessa forma um dos “inventores” desta geometria. Para Gauss a matemática deveria abarcar o mundo real. Dentre as várias obras publicadas por Gauss, destacamos a Disquisitiones, arithmeticae (Investigações aritméticas), considerada o marco inicial da teoria dos números atual. Quão grande sua importância, esta obra tornou-se um clássico da literatura matemática. Essa obra célebre é a principal responsável pelo desenvolvimento da

linguagem e notação do ramo da teoria dos números conhecido como álgebra das congruências que fornece um exemplo de classes de equivalência. A exposição começa com a definição: Se um número a divide a diferença entre dois números b e c, então b e c dizem-se congruentes, de outra forma incongruentes; e a chama-se o módulo. Qualquer dos números diz-se um resíduo do outro, no primeiro caso, um não-resíduo no segundo caso. A notação que Gauss adotou foi a que se usa hoje $b \equiv c \bmod a$. (...) Nas Disquisitiones Gauss inclui o Teorema Fundamental de Aritmética.(...) Uma das contribuições de Disquisitiones foi uma prova rigorosa do teorema, conhecido desde os dias de Euclides, que diz que todo inteiro positivo pode ser representado de uma e só uma maneira (exceto pela ordem dos fatores)como produto de primos. BOYER (1996, p. 371-372).

Ainda abordando sobre contribuições de pensadores e pesquisadores que trouxeram contribuições às construções matemáticas e que hoje usufruímos em diversos setores do mundo globalizado em que vivemos para melhor nos estabelecermos nas relações, como bem destacado em RESENDE (2007, p.70-72)

> "Muitos dos problemas da Teoria dos Números foram tratados por Euclides nosElementos, em três dos treze livros. Os livros VII, VIII e IX, que têm no total cento e duas proposições, tratam do que poderia ser chamado de teoria elementar dos números. Neles encontram-se: a definição de número primo, o algoritmo, hoje denominado euclidiano que é um método para determinar o máximo divisor comum entre dois números, o estudo denúmeros perfeitos, a demonstração de que há infinitos números primos, feita por absurdo e que ainda hoje é encontrada nos livros." RESENDE (2007, p.70-72)

Outro matemático grego que deu contribuição significativa para a Teoria dos Números, foi Diofanto de Alexandria. Acredita-se que ele tenha vivido no século III de nossa era, teve uma importância enorme para o desenvolvimento da Álgebra e uma grande influência sobre os matemáticos que se dedicaram mais tarde à Teoria dos Números. Diofanto escreveu três trabalhos, sendo um deles Arithmetica, uma obra diferente das anteriormente publicadas, pois era um tratado caracterizado por um alto grau de habilidades matemáticas. É uma abordagem da teoria algébrica dos números. Contém 130 problemas que levam as equações de primeiro e segundo graus e uma cúbica. Não há métodos gerais, mas resoluções engenhosas para problemas específicos.

Inclusive, Diofanto só admitia respostas que fossem números racionais positivos, e satisfazia-se com, apenas, uma resposta do problema. Há, em sua obra, enunciados que mereceram

a atenção de matemáticos, como Viète, Fermat, Lagrange e Euler. Os problemas algébricos indeterminados em que se devem achar soluções inteiras tornaram-se conhecidos como equações diofantinas. Porém, Diofanto não foi o primeiro a se preocupar com estes problemas, mas talvez tenha sido o primeiro a dar uma notação algébrica. Ele tinha notações para a incógnita, para potências da incógnita até a de expoente seis, para a subtração, para igualdade e para inversos. Foi um passo importante para avançar da álgebra retórica para a álgebra sincopada. Por isso é considerado o fundador da álgebra.

Embora a matemática continuasse a ser estudada em outras civilizações, nos séculos seguintes ao III d.C, somente a partir do século XVII, a Teoria dos Números ganhou novo impulso, em especial, com as contribuições de grandes nomes da matemática, como os de Fermat, Euler, Lagrange e Gauss.

Pierre Fermat (1601-1665), magistrado francês, não era matemático por profissão, noentanto marcou o despertar da Teoria dos Números, pois, após Diofanto, que havia trabalhadosobre os números racionais, foi o primeiro a se restringir ao domínio dos números inteiros, o que para ele constituía o que é próprio da aritmética. Tendo entrado em contato com uma tradução da obra Arithmetica de Diofanto, leu o texto, anotando nas margens as ideias que lhe ocorriam. Deste modo e também através de correspondências com outros matemáticos, Fermat enunciou muitos teoremas ligados à Teoria dos Números, contribuindo também em outras áreas da matemática. Investigou números perfeitos e amigáveis, números figurados, quadrados mágicos e, sobretudo, os números primos. A sua famosa conjectura: Não existem inteiros positivos x, y, z, n de modo que $x^n + y^n = z^n$, com n>2, conhecida como o Último Teorema de Fermat, desafiou matemáticos durante mais de três séculos, embora Fermat afirmasse que tinha uma demonstração para ela, mas a margem do papel era muito estreita para contê-la. A busca da prova para essa conjectura suscitou muitos conhecimentos novos em matemática (por exemplo, a teoria dos ideais), tendo sido provada e publicada em 1995, por A. Wiles com a colaboração de R. Taylor.

Leonhard Euler (1707-1783), matemático suíço, altamente produtivo, também muito contribuiu para a Teoria dos Números, a partir do trabalho de Fermat, provando muitas das conjecturas por ele estabelecidas. Provou, por exemplo, o pequeno teorema de Fermat: Para todo número primo p e todo número a não divisível por p, tem-se $a^{p-1} \equiv 1 (\text{mod } p)$. Demonstrou também

que todo número primo da forma 4n + 1 é a soma de dois quadrados; fez uma teoria dos divisores das expressões $a^n + b^n$ e demonstrou o teorema de Fermat para n = 3e n = 4.

Joseph Lagrange (1736-1813), nascido em Turim, na Itália, grande matemático, deu contribuições importantes também à Teoria dos Números, provando que a equação Pell- Fermat, $x^2 – Dy^2 = 1$, tem infinitas soluções. Provou ainda que todo número inteiro positivo é a soma de, no máximo, quatro quadrados perfeitos, chamado o teorema de Lagrange dos quatro quadrados. Escreveu um livro sobre a Teoria dos Números em 1798.

Foi Carl Friedrich Gauss (1777-1855), um dos matemáticos mais produtivos de todos os tempos, chamado o “Príncipe dos Matemáticos”, em sua já citada e fantástica obra que a moderna Teoria dos Números se desenvolveu, especificamente falando se da álgebra da relação de congruência.

Segundo Dahan-Dalmedico & Peiffer (1987), com essa obra a Teoria dos Números deixou de ser um conjunto de resultados isolados, produto de intuições edescobertas geniais, para se transformar em uma nova disciplina, dotada de métodos próprios, mais profundos, fonte e modelo para as teorias aritméticas do século XIX. Em 1825, Gauss introduziu os números inteiros gaussianos, uma extensão da ideia de número inteiro, pois descobriu que muito da antiga teoria de Euclides sobre fatoração de inteiros poderia ser transportada para esse conjunto com consequências importantes para a Teoria dos Números (MENOCHI, 2006, p.1). Gauss afirmou: “a matemática é a rainha das ciências, e a teoria dos números é a rainha da matemática”, o que demonstra a sua preferência e apreciação desse campo.

A Teoria dos Números continuou a se desenvolver nos séculos XIX e XX com vários resultados importantes, ligados ao desenvolvimento de outros campos da matemática. No século XX, a prova do Último Teorema de Fermat, segundo Singh (2005), foi um marco paraa Teoria dos Números, pois ligou as conquistas do campo desse século, incorporando-as em uma poderosa demonstração. Ele criou técnicas matemáticas completamente novas e as combinou com técnicas tradicionais de um modo que nunca fora considerado possível. (...) a prova é a síntese perfeita da matemática moderna e uma inspiração para o futuro. (SINGH,2005, p. 282)

Percebam que essas considerações nos mostram que a Teoria dos Números tem raízes longínquas, com características bem enraizadas e ligadas aos mais remotos pensadores e

contribuidores como Tales e Pitágoras e de várias outras brilhantes mentes citadas; mas que é ainda um campo novo, enquanto conhecimento sistematizado, em pleno desenvolvimento, com contribuições importantes para a matemática, ainda que muitos dos procedimentos exijam um conhecimento avançado de teorias, tecnologias e técnicas, como é o caso da demonstração do Último Teorema de Fermat por exemplo, mas, encontramos brilhantes conexões com outros ramos da própria matemática.

3 ALGUNS TÓPICOS IMPORTANTES DA TEORIA DOS NÚMEROS QUE DÃO SUPORTE À RESOLUÇÃO DE PROBLEMAS

Após termos percebido a evolução e importância da teoria dos números no capítulo anterior, nesse capítulo iremos explorar conceitos como divisibilidade e suas propriedades, Divisão Euclidiana, Números primos, Pequeno Teorema de Fermat e para finalizar, trataremos das Equações Diofantinas Lineares; entendendo que tal exposição é de extrema importância como apresentação de caminhos e pré-requisitos que darão amparo à resolução de problemas aos quais são o principal elemento da motivação à que propomos neste trabalho.

Some-se à contribuição que os tópicos podem trazer, uma ainda mais importante deve e é mostrar uma postura de iniciar o despertar da mente para leitura, entendimento e consequente resolução dos problemas que serão enfrentados pelos estudantes não só em conteúdo específico aqui proposto, mas em qualquer situação que o desafiado esteja na busca de solução, mesmo considerando outras ciências e disciplinas; não é à toa, a clareza com que observamos estudantes que participam de olimpíadas de matemática por exemplo e que praticam bem a ciência, de um modo geral serem também grandes alunos(as) em qualquer outra área do conhecimento proposta no ambiente escolar. Isso não pode ser coincidência, sem dúvida é a "herança" didática adquirida quando estes realizam uma boa convivência com conteúdos lógicos matemáticos e quando faz uso de bons operadores básicos.

3.1 Divisibilidade

A base fundamental para o trabalho aqui proposto é resultante da operação básica de divisão; observando que seus componentes e sua operacionalização são as ações necessárias e que fazem parte de um pré-requisito importante e decisivo para a sequência do estudo da Teoria dos Números, sobretudo no que diz respeito à Congruência Modular. Então, examinemos com cuidado cada situação apresentada a seguir:

Considerando o conjunto Z = {..., −4, −3, −2, −1, 0, 1, 2, 3, 4, ...}, encontramos a definição a seguir:

Definição : Considerando dois números inteiros $a \in Z$ e $b \in Z$, com $a \neq 0$, pois, não existe a divisão por 0; diz-se que a divide b , $(a \mid b)$ quando existir um número inteiro k, tal que $b = a \cdot k$, $k \in Z$. Neste caso, podemos dizer que são válidas as afirmações:

1ª) a é um divisor de *b* ou dizemos que a divide *b,* simbolizado por $(a \mid b)$;

2ª) a é considerado um fator de *b, ou seja, é um elemento da multiplicação*;

3ª) b é um múltiplo de *a*, pois, b é resultante do produto de a por um número inteiro k;

Proposição 3.1: Considere os números naturais a, b, c e $d \in Z$, com $a \neq 0$. Temos:

- $1 \mid a$; qualquer que seja a;
- $a \mid a$; pois, essa divisão resulta em exatamente 1;
- $a \mid 0$; pois, 0 dividido por um número qualquer, resulta em 0;
- Se $a \mid b$ e $b \mid c$, então $a \mid c$; assim, estamos diante da propriedade reflexiva;
- Sejam a, b, c e d, números naturais, com $a \neq 0$ e $c \neq 0$ então , se $a \mid b$ e $c \mid d$, então $(ac) \mid (bd)$;
- Se $a \mid b$ e $a \mid c$, então $a \mid b \pm c$;
- Se $a \mid b$, então $a \mid bc$;
- Se $a \mid b$ e $a \mid c$, então $a \mid m \cdot b + n \cdot c$, quaisquer $m, n \in Z$.

● Sejam a e b números naturais, ambos $\neq 0$, tem-se que se $a \mid b$, então $a \leq b$

● Se $b \mid a$ e $a \ddagger 0$ então $|b| \leq |a|$. (Todo divisor de $a \leq |a|$) ;

● Se $b \mid a$ e $a \mid b$, então $a = \pm b$;

● Se $b \mid 1$, então $b = \pm 1$;

● $a \mid b \Leftrightarrow -a \mid b \Leftrightarrow a \mid -b \Leftrightarrow -a \mid -b$

Demonstração :

(1) De fato, $1 \mid a$ pois $a = a.1$ para todo inteiro a.

(2) De fato, $a \mid a$ pois $a = 1.a$ (Propriedade reflexiva). De fato, $a \mid 0$ pois $0 = a.0$

(3) Se a *é* divisor de b então, existe um número natural k, tal que $b = ak$.

(4) Da mesma forma, se b *é* divisor de c então, $\exists$ um natural q, tal que $c=b.q$, Logo:

$c = b \cdot q \Rightarrow c = a \cdot k \cdot q \Rightarrow c = a \cdot (kq)$. Ou seja, a *é* divisor de c.

(5) Se a divide b, então $\exists$ um número natural k, tal que $b = ak$.

Da mesma forma, se c divide d, então $\exists$ um número natural q, tal que

Temos que: $d= cq.bd = (ak) \cdot (cq) = (ac) \cdot (kq)$.

Ou seja, $(a \cdot c)$ é um fator de $(b \cdot d)$, demonstrando a proposição.

(6) Se $a \mid b$ e $a \mid c$ então $\exists\ q_1$ e q_2 inteiros tais que: $b = a \cdot q_1$ e $c = a \cdot q_2$.

Somando as duas equações temos:

$b + c = a\ (q_1 + q_2)$.

Portanto $a \mid b + c$.

Observação: Para a subtração, demonstra-se de maneira análoga.

(7) Se ab então $\exists$ um número inteiro q tal que, $b = aq$.

Multiplicando a equação por um inteiro c temos que, $bc = a \cdot (qc)$. Portanto se $a \mid b$ e $a \mid c$ temos pelo item anterior que $a \mid bm$ e $a \mid cn$ para quaisquer inteiros m e n.

Logo, pelo item (6) segue que $a \mid bm + cn$

(8) $a \mid b \Rightarrow b = aq;\ q \in Z$,

$b = (-a).\ (-q);\ -q \in Z$,

$-b = a:(-q);\ q \in Z$,

$-q \in Z \Rightarrow -b = (-a).\ q;\ -q \in Z$

$-b = (-a).\ q;\ q \in Z$

(9) Se $a \mid b$ com $b \neq 0$; então $\exists$ um inteiro $q \neq 0$ tal que $b = aq$.

Logo: $|b| = |aq| = |b| \ .\ |q| > |a|$

Portanto, $|a| \leq |b|$

(10) Suponhamos que $a \mid b$ e que $b \mid a$. Se $a = 0$ ou $b = 0$, temos que $a = b = 0$.

No caso $a;\ b \neq 0$ temos pelo item (9) que $|a| \leq |b|$ e $|b| \leq |a|$.

Logo, $|a| = |b|$, $\Rightarrow$ que $a = b$ ou $a = -b$

(11) Suponhamos que $a \mid 1$. Do item (i) temos que $1 \mid a$ para todo inteiro a.

Logo pelo item anterior segue que $a = 1$ ou $a = -1$

A noção, definição, proposição e demonstração contidas no tópico, foram encontradas em (HEFEZ, 2013).

3.2 Divisão Euclidiana

Na aritmética, a o método proposto por Euclides de Alexandria (Também conhecida como divisão com resto) é o processo de dividir um inteiro (o dividendo) por outro (o divisor), de forma que produza um quociente e um resto menor que o divisor.

Uma propriedade fundamental é que o quociente e o resto existem e são únicos, sob algumas condições. Por causa dessa singularidade, a divisão euclidiana é frequentemente considerada sem referência a nenhum método de cálculo e sem calcular explicitamente o quociente e o resto.

A divisão euclidiana e os algoritmos para calculá-la são fundamentais para muitas questões relativas a inteiros, como o algoritmo euclidiano para encontrar o maior divisor comum de dois inteiros, e aritmética modular, para a qual apenas restos são considerados. A operação que consiste em calcular apenas o resto é chamada de *operação módulo*, e é frequentemente usadaem matemática e na ciência da computação.

O Teorema da Divisão então pode ser facilmente entendido: dados dois inteiros a e b, com $b \neq 0$, existem inteiros únicos q e r tais que $a=bq + r$, e $0 \leq r < |b|$, onde b denota -se como o valor absoluto de b.

No teorema acima, cada um dos quatro inteiros tem um nome próprio: a é chamado de *dividendo*, b é chamado de *divisor*, q é chamado de *quociente* e r é chamado de *resto*.

O cálculo do quociente e do resto do dividendo e do divisor é chamado de *divisão* ou em caso de ambiguidade , *divisão euclidiana*. O teorema é frequentemente referido como algoritmo de divisão (embora seja um teorema e não um algoritmo), porque sua demonstração, conforme fornecida a seguir, se presta a um algoritmo de divisão simples para calcular q e r e , a divisão não é definida no caso em que b = 0;

Para o resto e a operação módulo, existem convenções diferentes de $0 \leq r < |b|$

Demonstração:

Considere primeiro o caso $b < 0$. Definindo $b_1 = - b$ e $q_1 = - q$, a equação $a = bq + r$ pode ser reescrita como $a = b_1q_1 + r_1$ e a desigualdade $0 \leq r < |b|$ pode ser reescrita como $0 \leq r_1 < |b|$,

Isso reduz a existência do caso $b < 0$ àquela do caso $b > 0$.

[1] https://pt.wikipedia.org/wiki/Divis%C3%A3o_euclidiana , acesso em: 06.05.2023.

Da mesma forma, se $a < 0$ e $b > 0$ definindo , $a_1 = -a$ e , $q_1 = -q - 1$ e $r_1 = b - r$ a equação $a = bq + r$ pode ser reescrita como $a_1 = bq_1 + r_1$, e a desigualdade $0 \leq r < |b|$ pode ser reescrito como $0 \leq r_1 < |b|$.

Assim, a prova da existência fica reduzida ao caso $a \geq 0$ e $b > 0$. Que será considerado no restante da prova.

Sejam $q_1 = 0$ e $r_1 = a$, então esses são números não negativos tais que $a_1 = bq_1 + r_1$. Se $r_1 < b$, então a divisão está completa, então suponha que $r_1 \geq b$. Então, definindo $q_2 = q_1 + 1$ e $r_2 = r_1 - b$, temos $a = bq_2 + r_2$, com $0 \leq r_2 < r_1$.

Como existem apenas r_1 inteiros não negativos menores que r_1, basta repetir este processo no máximo r_1 vezes para atingir o quociente final e o resto. Ou seja, existe um número natural $k \leq r_1$ tal que $a = bq_k + r_k$.

Isso prova a existência e também fornece um algoritmo de divisão simples para calcular o quociente e o restante. Porém, este algoritmo não é eficiente, pois seu número de passos é da ordem de a/b.

3.3 Máximo Divisor Comum

A definição de MDC é muito simples, principalmente se partirmos do conceito de divisores de um número inteiro qualquer, explicitar seus divisores um a um e, mostrar os números que coincidem em ambos os conjuntos escritos; óbvio que a reflexão seguinte seria: Mas como estabelecer o conjunto de divisores comuns à dois números caso esses sejam excessivamente grandes? Daí, certamente viria a reflexão sobre a necessidade da busca de algo mais prático que apontasse o resultado sem necessariamente termos que escrever todos os divisores de cada número.

Pensando no Ensino Médio e nas avaliações externas enfrentadas pelos alunos, sabemos que o fator tempo é um inimigo forte.

Então, veremos o exemplo abaixo, para relembrarmos o conceito de MDC e, em seguida, a apresentação de algo que torne bem prático tal procedimento:

Consideraremos os números 20 e 45 como exemplo; vejamos:

Indicando por $D_{(20)}$ os divisores de 20 e $D_{(45)}$ os divisores de 45; a seguir, faremos uma listagem de tais divisores e, assim visualizaremos com um grau maior de facilidade a definição em seguida:

$$D_{(20)}=\{1,\ 2,\ 4,\ 5,\ 10,\ 20\}$$

$$D_{(45)}=\{1,\ 3,\ 5,\ 9,\ 15,\ 45\}$$

Da listagem acima, segue que a intersecção entre os dois conjuntos elencados acima é: $D_{(20)} \cap D_{(45)} = \{1,\ 5\}$, sendo que M x $D_{(20)} \cap D_{(45)} = 5$, ou seja, 5 o maior número pertencente ao conjunto interseção de $D_{(20)}$ e $D_{(45)}$.

A seguir, apresentaremos definição, lema, proposição e demonstração, todos relacionados ao tema ; encontrados em (HEFEZ , 2013, apud FRANCO, 2016, p. 17 à p. 20)

Definição : Dados $a, b \in Z$, ambos não nulos, dizemos que $d \in Z^*$ e é divisor comum de a e b se $d|a$ e $d|b$.

Exemplo 3.1: Tem-se que 3 divisor comum de 90 e 45 pois $3 \mid 90$ e $3 \mid 45$.

Definição : Dados $a, b \in Z$, ambos não nulos, dizemos que $d \in Z^*$, Máximo Divisor Comumde a e b, quando d cumpre duas condições:

$d \mid a$;

$d \mid b$.

1ª) Se $e \in Z$, tal que $e \mid a$ e $e \mid b$, então $e \mid d$, ou seja, d o maior divisor comumde a e b.

A definição pode ser estendida para uma quantidade infinita de n inteiros $a_1, a_2, a_3, ..., a_n$ e esta ser denotada simplesmente por $mdc\ (a_1, a_2, a_3, ..., a_n)$.

Lema : Dados $a, b, q, r \in Z$ tais que, $a = bq + r$, então $mdc(a, b) = mdc(b, r)$.

Demonstração :

Considere $a, b \in Z$. Notemos que caso, $a \mid b$ ou $a = 1$, temos $mdc(a, b) = |a|$.Assim podemos supor que $1 < a < b$ e que a não divide b.

Assim sendo, como consequência do já relatado algoritmo da divisão, $\exists\, q_1, r_1$, de modo que:

$b = aq_1 + r_1$, com $0 < r_1 < a$

Da surgem duas possibilidades:

1ª) Se $r_1 \mid a$, então usando o lema 1 temos que:

Se $r_1 = mdc\,(a, r_1) = mdc\,(a, b - q_1a)$, $r_1 = mdc\,(a, b)$

2ª) $r_1 \neq a$, aplicando o Algoritmo de Euclides em a e r_1 , desta maneira $\exists$ inteiros q_2 e r_2, tais que:

$a = r_1q_2 + r_2$, com $0 < r_2 < r_1 < a$.

O que também nos dá duas possibilidades:

$r_2 \mid r_1 \Rightarrow r_2 = mdc\,(r_1, r_2) = mdc\,(r_1, a - q_2r_1) = mdc\,(r_1, a) = mdc\,(b - q_1a, a) = mdc(a, b)$.

Se $r_2 \neq r_1$.

Aplicando novamente o Algortimo de Euclides, vimos que $\exists$ inteiros q_3 e r_3, tais que:

$r_1 = r_2q_3 + r_3$, $0 < r_3 < r_2 < r_1 < a$.

Com este procedimento no infinito, a sequência $a > r_1 > r_2 > r_3...$, possui um menor elemento.

Portanto, para algum n teremos que $r_n \mid r_n = 1$, pois em algum momento teremos que o resto igual a zero, implicando em $mdc(a, b) = r_n$.

Para provar a unicidade suponhamos que $mdc(a, b) = d$ e $mdc(a, b) = d_0$.

Notemos que tanto d, quanto d_0 s os divisores comuns de a e b, assim $d|d_0$ e

$d_0|d$, e como d e d_0 são ambos positivos segue que $d = d_0 = mdc(a, b)$.

Proposição 3.2: Sejam os números inteiros a, b, c, d, d_0 com d e d_0 positivos. Se $d = Mdc\,(a, b)$ e $d_0 = mdc\,(a, b, c)$, então $d_0 = mdc\,(mdc\,(a, b), c) = mdc\,(d, c)$.

Demonstração :

Sabendo d_0 é igual ao $mdc\,(a, b, c)$ e d_1 é igual ao $mdc\,(d, c)$, com d igual ao $mdc\,(a, b)$, temos que $d_0 \mid d_1$ e $d_1 \mid d_0$.

Daí, como d_0 e d_1 são positivos por definição, então, $d_0 = d_1$

De $d_0 = mdc\,(a, b, c)$, segue por definição que $d_0 \mid a$ e $d_0 \mid b$, e como $d = mdc\,(a, b)$ então $d_0 \mid d$, e pelo fato de $d_0 \mid c$, segue que $d_0 \mid d_1$, pois $d_1 = mdc\,(d, c)$.

Por outro lado, $d_1 = mdc\,(d, c)$ por definição, $d_1 \mid d$ e $d_1 \mid c$.

Agora como $d = mdc\,(a, b)$, por definição o $d \mid a$ e $d \mid b$, da segue que $d_1 \mid a$ e $d_1 \mid b$,mas $d_1 \mid c$, logo $d_1 \mid d_0$, pois $d_0 = mdc\,(a, b, c)$.

Donde concluímos que $d_1 = d_0$.

Proposição 3.3:

Dados a, b ∈ Z e d sendo o resultado do mdc (a, b), então as

seguintes afirmações são verdadeiras:

1ª) Se $a = 0$ e $b = 0$, então $d = |b|$, j que $d \in Z^*$;

2ª) Se $d = mdc\,(a, b)$, então $d = mdc\,(-a, b) = mdc\,(a, -b) = mdc(-a, -b)$.

Demonstração :

I. Se $a = 0$ e $b = 0$, teremos que existe $d \in Z$; $d = mdc\,(0, 0) \Rightarrow d = 0$

II. Dados $a, b \in Z$, ambos não nulos. Temos que o maior divisor de a e $-a$ $|a|$. Dessa forma, $mdc\,(a, b) = mdc\,(-a, b)$ e analogamente

III. $mdc\,(a, -b) = mdc\,(-a, -b) = mdc\,(a, b)$.

Esses resultados apresentam uma maneira recursiva de se utilizar o Algoritmo Euclidiano, sendo que de acordo com Hefez (2013, apud FRANCO, 2016, p.16 à 19) houveram apenas aperfeiçoamentos do processo apresentado pelo próprio Euclides em Os Elementos que é o mais utilizado nos dias atuais. Ele consiste em dividir o maior número pelo menor e no processo seguinte fazer o mesmo utilizando o quociente e o resto da divisão o anterior tal que o resto não seja zero, assim, o máximo

divisor comum ser o menor resto, diferente de zero. Este tópico é muito importante dentro do contexto da Teoria dos Números. Veja o exemplo a seguir.

Exemplo 3.2: Determine o m d c (680, 150):

Solução: $680 = 150 \cdot 4 + 80$

$$150 = 80 \cdot 1 + 70$$
$$80 = 70 \cdot 1 + 10$$
$$70 = 10 \cdot 7$$

Verificamos que o resto zero aparece quando dividimos 70 por 10, assim o menor resto diferente de zero é o Máximo divisor comum entre 680 e 150. Portanto, o *mdc* (680, 150) é 10.

Teorema 3.1: (Relação de Bezout) Dados os inteiros a e b, quaisquer, mas não ambos nulos,existem dois inteiros n e m tais que $mdc\,(a, b) = a \cdot n + b \cdot m$.

Em outras palavras, a relação diz que o *mdc* (*a, b*) pode ser escrito como combinação linear de a e b.

Demonstração :

Consideremos o conjunto de todos os números positivos da forma $a \cdot n + b \cdot m$, onde o m e o n podem variar ao longo dos inteiros. Óbvio que esse conjunto contém alguns elementos, mesmo que a e b sejamnegativos, porque se pusermos $m = a$ e $n = b$ temos que $a^2 + b^2$ um número positivo e por isso pertence a esse conjunto.

Obviamente *mdc* (*a, b*) divide todos os elementos desse conjunto. Seja d o menor desses números. Usando o Algoritmo de Euclides, existem q e r, inteiros tais que:

$$a = qd + r.$$

Mas $d = am + bn$, logo:

$$r = qd - a = q(am + nb) - a = (qm - 1)a + nb.$$

Portanto r pertence ao conjunto. Uma vez que d é o menor elemento do conjunto, obtemos que $r = 0$.

Assim: $d \mid a$.

Realizando o mesmo procedimento e desenvolvendo o mesmo raciocínio, demonstraríamos que $d \mid b$.

Se houvesse algum número c maior que d tal que $c \mid a$ e $c \mid b$, então $c \mid d$, o que entra em contradição com $c > d$. Assim d é o $mdc(a, b)$ e portanto $mdc(a, b)$ pode ser escrito da forma $am + bn$.

Exemplo 3.3: Aplicar o teorema de Bézout para os inteiros $a = 41$ e $b = 12$.

Solução:

Fazendo as divisões temos que:

$41 = 12.3 + 5 \Rightarrow 5 = 41\ 12.3$

$12 = 5.2 + 2 \Rightarrow 2 = 12\ \ 5.2$

$5 = 2.2 + 1 \Rightarrow 1 = 5\ \ 2.2$

Substituindo as equações, temos que:

$5\ 2.2 = 1 \Rightarrow 5\ 2.(12 - 5.2) = 1.$

Assim, percebemos que o Teorema de Bézout auxilia na busca do Máximo Divisor Comum (MDC) e que este é um tópico bem ligado à divisão mostrando como esta pode ser útil na manipulação numérica para descoberta de uma solução em problemas, sobretudo ligados à Teoria dos Números.

3.4 Números Primos

Os números primos possuem um papel fundamental na matemática e facilitam o entendimento e resolução de inúmeros problemas que vêm sendo resolvidos ao longo de várias gerações matemáticas. Esses números são os próprios átomos da aritmética. São os números indivisíveis que não podem ser representados pela multiplicação de dois números menores. A importância matemática dos primos se deve à sua capacidade de gerar todos os demais números (SAUTOY, 2007).

Apresentaremos a seguir, definições e teoremas relevantes para o entendimento deste conceito, pois, serão fundamentais para a boa absorção das aplicações a serem apresentadas e para alguns critérios de divisibilidade.

Definição : Um número natural maior que 1 que só possui como divisores positivos o 1 e ele mesmo é chamado de número primo.

Sejam a, p e q números inteiros, p e q primos e q n o nulo, da definição acima decorre que:

(1) Se $p \mid q$, então , $p = q$;

(2) Se *p não divide a*, então, $mdc\ (p, a) = 1$.

Exemplo 1: Seja p=3 e q primo, se $p \mid q$ temos que $q = 3$. Por outro lado, sendo p =3 e a = 5temos que $3 \neq 5$, logo $mdc\ (3, 5) = 1$.

Definição : Diz-se que dois números a e b são primos entre si se $mdc\ (a, b) = 1$. Um número maior que 1 e que não primo ser dito número composto.

Proposição 3.4: Seja n $a, b, p \in Z$, com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$

Demonstração:

Basta provar que, se $p \mid ab$ e $p \neq a$, então $p \mid b$. Mas, se p ≠ a, temos que $mdc\ (p, a)$ =1, então o resultado segue de forma direta.

Corolário: Se $p, p_1, \cdots, p_n$ são números primos e $p \mid p_1 \cdots p_n$, então $p = p_i$ para algum $i = 1, \cdots, n$. (A demonstração deste resultado é feita por indução sobre n).

Teorema 3.2: (Teorema Fundamental da Aritmética): Todo número natural n maior doque 1 ou primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.

Demonstração:

Se $n = 2$, o resultado claramente verificado, pois $2 = 1 \cdot 2$.

Suponhamos que o resultado seja válido para todo número menor do que n. Vamos provar que pra n também vale. Se o número primo, nada temos a demonstrar.

Suponhamos então que n seja composto, assim existem números naturais n_1 e n_2 tais que:

$n = n_1 . n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$.

Por hipótese de indução, temos que existem números primos $p_1, ..., p_r$ e $q_1, ..., q_s$,

$$n_1 = p_1 \cdots p_r \text{ e } n_2 = q_1 \cdots q_s.$$

$$n = p_1 \cdots p_r q_1 \cdots q_s.$$

Portanto:

Para mostrar a unicidade suponha que $n = p_1 \cdots p_r = q_1 \cdots q_s$, com p_i e q_j primos, onde $i = (1, \cdots, r)$ e $j = (1, \cdots, s)$

Como $p_1 \mid q_1 \cdots q_s$, pelo corolário anterior, temos que $p_i = q_j$ para algum i e j. Após reordenamento de $q_1, \cdots, q_s$ podemos supor que seja q_1. Portanto $p_2 \cdots p_r = q_2 \cdots q_s$. Como $p_2 \cdots p_r < n$.

Pela hipótese de indução, entendemos que $r = s$ e os p_i e os q_j são iguais aos pares.

Segundo Hefez (2013), outro fato importante, bem explorado e fixado por Euclides em Os Elementos (Livro IX) é a questão da infinidade dos números primos e sua distribuição, que seguem no teorema seguinte.

Teorema 3.3: Existem infinitos números primos.

Demonstração:

Supondo, por absurdo, que exista um número finito de números primos $p_2, \cdots, p_r$, ,considere o número natural :

$n = p_2 \cdots p_r + 1$

Pelo teorema fundamental da aritmética temos que o número n possui um fator primo p que, portanto deve ser um dos $p_1, \cdots, p_r$, e, consequentemente, divide o produto $p_1 p_2 \cdots p_r$. Mas isto implica que p divide 1, o que é absurdo.

Lema: Se um número natural $n > 1$, não é divisível por nenhum primo p tal que $p^2 \leq n$, então ele é primo.

Demonstração:

Supondo, por absurdo, que n não seja divisível por nenhum número primo p tal que $p^2 \leq n$ e que não seja primo. Seja q o menor número que divide n; então, $n = qn_1$, com $q \leq n_1$.

Segue da que: $q^2 \leq qn_1 = n$. Logo n é divisível por um número primo q tal que $q^2 \leq n$, absudo.

Exemplo 3.4: Verifique se o número 353 é primo ou composto.Solução:

De acordo com o resultado anterior se verificamos que 353 não é divisível pelos primos: 2, 3, 5, 7, 11, 13 e 17 terminaremos o processo, visto que $19^2 \geq 353$. Caso contrário ser composto. Pelo Algoritmo de Euclides temos que:

$$353 = 2 \cdot 176 + 1$$

$$353 = 3 \cdot 117 + 2$$

$$353 = 5 \cdot 70 + 3$$

$$353 = 7 \cdot 50 + 3$$

$$353 = 11 \cdot 32 + 1$$

$$353 = 13 \cdot 27 + 2$$

$$353 = 17 \cdot 20 + 13$$

Logo 353 é primo.

Proposição 3.5: Dois números inteiros a e b são primos entre si se, e somente se, existemnúmeros inteiros m e n tais que $ma + nb = 1$.

Demonstração:

($\Rightarrow$) Sejam a e b dois inteiros primos entre si, ou seja, $mdc(a, b) = 1$.

Pelo Teorema de Bezout, existem m, n, números inteiros, tais que $ma+nb = 1$.

($\Leftarrow$) Seja $d = mdc(a, b)$, então $d|a$ e $d|b$, implica que $d|(ma + nb)$, ou seja,

$d \mid 1$.

Portanto, $d = 1$.

3.5 Crivo de Eratóstenes e os Números Primos

Os números primos apesar de muito discretos e de aparente inexpressividade, são observados e estudados por matemáticos em todo mundo há mais de 2000 anos; eles representam um tópico super importante no contexto da Teoria dos Números e até mesmo na praticidade da vidacotidiana e podem produzir situações favoráveis quando utilizados em algumas nuances do mundoreal, basta considerarmos algumas situações que serão expostas mais à frente. O Crivo de Eratóstenes aparece em um contexto que buscava identificar os números primos de forma prática, principalmente à medida que fossem ficando maiores, para que, uma vez encontrados, dessem suporte à resolução de problemas ainda não resolvidos.

Definição: Os números primos são aqueles em que possuem apenas dois divisores positivos: O número 1 e o próprio número em análise.

Agora, vamos identificar alguns números primos segundo a definição acima a partir do conjunto dos naturais N = {0, 1, 2, 3, 4, 5, 6, ...}. Os números primos menores que 100 são:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

Os números 0, 1, 4, 6, 8, 10 e 12 claramente não são primos pois possuem mais de um divisor, por exemplo, o 10 pode ser dividido por 1, 2, 5 e o próprio 10. O 12 é dividido por 1, 2, 3, 4, 6 e 12. O zero não pode ser primo, pois ele pode ser dividido por qualquer outro número sem exceção e que, ainda assim seria zero, o que nos leva uma infinidade de divisores. Já o 1 também não pode ser primo pois ele possui um único divisor, ele mesmo. O número 2 é o menor primo e o único par. A complexidade começa aqui: Como saber se um número é primo ou não? Para números pequenos é fácil responder a esta pergunta, mas quando pensamos na infinidade de números naturais que existem, escolhermos um e ainda identificar se ele é primo ou não, é um desafio e tanto! Infelizmente, não existe uma fórmula fixa e fria que determine se um número é, ou não, primo, mas há diversas ferramentas para nos ajudar nesta tarefa. Um método bem prático é o Crivo (ou

Algoritmo da Divisão) de Eratóstenes. Este método consiste basicamente em testar se o número é, ou não, divisível por algum número natural menor do que ele próprio.

Vejamos o funcionamento de tal método na determinação de todos os números primos de 1 a 100:

Veja os seguintes passos até chegar ao objetivo:

1º) Escreva todos os números de 1 a 100 numa tabela.

2º) Elimine todos os múltiplos de 2, exceto o próprio 2 que já sabemos que é primo.

3º) Depois, faça isto com os múltiplos de 3, exceto o 3 que também é primo.

4º) O próximo da lista não riscado seria o 5, risque os múltiplos também.

Seguindo este método recursivamente, como vemos na tabela abaixo, os números verdes são os primos, os outros são números que são múltiplos de algum primo e portanto, considerado número composto.

Tabela 1

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	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90

91	92	93	94	95	96	97	98	99	100

Fonte:

Teorema de Eratóstenes[2]

Dado x ≥ 2, para garantirmos que é primo basta mostrar que nenhum número primo

$$p \leq \sqrt{x}\ , \textit{divida } x.$$

Isto significa que para determinarmos se um número x ≥ 2 é primo, dividimos sucessivamente x até somente raiz quadrada de x . Se uma dessas divisões for exata, constatamos que *x* não é primo, ou seja, que é um número composto. Do contrário, se nenhuma for exata, então *x* é primo. No caso acima, como $\sqrt{100} = 10$, então bastaríamos eliminar os múltiplos de 2, 3, 5 e 7.

3.6 Pequeno de Teorema Fermat

Pierre de Fermat foi considerado o "Príncipe dos Amadores". Fermat nunca teve formalmente a matemática como a principal atividade de sua vida. Estudou Direito em Toulouse na França, onde serviu no parlamento local, primeiro como advogado, mais tarde como conselheiro. Dedicava se à Matemática apenas nas suas horas de lazer e, mesmo assim, foi considerado um dos maiores matemáticos de seu tempo (BOYER. 2003).

Por isso um de seus resultados irá nos auxiliar em se tratando de congruências modulares O Pequeno Teorema de Fermat, que além de facilitar muito a resolução de algumas situações-problema, considerado a base para a criação dos Testes de Primalidade modernos, sendo que a maioria destes testes foi uma modificação o ou uma generalização do Teste de Fermat que tem como base o Pequeno Teorema de Fermat, provado a seguir.

[2] https://www.infoescola.com/matematica/numeros-primos/ - Acesso em 26 de abril de 2023

Teorema 3.4: (Pequeno Teorema de Fermat): Dado um número primo p, tem-se que p divide o número $a^p - a$, para todo a $\in$ Z.

Demonstração:

Se $p = 2$, o resultado é imediato, visto que o resultado $a^2 - a = a(a-1)$ que suponhamos p *um número ímpar*. Neste caso basta mostrar o resultado para $a \geq 0$.

Vamos provar por indução sobre a. O resultado vale para $a = 0$, pois $p \mid 0$.

Supondo o resultado válido para a, mostraremos que também vale para $a+1$.

Pelo Binômio de Newton, temos:

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

Por hipótese de indução, o segundo membro da igualdade acima divisível por p, ou seja, temos que o resultado verdadeiro para todo p primo e $a \in$ R.

Corolário: Se p é um número primo e se a é um número natural não divisível por p,então o p divide $a^{p-1} - 1$.

Demonstração:

Como pelo Pequeno Teorema de Fermat, $p \mid (a^{p-1} - 1)$ e como $mdc\ (a,\ p) = 1$,segue imediatamente que p divide $a^{p-1} - 1$.

Esse resultado considerado também como parte do teorema, visto ser um caso particular do mesmo.na história da humanidade o Pequeno Teorema de Fermat se destaca, pois, há várias aplicações para o desenvolvimento dos critérios de divisibilidade, potenciação de congruências e principalmente na parte de criptografia a avançada, a qual não será abordada nesta dissertação, tendo em vista o público-alvo.

3.7 Equações Diofantinas Lineares (EDL)

As Equações Diofantinas Lineares (EDL) são aplicações muito importantes do conceito de divisibilidade. Vejamos o seguinte problema:

Uma corporação militar adquiriu automóveis e motocicletas. Considerando que a soma dos 2 pneus de cada moto e dos 4 pneus de cada automóvel igual a 152 pneus, determine as quantidades possíveis de carros e motos?

Esse tipo de problema comum de se aparecer em livros didáticos das séries finais do ensino fundamental como: A conquista da Matemática - 8º Ano de Benedicto Castrucci / José Ruy Giovanni /José Ruy Giovanni Jr; ou na obra de Ayrton Olivares / José Roberto Bonjorno / Regina Azenha / Tânia Gusmão, entre outros vários livros. Na maioria das vezes definida para o aluno apenas como uma equação de primeiro grau com duas incógnitas. Sua resolução geralmente apresentada de tal forma que o aluno leve a dependência de uma dessas incógnitas a partir deum valor dado a outra. No entanto o verdadeiro teor do problema deixado a mercê.

Vejamos como é apresentado o processo de resolução por livros didáticos:

Como se tratam de veículos, então os valores de x e y devem necessariamenteser positivos maiores ou iguais a 1 .

Tomando:

x= número de motos compradas;

y= número de carros.

Teremos uma equação do tipo: $2x + 4y = 152$.

Subtraindo $4y$ a ambos os membros da igualdade teremos:

$2x = 152 - 4y$.

Dividindo por 2 ambos os membros, reduziremos equação semelhante:

$x = 76 - 2y$

Através de tabelas podemos atribuir valores para y, determinado assim obtendo os valores de x. Note que:

Tabela 2

y	$x = 76 - 2y$	x

1	$x = 76 - 2 \cdot 1$	74
2	$x = 76 - 2 \cdot 2$	72
3	$x = 76 - 2 \cdot 3$	70
4	$x = 76 - 2 \cdot 4$	68
...	...	...
37	$x = 76 - 2 \cdot 37$	2

Fonte: FRANCO, Tânia R. Rodrigues (Dissertação de mestrado – Divisibilidade e congruências – Aplicações no Ensino Fundamental II) - UFG/GO – 2016 , p.28.

Ao analisarmos o processo feito, percebemos que podem haver vários valores pra ambas as incógnitas. Isto deve ser bem definido para o aluno(a), ou seja, o fato de a solução não ser única, visto que na medida que um foi aumentando o outro foi diminuindo, mas o valor final de rodas continuou o mesmo.

Uma Equação Diofantina Linear é uma equação polinomial que permite a duas ou mais variáveis assumirem apenas valores inteiros. A designação de equação diofantina, é uma singela homenagem dos matemáticos a Diofante de Alexandria - grego do século III d.c. Muito pouco se sabe sobre a vida do matemático Diofante, que deve ter vividoapenas 84 anos, segundo interpretações dos livros de História da Matemática.

Definição: Denomina-se equação Diofantina Linear, toda equação da forma $ax+by=c$ onde a, b e $c \in Z$ e x e y incógnitas a serem determinadas em Z.

Existem algumas perguntas feitas em uma análise acerca de uma equação Diofantina:

- Existe alguma solução?
- Existe alguma solução daquelas achadas facilmente por inspeção?
- Existe uma quantidade finita ou infinita de soluções?
- Todas as soluções podem ser achadas em teoria? É possível computar todas assoluções?

Estes problemas tradicionais comumente ficaram por séculos sem solução até alguns matemáticos começarem a entender sua profundidade (em alguns casos), ao invés detrata -los como quebra-cabeças. A resposta destes questionamentos podem ser respondidas pelas proposições abaixo.

Proposição 3.6: Uma equação diofantina $ax+by = c$ admite infinitas soluções nos inteiros se, e somente se, $mdc(a, b)$ divide c.

Demonstração:

(⇒)Seja $ax + by = c$, onde a, b e c são inteiros e que possua uma solução inteira, ou seja, existem x_0 e y_0 inteiros tais que:

$$ax_0 + by_0 = c.$$

Suponha que $d = mdc(a, b)$, assim existem m e n inteiros tais que:

$$a = dm \text{ e } b = dn, \text{ pois } d \mid a \text{ e } d \mid b.$$

Substituindo na outra equação, temos:

$$c = ax_0 + by_0 = dmx_0 + dny_0c = d.(mx_0 + ny_0).$$

Como $mx_0 + ny_0$ inteiro, obtemos:

$$dq = ax_0q + by_0q.$$

(⇐) Como $c = dq$, substituindo:

$$c = a(x_0q) + b(y_0q).$$

Se chamarmos de x_0q e y_0q de x e y respectivamente, temos $c = ax + by$. Portanto se $d \mid c$ existem x e y que ser o soluções da equação diofantina linear.

Exemplo 3.5: Resolver a equação diofantina linear $3x + 6y = 18$.

Solução:

Por se tratar de uma equação que apresenta números pequenos podemos obtero resultado por tentativa e erro. Desse modo, temos que:

$3 \cdot (4) + 6 \cdot (1) = 18$

$3 \cdot (-6) + 6 \cdot (6) = 18$

$3 \cdot (10) + 6 \cdot (-2) = 18.$

Logo, os pares de inteiros: 4 e 1, −6 e 6, 10 e −2, são soluções da equação.

Exemplo 3.6: possível se criar galinhas e coelhos, tal que a soma de seus pés seja 95?

Modelando o problema dado podemos representa-lo pela Equação Diofantina Linear: $2x + 4y = 95$.

No entanto temos que *mdc* (2, 4) não divide 95.

Logo não há solução inteira para equação formada. Portanto a situação do problema é impossível.

Proposição 3.7: Seja x_0, y_0 uma solução da equação $ax + by = c$, onde $mdc(a, b) = 1$. Então, as soluções x, y em Z da equação :

$$x = x_0 + bt$$

$$y = y_o - at$$

$$onde\ t \in Z$$

Demonstração:

Seja x, y uma solução de $ax + by = c$. Assim:

$$ax_0 + by_0 = ax + by = c.$$

Consequentemente:

$a(x - x_0) = b(y_0 - y)$.

Como $mdc\ (a, b) = 1$, segue que $b \mid (x - x_0)$.

Logo: $x - x_0 = bt$, $t \in Z$.

Substituindo a expressão de $(x - x_0)$ acima , segue-se que:

$y_0 - y = at$.

Por outro lado verifica-se que $x = x_0 + bt$ e $y = y_0 - at$, solução, pois:

$ax + by = a\,(x_0 + bt) + b\,(y_0 - at) = ax_0 + by_0 = c$

Exemplo 3.7: Determine todas as soluções da equação 172x +20y=1000

Solução:

Determinamos inicialmente o *mdc* (172, 20) pelo algoritmo de Euclides, visto que o processo de inspeção se torna exaustivo. Assim segue que:

$172 = 20 \cdot 8 + 12 \Rightarrow 12 = 172 - 20 \cdot 8$

$20 = 12 \cdot 1 + 8 \Rightarrow 8 = 20 - 12 \cdot 1$

$12 = 8 \cdot 1 + 4 \Rightarrow 4 = 12 - 8 \cdot 1$

$8 = 4 \cdot 2 + 0$

Portanto, o *mdc* (172, 20) = 4 e como 4 |1000, segue-se que a equação dada tem solução.

Agora devemos obter a expressão do inteiro 4 como combinação linear de 172 e 20. Substituindo os restos na equação de trás pra frente a partir do *mdc* (172, 20) teremos:

$4 = 12 - 8 \cdot 1$

$4 = 12 - (20 - 12 \cdot 1) \cdot 1$

$4 = 12 - 20 \cdot 1 + 12 \cdot 1$

$4 = 2 \cdot 12 - 20 \cdot 1$

$4 = 2 \cdot (172 - 20 \cdot 8) - 20 \cdot 1$

$4 = 172 \cdot 2 - 20 \cdot 16 - 20 \cdot 1$

$4 = 172 \cdot 2 - 20 \cdot 16 - 20 \cdot 1 \Rightarrow 4 = 172 \cdot 2 - 20 \cdot 17.$

Logo temos a equação:

$4 = 172 \cdot 2 + 20 \cdot (-17).$

Como queremos uma solução para a combinação que resulta 1000, multipliquemos ambos os membros desta igualdade por 1000/4 = 250 e obtemos:

$1000 = 172 \cdot 500 + 20(-4250)$.

Portanto, o par de inteiros $x_0 = 500$, $y_0 = -4250$ uma solução particular da equação proposta, e todas as outras soluções dadas pelas fórmulas:

$x = 500+5t$

$y= - 4250 - 43$

onde *t é* arbitrário e $t \in Z$.

4 CONGRUÊNCIA MODULAR

A Congruência Modular é uma ferramenta que pode auxiliar muito no desenvolvimento do pensamento aritmético e algébrico de nossos alunos. Um tema gerador de excelentes oportunidades de contextualização, pois apresenta a realização de operações aritméticas de uma forma diferente da utilizada normalmente pelos alunos (as) (BARBOSA. 2013).

Desenvolvendo uma pesquisa sobre o tema percebe-se que é um assunto bastante abordado por mestrandos do PROFMAT. Para Esquinca (2013), ela colabora com a solução de algum problema da atualidade, agilizando o processo de resolução destes no ensino básico. Por outro lado Souza (2015), salienta que é um forte aliado na preparação de alunos para as Olimpíadas Brasileira de Matemática das Escolas Públicas (OBMEP). Assim por ser um tema bastante atual e que pode ser trabalhado desde o Ensino Fundamental; formalizaremos os principais conceitos de congruência e suas propriedades para que possamos no capítulo seguinte, mostrar processos de aplicações em situações cotidianas, através de atividades didáticas desafiadoras, porém, imbutindo a perspectiva de ser algo bem palpável e útil no cotidiano dos alunos.

4.1 O Conceito de Congruência módulo m

O conceito de congruência aparece da relação entre dois números que, divididos por um terceiro, chamado módulo de congruência, deixam o mesmo resto. Por exemplo, o número 9 é

congruente ao número 2, módulo 7, pois, ambos deixam resto 2, ao serem divididos por 7. Representamos essa congruência do exemplo por $9 \equiv 2 \bmod 7$. Essa relação tem um comportamento semelhante à igualdade.

Definição: Dados $m, a, b \in Z$. Diremos que a e b são congruentes módulo m, quando o resto das divisões Euclidianas de a e b por m forem os mesmos. Denotaremos que a é congruente ab módulo m da seguinte forma:

$$a \equiv b \bmod(m).$$

Proposição 4.1: Considere $a, b \in Z$. Temos $a \equiv b \bmod (m)$ se, e somente se, $m \mid b - a$.

Demonstração:

($\Rightarrow$) Suponhamos que $a \equiv b \bmod (m)$. Pela definição temos que: $a = qm + r$

e $b = q_1 . m + r$, com $0 < r < m$ e $q, q_1 \in Z$.

Segue então que: $b - a = (q_1 - q)m \Rightarrow m \mid (b - a)$.

($\Leftarrow$) Suponhamos que $m \mid (b - a)$.

Logo existe $q \in Z$ tal que $b - a = mq$.

Daí: $b = a + mq$.

Sejam r e q_1 o resto e o quociente respectivamente da divisão euclidiana de b por m, isto é:

$b = mq_1 + r$,

com $0 < r < m$, das equações anteriores temos que: $a+mq = mq_1+r$, logo, $a = m(q_1 - q)+r$, com $0 < r < m$.

Portanto r também é o resto da divisão euclidiana de a por m.

Para exemplicar, podemos argumetar que $5 \equiv -6 \bmod(11)$, pois deixam o mesmo resto na divisão por 11, ou seja $11 \mid 5 - (-6)$,o que implica que: $11 \mid 11$.

Observação:

$x = 1 \cdot x + 0$ para todo $x \in Z$, ou seja, todo número inteiro quando dividido por 1 deixa resto zero. Portanto para nosso trabalho admitirenos apenas a congruência módulo m, para valores de m maiores que 1, pois o caso m = 1 é trivial.

4.2 Propriedades da Congruência Modular

As proposições apresentadas abaixo mostram que a relação de congruência módulo m possui algumas propriedades relevantes tornando-a uma relação de equivalência em Z e ainda mostrando que a congruência é compatível à adição e à multiplicação.

Nas propriedades, não se utiliza o caso m = 1, pois se usássemos congruência módulo 1, obteríamos $a \equiv b \bmod (1)$ que é o mesmo que $1|a - b$, o que é sempre verdade para quaisquer a e b. Porisso excluímos essa possibilidade.

Proposição 4.2: Dados m, a, b ∈ N tais que m > 1. São verdadeiras as sentenças:

i) $a \equiv a \bmod (m)$;

ii) Se $a \equiv b \bmod (m)$, então $b \equiv a \bmod (m)$;

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

Demonstração:

i) Como $m \mid 0$, então $m \mid a - a$, o que nos diz que $a \equiv a \bmod (m)$;

ii) Se $a \equiv b \bmod (m)$, temos que $m \mid a - b$, logo $a - b = mk$.

Multiplicando essa última igualdade toda por (−1), temos que $-(a - b) = -mk$. Assim, $b - a = m(-k)$, logo $b \equiv a \bmod (m)$;

iii) Se $a \equiv b \bmod (m)$ e $b \equiv c \bmod (m)$, então existem inteiros k e k' tais que: $a - b = mk$ e $b - c = mk'$.

Somando membro a membro as duas igualdades anteriores, temos: $(a - b) + (b - c) = mk + mk' \Rightarrow a - c = m(k + k')$. Logo: $m|(a - c) \Rightarrow a \equiv b \bmod (m)$.

Para melhor exemplicar as propriedades de reflexão, simetria e transitividade observe os exemplos seguintes:

● $3 \equiv 3 \bmod (2) \Leftrightarrow 2 \mid (3-3) \Leftrightarrow 2 \mid 0$;

● $5 \equiv 7 \bmod (2)$ e $7 \equiv 5 \bmod (2) \Leftrightarrow 2 \mid (5-7)$ e $2 \mid (7-2) \Leftrightarrow 2 \mid -2$ e $2 \mid 2$;

● $15 \equiv 3 \bmod (4)$ e $3 \equiv 7 \bmod (4) \Rightarrow 15 \equiv 7 \bmod (4) \Leftrightarrow 4 \mid (15-3)$ e $4 \mid (3-7) \Rightarrow 4 \mid 12$ e $4 \mid -4$.

4.3 Propriedades Operatórias

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

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

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

(iv) Se $a \equiv b \bmod (m)$, então $an \equiv bn \bmod (m)$, para todo n.

(v) $a \equiv b \bmod(m)$ e $n|m$, então $a \equiv b \bmod(n)$.

Demonstração:

(i) Se $a \equiv b \bmod (m)$ e $c \equiv d \bmod (m)$, então existem inteiros k e k' tais que: $a - b = mk$ e $c - d = mk'$. Somando membro a membro as duas igualdades anteriores, temos:

$(a - b) + (c - d) = mk + mk' \Rightarrow (a + c) - (b + d) = m(k + k')$.

Logo resulta que: $m \mid [(a + c) - (b + d)] \Rightarrow a + c \equiv b + d \ (\bmod m)$.

(ii) A demonstração é análoga ao item (i).

(iii) Se $a \equiv b \bmod (m)$, temos que $a - b = mk$. Somando e subtraindo c no primeiro membro da igualdade, temos: $a - b + c - c = mk \Rightarrow (a + c) - (b + c) = mk$.

Assim temos que: $a + c \equiv b + c \bmod (m)$.

(iv) Se $a \equiv b \bmod (m)$, então, $m \mid ab$. Sabemos que:

an - bn = (a - b).n = (m . k) . n = m . (k . n)

Como m | a - b, então m | na - bn.

Assim, an ≡ bn mod (m).

(v) Se a ≡ b mod (m), então m | a - b. Como n|m⇒ n | a - b. Logo, a ≡ b mod(n) .

Das propriedades operatórias demonstradas seguem respectivamente alguns exemplos numéricos de aplicação das mesmas:

Exemplo: Temos que: 7 ≡ 2 mod (5) e 6 ≡ 1 mod (5), pois 5 | (7 − 2) e 5 | (6 − 1).

Multiplicando ambas congruências membro a membro, segue que:

42 ≡ 2 mod (10) ⇔ 5 | 40.

Se 8 ≡ −1 mod(3),pois 3 | (8 + 1), somando 5 a ambos os lados da congruência teremos que: 13 ≡ 4 mod (3), pois, 3 | (13 − 4) ⇒ 3 | 9.

Note que: 7 ≡ −3 mod (10) ⇔ 10 | 10.

Multiplicando por 3 os membros da congruência teremos:

21 ≡ −9 mod (10), pois 10 | (21 + 9).

Entretanto a recíproca não é verdadeira, pois 54 ≡ 30 mod (8), mas 96=5 mod (8).

Sabemos que: 21 ≡ −9 mod (10), pois 10 | 30, e ainda, 5 | 10. 42.

Logo, 21 ≡ −9 mod(5) ⇔ 5 | 30.

Ainda levando em consideração as propriedades apresentadas nos itens (i) e (ii) das propriedades operatórias deriva o resultado abaixo.

Corolário:

Para todo n ∈ N, a e b ∈ Z, se a ≡ b mod (m), então tem-se que $a^n \equiv b^n$ mod (m).

Outro fato que também é importante e já foi demostrado anteriormente é o caso do Pequeno Teorema de Fermat que pode ser expressado claramente em termos de congruência e fica ainda dividido em dois casos específicos:

1º) Se p é um número primo e a ∈ Z e p | a, então: $a^p \equiv a \bmod (p)$

2º) Se p não divide a, então: $a^{p-1} \equiv 1 \bmod (p)$ Decorrente do

Pequeno Teorema de Fermat com p primo e a, b ∈ Z temos ainda três importantes resultados que irão nos auxiliar nas aplicações de congruências tratadas no próximo capítulo:

(i) $(a + b)^p \equiv a^P + b^P \bmod (p)$

(ii) $(a - b)^p \equiv a^P - b^P \bmod (p)$

(iii) $a^P \equiv b^P \bmod (p^2)$

Demonstração:

(i)$(a + b)^p \equiv (a+b) \equiv a^p + b^p \bmod (p)$

(ii) $a^p \equiv (a - b+b)^p \equiv (a - b)^p + b^p \bmod (p)$.

Subtraindo b^p em ambos os lados da congruência segue que: $a^p - b^p \equiv (a - b)^p \bmod (p) \Leftrightarrow (a - b)^p \equiv a^p - b^p \bmod (p)$

(iii) Do item (ii) sabemos que: $(a - b)^p \equiv a^p - b^p \bmod (p)$.

Por hipótese, temos que p divide ap − bp e da congruência acima segue que: p | (a − b) p.

Logo $p \mid a - b \Rightarrow a \equiv b \bmod(p) \Rightarrow a^i \equiv b^i \bmod (p)$ para todo i ∈ N.

Daí tem-se que: $a^{p-1} + ba^{p-2} + \cdots + b^{p-2}a + \ldots\ldots + b^{p-1}$ e ambos os fatores do lado direito são divisíveis por p.

4.4 Aritmética dos Restos

As propriedades das congruências podem facilitar muito o cálculo do resto de uma divisão de dois números inteiros.

Exemplo 4.1 : Determinar o resto da divisão de 25 por 11 é muito simples.Imagine descobrir o resto da divisão de 2545 por 11 por exemplo?

Se não tivermos o conhecimento das propriedades acima citadas se torna uma tarefa exaustiva. Porém não o é, tendo estas ferramentas à mão.

Exemplo 4.2: Deteminar o resto da divisão de 2545 por 11.

Solução:

Como 11primo e 11 não divide 25, temos pelo Teorema de Fermat que:

$25^{11} \equiv 25 \; mod \; (11) \Rightarrow 25^{11} \equiv 3 \; mod \; (11)$.

Sabemos que:

$25^{44} \equiv 4 \; mod \; (11)$

Das propriedades, temos que:

$25^{45} \equiv 100 \; mod \; (11) \Rightarrow 25^{45} \equiv 1 \; mod \; (11)$.

Portanto o resto da divisão é 1.

Exemplo 4.3: Prove que $2^{70} + 3^{70}$ é divisível por 13.

Solução:

Notemos que, *mdc* (2, 13) = 1, então pelo teorema de Fermat:

$2^{12} \equiv 1 \; mod \; (13)$.

Pelo Corolário, temos que:

$2^{60} \equiv 1 \; mod \; (13)$.

$2^4 \equiv 3 \; mod \; (13)$.

$2^{60}.2^4.2^4.2^2 \equiv 1.3.3.4 \; mod \; (13)$,

logo,

$2^{70} \equiv 10 \; mod \; (13)$

Por outro lado, ainda pelo teorema de Fermat

$3^{12} \equiv 1 \; mod \; (13)$ e $3^4 \equiv 243 \equiv 1 \; mod \; (13)$.

Assim:$3^{60} \equiv 1 \; mod \; (13)$.Temos também que:

$3^{70} \equiv 3 \; mod \; (13)$.

Agora, somemos as duas congruências consideradas

Agora somando as equações e usando as propriedades operatórias,concluímos que:

$2^{70}+3^{70} \equiv 0 \ mod\ (13)$.

Portanto $2^{70}+3^{70}$ divisível por 13.

Exemplo 4.4: Determine o resto da divisão de $5^{85} + 7^{85} + 11^{85} + 25^{85}$ por 8.

Solução:

:Observe que:

$$5 \equiv -3 \ mod\ (8) \Rightarrow 5^{85} \equiv (-3)^{85} \ mod\ (8)$$

$$7^{85} \equiv -1 \ mod\ (8) \Rightarrow 7^{85} \equiv (-1)^{85} \ mod\ (8)$$

$$11 \equiv 3 \ mod\ (8) \Rightarrow 11^{85} \equiv 3^{85} \ mod\ (8)$$

$$25 \equiv 1 \ mod\ (8) \Rightarrow 25^{85} \equiv 1^{85} \ mod\ (8)$$

Somando membro a membro as quatro congruências:

$5^{85} + 7^{85} + 11^{85} + 25^{85} \equiv (-3)^{85} + (-1)^{85} + 3^{85} + 1^{85} \ mod\ (8)$.

Assim,

$5^{85} + 7^{85} + 11^{85} + 25^{85} \equiv 0 \ mod\ (8)$.

Portanto o resto da divisão é zero.

Exemplo 4.5: Determine o resto da divisão do número $2222^{5555} + 5555^{2222}$ por 7.

Solução:

Sendo: $2222 = 7 \cdot 317 + 3 \equiv 3 \ mod\ (7)$, temos:

$2222^{5555} \equiv 3^{5555} \ mod\ (7)$.

Analogamente: $5555 = 7 \cdot 793 + 4 \equiv 4 \ mod\ (7)$, donde:

[3] Profmat-AV2 2014-Questão 1

$5555^{2222} \equiv 4^{2222}\ mod\ (7)$.

Obtemos assim:

$2222^{5555} + 5555^{2222} \equiv 3^{5555} + 4^{2222}\ mod\ (7)$.

Como $mdc(3, 7) = mdc(4, 7) = 1$, usando o Pequeno Teorema de Fermat,segue que:

Escrevendo: $3^6 \equiv 1\ mod\ 7$ e $4^6 \equiv 1\ mod\ (7)$.

$5555 = 6 \cdot 925 + 5$ e $2222 = 6 \cdot 370 + 2$, teremos:

$35555 + 42222 = 3^{6\cdot 925} \cdot 3^5 + 4^{6\cdot 370} \cdot 4^2 \equiv 3^5 + 4^2\ mod\ 7$.

Assim:

$2222^{5555} + 5555^{2222} \equiv 3^{5555} + 4^{2222} \equiv 3^5 + 4^2 \equiv 5 + 2 \equiv 0\ mod\ (7)$.

Portanto, o resto da divisão de $2222^{5555} + 5555^{2222}$ por 7 é zero.

Exemplo 4.6: Ache o resto da divisão por 17 do número

$S = 1^{16} + 2^{16} + 3^{16} + \cdots + 85^{16}$.

Solução:

Pelo Pequeno Teorema de Fermat temos que:

$a^{16} \equiv 1 \bmod (17)$, se 17 nao divide a

$a^{16} \equiv 0 \bmod (17)$, se 17 divide a

Como $85 = 17 \cdot 5$, temos que de 1 a 85 h 5 múltiplos de 17 e 85 - 5 = 80 não múltiplos de 17 (i.e., primos com 17).

Logo:

$S \equiv 80 \cdot 1 \equiv 12\ mod\ (17)$.Portanto, o resto da divisão de S por 17 é 12.

Exemplo 4.7: Determine o resto da divisão por 7 do número $1^7 + 2^7 + 3^7 + \cdots + 100^7$.

[4] Profmat- AV2 2011-Questão 2
[5] Profmat-AV2 2012- Questão 2 (*b*)

Solução:

Usando o Pequeno Teorema de Fermat, vemos que:

$a^7 \equiv a \bmod (7);\ a = 1, 2, 3, 4, 5, 6.$

Além disso, se n = 7k + a, então:

$n^7 = (7k + a)^7 \equiv a^7 \equiv a\ mod\ (7);\ a = 1, 2, 3, 4, 5, 6.$

Desta forma:

$1^7 + 2^7 + 3^7 + \cdots + 100^7 \equiv (1 + 2 + 3 + 4 + 5 + 6 + 0) + \cdots + (1 + 2 + 3 + 4 + 5 + 6 + 0) + 1 + 2 = \frac{7 \cdot 6}{2} \cdot 14 + 3 = 21 \cdot 14 + 3 \equiv 3\ mod\ (7).$

Portanto, o resto da divisão de $1^7 + 2^7 + 3^7 + \cdots + 100^7$ por 7 é 3.

4.5 Divisibilidade/Congruência - Outras Aplicações

Conceitos como divisibilidade e congruência são assuntos muito presentes no nosso dia-a-dia, porém, divisibilidade se trabalha de maneira a memorizar conceitos e congruência não está presente nos currículos do fundamental II. No entanto, a proposta aqui apresentada visa mostrar algumas aplicações de forma interessante, estabelecendo relações entre divisibilidade/congruências e situações do cotidiano, com o intuito de fazer com que o aluno(a) perceba que matemática não é nada posto por uma hierarquia de cima pra baixo pra complicar a vida escolar dele(a); e sim algo que pode abrir horizontes para a vitória profissional. Por definição, como já vimos, congruência simplesmente é a relação entre dois números que, divididos por um terceiro, chamado módulo, deixam o mesmo resto.

Apresentaremos neste capítulo algumas aplicações de divisibilidade e congruência modular além das já apresentadas em alguns dos capítulos anteriores. Dentre elas os Critérios clássicos de divisibilidade por 2, 3 e 11; Dígitos de verificação emcódigos como: o de barras, International Standard Book Number(ISBN), o Cadastro de Pessoas Físicas (CPF); alguns problemas com Calendários e a incrível situação em que a boa atuação do assunto posto, pode detectar um erro na

leitura de um código de barras qualquer; ou seja, identificaria uma falsificação ou algo do tipo, infelizmente um tipo penal comum no mundo moderno.

Procuramos apresentar uma metodologia contextualizada e simples ao se abordar problemas que podem ser trabalhados com alunos do ensino básico.

4.6 Critérios Clássicos de divisibilidade

Os critérios de divisibilidade são um conteúdo que faz parte do currículo escolar do ensino fundamental, entretanto, são apresentados como um conjunto de regras a serem memorizadas e aplicadas de maneira direta. O erro não estaria em expor tais regras para os estudantes e sim a forma como está sendo colocada. Estas regras são muito úteis na resolução de problemas. Mas de que maneira esses conceitos são transmitidos para os alunos? Será que os alunos foram instigados a elaborar esses conceitos? A atual metodologia prioriza o resultado imediato e deixa a desejar o desenvolvimentodo pensamento analítico no aluno (SANT'ANNA. 2013).

Na realidade, grande parte dos professores antecipam conceitos, perdendo a ordem dos fatos e consequentemente argumentações para justificá-los perante ao público discente.Isto muitas vezes gera, desconfiança e falta de estímulo.

Nosso objetivo nesta parte é apresentar alguns critérios de divisibilidade, formula dos através de procedimentos de congruência modular, de tal forma a levar os alunos a uma compreensão lógico dedutiva dosresultados e gerar especulações sobre outros critérios não apresentados.

Para estabelecer um critério de divisibilidade por m, a ideia é descobrir uma expressão mais simples em termos dos dígitos $a_n, a_{n-1}, a_{n-2}, \cdots, a_1, a_0$ e qual é o polinômio côngruo módulo$m$, depois usar o fato de que se a e b são congruentes módulo m, o resto das divisões de a e b por m são os mesmos. Iniciaremos o critério com um exemplo numérico para depois escrevê-lo de forma generalizada.

4.6.1 Divisibilidade por 2

Utilizaremos neste e nos demais exemplos sobre critérios de divisibilidade a forma estendida da base 10 de um número e através de congruências módulo m, desenvolveremos todo o processo.

Exemplo 4.8: Verifique se 1987 e 25384 são divisíveis por 2.

Solução:

Notemos que 1987 se escreve na base 10 da seguinte forma:

$1 \cdot 10^3 + 9 \cdot 10^2 + 8 \cdot 10 + 7.$

Aplicando congruência modular teremos:

$1987 \equiv 1 \cdot 10^3 + 9 \cdot 10^2 + 8 \cdot 10 + 7 \ mod\ (2)$

Por outro lado sabemos que: $10 \equiv 0 \ mod\ (2)$.

Desse modo:

$1987 \equiv 1 \cdot 0 + 9 \cdot 0 + 8 \cdot 0 + 7 \equiv 7 \ mod\ (2).$

Como, $7 \equiv 1 \ mod\ (2)$, por transitividade, temos que o número $1987 \equiv 1 \ mod\ (2)$.

Logo 1987 não divisível por 2.

Fazendo o mesmo processo para o número 25384:

$25384 \equiv 2.10^4 + 5.10^3 + 3.10^2 + 8.10 + 4 \ mod\ (2).$

Logo,

$25384 \equiv 4 \ mod\ (2)$ e $4 \equiv 0 \ mod\ (2)$.

Assim:

$25384 \equiv 0 \ mod\ (2).$

Portanto 25384 é divisível por 2.

Para fazer a generalizaç ã o do resultado acima consideremos como N um número natural dado. Sua forma estendida na base 10:

$N = a_n a_{n-1} a_{n-2} a_1 a_0 = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + 10 \cdot a_1 + a_0$;

$n \in \mathrm{N}$

Note que:

$a_1 .10 \equiv 0 \bmod 2$

$a_2 .10^2 \equiv 0 \bmod 2$

$a_3 .10^3 \equiv 0 \bmod 2$

.

.

$a_n .10^n \equiv 0 \bmod 2$

Nosso objetivo é chegar no valor de N.

Multiplicando uma a uma as congruências acima, por $a_1, a_2, \cdots, a_n$, respectivamente, teremos:

Agora somando membro a membro segue que:

$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + 10 \cdot a_1 \equiv 0 \; mod \; (2)$

Das propriedades operatórias vem:

$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + 10 \cdot a_1 + a_0 \equiv a_0 \; mod \; (2)$.

Portanto um dado número só é divisível por 2 se seu termo a_0 o é . Isso

ocorre se a_0 for par.

Observação: É de bom alvitre lembrar que a divisibilidade por 5 e por 10 decorrem no mesmo sentido.

4.6.2 Divisibilidade por 3

Exemplo 4.9: Verifique se os números 12564890 e 1235 são divisíveis por 3.

Solução:

Para o número 12564890 temos que:

$12564890 \equiv (1.107 + 2 \cdot 106 + 5 \cdot 105 + 6 \cdot 104 + 4 \cdot 103 + 8 \cdot 102 + 9 \cdot 10 + 0) \bmod (3)$.

Como $10 \equiv 1 \bmod (3)$ e por consequência $10^n \equiv 1 \bmod (3)$,

temos que: $12564890 \equiv (1 + 2 + 5 + 6 + 4 + 8 + 9 + 0) \bmod (3)$.

Logo, $12564890 \equiv 45 \bmod (3)$ e $45 \equiv 0 \bmod (3)$. Por transitividade tem-se que: $12564890 \equiv 0 \bmod(3)$. Portanto 12564890 é divisível por 3.

Da mesma forma, temos:

$1235 \equiv (1.103 + 2.102 + 3.10 + 5) \bmod (3)$.

Logo, $1235 \equiv (1 + 2 + 3 + 5) \bmod (3)$.

Assim, $1235 \equiv 11 \bmod (3)$ e $11 \equiv 2 \bmod (3)$, que implica, $1235 \equiv 2 \bmod (3)$.

Portanto 1235 não é divisível por 3.

O critério de divisibilidade por 3 é exatamente igual ao critério de divisibilidade por 9, visto que o número 10, deixa o mesmo resto na divisão por ambos.

Assim como na generalização da divisibilidade por 2, consideremos:

$a_1 .10 \equiv a_1 \bmod 3$

$a_2 .10^3 \equiv a_2 \bmod 3$

$a_3 .10^3 \equiv a_3 \bmod 3$

.

.

$a_n.10^n \equiv a_n \bmod 3$

Somando membro a membro da congruência o termo independente a_0, teremos:

$a_n \cdot 10^n + a_n - 1 \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + 10 \cdot a_1 + a_0 \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \bmod 3$.

Percebemos assim, que um número é divisível por 3, se a soma de seus algarismos for um número divisível por 3.

4.6.3 Divisibilidade por 11

Exemplo 4.10: Verifique se o número 1327 é divisível por 11.

Solução:

Sabemos que: $1327 = 3 \cdot 104 + 1 \cdot 103 + 3 \cdot 102 + 2 \cdot 10 + 7$. Por congruência modular temos: $31327 \equiv 3 \cdot 104 + 1 \cdot 103 + 3 \cdot 102 + 2 \cdot 10 + 7 \bmod (11)$.

Notemos ainda que:

$10 \equiv -1 \bmod (11)$

$10^2 \equiv (-1)^2 \bmod (11)$

$10^3 \equiv (-1)^3 \bmod (11)$

$10^4 \equiv (-1)^4 \bmod (11)$.

Assim,

$10 \equiv -1 \bmod (11)$

$10^2 \equiv 1^2 \bmod (11)$

$10^3 \equiv -1 \bmod (11)$

$10^4 \equiv 1 \bmod (11)$.

No entanto:

$31327 \equiv 3 \cdot 1 + 1 \cdot (-1) + 3 \cdot 1 + 2 \cdot (-1) + 7 \bmod (11)$.

Logo, $31327 \equiv 10 \bmod (11)$.

Portanto, 31327 não é divisível por 11.

Para determinar a forma genérica de divisibilidade por 11, considere um natural dado tal que:

$N = a_n . a_{n-1} .. a_{n-2} . a_1 . a_0 = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + 10 \cdot a_1 + a_0$; $n \in N$

E observando o fato de que:

$10 \equiv -1 \bmod (11)$

$10^2 \equiv 1 \bmod (11)$

$10^3 \equiv -1 \bmod (11) \ldots 10n \equiv 1 \bmod (11)$; se n é par e $-1 \bmod (11)$; se n é ímpar.

Novamente multiplicando por a1, a2, · · ·, an simultaneamente em cada congruência e somando o termo a0, teremos:

$a_1 \cdot 10 \equiv -1 \cdot a_1 \bmod (11)$

$a_2 \cdot 10^2 \equiv 1 \cdot a_2 \bmod (11)$

$a_3 \cdot 10^3 \equiv -1 \cdot a_3 \bmod (11)$

$a_n \cdot 10^n \equiv 1 \cdot a_n \bmod (11)$; se n é par e $-1 \cdot a_n \bmod (11)$; se n é ímpar.

Portanto,

$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + 10 \cdot a_1 + a_0 \equiv a_n \cdot (-1)^n + a_{n-1} \cdot (-1)^{n-1} + \cdots - a_1 + a_0 \bmod (11)$.

Exemplo 4.11: Verifique se o número 1327 divisível por 11.

Solução:

Sabemos que:

$1327 = 3 \cdot 10^4 + 1 \cdot 10^3 + 3 \cdot 10^2 + 2 \cdot 10 + 7.$

Por congruência modular temos:

$31327 \equiv 3 \cdot 10^4 + 1 \cdot 10^3 + 3 \cdot 10^2 + 2 \cdot 10 + 7 \ mod \ (11).$

Notemos ainda que:

Logo,

$31327 \equiv 3 \cdot 1 + 1 \cdot (-1) + 3 \cdot 1 + 2 \cdot (-1) + 7 \; mod \; (11)$.

$31327 \equiv 10 \; mod \; (11)$.

Portanto, 31327 não é divisível por 11.

Para determinar a forma genérica de divisibilidade por 11, considere um natural dado tal que:

$$N = a_n a_{n-1} a_{n-2} a_1 a_0 = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + 10 \cdot a_1 + a_0; \; n \in N$$

Portanto, percebemos que sempre que há um algarismo de ordem par, este será positivo e o algarismo de ordem ímpar será negativo.

Então, um número será divisível por 11 se a soma dos algarismos de ordem par, subtraída da soma dos algarismos de ordem ímpar, for um número divisível por 11.

Observação: As divisibilidades não citadas é porque simplesmente possuem de certa forma a mesma linha de raciocínio em suas demonstrações e, já são amplamente discutidas e conhecidas como por exemplo a divisibilidade por 6 que decorre da divisibilidade por 2 e por 3; a divisibilidade por 4 que é quando os dois últimos algarismos do número forma um número divisível por 4; a divisibilidade por 8, quando o número tem seus três últimos algarismos um número divisível por 8; a divisibilidade por 5 que, dizemos que um número ser divisível por 5 quando o mesmo termina em zero ou 5, por 10, quando termina em zero.

4.7. Aplicações no Cotidiano

Veremos a seguir aplicações de muita utilidade e atualmente com muita efetividade no mundo globalizado; situações que vão buscar na teoria dos números as ferramentas matemáticas para resolver importantes nuances reais; exemplos que contribuem essencialmente com o fito de controle e monitoramento de produtos e Serviços; até mesmo de pessoas como é o caso do CPF; elencamos abaixo então tais situações conforme (FRANCO, 2016).

4.7.1. Dígitos de Verificação

Os Digitos de verificação (DV) são números que estão sempre presentes no nosso dia-a-dia em Códigos de barras, CPF, RG, Números de Contas Bancárias, bilhetes emitidos para eventos artísticos, culturais entre outras sequências numéricas. Geralmente em uma sequência de números ele é o ultimo algarismo, exceto no caso do CPF que são dois dígitos de verificação. Eles servem para validar o código e evitar fraudes. Esse dígito pode variar de zero à nove ou ainda pode ser uma letra (no caso usam X) o que será explicado na sequência. A determinação do DV é uma aplicação de congruência modular, que pode facilmente ser compreendida e levada como apoio pedagógico para as aulas de matemática, até mesmo considerando séries mais iniciais.

4.7.2 Código de Barras

Normalmente ao comprar algum produto percebemos uma marca presente denominada código de barras. A vantagem das barras é que elas podem ser identificadas rapidamente, e sem risco de erros, por aparelhos decodificadores portáteis de leitura óptica, como os usados pelos caixas de supermercados. Mas o que realmente importa para identificar o produto é sua sequêncianumérica, que também pode ser digitada manualmente pelos operadores de caixa. O código de barras funciona como uma espécie de RG do produto. Como não existem duas pessoas com o mesmoRG, não existem dois produtos diferentes com o mesmo código. O interessante disso tudo é que o Código de Barras é gerado por uma matemática pura e pode ser utilizado como ferramenta no ensinode alguns tópicos de matemática na sala de aula (ESQUINCA. 2013). O código de barras UniversalProduct Code (UPC) ou European Article Number (EAN) nada mais é do que a representação gráfica da sequência de algarismos que vem impressa logo abaixo das barras. Este é um conjunto de normas comercial. Originalmente criado nos Estados Unidos em 1973 pela empresa Uniform Code Council(UCC) para auxiliar os mercados a aumentar a velocidade do processo de verificaçãona saída de produtos e melhorar o controle de inventário. Mais tarde, constatou-se a essência dessetipo de código e sua utilização foi estendida rapidamente para o Brasil em 1983. O Brasil deu um grande passo à frente de outros países da América Latina, aderindo ao sistema de código de barras na maioria das cidades e estados. Muitas empresas sentem a necessidade e a obrigação de adquiri-

los quando a produção aumenta e quando os códigos de barras são exigidos pelos varejistas. Com isso, a demanda e a adesão aos códigos de barras no Brasil vêm aumentando cada vez mais (PEREIRA DE SÁ. 2015). A EAN é a organização internacional que gerencia a distribuição dos códigos no mundo e tem uma representação no Brasil, porém existem várias formas de representar os códigos de barras nos diversos países. Enquanto os americanos usam uma sequência numérica de 12 dígitos (EAN12), os europeus optaram por um padrão com 13 (EAN13), que foi adotado no resto do mundo, inclusive no Brasil. Existem ainda outros tipos de códigos especiais, como o formado por 14 dígitos (EAN14), usado em caixas de papelão para informar a quantidade de produtos guardados e o de 8 dígitos (EAN8) utilizado quando a embalagem do produto é muito pequena. Vejamos como exemplo a imagem de um código de barras do sistema mais comum e utilizado no Brasil, o EAN-13, que usa 13 algarismos para cada produto:

Figura 1. Código de barras

Fonte: http://www.proteste.org.br/familia/nc/noticia/entenda-o-codigo-de-barras

As duplas de barras mais compridas são uma sinalização, fazem separação indicando que a seguir vem o código do produto. As barras e seus respectivos algarismos não ficam alinhados, por isso o número 7 vem antes das barras de sinalização. Os três primeiros números (789) é o registro nacional, que indicam que o produto foi cadastrado no Brasil, apesar de não, necessariamente, ter sido fabricado aqui. Cada país tem uma combinação própria. A da Argentina, por exemplo, é 779. A segunda sequência de números (8357) que pode variar de quatro a sete algarismos é a identificação da empresa fabricante (RG do fabricante). Esse número é fornecido pela EAN, que faz o controle para que não sejam distribuídos números iguais.

A terceira sequência (41001) identifica o produto em si. A numeração varia conforme o tipo, o tamanho, a quantidade, o peso e a embalagem do produto - um refrigerante em lata, por exemplo, tem uma sequência diferente de um refrigerante em garrafa. O último número (5) é um dígito verificador. Ao ler todo o código do produto, o computador faz um cálculo simples:

● Efetua ordenadamente da esquerda para a direita o produto de cada algarismo por 1 e 3 de forma alternada;

● A partir da soma desses produtos, calcula-se o resto da divisão pelo número 10;

● O resto encontrado será o DV do produto.

Se a leitura estiver correta, o resultado desse cálculo é igual ao do dígito verificador. O interessante para nós é que esse dígito verificador nada mais é do que uma simples aplicação de congruência modular. Observe o cálculo detalhado do procedimento descrito anteriormente para a figura acima.

A sequência dos 12 primeiros dígitos do código é 789835741001 que matematicamente pode ser escrita na forma: $a_1\, a_2\, a_3\, a_4\, a_5\, a_6\, a_7\, a_8\, a_9\, a_{10}\, a_{11} a_{12}$. Devemos multiplicá los, nessa ordem, pela base {1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3} e somar os produtos obtidos. Essa soma acrescida do algarismo a_{13} deve ser um múltiplo de 10, ou seja, o algarismo procurado é obtido da seguinte relação de congruência:

$$1 \cdot a_1 + 3a_2 + 1a_3 + 3a4 + 1a_5 + 3a_6 + 1a_7 + 3a8 + 1a_9 + 3a_{10} + 1a_{11} + 3a_{12} + a_{13} \equiv 0\ mod\ (10).$$

Efetuando os produtos do código de barras pela base de multiplicação, teremos:

$$1 \cdot 7 + 3 \cdot 8 + 1 \cdot 9 + 3 \cdot 8 + 1 \cdot 3 + 3 \cdot 5 + 1 \cdot 7 + 3 \cdot 4 + 1 \cdot 1 + 3 \cdot 0 + 1 \cdot 0 + 3 \cdot 1 + a_{13} \equiv 0\ mod\ (10).$$

Assim,

$$7 + 24 + 9 + 24 + 3 + 15 + 7 + 12 + 1 + 0 + 0 + 3 + a_{13} \equiv 0\ mod\ (10).$$

Então,

$$105 + a_{13} \equiv 0\ mod\ (10).$$

Somando (-105) a ambos os lados da congruência segue que:

$$a_{13} \equiv -105\ mod\ (10).$$

$$a_{13} \equiv 5\ mod\ (10).$$

Portanto o DV correspondente ao código de barras apresentado é 5, o qual se completa conforme a figura acima apresentada.

Logo,

$a_{13} \equiv 5 \mod (10)$.

Portanto o DV correspondente ao código de barras apresentado é 5, o qual se completa conforme a figura acima.

4.7.3. A Detecção de erros em um código de Barras

A teoria de códigos voltada aos dígitos verificadores não só analisa tipos de erros, como detecta e os corrige quando são mais comuns. Conforme o matemático Jacobus Koos, os erros mais comuns são chamados de erro único ou de transposição.

O erro único ou consistente ocorre em setenta e nove por cento dos casos e ele acontece por meio da troca de um dígito por outro (a por b). Neste caso, se o produto matricial não for múltiplo de 10, o erro será detectado possibilitando a correção.

Nos erros de transposição os algarismos são digitados com mudança de ordem dos dígitos consecutivos. Esses erros acontecem em onze por cento dos casos (ab por ba ou abc por cba). (LAGE , 2018).

Com base em um teorema consistente, demonstrado, podemos concluir que para detectar erros consistentes ou de transposição, um sistema de verificação de dígitos precisa ter um número primo como número do divisor, ou seja, *m* deve ser primo.Essa detecção de erros quando constatada, pode auxiliar até mesmo em trabalhos periciais, contra fraudes.

Percebe-se, com facilidade até, que nas situações mais específicas e talvez em que alguém menos pudesse acreditar que a matemática poderia está presente e utilizar-se de sua beleza para atuar e resolver uma situação, ela intercede e dignifica uma problemática bem real e contemporânea. Imaginemos, pois, esses acontecimentos, essas características, esses poder dessa magnífica ciência sendo bem externadas aos nossos estudantes, sem dúvida teríamos mais adesão, mais foco, mais interesse e consequentemente mais rendimento.

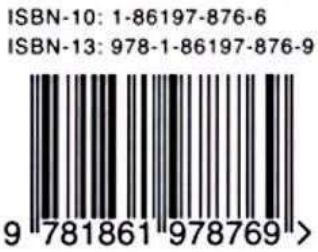
4.7.4. (ISBN)

Esse sistema foi criado nos anos 1960 e em linhas gerais tem o intuito de controle relacionado às obras em geral como (livros, CDs e outros trabalhos) dando uma identidade e padrão internacional e oficializado como norma; como se fosse o RG de cada obra; através de várias codificações relacionadas ao país, às distribuidoras e outros controles com o fito de dar individualização e caracterização aos mesmos. É bem mesmo no sentido de proteção e controle autoral. Pode ser notado na mais abaixo da contra – capa e com o código de barras.

Um dígito errado ou a troca de dígitos adjacentes são os dois erros mais comuns. A única garantia é que esses dois erros sempre serão detectados, de acordo com o método de cálculo de verificação de dígito do ISBN. Não sendo detectado o livro será editado com ISBN inválido.

Para a produção desses grupos de números, mais uma vez usaremos ferramentas da matemática para a confecção desses "RGs das obras", mais especificamente utilizando-se da congruência modulo m para resolver esta situação. Observemos as figuras seguintes:

Figura 2



Fonte:http://quezi.com/wp-content/uploads/2009/01/2175016522_ecbf98c8b4_o.jpg

Figura 3. Ilustra e evidencia a função de cada grupo de dígitos do código

Observando a figura 2, para o sistema ISBN-10 podemos verificar o dígito teste da seguinte maneira:

● Determinemos o resto da divisão por 11 tomando a base 10, tal que os números {10, 9, 8, 7, 6, 5, 4, 3, 2, 1}, nesta ordem sejam multiplicados termo a termo com os algarismos apresentados pelo sistema da esquerda para a direita;

● Efetuamos a soma dos 9 primeiros produtos;

● A diferença entre o que falta para o próximo múltiplo de 11 é o número procurado (termo a_{10}), ou seja, efetuando a seguinte congruência:

$$10a_1 + 9a_2 + 8a_3 + 7a_4 + 6a_5 + 5a_6 + 4a_7 + 3a_8 + 2a_9 + 1a_{10} \equiv 0 \; mod\,(11)$$

Observaç ã o : . a_{10} é substituído por X caso a congruência deixe resto 10.

Assim, no caso em questão o dígito de controle (6) é determinando efetuando o seguinte cálculo:

$10 \cdot 1 + 9 \cdot 8 + 8 \cdot 6 + 7 \cdot 1 + 6 \cdot 9 + 5 \cdot 7 + 4 \cdot 8 + 3 \cdot 7 + 2 \cdot 6 + a_{10} \equiv 0 \; mod\,(11)$, que equivalente a:

Logo,

$291 + a_{10} \equiv 0 \; mod\,(11)$

$a_{10} \equiv -291 \; mod\,(11)$

Portanto,

$a_{10} \equiv -5 \; mod\,(11) \Rightarrow a_{10} = 6$

Conclui-se que quando fazemos aplicações utilizando a congruência módulo “m”, estamos visando uma facilidade durante o processo de aplicação. Este tema nos ajuda bastante, pois se não fosse com essas aplicações seria bem difícil conseguir gerar números, ou códigos distintos para pessoas diferentes. Verificamos como são feitas algumas aplicações, utilizando a congruência módulo “m”, alguns cálculos foram mostrados, e chegados à conclusão dos dígitos criados. Mas não só foi a criação de números distintos apontados neste trabalho. Visamos, também, como são calculados os problemas de longas terminações e, se números fossem calculados de um por um, consumiria muito tempo até chegar à conclusão; conforme observamos em (Bitencourt, Santos, Silva, Villar e Oliveira, 2015).

4.7.5 Cadastro de Pessoas Físicas (CPF)

O CPF é outro exemplo importante, do nosso cotidiano; no Brasil, o cadastro de Pessoas Físicas junto à Receita Federal (CPF) é composto por 11 dígitos, dividido em dois blocos: um primeiro bloco com 9 algarismos e um segundo bloco com dois, que são os dígitos de controle. Para determinarmos os dígitos de controle, utilizamos também a congruência módulo m, conforme (Sá, 2007).Estes, assim como no ISBN e nos códigos de barra, são os dígitos de controle, que servem para garantir a autenticidade do documento.

A determinação desses dois dígitos de controle pode ser feita utilizando congruência modular. A diferença entre o CPF e os códigos de barras são que estes aqui tratados possuem o DV munido de dois algarismos, tal que o primeiro deles é o resultado de uma congruência módulo 11, obtido por uma operação dos nove primeiros, e o segundo é determinado incluindo-se o dígito encontrado e resolvendo novamente outra congruência módulo 11.

Suponhamos um CPF com os nove primeiros dígitos sendo 002007571. Primeiramente lembremos que todo CPF é um número da forma: $a1a2a3a4a5a6a7a8a9 - a10a11$.

A seguir, veja os procedimentos que dentre outras coisas utiliza a congruência modular para obter o primeiro dígito verificador e, em seguida, o segundo dígito verificador:

. ● Multiplicar da esquerda para direita os nove primeiros algarismos do CPF, pelos 9 números (1; 2; 3; 4; 5; 6; 7; 8; 9); nesta ordem;

- Somar os produtos obtidos;
- O dígito a_{10}, ser subtraído da soma obtida gerando um múltiplo de 11.

Observe o procedimento a seguir com a respectiva manipulação algébrica usando congruência modular:

Como,

$$1a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 - a_{10} \equiv 0 \, mod\,(11),$$

então:

$1a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 \equiv a_{10}\ mod\ (11)$.

Aplicando a propriedade simétrica teremos:

$a_{10} \equiv (1a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9)\ mod\ (11)$.

Desse modo:

$a_{10} \equiv (1 \cdot 0 + 2 \cdot 0 + 3 \cdot 2 + 4 \cdot 0 + 5 \cdot 0 + 6 \cdot 7 + 7 \cdot 5 + 8 \cdot 7 + 9.1)\ mod\ (11)$,

Logo,

$a_{10} \equiv 148\ mod\ (11)$

Assim,

$a_{10} \equiv 5\ mod\ (11)$

Portanto, $a_{10} \equiv 5\ mod\ (11)$

A determinação do segundo dígito verificador feita de maneira similar com a congruência módulo 11. No entanto, acrescentamos o dígito encontrado anteriormente estendendo agora a base de multiplicação para 10 algarismos, a começar do zero.

Assim teremos:

$0a_1 + 1a_2 + 2a_3 + 3a_4 + 4a_5 + 5a_6 + 6a_7 + 7a_8 + 8a_9 + 9a_{10} - a_{11} \equiv 0\ mod\ (11)$.

Logo,

$(0 \cdot 0 + 1 \cdot 0 + 2 \cdot 2 + 3 \cdot 0 + 4 \cdot 0 + 5 \cdot 7 + 6 \cdot 5 + 7 \cdot 7 + 8 \cdot 1 + 9 \cdot 1) - a_{11} \equiv 0\ mod\ (11)$.

Assim:

$0 \cdot 0 + 1 \cdot 0 + 2 \cdot 2 + 3 \cdot 0 + 4 \cdot 0 + 5 \cdot 7 + 6 \cdot 5 + 7 \cdot 7 + 8 \cdot 1 + 9 \cdot 1 \equiv a_{11}\ mod\ (11)$.

Portanto, $171 \equiv a_{11}\ mod\ (11)$. Aplicando a propriedade simétrica:

$a_{11} \equiv 171\ mod\ (11) \Rightarrow a_{11} \equiv 6\ mod\ (11)$; Logo, o segundo dígito de controle 6 e portanto concluimos que o CPF completo ser: 00200757156, conforme vimos em (FRANCO , 2016).

4.7.6. O Calendário

Há centenas de anos o homem se preocupa em registrar de forma empírica o passar do tempo. O dia e o ano, por exemplo, podem ser observados por qualquer pessoa, já que suas definições se baseiam em considerações astronômicas. No entanto, as definições de semana e mês são muito dependentes da cultura de cada povo ao longo da história.

Para a contagem do tempo desenvolveu-se o calendário, que é um sistema de contagem e agrupamento de dias, que visa atender principalmente às necessidades civis e religiosas de uma cultura, organizadas com o propósito de medir e registrar eventos ao longo de "grandes períodos" (PEREIRA DE SÁ. 2015).

Na atualidade existem aproximadamente 40 Calendários em uso no mundo, que podem ser classificados em três tipos:

● Solares: Baseados no movimento da Terra em torno do Sol; os meses não têm conexão com o movimento da Lua. (exemplo: Calendário Cristão e Gregoriano);

● Lunares: Baseados no movimento da Lua; o ano não tem conexão com o movimento da Terra em torno do Sol. (exemplo: Calendário Islâmico). Os meses de um Calendário Lunar, como o Islâmico, sistematicamente vão se afastando dos meses de um Calendário Solar, como o nosso;

● Lunisolares: Os anos estão relacionados com o movimento da Terra em torno do Sol e os meses com o movimento da Lua em torno da Terra; ou seja, nesse há a observação em relação à movimentação do sol e da lua. O Calendário Hebreu possui uma sequência de meses baseada nas fases da Lua, mas de tempos em tempos um mês inteiro é intercalado para o Calendário se manter em fase com o ano tropical.

Nos calendários solares, que são os mais utilizados, a unidade básica para a contagem do tempo é o dia, este que possui por sua vez 24 horas, divididas em duas etapas, que são intercaladas entre o nascer e o pôr do sol. O ano solar, também conhecido como ano trópico, é o período de tempo decorrido para completar um ciclo de estações (primavera, verão, outono e inverno), tendo a duração de aproximadamente 365 dias, 5 horas, 48 minutos e 47 segundos (365,2422 dias). Assim por excesso a cada quatro anos, as horas extra acumuladas são reunidas no dia 29 de Fevereiro, formando o ano bissexto, ou seja, o ano com 366 dias (BRASIL, 2009).

No Brasil utilizamos o Calendário Gregoriano, que deriva do calendário solar. Os anos são formados por meses constituídos por 30 ou 31 dias; com exceção de fevereiro constituído por 29 dias nos anos bissextos e 28 nos demais anos. No Calendário Gregoriano, existem 97 anos de 366 dias (que chamamos de bissextos) em cada período de 400 anos. Os anos bissextos são determinados pela seguinte regra (BRASIL. 2009):

I- Todo ano bissexto é divisível por 4;

II- Todo ano divisível por 4, exceto os centenários não divisíveis por 400, é bissexto;

Um exemplo pra melhor entender os critérios acima é comparar os anos 1900 e 2000. O primeiro não foi bissexto pois 1900 não é um número divisível por 400, o que já acontece com o ano de 2000.

Percebendo que há um grande envolto matemático ao se tratar de calendários, uma vez que é dividido de forma periódica e sequencial, por dias, semanas, meses e anos, apareceram em vários programas de televisão pessoas que dizem apresentar habilidades especiais para memorizar dias da semana de anos anteriores. Será que realmente são habilidades especiais ou facilidade em utilizar algoritmos?

Provavelmente a segunda resposta seria mais conveniente ao chamarmos de verdade. O calendário possui alguns elementos arbitrários onde podemos usar algoritmos com operações básicas de matemática para relacionar uma data estabelecida ao dia da semana em que ela se deu (OLIVEIRA. 2015). O procedimento envolvido nesses algoritmos é acessível para qualquer pessoa que saiba usar as quatro operações básicas. O desafio, na verdade, é criar uma sequência de passos que direcionem o exercício mental. Saber criar e lidar com algoritmos é interessante e pode ser útil no mundo informatizado de hoje.

Observemos também a relação de uma simples congruência modular com o calendário, referente ao mês de setembro de 2014.

Figura 4: Calendário 2014

Fonte: http://arterocha.blogspot.com.br/2013/11/calendario-mes-de-setembro-2014.html

Notemos que ao analisar a disposição dos dias no mês de setembro em relação congruência modulo m teremos:

Domingo- $n \equiv 0 \ mod\ (7)$;

Segunda – $n \equiv 1 \ mod\ (7)$;

Terça - $n \equiv 2 \ mod\ (7)$;

Quarta - $n \equiv 3 \ mod\ (7)$;

Quinta - $n \equiv 4 \ mod\ (7)$;

Sexta - $n \equiv 5 \ mod\ (7)$;

Sá bado- $n \equiv 6 \ mod\ (7)$.

Se quisermos, por exemplo, determinar em qual dia da semana foi 27 de setembro de2014, sem olhar no calendário, bastaria apenas sabermos a que classe de congruência, este pertenceria, módulo 7. Assim dividindo 27 por 7, resultaria quociente 3 e resto 6. Desse modo teriamos que $27 \equiv 6 \ mod(7)$, ou seja, tomando segunda-feira como dia 1(data inicial do mês) a classe de restos 6 pertenceria nesta sequência aos sábados. Logo dia 27 de setembro de 2014 foi um sábado (verifique figura 4).

O fato mais interessante nesta parte da aritmética que ela nos permite ainda verificar dias da semana de datas muito anteriores aos dias atuais. A história registra seus fatos, basicamente, pelas datas. Para entender como funciona tal procedimento faremos alguns exemplos retirados da video aula

37 do professor Fabio Henrique Teixeira de Souza , direcionada aos alunos da OBMEP e que trata de problemas com calendários.

> Exemplo 4.11: O ano de 2013, começou em uma terça-feira. Qual o dia da semana termina o referido ano?

Solução:

Primeiramente devemos observar que aqui é um caso geral onde o respectivo ano possui 365 dias, agrupados de 7 em 7 dias, que são as semanas. Neste caso ao dividir 365 por 7, obteremos 52 ciclos semanais completos e sobrar um dia. Sendo que cada ciclo inicia-se na terça-feira e termina na segunda, devemos acrescentar 1 dia ao próximo ciclo. Assim sendo o ú l ltimo dia do ano ser também uma terça-feira. Observe o cálculo:

Portanto,

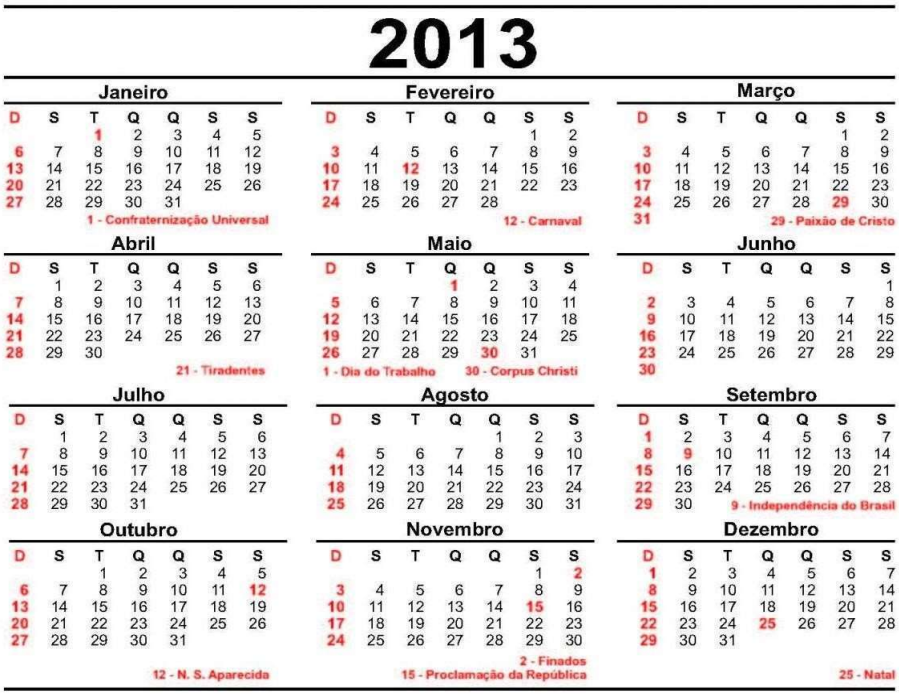
$365 \equiv a \ mod\ (7)$, onde *a é* o resto.

$365 \equiv 1 \ mod\ (7)$.

Observação: Em geral, exceto os anos bissextos, todos os anos começam e terminam no mesmo dia da semana.

A figura a seguir se trata da imagem de um calendário do ano de 2013. Faremos alguns exemplos para que possamos mostrar ao aluno que tendo apenas um ponto de partida, ou seja, uma data inicial, conseguimos determinar qualquer outra.

Figura 5: Calendário 2013



2013

Janeiro

D	S	T	Q	Q	S	S
		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		

1 - Confraternização Universal

Fevereiro

D	S	T	Q	Q	S	S
					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		

12 - Carnaval

Março

D	S	T	Q	Q	S	S
					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						

29 - Paixão de Cristo

Abril

D	S	T	Q	Q	S	S
	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				

21 - Tiradentes

Maio

D	S	T	Q	Q	S	S
			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	

1 - Dia do Trabalho 30 - Corpus Christi

Junho

D	S	T	Q	Q	S	S
						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						

Julho

D	S	T	Q	Q	S	S
	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			

Agosto

D	S	T	Q	Q	S	S
				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

Setembro

D	S	T	Q	Q	S	S
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					

9 - Independência do Brasil

Outubro

D	S	T	Q	Q	S	S
		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		

12 - N. S. Aparecida

Novembro

D	S	T	Q	Q	S	S
					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

2 - Finados
15 - Proclamação da República

Dezembro

D	S	T	Q	Q	S	S
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				

25 - Natal

Fonte:http://www.tatendoaqui.com/wp-content/uploads/2013/01/calendario-2013.jpg

Exemplo 4.12: Sabendo que o ano de 2013 começou em terça-feira, qual dia da semana aconteceu o 1º de janeiro de 2016?

Solução:

Como entre 2013 e 1º de janeiro de 2016 não hã nenhum ano bissexto, então, podemos raciocinar da seguinte maneira:

2013 começa e termina em uma terça-feira;

2014 começa e termina em uma quarta-feira;

2015 começa e termina em uma quinta-feira.

Então 1º de janeiro de 2016 será uma sexta-feira.

Exemplo 4.13: Sabendo que o 2013 começou em uma terça-feira, qual dia da semana será 31 de dezembro de 2016?

Solução:

Neste caso devemos levar em consideração que 2016 foi um ano bissexto, visto ser um número divisível por 4 e não terminado em 00. Assim não podemos dizer que terminou no mesmo dia da semana, pois agora o mês de fevereiro possui 29 dias. Poderíamos pela informaçã o do exemplo em questão acrescentar 1 dia o que nos forneceria domingo. Caso não tivéssemos esses dados, procederíamos da seguinte maneira:

2013, 2015 e 2015(365 dias)

2016(366 dias)

Então,

Logo, $365 + 365 + 365 + 366 \equiv a \bmod (7)$.

$1461 \equiv a \bmod 7$

Portanto, se o ciclo se inicia na terça-feira acrescentando 5 unidades a este ciclo teremos que o último dia de 2016 ser um sábado (verificação a partir da figura 5)

Contudo podemos dado uma data qualquer como ponto de partida, determinar qualquer outra anterior ou posterior a ela.

4.7.7 Curiosidades

Os anos terminados em 00 que não são divisíveis por 400, não são bissextos devido as chamadas de exceções seculares, fato que ocorre em função do tempo que a Terra leva para dar a volta em torno do Sol que é estimado (em aproximadamente 365 dias, 5 horas, 48 minutos e 46 segundos) e não exato, tal que essa pequena diferença de menos de 12 minutos poderia provocar erros a cada cerca de 100 a 120 anos. Contudo, a diferença de 46 segundos pode provocar novas revisões no calendário no ano 3000. Porém os astrônomos têm corrigido os relógios mundiais em 1 segundo em algumas passagens de ano, o que poderá dispensar tal revisão.

Existem 14 formatos diferentes para o calendário que usamos. Sete deles formados com início e fim no mesmo dia da semana (seg-seg), ou seja para anos não bissextos, e os outros 7 com início em um determinado dia e em um dia posterior da semana(ex: seg-ter).

Finalizo esclarecendo que as aplicações relativas ao assunto proposto, iniciando com a análise e surgimento dos números naturais, o contexto histórico desde as eras mais remotas e a evolução ao longo do tempo a partir das necessidades globais, passando pelos principais expoentes que contribuíram para esta dinamicidade até chegar aos fundamentos teóricos necessários para entender a matemática pura e simples presente, desde que examinada com zelo , contidas nessas preciosas situações do mundo real ao nosso redor, devem ser objetos de estratégias didáticas e prioritárias postas no currículo dos estudantes como ferramenta poderosa que mostra a necessidade de enfrentar tal conteúdo e que uma vez bem aplicada e bem considerada, desenvolve a mente para que se conquiste o letramento matemático.

Lembrando ainda que o desenvolvimento cognitivo não produz herança positiva apenas na matemática e sim em toda área do conhecimento humano; conclusão científica já bem consolidada.

A seguir, mostraremos algumas aplicações feitas em sala de aula com estudantes do ensino médio de uma Escola de Ensino Médio em Tempo Integral (EEMTI) de Fortaleza no Estado do Ceará.

5 APRENDIZAGEM BASEADA EM PROBLEMAS

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

O ensino de matemática e de outras ciências ainda é feito através de uma metodologia centrada na figura do professor como detentor do saber. Tal prática ainda se faz presente em escolas do Brasil e no mundo em pleno século XXI. Dessa observação não faremos críticas à essa postura, esse tipo de aula pode e deve acontecer; a crítica é feita quando essa estratégia é a única forma de tentar produzir com boa efetividade o binômio Ensino – Aprendizagem.

Uma alternativa para se superar o modelo de ensino centrado numa metodologia meramente reprodutiva é a Aprendizagem Baseada na Resolução de Problemas. Sem dúvidas é um método inovador, focado na aprendizagem e que vem ganhando espaço em todos os níveis de ensino no Brasil e no mundo. A primeira aplicação dessa metodologia se deu no ano de 1969 no curso de Ciências da Saúde da Universidade de McMaster University, no Canadá. Vários estudiosos do método tentaram conceituar essa temática, trazendo grandes contribuições acerca da abrangência, da importância, da relevância, etc., dessa temática.

Para BARROWS (1986) *apud* SOUZA e DOURADO (2015) é um método de aprendizagem que tem como base a utilização de problemas como ponto de partida para integrar e adquirir novos conhecimentos. Assim, a estratégia parte de um contexto e a partir daí é que se desenvolve a aprendizagem e a integração dessa com outras áreas do conhecimento.

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

LEITE E ESTEVES (2005) *apud SOUZA* e DOURADO (2015) entendem a inovação didática como um caminho que conduz o aluno para a aprendizagem. Nesse contexto, a relação entre o aluno e os problemas de uma área de conhecimento vai promovendo, gradativamente, uma evolução na aprendizagem desse aluno, visto que este desempenha um papel ativo através da investigação, da análise e da síntese do conhecimento investigado.

5.1 Aprendizagem Baseada em Problemas na Matemática

A proposta de se ensinar a matemática através da nova ideia didática ainda é desafiador no contexto de muitas escolas; isso requer formação de professores e, como consequência, recursos financeiros demandados para tal. A perspectiva é que a abordagem problematizadora pode motivar

os alunos a descobrir a beleza da matemática e que se possa mostrar que ela se faz presente em vários campos da atividade humana. Para SOUZA e DOURADO (2015) o problema pode ser modesto, mas se ele desafiar a curiosidade e colocar em jogo as faculdades inventivas, quem o resolver por seus próprios meios, experimentará a tensão e gozará do triunfo da descoberta. ”

A ideia de ensinar a matemática fora da “mesmice”, fora da “caixinha”, emite prazer ainda no planejamento e, na efetivação prática, produz uma sensação de realização maravilhosa e de otimização da auto estima tanto do discente quanto do docente; pode ser uma ferramenta capaz de motivar o raciocínio lógico dos alunos, através de uma ação motivadora, inovadora, exigindo do mesmo uma postura reflexiva diante da situação em que ele é exposto.

> Ainda de acordo com SOUZA e DOURADO (2015), um professor de Matemática tem, assim, uma grande oportunidade. Se ele preenche o tempo que lhe é concedido a exercitar seus alunos em operações rotineiras, aniquila o interesse e tolhe os desenvolvimentos intelectuais dos estudantes, desperdiçando, dessa maneira, a sua oportunidade. Mas se ele desafia a curiosidade dos alunos, apresentando-lhes problemas compatíveis com os conhecimentos destes e auxiliando-os por meio de indagações estimulantes, poderáincutir-lhes o gosto pelo raciocínio independente e proporcionar-lhes certos meios para alcançar este objetivo.

Percebe-se nas palavras de (SOUZA e DOURADO, 2015) que propor problemas aos alunos serve como um estimulante para que estes aprendam matemática. Desenvolver o gosto pelo raciocínio independente, como afirma o autor, contribuirá para que os alunos possam desenvolver novas aplicações que poderão trazer novos benefícios para toda a sociedade. Esses passos ajudam os alunos a desenvolver um ciclo de aprendizagem através da metodologia proposta pela ABP (Aprendizagem Baseada em Problemas), levando-os a se tornarem protagonistas da sua própria aprendizagem. A inovação proposta ajuda a ressignificar o processo ensino-aprendizagem, trazendo ideias e metodologias que colocam sempre o aluno como principal sujeito no processo, exercendo um protagonismo na aprendizagem, sem deixar de ressaltar que o professor sempre terá o seu grau de importância privilegiado; ele apenas não figura como principal componente do contexto; é um monitor que dar suporte mas, tem o seu papel fundamental.

Por isso, conforme SOUZA e DOURADO (2015) o trabalho em grupo destaca-se como uma forma de atividade em que o aluno valoriza a convivência e se dispõe a participar, de forma

criativa, do processo de aprendizagem, buscando criar espaços para o trabalho cooperativo, no qual todos são protagonistas, colaborando para uma aprendizagem mútua e integral.

5.2 Congruência Modular na Sala de Aula

O objetivo desse trabalho é dissertar sobre a inserção do tema aritmética modular no ensino básico, buscando técnica inovadora. Para tanto, foram aplicadas algumas questões relacionadas à temática estudantes da Escola de Ensino médio em Tempo Integral Visconde do Rio Branco, na cidadede Fortaleza, no estado do Ceará. Os alunos foram divididos em duplas e foram necessárias duas aulas de 50 minutos para cada aplicação de toda a atividade. O experimento consistia em resolver problemas de aritmética modular através da metodologia proposta pela Aprendizagem Baseada na Resolução de Problemas.As questões foram elaboradas de forma tal que os níveis de dificuldades fossem aumentando à medida que os alunos fossem avançando na resolução de cada questão. A adoção da metodologia proposta pela Aprendizagem Baseada na Resolução de Problemas foi importante na elaboração dessas questões visto que os problemas presentes nesse experimento fazem parte de um contexto social e tecnológico no qual todos nós estamos inseridos, facilitando assim a compreensão desse estudo. Os materiais necessários para a realização da atividade foram papel A4, lápis, caneta e borracha. Participaram da atividade 30 alunos entre 15 e 18 anos.

5.3 Resultados das Atividades

Na Escola em Tempo Integral à qual aplicamos as atividades, Inicialmente escolhemos uma amostra de alunos por turma; a escola possui 6 turmas de Ensino Médio, sendo três turmas de primeiro ano, duas turmas de segundo ano e uma turma de terceiro ano; escolhi 5 alunos por turma o que perfaz 30 alunos, separei – os em duplas , utilizando o critério de um aluno da dupla ter mais afinidades com os conteúdos e outro com um grau maior de dificuldade, daí, mostramos nuances teóricas da congruência modular, partindo de uma exposição no quadro; em seguida, fomos

colocando questões no quadro em grau crescente de dificuldade, desde a transformação da divisão do formato euclidiano ao formato de congruência modular; essa situação específica, os alunos acertaram de forma plena e não tiveram dificuldade, serviu para que ganhassem confiança e segurança para situações seguintes.

Em seguida, coloquei questões que contemplassem o uso das propriedades operatórias das congruências; que buscassem o resto de uma divisão por 7 por exemplo, de um número bastante elevado como 2^{100}, onde eles precisariam manipular os membros da congruência para se chegar ao resultado esperado.Nessa questão, o número de acertos foi bem menor, porém, percebi que os ânimos melhoraram exatamente nesse ponto , pois, os relatos foram relacionados à percepção clara sobre o que o conteúdo poderia lhes ser útil.

Na sequência, propus uma questão que lhes fizessem perceber que o conteúdo proposto realmente goza de um lugar de destaque quando debatemos sobre importância do que está sendo visto e seu liame com as situações reais e cotidianas, coloquei uma questão que mostrava a congruência modular na produção dos dígitos do CPF de uma pessoa e o sentido da variação de tais dígitos de acordo com a região em que o cidadão nasceu e demais variações que envolvem tal controle. Após a proposição dessa questão, acreditamos que se havia algum aluno que ainda estava com dúvida dos objetivos do trabalho e até onde estes poderiam lhe fornecer ganhos úteis de aprendizagem, nesse momento, não havia mais nenhum que não estivesse com uma postura de interesse e atenção devidos.

Conhecer os fundamentos e a razão de ser de cada número ali presente é de fundamental importância para compreender como a matemática se faz presente em todos os segmentos da sociedade pós-moderna. Nessa questão foram dadas uma tabela contendo os números correspondentes a cada estado pertencente as regiões fiscais do Brasil, disponibilizados pela Receita Federal. Também foram dados o algoritmo do cálculo dos dígitos verificadores de um CPF fictício, sendo dados os nove primeiros dígitos 571.567.878.

Cabia aos alunos identificar a região fiscal onde aquele documento foi emitido e calcular os seus dígitos verificadores. Aproximadamente 70% alunos conseguiram responder completamente à questão, sendo que os restantes conseguiram responder apenas parcialmente.

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

Uma outra questão desse trabalho aplicada aos alunos trouxe um instrumento muito utilizado nas transações comerciais e que desperta muitos questionamentos sobre a sua eficiência e funcionamento por parte das pessoas: o cartão de crédito. Na questão foi dado aos alunos alguns dígitos fictícios de cartão de crédito, sendo estes 4516 6497 3588 952; e foi pedido a eles que a partir desses dados, que identificassem a bandeira de cartão, e o seu dígito verificador, ver figura. Como já tinham feito algo semelhante no processo do cálculodo CPF, os alunos pareciam ter mais segurança para determinar o dígito verificador do cartão de crédito. Dentre os 30 alunos, 24 conseguiram responder às questões integralmente, o que corresponde a aproximadamente 80%.

Uma última questão a ser respondida pelos alunos estava relacionada à cifra de César. Método utilizado pelo imperador romano Júlio César para manter o sigilo das mensagens que ele enviava para os seus comandados do exército romano. É uma espécie de criptografia, se for considerada sua principal finalidade, que é proteger o sigilo das mensagens. A atividade consistia em transpor em três casas para frente as letras da frase “A MATEMÁTICA É O ALFABETO COM O QUAL DEUS ESCREVEU O UNIVERSO”, e escrevê-la de acordo com essa transposição. A última parte dessa atividade consistia em codificar numericamente essa atividade.Nessa atividade, cerca de 30 % dos alunos, o que corresponde a 9 alunos responderam essa questão.Outros 20 % responderam apenas parcialmente, sendo 6 o número desses alunos.

Nos encontros destinados aos cálculos em geral e resolução de problemas, percebemos um avanço no quesito *know-how*, no entanto, ao solicitar que produzissem as questões para serem resolvidas no quadro, notamos grande dificuldades na interpretação do enunciado do problema, ou seja, eles geralmente não entendiam o que estava sendo pedido; notamos que, uma vez entendida a pergunta do problema, eles avançavam em busca da solução, o que é natural concluir que a competência leitora deve também ser bem trabalhada.

Diante de tal constatação utilizamos a dinâmica de divisão em grupos, sempre colocando como liderança um aluno com maior nível de destaque na captação das ideias e esse utilizado como monitor; e, lógico, comigo sempre fazendo a boa gestão dos trabalhos e fazendo interceptações que ajudassem no crescimento; o mais interessante e gratificante no processo foi perceber o “brilho no olho” do(a) estudante, a vontade, que na minha opinião, superou qualquer expectativa.

Outro fato bem positivo e muito notório foi o quesito auto estima e, percebi que como consequência desta, outros ganhos no processo foram adquiridos até com um certo grau de facilidade.

Na verdade, antes mesmo de começar os trabalhos, percebi uma satisfação imensa pelo simples fato de estarmos os chamando em suas respectivas salas de aula e eles se sentindo respeitados, importantes e protagonistas de um processo. Ou seja, senti que foi aquela recepção de imaginar que alguém estava preocupado com eles e assim vi o semblante renovado florescendo grandemente mesmo antes da aplicação das ideais. A vontade de aprender, para assim aplicá-los em casa ou com grupos de amigos, favorecendo dessa forma, os cálculos de "cabeça". Destacamos ainda, que os problemas de aritmética dos restos, trabalhados em sala, despertou o "pensar" dos alunos. Enquanto professor da turma, percebemos que a aplicação da aritmética dos restos favoreceu o desenvolvimento do raciocínio lógico nos estudantes que participaram do projeto.

Mas, o que foi gratificante observar foi a auto estima elevada com que os alunos enfrentaram tais questões, com confiança e percebendo a utilidade real daquele instrumento; acreditamos que, os raciocínios desenvolvidos, além de os desenvolverem especificamente para a Matemática, os ajudam a desenvolver qualquer parte do conhecimento humano independente de ser algo relacionado à matemática ou não, pois, acima de tudo o legado deixado pela prática e pela proposta é o desenvolvimento da mente.

6 CONSIDERAÇÕES FINAIS

Neste trabalho exploramos a congruência modular como aplicação da divisão Euclidiana e divisibilidade e o suporte na resolução de problemas; houve também a intenção de mostrar ao aluno que de certa forma tínhamos a essência do conteúdo, na sua mais primitiva origem como agente que oferecesse instrumento real ao ensino – aprendizagem. Isto porque de um lado tínhamos a relevância do assunto e por outro, o insucesso de muitos alunos, principalmente, no ambiente de ensino médio, sobretudo em atividades e avaliações externas aplicadas no âmbito da escola pública, níveis estes que, em conformidade com as pesquisas feitas ao longo do tempo e no teor dos documentos oficiais, deveriam os alunos possuírem nesta fase de ensino, tais habilidades e competências; propusemos então a trabalhar com estudantes de primeiro, segundo e terceiros anos, e, nos colocando no lugar desses alunos, para entender e compartilhar angústias e nos colocarmos à disposição para a minimização desses anseios, apresentamos as ferramentas disponibilizadas pelas congruências modulares como amparo à facilitação da resolução de problemas; assim sendo,

entendemos contribuir com a amenização de tão grande deficiência encontrada pelos discentes em relação a “operações” elementares de matemática, pois entendemos que estes alunos já estudaram o conteúdo mencionado, pelo menos em sua base; refiro-me mesmo às operações básicas e seria uma revisão diferenciada; cabe também ao profissional, uma habilidade de percepção e de escuta das angústias dos alunos caso queiramos realmente ser um agente transformador; se colocar no lugar do outro aumenta a chance de sensibilização e uma consequente reflexão e produção de estratégias que possam contribuir com a melhoria do ensino - aprendizagem. Daí o próximo mandamento: Procure ler o semblante dos seus alunos; procure enxergar suas expectativas e suas dificuldades; ponha-se no lugar deles, (PÓLYA, 1987).

Diante de tais dificuldades, propusemos inicialmente trabalhar uma revisão dos números inteiros, números primos, seguida de divisores e múltiplos de números inteiros positivos, e então “puxamos” para tópicos mais complexos, da teoria dos números em que tais conteúdos estão conectados à operações básicas, mostrando seus significados e importâncias na prática.

Por fim, fazendo uma análise de todo o processo, entendemos que se faz necessário, sempre que possível, aplicação de projetos de intervenções pedagógicas inovadoras nas escolas; projetos estes pautados na aprendizagem ativa, isto é, projetos que levem os discentes a pensarem, a produzirem e que os conduzam ao letramento matemático.

REFERÊNCIAS

BITENCOURT, Larisse Araújo; SANTOS, Mayra Caroline Silva; SILVA, Stheffany Gabrielle da; VILLAR, Victor Brito e OLIVEIRA, Cassius Gomes de; 2015 , Artigo Sobre Aplicações de Congruência Módulo m.

BOYER, C. B. História da Matemática. 2a edição. [S.l.: s.n.], 1996.

BRASIL. Ministério da Educação. Secretaria de Educação a Distância. A matemática dos Calendários. Guia do professor. FNDE. Unicamp. 2009.

BRASIL. Ministério da Educação. Base nacional comum curricular. Brasília: MEC/SEB, 2017. Disponível em: http://basenacionalcomum.mec.gov.br/ . Acesso em 03 jan. 2023.

CARAÇA, B. d. J. Conceitos fundamentais da Matemática. [S.l.]: Gradiva, 2003.

COLOMBO, J.P.E. Aritmética: Códigos de Barras e outras Aplicações de Congruências. 2013. 63 f. Dissertação (Mestrado Profissional em Matemática em Rede nacional - PROFMAT). Universidade Federal de Mato Grosso do Sul. Campo Grande – MS.

COSTA, E. A.; SANTOS, R. A. Números: dos naturais aos reais. Proceedings do XXIII Semana do IME/UFG, p. 10, 2008. Disponível em: https://files.cercomp.ufg.br/weby/up/34/o/min_eudes_ronaldo.pdf – Acesso em 02 janeiro 2023.

FRANCO, Tânia R. Rodrigues (Dissertação de mestrado – Divisibilidade e congruências – Aplicações no Ensino Fundamental II) - UFG/GO – 2016. https://www.infoescola.com/matematica/numeros-primos/ - Acesso em 26 de abril de 2023

HEFEZ, Abramo. Aritmética. 1ª Edição. Rio de Janeiro: SBM,2013.

HEFEZ, A., Elementos de Aritmética, Coleção Textos Universitários. 2a edição. Rio de Janeiro: SBM, 2006.

IFRAH, G., Os números: história de uma grande invenção O Georges Ifrah: tradução de Stella Maria de Freitas Senra: revisão técnica: Antônio José Lopes, Jorge José de oliveira.11a edição. São Paulo: Globo, 2005.

LAGE, Francisca Daniella Andreu Simões Moraes, Um estudo de aritmética modular para a educação básica [manuscrito] / Francisca Daniella Andreu Simões Moraes Lage. - 2018. Universidade Federal de Ouro Preto.

LIMA, Abizai C. (Dissertação de mestrado – Aplicações de aritmética Modular na Educação Básica a partir da Resolução de Problemas – Universidade Estadual do Sudoeste da Bahia – Vitória da Conquista – 2019)

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

OBMEP: Banco de Questões. Rio de Janeiro: IMPA, 2010. Disponível em: . Consultado em: 05/08/2016. Pinto, H. Sistemas de Identificação com Algarismos de Controlo. Educação e Matemática No. 86 (Janeiro/Fevereiro). p. 19 a 21. 2006.

PEREIRA DE SÁ, I. A aritmética modular e suas aplicações no cotidiano. Disponível em: <www.magiadamatematica.com> Acesso em: 05 maio. 2023

RESENDE, MARILENE R. (Tese de Doutorado – Re-significando a disciplina teoria dos números na formação do professor de matemática na licenciatura. PUC/SP – 2007.

SOUZA, S.C e DOURADO, L. Aprendizagem Baseada em Problemas: Um Método de Aprendizagem Inovador para o Ensino Educativo. IFRN, 2015. Disponível em< http://www2.ifrn.edu.br/ojs/index.php/HOLOS/article/download/2880/1143 >. Acesso em abril de 2023.