SOCIEDADE BRASILEIRA DE MATEMÁTICA
FUNDAÇÃO UNIVERSIDADE FEDERAL DE RONDÔNIA
MESTRADO PROFISIONALEM MATEMÁTICAEM REDE NACIONAL

Guilherme Henrique Zangrando

UM ESTUDO SOBRE OS EXERCÍCIOS DE ARITMÉTICA NA OBMEP DE 2019/2020

PORTO VELHO
2022

Guilherme Henrique Zangrando

Um estudo sobre os exercícios de aritmética na OBMEP de 2019/2020

Trabalho de Conclusão apresentado ao Mestrado Profissional em Matemática em Rede Nacional – PROFMAT no Polo da Universidade Federal de Rondônia – UNIR, como requisito para obtenção de Mestre em Matemática Profissional.

Orientador: Prof. Dr. Tomás Daniel Menéndez Rodríguez.

PORTO VELHO

2022

Dados Internacionais de Catalogação na Publicação

Fundação Universidade Federal de Rondônia

Gerada automaticamente mediante informações fornecidas pelo(a) autor(a)

Z29e Zangrando, Guilherme Henrique.

Um estudo sobre os exercícios de aritmética na OBMEP de 2019/2020 / Guilherme Henrique Zangrando. -- Porto Velho, RO, 2022.

73 f.

Orientador(a): Prof. PhD Tomás Daniel Menéndez Rodríguez

Dissertação (Mestrado Profissional em Matemática) - Fundação Universidade Federal de Rondônia

1.Profmat. 2.Aritmética. 3.OBMEP. 4.Estudo. 5.2020. I. Rodríguez, Tomás Daniel Menéndez. II. Título.

CDU 511.1

Bibliotecário(a) Renata Cortinhas Bulhões CRB 11/1010

MINISTÉRIO DA EDUCAÇÃO
FUNDAÇÃO UNIVERSIDADE FEDERAL DE RONDÔNIA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

ATA DE DISSERTAÇÃO

ATA Nº 61

ATA DA SEXAGÉSIMA PRIMEIRA SESSÃO DE DEFESA DE DISSERTAÇÃO DE MESTRADO – PROFMAT/UNIR, POLO PORTO VELHO.

MESTRANDO: GUILHERME HENRIQUE ZANGRANDO

INÍCIO DO CURSO: março/2019

Aos oito dias do mês de abril de dois mil e vinte e dois, às nove horas e trinta minutos, por videoconferência no Google Meet, foi realizada a sessão de defesa de dissertação do mestrando **Guilherme Henrique Zangrando**, como requisito obrigatório estabelecido nos termos dos artigos 37, 41, 42 do Regimento Interno do PROFMAT/UNIR. A Comissão Examinadora, designada pelo Colegiado do Programa, foi composta pelos membros: Prof. Dr. Tomás Daniel Menéndez Rodrigues (orientador) - UNIR, Prof. Dr. Adeilton Fernandes da Costa (membro interno) - UNIR e Profa. Dra. Maria das Graças Viana de Souza (membra externa ao Programa) - UNIR, sob a presidência do primeiro, julgou o trabalho intitulado **"Um estudo sobre os exercícios de aritmética na OBMEP de 2019 /2020".** Após a defesa apresentada pelo mestrando e arguições pela Comissão, o trabalho foi considerado "APROVADO" e, em razão das recomendações dos membros da Comissão, o Senhor Presidente se comprometeu a orientar a sequência do processo da elaboração da versão final com a inclusão das recomendações realizadas. Nada mais havendo a tratar, foi encerrada a sessão e, para constar, foi lavrada a presente ATA, que vai assinada digitalmente pelos membros da Comissão Examinadora e o Mestrando.

Documento assinado eletronicamente por **TOMAS DANIEL MENENDEZ RODRIGUEZ**, **Presidente da Comissão**, em 08/04/2022, às 12:04, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **ADEILTON FERNANDES DA COSTA**, **Docente**, em 08/04/2022, às 12:05, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **MARIA DAS GRACAS VIANA DE SOUSA**, **Docente**, em 09/04/2022, às 20:09, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **guilherme henrique zangrando**, **Usuário Externo**, em 12/04/2022, às 13:04, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.unir.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0931875** e o código CRC **9A74D45C**.

"O Senhor Deus os livrou das suas aflições. Ele os tirou da escuridão, das trevas. E quebrou em pedaços as correntes que os prendiam.".

(Salmos 107;13)

DEDICATÓRIA

À minha mãe Zuleide, meu pai Pedro e minha irmã Aline. Amo vocês.

A todos os meus professores do PROFMAT.

AGRADECIMENTOS

A Deus por ser misericordioso e paciente comigo e me ter concedido saúde, sabedoria e persistência para que eu conseguisse realizar esse sonho.

Ao meu orientador Prof. Dr Daniel Menéndez Rodríguez pela urbanidade, cooperação e paciência no desenvolver desse trabalho.

A minha mãe Zuleide e meu pai Pedro por terem me educado e oportunizado os estudos.

Aos professores Ronaldo Chaves, Tomás Daniel, Marinaldo Rodrigues e Adeilton Costa pelos ensinamentos prestados, os quais não teria acesso se não fosse por esse programa de capacitação .

Aos meus amigos de curso pela imensa colaboração e espírito de união.

RESUMO

Este trabalho objetiva realizar um estudo comentado sobre os exercícios de aritmética aplicada na OBMEP , mostrando a resolução de vários exercícios e entendendo o padrão das provas ao relacioná-las com a aritmética, seus fundamentos e aplicações. Para elaborá-lo foi necessário a realização de pesquisas bibliográficas dos conteúdos relacionados a conceitos aritméticos e sobre suas aplicações na educação básica. Também se realizaram estudos acerca de divisibilidade, aritmética modular, teorema dos restos, dentre outros. No trabalho são apresentados exemplos e situações problema – informações essas que ajudam ao leitor na compreensão acerca da temática e instigam-no a tecer análises matemáticas. Contudo, o desfecho mais relevante desse trabalho é a busca pela apresentação da teoria de forma prática no âmbito escolar da educação básica.

Palavras-chave: OBMEP**.** Aritmética. Teorema dos restos. números primos.

ABSTRACT

This work aims to perform a commented study on the exercises of applied arithmetic's in OBMEP, showing the resolution of several exercises and understanding the pattern of the tests when relating them with the arithmetic, its foundations and applications. To elaborate it, it was necessary to conduct bibliographic research of the contents related to arithmetic concepts and about their applications in basic education. Studies were also conducted on divisibility, modular arithmetic, remains theorem, among others. In the work are presented examples and problem situations - information that helps the reader in understanding about the theme and encourage him to weave mathematical analyses. However, the most relevant outcome of this work is the search for the presentation of theory in a practical way in the school environment of basic education.

Keywords: OBMEP. arithmetic. Theorem of remains. prime numbers.

LISTA DE SIGLAS

OBMEP - Olimpíada Brasileira de Matemática das Escolas Públicas

OBM - Olímpiada Brasileira de Matemática.

SBM - Sociedade Brasileira de Matemática.

IMPA - Instituto de Matemática Pura e Aplicada.

BNCC - Base Nacional Comum Curricular.

MCTIC – Ministério da Ciência, Tecnologia, Inovações e Comunicações.

PIC - Programa de Iniciação Científica Junior.

POTI - Polos Olímpicos de Treinamento Intensivo.

CAPES - Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

CNPq - Conselho Nacional de Desenvolvimento Científico e Tecnológico.

PICME - Programa De Iniciação Científica e Mestrado.

LDBEN - Lei de Diretrizes e Bases da Educação Nacional.

PCNs - Parâmetros Curriculares Nacionais.

CONAE - Conferência Nacional de Educação.

PNAIC - Pacto Nacional pela Alfabetização na Idade Certa.

FNE - Fundo Nacional de Educação.

E.F. - Ensino Fundamental.

LISTA DE TABELAS

LISTA DE FIGURAS

SUMÁRIO

SEÇÃO 1. INTRODUÇÃO

Na primeira seção vamos abordar as informações pertinente a esse tipo de olimpíadas, Em seguida, na segunda seção, apresentamos definições e resultados relativos a conteúdos vistos no Ensino Básico ou Superior que auxiliarão na resolução das questões selecionadas, destacando-se a teoria sobre, números naturais, números inteiros, divisibilidade, algoritmo da divisão Euclidiana, Máximo Divisor Comum e Mínimo Múltiplo Comum(juntamente com suas aplicações), Números primos, sistema de numeração, teorema de Legendre, quadrados mágicos, congruências modulares e noções de equações Diofantinas. Por fim, iremos tratar as resoluções dos problemas de aritmética analisados desde o ano de 2005 até o ano de 2021 comparando as resoluções proposta da OBMEP com algumas soluções sugeridas propondo ao leitor ideias e comentários a serem vivenciados e observados em sala de aula a fim de ter um material de apoio para os professores de Matemática.

A Olimpíada Brasileira de Matemática das Escolas Públicas - OBMEP é um projeto nacional dirigido às escolas públicas e privadas brasileiras, realizado pelo Instituto de Matemática Pura e Aplicada - IMPA, com o apoio da Sociedade Brasileira de Matemática – SBM, e promovida com recursos do Ministério da Educação e do Ministério da Ciência, Tecnologia, Inovações e Comunicações – MCTIC.

Criada em 2005 para estimular o estudo da matemática e identificar talentos na área, a OBMEP tem como objetivos principais:

- Estimular e promover o estudo da Matemática;

- Contribuir para a melhoria da qualidade da educação básica, possibilitando que um maior número de alunos brasileiros possa ter acesso a material didático de qualidade;

- Identificar jovens talentos e incentivar seu ingresso em universidades, nas áreas científicas e tecnológicas;

- Incentivar o aperfeiçoamento dos professores das escolas públicas, contribuindo para a sua valorização profissional;

- Contribuir para a integração das escolas brasileiras com as universidades públicas, os institutos de pesquisa e com as sociedades científicas;

- Promover a inclusão social por meio da difusão do conhecimento.

O público-alvo da OBMEP é composto de alunos do 6º ano do Ensino Fundamental até último ano do Ensino Médio. Em 2019, mais de 18 milhões de alunos de participaram da olimpíada (OBM).

Um pouco sobre aritmética. O que é aritmética?

Surge por volta de 300 AC, em Alexandria, um tratado que se tornaria um dos marcos mais importantes da Matemática, Os Elementos de Euclides . Pouco se sabe sobre os dados biográficos deste grande matemático, tendo chegado a nós, através de sucessivas edições, este tratado composto por treze livros, onde se encontra sistematizada a maior parte do conhecimento matemático da época. Aparentemente, Euclides não criou muitos resultados, mas teve o mérito de estabelecer um padrão de apresentação e de rigor na Matemática jamais alcançado anteriormente, tido como o exemplo a ser seguido nos milênios que se sucederam. Dos treze livros de Os Elementos, dez versam sobre geometria e três, sobre aritmética. Nos três livros de aritmética, Livros VII, VIII e IX, Euclides desenvolve a teoria dos números naturais, sempre com uma visão geométrica (para ele, números representam segmentos e números ao quadrado representam áreas).

No Livro VII, são definidos os conceitos de divisibilidade, de número primo, de números perfeitos, de máximo divisor comum e de mínimo múltiplo comum, entre outros. No mesmo livro, além das definições acima, todas bem postas e até hoje utilizadas, encontra-se enunciada (sem demonstração) a divisão com resto de um número natural por outro, chamada divisão euclidiana. Com o uso iterado desta divisão, Euclides estabelece o algoritmo mais eficiente, até hoje conhecido, para o cálculo do máximo divisor comum de dois inteiros, chamado de Algoritmo de Euclides,. No Livro VIII, são estudadas propriedades de sequências de números em progressão geométrica. No Livro IX, Euclides mostra, de modo magistral, que a quantidade de números primos supera qualquer número dado; em outras palavras, existem infinitos números primos. Euclides também prova que todo número natural se escreve de modo essencialmente único como produto de números primos, resultado hoje chamado de Teorema

Fundamental da Aritmética. É também provado um resultado que dá uma condição necessária para que um número natural seja perfeito (Proposição 35 em Os Elementos). Após Euclides, a aritmética estagnou por cerca de 500 anos, ressuscitando com os trabalhos de Diofanto de Alexandria, que viveu por volta de 250 DC. A obra que Diofanto nos legou chama-se Aritmética e foi escrita em treze volumes, dos quais apenas sete nos chegaram. Trata-se do primeiro tratado de álgebra hoje conhecido, pois a abordagem de Diofanto era totalmente algébrica, não sendo revestida de nenhuma linguagem ou interpretação geométrica, como o faziam todos os seus predecessores. A maioria dos problemas estudados por Diofanto em Aritmética visava encontrar soluções em números racionais, muitas vezes contentando-se em encontrar apenas uma solução, de equações algébricas com uma ou várias incógnitas. Um dos problemas tratados por Diofanto era a resolução em números racionais, ou inteiros, da equação pitagórica $x^2 + y^2 = z^2$, chegando a descrever todas as suas soluções. Este problema teve o poder de inspirar o matemático francês Pierre Fermat mais de 1300 anos depois, traçando os rumos futuros que a Matemática iria tomar, como veremos mais adiante (ABRAMO HEFEZ)

1.1. Objetivo Geral

O trabalho tem como objetivo geral realizar um estudo comentado sobre os exercícios de aritmética aplicada na OBMEP, propiciando, para o público interessado na área, informações, comentários e resoluções alternativas sobre a importância da aritmética, usando como base as questões sobre o assunto, aplicadas na OBMEP 2019/2020.

1.2. Objetivos Específicos

A fim de conduzir o leitor ao desenvolvimento do tema, listam-se como objetivos específicos:

- Apresentar fundamentos teóricos e conceituais correlatos ao tema;
- Apresentar fundamentos teóricos e conceituais de aritmética;

- Abordar a aritmética aplicada na OBMEP 2019/2020;
- Apresentar aplicação da aritmética nas provas da OBMEP mostrando comentários, soluções práticas, alternativas e dinâmicas na resolução das questões da prova.
- Apresentar alguns teoremas da aritmética como ferramentas para resolver problemas da OBMEP;
- Mostrar a importância da aritmética nas provas de Olimpíadas de Matemática;
- Contribuir para o ensino-aprendizagem da aritmética na educação básica;

1.3. Justificativa e Estrutura

Os resultados das escolas públicas do Estado de Rondônia nas Olimpíadas de Matemática das Escolas Públicas – OBMEP são ainda bem abaixo do que gostaríamos, com muitas questões deixadas em branco pelos alunos que participam. É preciso criar inciativas por parte das escolas e seus professores de matemática para melhorar os conhecimentos sobre a matemática dos estudantes e assim obter melhores resultados na competição Na tentativa de contribuir neste sentido faz-se este trabalho onde se mostram outras soluções, sugerem-se métodos de ensino e adicionam-se comentários às respostas das questões, na tentativa de que este material, faça a função de mediador entre o professor e o estudo de exercícios de aritmética da OBMEP.

A educação é transformadora e melhora a vida do aluno e da sociedade como um todo. Essa melhoria passa por vestibulares, faculdades, concursos públicos e a OBMEP. Desde 2005 a OBMEP vem tentando transformar a forma como as pessoas veem a matemática, com diversas premiações: títulos, medalhas e bolsas de estudos. Com programas voltados desde a qualificação de professores, para que atuem juntamente às escolas, direcionando um treinamento que explore o potencial do aluno; até um programa que oferece aos estudantes medalhistas a oportunidade de cursar um mestrado juntamente com a graduação, com bolsa fornecida pela Capes

O principal trunfo da OBMEP (e de outras competições estudantis) veio a pouco tempo. A partir de 2018, as mais conceituadas instituições de Ensino Superior do país (Unicamp, USP, Unesp), passaram a ceder vagas à cursos específicos através dos resultados obtidos por alunos de escolas públicas e particulares na OBMEP e OBM, respectivamente. O aluno então, passou a ter uma ponte pra realizar o sonho de entrar em uma faculdade pública, pois ao invés de disputar com milhares de adolescentes, vagas nos mais concorridos vestibulares, tendo de se aprofundar em todas as disciplinas da grade curricular, agora poderia simplesmente se dedicar mais àquela que de fato tem interesse, ou facilidade.

O docente dispõe então, de uma ferramenta poderosa para incentivar seus alunos, e este trabalho tem o intuito de evidenciar como a tarefa de propor questões da OBMEP com a temática de aritmética, pode ser fácil, mesmo para o professor que antes não tinha tal hábito sendo que os livros didáticos não trazem conceitos mais profundos de aritmética, como por exemplo: aritmética modular, divisibilidade, Euler, equações diofantinas entre outros. Mostrando assim outras soluções, sugerindo métodos de ensino e adicionando comentários às questões, esse material, faz a função de mediador entre o professor e o estudo de exercícios de aritmética da OBMEP.

A pesquisa, segundo (PCN, 1999) e (PCN+, 2002) visa fomentar o conhecimento acadêmico científico-profissional em docentes do ensino médio, agregando seu repertório e cooperando para uma atuação educacional mais diversificada e em um contexto mais próximo dos alunos do ensino médio gerando assim um maior engajamento.

Além da pertinência temática e do exposto acima, podemos destacar o fato de no Banco de dissertações do PROFMAT haver poucas dissertações contendo no título o termo "ARITMÉTICA NA OBMEP", podendo ser um indicativo de escassez de trabalhos utilizando essa temática no âmbito do Mestrado Profissional em Rede.

TABELA 1 - QUANTIDADE DE REGISTROS CONTENDO A FERRAMENTA ESPECIFICADA NO TÍTULO DA TESE

Ferramenta	Registros localizados
ARITMÉTICA	103
OBMEP	66
ARITIMÉTICA - OBMEP	0

Fonte: Produzida pelo autor com base em pesquisas no banco de dissertações do PROFMAT[1]

[1] Disponível em: <https://www.profmat-sbm.org.br/dissertacoes/?polo=&titulo=&aluno=> Acessado em 08 ago. 2021.

Como são tão poucos os registros contendo a palavra “OBMEP” no título da dissertação, podemos listar alguns :

TABELA 2 - QUANTIDADE DE REGISTROS CONTENDO O TERMO OBMEP NO TÍTULO DA TESE

DATA DE DEFESA	ALUNO	TÍTULO DA DISSERTAÇÃO	INSTITUIÇÃO
31/03/2021	Waleff Mesquitas Leal	Resoluções de problemas de geometria no ensino médio: uma análise de erros em provas da OBMEP	EFMA
31/03/2021	Aline de Carvalho Silva	OBMEP na escola com instrumento de ensino e aprendizagem	UFPI
26/02/2021	Drielle Passos Alves	O portal OBMEP do saber como ferramenta de suporte para o ensino da geometria analítica	UFT
11/02/201	José Railon da Silva Dantas	Matemática discreta abordada nas questões e material da OBMEP	UFCG

Fonte: produzida pelo autor com base em pesquisas no banco de dissertações do PROFMAT .[2]

Desses registros (TABELA 2 – QUANTIDADE DE REGISTROS CONTENDO O TERMO OBMEP NO TÍTULO DA TESE) podemos destacar que nenhum abordou questões de aritmética , que é uma matéria muito importante nas aplicações do dia a dia. Sendo isso um fato controverso, visto que devido às suas características de fácil aprendizado e de aplicação e uso ágil, principalmente na solução de problemas numéricos, é indispensável para estudos na área da matemática. E por ser de grande relevância na prova da OBMEP, merece uma abordagem mais especial.

[2]Disponível em: <https://www.profmat-sbm.org.br/dissertacoes/?polo=&titulo=scilab&aluno=> Acessado em 08 ag. 2021.

Na **Seção 01**, é feita a introdução ao trabalho com apresentação dos objetivos, da justificativa e estrutura do trabalho. Na **Seção 02**, são apresentados os conceitos de aritmética, divisibilidade, módulos e seus fundamentos e conceitos. Em seguida abordamos os principais temas matemáticos relacionados aos objetivos traçados.

Em seguida na **Seção 03**, abordamos aspectos teóricos matemático do trabalho, aplicação dos conceitos na resolução de problemas da OBMEP, usando sempre maneiras didáticas e pratica para o mesmo. Posteriormente na **Seção 04**, realizam-se as considerações finais sobre o trabalho e conhecimento gerado, além de destacar a importância do PROFMAT.

SEÇÃO 2. OBMEP NA EDUCAÇÃO BRASILEIRA

Esta seção trata-se sobre a OBMEP e seu papel na educação matemática das escolas e seus benefícios e contribuições para a sociedade educacional .

A Olimpíada Brasileira de Matemática das Escolas Públicas - OBMEP é um projeto nacional dirigido às escolas públicas e privadas brasileiras, realizado pelo Instituto de Matemática Pura e Aplicada - IMPA, com o apoio da Sociedade Brasileira de Matemática – SBM, e promovida com recursos do Ministério da Educação e do Ministério da Ciência, Tecnologia, Inovações e Comunicações – MCTIC.

As olimpíadas seguem a BNCC, e constrói sua prova e seus exercícios em cima dos parâmetros curriculares nacionais, respeitando em cada nível de prova o assunto visto e ensinado em cada ano da educação básica, mantendo uma coerência da sua prova os assuntos ensinados (BRASIL,2017,p.43)

2.1. Impactos da OBMEP na educação

Os sucessivos recordes de participação em cada ano subsequente fazem da OBMEP a maior competição de matemática do mundo, em quantitativo de estudantes escritos. É importante salientar que grande parte desses números, deve-se ao fato de que cada escola participante tem seus alunos automaticamente inscritos. Em 2010 a OBMEP atingiu o seu número máximo de candidatos inscritos para realizar esse exame, foi um total de 19.665.928 estudantes. A olimpíada é realizada pelo ministério da Educação e da Ciência e Tecnologia e pelo Instituto de Matemática Pura e Aplicada (IMPA). Conta ainda com o apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) e da Sociedade Brasileira de Matemática (SBM).

O ensino da Matemática pode de certa forma se tornar mais atrativo quando é aplicado a uma realidade mais próxima do estudante, motivando-o e desafiando-o a interpretar e resolver situações problemas. Jogos, desafios e gincanas podem ser considerados como exemplos e metodologias no ensino da Matemática. Nesse aspecto, as olimpíadas de Matemática ganham um destaque no Ensino Básico e vêm a cada ano crescendo no Brasil. Através das olimpíadas os estudantes podem se sentir mais instigados a desenvolver um raciocínio lógico matemático surpreendente, assim pode ser possível filtrar os candidatos com grandes habilidades nessa disciplina. As olimpíadas de Matemática podem ser muito importante na motivação de aprendizagem e incentivo ao raciocínio lógico usado em problemas interessantes e aplicáveis ao cotidiano dos estudantes.

Quase sempre é necessário uma boa estratégia de solucionar um determinado problema. É onde entra a criatividade e experiência do professor para tornar o conteúdo bem aceito pelos estudantes. É possível que o professor consiga motivar os seus estudantes a gostarem mais de Matemática usando problemas interessantes na concepção do aluno, pois para muitos deles a Matemática não é a disciplina preferida e sim, uma das mais difíceis, mas ao terem contato com os problemas mais difíceis de aritmética das provas de Olimpíadas Brasileira de Matemática nas Escolas Públicas (OBMEP), o estudante pode ficar curioso e despertar uma maior interação com os colegas e professor.

Um dos objetivos desse trabalho é fazer uma análise que sirva para uma elaboração de material por parte dos professores atribuindo um suporte a mais para estudar e discutir em sala de aula as questões de aritmética da Olimpíadas Brasileiras de Matemática das Escolas Públicas desde o ano de 2005 até 2021. A importância desse material consiste em poder ser usado como banco de questões para que o professor otimize seu tempo elaborando aulas sobre esse tema.

Inicialmente quando foi definido o tema para esse trabalho de conclusão de curso, foi feita uma análise em todas as questões da primeira fase OBMEP de 2005 até 2021. Foram várias provas analisadas nas quais eram compostas por 20 questões no total, de diversos conteúdos da grade curricular de Matemática, mas em média apareciam entre 2 ou 3 questões de aritmética em cada ano. Essas questões foram encontradas no site oficial das olimpíadas brasileira de Matemática nas escolas públicas (OBMEP, 2021). Em seguida, buscou-se resolver cada problema sem verificar as respostas disponibilizadas no site da OBMEP. Posteriormente, comparou-se as respostas obtidas e analisou-se quais conteúdos poderiam ser contemplados em cada questão selecionada. Por fim, pensou-se em propor atividades e/ou abordagem baseadas em cada uma dessas questões que pudessem ser aproveitadas pelo professor em sala de aula.

2.2. Cronologia sobre as Olimpíadas de Matemática

Segue a baixo algumas mudanças sofridas pela OBM desde 1997 em ordem cronológica.(OBM,)[3]

- **1997** Criação da primeira Olimpíada Brasileira de Matemática;

- **1991**-divisão das olimpíadas em 2 níveis de dificuldade, onde o critério dessa divisão seria a idade ou escolaridade. O nível Júnior criado para alunos completando no máximo 15 anos em 1991 e uma segunda categoria chamada de nível sênior para alunos cursando o ensino médio;

- **1992** - Divisão em 2 fases de exame, sendo a primeira fase com 25 questões de múltipla escolha. Já a segunda fase sendo avaliada em 2 dias contendo 3 questões discursiva sem cada dia.

- **1998** - Nesse momento o nivelamento começa a ser separado por séries de ensino, como nos dias de hoje. Então, no nível I se submetem a prova estudantes do 6ºe 7ºano do ensino fundamental. no nível II se submetem a prova estudantes do 8º e 9º ano do ensino fundamental. Por fim, no nível III se submetem a prova estudantes do ensino médio. Nesse ano, também foram definidas três fases de provas, sendo na primeira fase com 20 ou 25 questões de múltipla escolha.

- **1999**- Aprovado nível II passa a ser realizada em dois dias.

- **2001** -É criado o nível universitário, com duas fases. Essa modalidade é destinada aos estudantes de graduação em qualquer curso superior e em qualquer período. Basta apenas que os interessados entrem no site oficial e façam suas inscrições.

---

[3] Disponível em: <https://www.obmep.org.br>.

- **2017** - A OBM se integra à Olimpíada Brasileira de Matemática nas Escolas Públicas (OBMEP), realizando apenas a fase única para os níveis I, II e III. Mantendo o nível universitário realizado em duas fases.

- **2018-2019** Estudantes premiados pela OBM ou OBMEP nos anos de 2017 e 2018 puderam se inscrever em um novo processo de ingresso ao ensino superior na Universidade Estadual de Campinas (UNICAMP). Dos 76 estudantes que garantiram vaga na graduação da UNICAMP por meio de uma nova modalidade de inserção ao Ensino Superior, destinada a premiados em competições de conhecimentos, 23 são medalhistas de ouro, prata ou bronze na OBMEP e na OBM.

SEÇÃO 3. ARITMÉTICA E SEUS FUNDAMENTOS

Nesta seção serão abordadas definições e propriedades elementares referentes à relação de aritmética no conjunto dos números inteiros. Os conteúdos apresentados nesta seção foram extraídos de " HEFEZ, A. a*ritmética,(Coleção Profmat)*. Rio de Janeiro: SBM, 2014 "

3.1. Divisibilidade

Dados dois números inteiros a e b, com $b \neq 0$, diremos que b divide a, escrevendo $b \mid a$ quando existir c tal que $a = bc$. Neste caso, diremos também que a **divisível** por b, que b é **divisor** de a ou ainda que a é um **múltiplo** de b.

Assim,

$b \mid a \Leftrightarrow a = bc$ para algum $c \in \mathbb{Z}$.

Caso b não divida a, indicaremos por $b \nmid a$. Por exemplo: $4|16$, $-7|28$ e $5 \nmid 13$.

Para um número inteiro a, indicaremos seu conjunto de divisores por D_a e para $a \neq 0$, denotaremos seu conjunto de múltiplos positivos por M_a, ou seja, $D_a = \{n \in N : n|a\}$ e $M_a = \{n \in N\colon a|n\}$

É claro que $D_a = D_{-a}$ e $M_a = M_{-a}$ (NETO,2014,P.55)

Teorema 3.1.1 *Quaisquer que sejam* a,b,c e $d \in \mathbb{Z}$*, temos*

$i)$ $a|a$.

$ii)$ Se $a|b$ e $b|c$, então $a|c$.

$iii)$ Se $a|b$ e $c|d$ então $ac|bd$.

$iv)$ Se $a|b$ e $a|c$, então $a|(b + c)$ e $a|(b - c)$.

$v)$ Se $a|b$ e $a|c$, então $a|(mb + nc)$ $\forall$ $m,n \in \mathbb{Z}$.

Demonstração.

i) Note que podemos escrever $a \cdot 1 = a$, logo, $a|a$.

ii) Se $a|b$ e $b|c$, então existem q_1 e $q_2 \in \mathbb{Z}$ tais que $b = aq_1$ e $c = bq_2$. Substituindo o valor de b em c obtemos $c = a(q_1q_2)$, ou seja, $a|c$.

iii) Temos que $b = aq_1$ e $d = cq_2$. Multiplicando membro a membro, obtemos $bd = ac(q_1q_2)$, isto é, $ac|bd$.

iv) Temos que $b = aq_1$ e $d = cq_2$. Assim, dados inteiros m e n temos $mb = amq_1$ e $nc = naq_2$, somando membro a membro obtemos $mb + nc = a(mq_1 + nq_2)$ e, portanto $a|(mb + nc)$.

3.2. Divisão Euclidiana

Axioma 3.2.1. (Princípio da Boa Ordenação – PBO) Se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então ele possui um menor elemento. Como todo subconjunto não vazio de $\mathbb{N}$ é limitado inferiormente, então para o conjunto dos números naturais, o PBO se reduz à afirmação: todo subconjunto não vazio S de $\mathbb{N}$ possui um menor elemento.

Proposição 3.2.2. (Propriedade Arquimediana) Se a e b são números naturais, então existe um número natural n tal que $na \geq b$.

Demonstração. Suponha por absurdo que a afirmação não seja verdadeira, assim para todo natural n, $na < b$. Logo, o conjunto $S = \{b - na: n \in \mathbb{N}\}$ é formado apenas por números naturais. Assim, pelo Princípio da Boa Ordenação, S possui elemento mínimo, digamos $m = min(S)$. Como $m \in S$, existe $n_0 \in \mathbb{N}$ tal que $m = b - n_0a$. Por outro lado, o elemento $m1 = b - (n_0 + 1)a$ pertence a S, pois S contém todos os elementos dessa forma. Além disso, $m1 = b - (n_0 + 1)a = b - n_0a - a = m - a < m$, pois $a > 0$. Assim, $m1 \in S$ e $m1 < m$, o que contraria o fato de m ser o menor elemento de S.

Teorema 3.2.1. Dados a e b dois números inteiros com $b \neq 0$. Existem dois únicos números inteiros q e r tais que $a = bq + r$, com $0 \leq r < |b|$

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

Existência:

Pela propriedade Arquimediana, existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$, logo $a - nb > 0$, o que mostra que S é não vazio. O conjunto S é limitado inferiormente por *0*, logo, pelo Princípio da Boa Ordenação, temos que S possui um menor elemento r. Suponhamos então que $r = a - bq$. Sabemos que $r \geq 0$. Vamos mostrar que $r < |b|$. Suponhamos por absurdo que $r \geq |b|$. Portanto, existe $s \in N\cup\{0\}$ tal que $r = |b| + s$, logo $0 \leq s < r$. Mas isso contradiz o fato de r ser o menor elemento de S, pois $s = a - (q \pm 1)b$, com $s < r$.

Unicidade:

Suponha que $a = bq + r = bq' + r'$, onde $q, q', r, r' \in Z$, $0 \leq r < |b|$ e $0 \leq r' < |b|$. Assim, temos que $-|b| < -r \leq r' - r \leq r' < |b|$. Logo, $|r' - r| < |b|$. Por outro lado, $b(q - q') = r' - r$, o que implica que $|b||q - q'| = |r' - r| < |b|$, o que só é possível se $q = q'$ e consequentemente, $r = r'$.

Exemplo:

Determine o quociente e o resto da divisão de 41 por 7 e o resto da divisão de −1243 e −4.

Solução:

Como $41 = 7.5 + 6$ e $6 < 7$, então $q = 5$ e $r = 6$.

Para −1243 e −4, efetuamos a divisão natural de 1243 por 4. Posteriormente manipulamos a expressão de forma conveniente. Assim, como $1243 = 4.310 + 3$, então $-1243 = 310\cdot(-4) - 3 = 310\cdot(-4) - 3 - 4 + 4 = (-4)\cdot(310 + 1) + 1 = (-4) \cdot 311 + 1$, onde $q = 311$ e $r = 1$

3.3. Sistemas de Numeração

Desde os tempos antigos, sabe-se que a forma de representar números surgiu como um modo de contagem de animais ou de quaisquer bens. Para isso, é muito comum o uso de símbolos para designar quantidades, os quais eram inscritos em paus, tábuas, pedras , etc (BOYER, 1991).

Quando um número natural é formado pelos algarismos 0,1,2,3,4,5,6,7,8 e 9, dizemos que ele é escrito na *representação decimal.* Por exemplo, o número $a = 284301$ está na representação decimal, o qual pode ser escrito da seguinte forma:

$a = 2\cdot10^5 + 8\cdot10^4 + 4\cdot10^3 + 3\cdot10^2 + 0\cdot10 + 1$

Teoricamente, entretanto, poderíamos escolher uma base de numeração arbitrária, como demonstraremos a seguir:

Teorema 3.3.1. Dados $a,b \in N$, com $b > 1$, existem únicos números naturais $r_0, r_1,..., r_n$ tais que $0 \leq r_i \leq b - 1$, $0 \leq i \leq n$, e satisfazendo

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

$$a = (r_n c_{n-1} ... r_1 r_0)_b,$$

para fazer referência a esta. Demonstração. Apliquemos sucessivamente a divisão euclidiana como segue:

$$a = bq_0 + r_0, \ \ r_0 < b,$$

$$q_0 = bq_1 + r_1, r_1 < b,$$

$$q_1 = bq_2 + r_2, r_2 < b,$$

$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

$$q_{j-1} = bq_j + r_j \ , \quad r_j < b,$$

e assim por diante. Como $a > q_0 > q_1 > q_2 > \cdot \cdot \cdot > q_{j-1}$, para algum $j = n$ deveremos ter que $q_{n-1} < b$. Logo, $q_j = 0$ para todo $j \geq n$, assim como $r_j = 0$ para todo $j \geq n + 1$. Das igualdades acima, para $1 \leq j \leq n$, tem-se

$$a = bq_0 + r_0,$$

$$bq_0 = b^2 q_1 + br_1,$$

$$b^2 q_1 = b^2 q_2 + b^2 r_2, (*)$$

$$\vdots \vdots \vdots \vdots$$

$$b^{n-1} q_{n-2} = b^n q_n + b^{n-1} q_{n-1}$$

$$b^n q_{n-2} = b^{n-1} q_{n-1} + b^n r_n.$$

Efetuando a soma de todas as igualdades em $(*)$ obtemos

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

A unicidade dos números r_i vem da unicidade dos restos na divisão euclidiana.

3.4. Máximo Divisor Comum

Definição 3.4.1. Sejam a e b inteiros diferentes de zero. O máximo divisor comum (mdc) entre a e b é o número d que satisfaz as seguintes condições:

i) d é um divisor comum de a e b, isto é, $d|a$ e $d|b$;

ii) Se c é um divisor comum de a e b, isto é, $c|a$ e $c|b$, então $c|d$.

Assim, denotamos o mdc entre a e b por $d = mdc(a,b)$ ou $d = (a,b)$. Se $(a,b) = 1$, então dizemos que a e b são primos entre si ou relativamente primos.

Exemplo: Temos que os divisores de 18 são $D_{18} = \{1, 2, 3, 6, 9, 18\}$ e os divisores de 12 são $D_{12} = \{1,2,3,4,6,12\}$. Assim o $mdc(12,18) = mdc(18,12) = 6$. Por outro lado, os divisores de 4 são $D_4 = \{1,2,4\}$ e os divisores de 15 são $D_{15} = \{1,3,5\ 15\}$, logo o $mdc(4,15) = 1$, assim os números 4 e 15 são primos entre si.

Observação: Dado um número inteiro b não nulo, temos:

$mdc(0,b) = |b|$;

$mdc(1,b) = 1$;

$mdc(b,b) = |b|$.

Teorema 3.4.2 (Teorema de Bachet-Bézout). Se d é o máximo divisor comum de a e b, então existem números inteiros x_0 e y_0 tais que $d = \text{mdc}(a,b) = ax_0 + by_0$.

Demonstração.

Dados inteiros a e b, com $b \neq 0$. Considere o conjunto $I(a,b)=\{\ ax+by : x,y \in \mathbb{Z}\}$. É claro que existe em $I(a, b)$ um inteiro positivo. De fato, $|b| \in I(a, b)$. Seja $d = ax_0 + by_0$ o menor inteiro positivo em $I(a, b)$.

Afirmação. d divide todo inteiro $n \in I(a, b)$.

Dado $n = ax_1 + by_1 \in I(a, b)$, sejam $q, r \in \mathbb{Z}$ tais que $n = qd + r$ com $0 \leq r < d$. Temos então $n - qd = a(x_1 - qx_0) + b(y_1 - qy_0) = r \in I(a, b)$, de modo que, como d é o menor inteiro positivo em $I(a, b)$, obrigatoriamente $r = 0$.

Agora, como a, $b \in I(a, b)$ (basta escolher $(x, y) = (1, 0)$ e $(x, y) = (0, 1)$, respectivamente), temos que d divide a e b. Logo, $d \leq mdc(a, b)$.

Por outro lado, $mdc(a, b)$ divide a e b, de modo que $mdc(a, b)$ divide d. Portanto, $mdc(a, b) \leq d$ e, consequentemente, $mdc(a, b) = d$.

Exemplo: $mdc(18,4) = 2 = 1 \cdot 18 + (-4) \cdot 4 = (-1) \cdot 18 + 5 \cdot 4$

3.5 Algoritmo de Euclides

Apesar de conhecermos propriedades teóricas do máximo divisor comum entre dois inteiros, para encontrar seu respectivo mdc não é uma tarefa das mais fáceis, para isso utilizaremos de um método descoberto por Euclides, chamado de Algoritmo de Euclides (BOYER, 1991).

Lema 3.5.1 (Lema de Euclides). Se $a = bq + r$, então $mdc(a,b) = mdc(b,r)$.

Demonstração: Basta mostrar que $D_a \cap D_b = D_b \cap D_r$, pois sendo estes conjuntos iguais seus máximos também os serão. Se $d \in D_a \cap D_b$, então $d|a$ e $d|b$, mas como $r = a - qb$, segue que $d|r$ e, por isso, $d \in D_b \cap D_r$. Por outro lado, se $d \in D_b \cap D_r$, então $d|b$ e $d|r$, de modo que $d|bq + r = a$, isto é, $d \in D_a \cap D_b$. Logo $D_a \cap D_b = D_b \cap D_r$ e, portanto, $mdc\ (a,b) = mdc(b,r)$.

Exemplo: Como $56 = 4.7 + 28$, então $mdc(56,4) = mdc(4,28) = 4$ e $mdc(56,7) = mdc(7,28) = 7$.

Como podemos observar, o resultado do Lema de Euclides é válido mesmo que r não seja o resto da divisão de a por b. No entanto, para o **Algoritmo de Euclides**, vamos assim considerar de modo a estabelecer uma sequência de restos estritamente decrescente de inteiros não negativos.

Consideremos os inteiros a e b, com $a > b > 0$. Logo, pela Divisão Euclidiana, obtemos o seguinte:

$$a=bq_1+r_1, \text{ com } 0\leq r_1<b.$$

Pelo **Lema 3. 5.2**, temos que $mdc(a,b) = mdc(b,r_1)$. Assim vamos considerar dois casos:

a) Se $r_1 = 0$, teremos:

$mdc(a,b) = mdc(b,r1) = mdc(b,0) = b$.

b) Se $r_1\neq 0$, em tal caso, iremos efetuar a divisão de b por r_1, daí segue que:

$$b= r_1q_2+ r_2, \text{ com } 0\leq r_2< r_1.$$

Mais uma vez teremos que analisar duas possibilidades:

c) Se $r_2 = 0$, teremos:

$$mdc(a, b) = mdc(b, r_1) = mdc(r_1, r_2) = mdc(r_1, 0) = r_1$$

d) Se $r_2 \neq 0$, em tal caso, iremos efetuar a divisão de r_1 por r_2, daí segue que:

$$r_1 = r_2q_3 + r_3, \text{ com } 0 \leq r_3 < r_2.$$

Mais uma vez procedendo como antes,

$$mdc(a, b) = mdc(b, r1) = mdc\ (r_1, r_2) = mdc(r_2, r_3),$$

e assim sucessivamente.

Continuamos com o procedimento até obtermos um resto nulo, pois caso isso não ocorra, teríamos uma sequência infinita de números naturais $b > r_1 > r_2 > \cdots > 0$. Assim, para algum índice n, temos que $r_{n-1} \neq 0$ e $r_{n+1} = 0$, o que implica que:

$$mdc(a, b) = mdc(b, r_1) = = mdc(r_n, r_{n-1}) = mdc(r_n, 0) = r_n.$$

Portanto, o último resto não nulo r_n é o mdc de a e b.

Podemos sintetizar o Algoritmo de Euclides através do seguinte procedimento prático:

Efetuamos a divisão de a e b, com $a > b$, em seguida efetuamos a divisão de b pelo primeiro resto obtido (r_1), posteriormente dividimos r_1 pelo próximo resto (r_2) e assim sucessivamente até encontrarmos um resto nulo. Daí o último resto não nulo será o $mdc(a, b)$.

	q_1	q_2	q_3	$\cdots$	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	$\cdots$	r_{n-2}	r_{n-1}	$r_n = (a,b)$
r_1	r_2	r_3	r_4	$\cdots$	r_n		

Exemplo: Calcule o mdc de 372 e 162:

Pelo algoritmo de Euclides temos:

$$372 = 162 \cdot 2 + 48 \quad 162 = 48 \cdot 3 + 18 \quad 48 = 18 \cdot 2 + 12 \quad 18 = 12 \cdot 1 + 6 \quad 12 = 6 \cdot 2 + 0$$

Assim, o $mdc(372, 162) = 6$

Pelo processo prático teremos:

	2	3	2	1	2
372	162	48	18	12	**6**
48	18	12	6	0	

Assim, o $mdc(372,162) = 6$.

3.6. Mínimo Múltiplo Comum

Definição 3.6.1. *Dados inteiros a e b diferentes de zero. Diremos que o número* $m \in \mathbb{N}$ *é um mínimo múltiplo comum* (mmc) *entre* a *e* b, *se m satisfaz as seguintes condições:*

i) m é um múltiplo de a e b, isto é, $a|m$ e $b|m$;

ii) Se c é um múltiplo comum de a e b, isto é, $a|c$ e $b|c$, então $m|c$.

Assim denotamos o mmc entre a e b por $m = mmc[a,b]$ ou $m = [a,b]$.

Exemplos:

Por exemplo, 12 é um múltiplo comum de 2 e 3, mas não é um mmc desses números. O 6 é o mmc de 2 e 3.

Teorema 3.6.2. Sejam $a,b \in \mathbb{N}$, com $d = mdc(a,b)$ e $m=mmc[a,b]$, então

$$m = \frac{ab}{d}$$

Demonstração. Consideremos $m_1 = \frac{ab}{d}$ e provemos que $m_1 = m$. Como $d|a$ e $d|b$, então $a=d\lambda_1$ e $b=d\lambda_2$, com λ_1 e $\lambda_2 \in \mathbb{N}$. Assim,

$$m_1 = \frac{ab}{d} = \frac{db\lambda_1}{d} = \lambda_1 b \Rightarrow b|m_1$$

Da mesma forma, prova-se que $a|m_1$. Tomemos agora m_2 o outro múltiplo comum de a e b, isto é, $m_2=a\alpha_1$ e $m_2=b\alpha_2$, com α_1 e $\alpha_2 \in \mathbb{N}$. Pela identidade de Bachet-Bézout (teorema 3.4), existem inteiros x e y tais que $d = ax + by$.

Logo $$\frac{m_2}{m_1} = \frac{m_2 d}{m_1 d} = \frac{axm_2 + bym_2}{ab} = \frac{ab\alpha_2 X + ab\alpha_1 Y}{ab} = \alpha_2 X + \alpha_1 Y \in \mathbb{Z},$$

ou seja, $m_1|m_2$. Isso mostra que $m_1 = m = ab\ d$.

Exemplo: Determine o $mmc[1028, 304]$.

Solução:

Pelo Algoritmo de Euclides, temos que $mdc(1028, 304) = 4$, logo pelo teorema anterior temos: $mmc[1028, 304] = 1028 \cdot 304\ 4 = 78128$

3.7. Números primos e compostos

Definição 3.7.1. Um número $p \in \mathbb{Z} - \{0, \pm 1\}$ é chamado **primo** quando seus únicos divisores positivos são 1 e $|p|$. Caso contrário, dizemos que p é **composto.**

Exemplo: Os números 3, −5 e 13, são primos.

Exemplo: O número 20 é composto pois $D_{20} = \{1, 2, 4, 5, 10, 20\}$.

Note que o número 1 não é nem primo e nem composto (isto se deve à uma condição especial de ser o elemento neutro da multiplicação) e que 2 e -2 são os únicos primos pares.

Teorema 3.7.2. Se $a > 1$, então existe um primo p tal que $p|a$.

Demonstração. Consideremos o conjunto $W = \{a \in \mathbb{N} : a > 1 \ e \ p \nmid a, \forall \ p \ primo\}$ Desejamos mostrar que $W = \emptyset$. Se $W \neq \emptyset$, então pelo Princípio da Boa Ordenação, existe $d \in W$, com $d = min(W)$. Como $d|d$, então d não pode ser primo.

Por isso, $d = bc$, com $1 < b, c < d$.

Desse modo, $b \notin W$, pois $d = min(W)$. Por conseguinte, sendo $b > 1$, deve existir um primo tal que $p|b$. Como $b|d$, então $p|d$, isto é, $d \notin W$, o que é impossível.

Esta contradição mostra que existe um primo p, com $p|a$.

3.8. Teorema Fundamental da Aritmética.

Todo número natural $a > 1$ pode ser escrito de forma única, a menos da ordem dos fatores, como um produto de primos. Especificamente,

$$a = p_1 \, p_2 \, p_3 \cdots p_n$$

em que $p_1 \, p_2 \, p_3 \cdots p_n$ são primos. Demonstração. Há duas coisas a serem demonstradas: a primeira é a existência dos primos, e a segunda é a unicidade da fatoração.

Existência:

Tomemos o conjunto $M = \{a \in \mathbb{N} : a > 1 \ e \ a \neq p_1 \, p_2 \, p_3 \cdots p_n \}$ para primos $p_1 \, p_2 \, p_3 \cdots p_n$. Se mostrarmos que $M = \emptyset$, então a existência dos números primos está provada. Por absurdo, se $M \neq \emptyset$, então pelo Princípio da Boa Ordenação, M possui um menor elemento m. É claro que m não pode ser primo e, por isso, é composto. Assim, podemos escrevê-lo na forma

$$m = b \cdot c, \text{ com } 1 < b, c < m.$$

Como $b < c$ e $c < m$, então $b \notin M$ e $c \notin M$, pois $m = min(M)$. Assim, sendo $b > 1$ e $c > 1$, segue que estes números são primos ou são produtos de primos. Logo, $m = b \cdot c$ é um produto de primos, o que é uma contradição. Desse modo, $M = \emptyset$.

Unicidade:

Suponhamos que $a = p_1 \, p_2 \, p_3 \cdots p_n = q_1 \, q_2 \, q_3 \cdots q_n$, sendo $p_1 \, p_2 \, p_3 \cdots p_n = q_1 \, q_2 \, q_3 \cdots q_n$ todos primos.

Logo $p_1 | q_1 q_2 \ldots\ldots q_m$ e, assim, temos que $p_1 = q_j$ para algum $j = 1, \ldots, m$ pois $p|ab$, então $p|a$ ou $p|b$, digamos que $p_1 = q_1$. Pela lei do cancelamento, temos que

$$p_2 \ldots\ldots p_n = q_2 \ldots\ldots q_n.$$

da mesma forma, temos $p_1 = q_j$ para algum $j = 2, \ldots., m$. Assumindo $p_2 = q_2$, obtemos

$$p_2 \ldots\ldots p_n = q_2 \ldots\ldots q_n.$$

Continuando este processo, e assumindo que $n > m$, temos

$$1 = p_{m+1} \ldots\ldots p_n \ ,$$

o que é impossível. Similarmente, se $n < m$, então

$$1 = p_{m+1} \ldots\ldots p_n,$$

que também é uma impossibilidade. Portanto, $m = n$ e $q_i = p_i$ para cada $i = 1, \ldots.. , n$.

Observação: Um processo prático utilizado para decompor um número em fatores

primos é o seguinte:

$$\begin{array}{r|l} 120 & 2 \\ 60 & 2 \\ 30 & 2 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array}$$

$$120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 23 \cdot 3 \cdot 5$$

Teorema 3.8.1. (Euclides) O conjunto P dos números primos é infinito.

Demonstração. Suponhamos por absurdo que P é um conjunto finito, e sejam $p_1\, p_2\, p_3 \cdots p_n$ todos os primos. Consideremos $a \in \mathbb{N}$ dado pelo produto dos p_i´s somado ao número 1, isto é,

$$a = p_1\, p_2\, p_3 \ldots\ldots p_{n+1}.$$

Como $a > 1$, então pelo teorema 3.2.6, existe um primo p que divide a, ou seja, $a = p_k$. Como por hipótese $p_1\, p_2\, p_3 \ldots\ldots p_n$ são os únicos primos, então $p = p_i$ para algum $i = 1, \ldots, n$, digamos que $p = p_1$. Assim,

$$p_k = pp_2 \ldots\ldots p_{n+1},$$

isto é, $p|1$, o que é uma contradição. Assim, P é infinito.

3.9. Noções de Equação Diofantina Linear

Nessa secção iremos discutir uma importante aplicação do Máximo Divisor Comum (MDC), que nos leva a resolver alguns problemas posteriores da seção 4. Na matemática, uma equação diofantina é uma equação polinomial que permite a duas ou mais variáveisassumirem apenas valores inteiros. Esse tipo de equação recebeu esse nome em homenagem a Diofanto de Alexandria (aproximadamente 300 d.c) que foi pioneiro nas descobertas de resoluções e publicação. Uma equação linear Diofantina é uma equação entre somas de monômios de grau um, como por exemplo $3x + 2y = 8$. Problemas Diofantinos possuem menos equações que variáveis e se resumem a achar inteiros que deverão funcionar corretamente para todas as equações.

As Equações diofantinas lineares assumem a forma ax+by = c. Sempre são possíveis de serem solucionadas desde que mdc(a, b) | c. Se c for igual ao maior divisor comum de a e b, ou seja, se c = mdc(a, b) então esta equação torna-se uma identidade de Bézout, o que permite uma quantidade infinita de soluções, também haverá uma quantidade infinita desoluções se c for um múltiplo do maior divisor comum de a e b. Caso contrário, a equação diofantina ax + by = c não possui solução. Como é tratado na proposição seguinte. Diremos que dois números naturais a e b são primos entre si quando o mdc(a, b) = 1.

Proposição 3.9.1. Sejam a e b $\in \mathbb{N}^*$ e c $\in \mathbb{N}^*$. A equação aX + bY = c admite soluções naturais se, e somente se, mdc(a, b) | c.

A demonstração dessa proposição poderá ser consultada em (HEFEZ, 2014, p.116).

Exemplo 3.9.2. Vejamos abaixo alguns exemplos de equações diofantinas e se elas têm ou não solução.

1. A equação $3x + 2y = 8$ possui solução, pois $mdc(2, 3) = 1$ e $1 \mid 8$ portanto a mesma tem solução, sendo $x_0 = 2$ e $y_0 = 1$. Generalizando, como o número 1 é um divisor natural de qualquer inteiro, então sempre que a e b são primos entre si, a equação diofantina possui ao menos uma solução.

2. A equação $4x + 6y = 7$ NÃO possui solução, pois $mdc(4, 6) = 2$ e 2 - 7.

Teorema 3.9.3. (Relação de Bézout). Dados inteiros a e b, quaisquer, não simultaneamente nulos, existem dois inteiros x e y tais que mdc(a, b) = ax + by.

A demonstração desse Teorema poderá ser consultado em (HEFEZ, 2011, p.58).

Proposição 3.9.4. Sejam x_0 e y_0 uma solução da equação ax+by = c onde mdc(a, b) = 1. Então, as soluções x, y $\in$ Z, da equação são

$$x = x_0 + bt \text{ e } y = y_0 - a\,t\,;\ \ t \in Z.$$

Caso o problema aborde ou especifique que as soluções x_0 e y_0 sejam apenas números naturais, então podemos escolher $x = x_0 + bt$ _ 0 e $y = y_0 - \ \ t \geq 0$, desta forma o parâmetro t nos dirá quantas são as possíveis soluções naturais para o devido problema. Esse tipo de aplicação é muito utilizada em problemas de contagem também, problemas que possam ser modelados por uma equação diofantina, mas ao mesmo tempo as soluções x_0 e y_0 não possam ser números negativos.

3.10. Congruência Modular

A ideia central que é explorada no estudo das congruências modulares é pensar nos restos das divisões euclidianas. Em Matemática, aritmética modular (chamada também de aritmética do relógio) é um sistema de aritmética para inteiros, no qual os números "voltam pra trás" quando atingem um certo valor, o módulo. O matemático suíço, Euler foi o pioneiro na abordagem de congruência por volta de 1750, quando ele explicitamente introduziu a ideia de congruência módulo um número natural n. O matemático Gauss, dentre outros estudou extensivamente sobre esse tema inclusive escreveu no seu livro *Disquisitiones Arithmeticae* publicado no ano de 1801. Em alguns livros, esse tema também é abordado como a "Aritmética dos Restos".

Definição 3.10.1. Sejam a, b números inteiros e considere ainda que m um número natural diferente de zero, então denotamos por $a \equiv b \ mod(m)$. De forma que a, b são chamados de congruentes módulo m se ambos têm o mesmo resto quando são divididos por m.

Uma maneira prática para saber se a e b são congruentes é verificar se $m|a - b$ ou $m|b - a$. Quando as diferenças de a e b resulta em um número múltiplo de m implica que a e b são congruentes módulo m. Quando a relação $a \equiv b \ mod(m)$ for falsa, diremos que a e b não são congruentes, ou que são incongruentes, módulo m. Escreveremos, neste caso, $a \equiv b \ mod(m)$ (HEFEZ, 2014, p.192).

Exemplo 3.10.2. observe que $38 \equiv 17 \ mod(7)$ pois os restos da divisão de 38 e do 17 por 7 é igual a 3. como o resto é igual então dizemos que 38 e 17 são congruentes módulo 7.

Na teoria dos números, a congruência modular é considerada uma relação de equivalência por obedecer às 3 propriedades citadas abaixo. (MOREIRA,2009,p. 65)

Proposição 3.10.3. Seja $m \in N$ com $m > 1$. Para todos a, b e $c \in N$, tem-se que

1. $a \equiv a \ mod(m)$. (Propriedade reflexiva);

2. $a \equiv b \ mod(m)$, então $b \equiv a \ mod(m)$. (Propriedade simétrica);

3. a ≡ b mod(m) e b ≡ c mod(m), então a ≡ c mod(m). (Propriedade transitiva);

A demonstração poderá ser encontrada em (HEFEZ, 2011, p.111).

Proposição 3.10.4. Seja a, b, c, d,m 2 N com m > 1. Tem-se que

1. a ≡ b mod(m) e c ≡ d mod(m), então a ± c ≡ b ± d mod(m).

2. a ≡ b mod(m) e c ≡ d mod(m), então a · c ≡ b · d mod(m).

A demonstração poderá ser encontrada em (HEFEZ, 2014, p.192).

Corolário 3.10.5. Para todos a, b e n ∈ Z no qual n > 0, temos que, se a ≡ b mod(m), então tem-se que an ≡ bn mod(m).

Basta usar n vezes o segundo resultado da proposição 3.2.15 que temos esse corolário por consequência. A demonstração faz-se por indução sobre *n*, para verificá-la detalhadamente, consulte em (HEFEZ, 2011, p.112).

Após verificar esses resultados iremos resolver um problema que usar essas aplicações de congruências modulares. Vejamos abaixo

Exemplo 10.6. (ENC - Exame Nacional de Cursos - Ano 1998) Qual é o resto da divisão de 12^{12} por 5?

Pela definição de congruência, temos que $12 \equiv 2\ mod(5)$ e usando o corolário 2.30 acima podemos escrever $12^4 \equiv 2^4\ mod(5)$, mas $16 \equiv 1\ mod(5)$ e sendo assim usando a propriedade transitiva de equivalência, temos $12^4 \equiv 1\ mod(5)$. Aplicando novamente o corolário anterior temos que $(12^4)^{3} \equiv 13\ mod(5)$ e sendo assim concluímos que $12^{12} \equiv 1$ $mod(5)$, então o resto da divisão de 12^{12} por 5 é igual a 1.

3.11. Congruências Lineares

Definição 3.5.3 Dados a e b inteiros, com a ≠ 0, uma congruência da forma ax ≡ b(mod m) é chamada congruência linear, em que x é uma incógnita. Nosso objetivo é determinar todas as soluções inteiras de ax ≡ b(mod m), isto é, todos os inteiros x_0 para os quais

$$ax_0 \equiv b \bmod m$$

Por exemplo, x_0 é uma solução de $4x \equiv 7 \pmod 5$, pois $4.3 = 12 \equiv 7 \pmod 5$. Por outro lado, a congruência linear $4x \equiv 3 \pmod 2$ não tem solução inteira, pois se x_0 € Z e $4x_0 \equiv 3$(mod 2), então $4x - 3 = 2k$, com k € Z, de maneira que 2 divide 3, o que não é possível. Inicialmente, vamos dar um critério para determinar se tais congruências, da forma como definidas acima, admitem solução.

Teorema 3.11.1 Dados a,b,m € Z, com $m > 1$, a congruência linear $ax \equiv b \pmod m$ admite solução inteira se, e somente se, $d|b$, em que $d = (a,m)$.

Demonstração: Suponhamos que x_0 seja solução de $ax \equiv b \pmod m$ e tomemos $d = (a,m)$. Assim, $ax_o - b = km$, isto é $b = ax_o - km$. Como, $d|a$ e $d|m$, então $d|b$.

Reciprocamente, suponha que $d|b$. Pela identidade de Bachet-Bézout, existem inteiros r e s tais que

$$d = a.r + s.m:$$

Como $b = dt$, com t € Z, $d|b$, então

$$b = (ar + sm)t = art + smt;$$

ou seja, $a(rt) \equiv b \pmod m$. Logo, $x_o = rt$ é solução de $ax \equiv b \pmod m$.

Corolário 3.11.2 A congruência $ax \equiv 1 \pmod m$ tem solução se, e somente se, $(a,m) = 1$.

A seguir vamos caracterizar as soluções de $ax \equiv b \pmod m$.

Teorema 3.12.3 Se x_0 é uma solução da congruência linear $ax \equiv b \pmod m$, então todas as soluções desta congruência são da forma

$$x = x_0 + \frac{m}{d}k; \text{ com } k \text{ € } Z$$

em que $d = (a,m)$.

Demonstração: Inicialmente, vamos provar que $x = x_0 + (\frac{m}{d})k$, com $d = (a,m)$, é uma solução de $ax \equiv b \pmod m$ para cada inteiro k. Desde que $ax_0 \equiv b \pmod m$, ou seja, $ax_0 = b + \gamma m$, com $\gamma \epsilon Z$, temos

$$ax = a[x_0 + (\frac{m}{d})k] = ax_0 + a(\frac{m}{d})k = b + m(\gamma + \frac{ak}{d}).$$

Portanto, $ax \equiv b \pmod{m}$, pois $\frac{ak}{d} \in Z$.

Agora, seja $x_1 \in Z$ tal que $ax_1 \equiv b(\text{mod } m)$. Como $ax_0 \equiv b(\text{mod } m)$, então, por transitividade,

$ax_0 \equiv ax_1(\text{mod } m)$. Assim, pelo Teorema 3.5.7, $x_0 \equiv x_1(\text{mod } \frac{m}{d})$, ou seja,

$$x_1 = x_0 + \frac{m}{d}k; \text{ com } k \in Z\text{: Em particular,}$$

Corolário 3.12.4 A solução geral da congruência linear $ax \equiv 1(\text{mod } m)$ com, $(a,m) = 1$, é dada por

$$x = x_0 + km; \text{ com } k \in Z;$$

em que x_o é uma solução inicial. Existem soluções de $ax \equiv b(\text{mod } m)$ que são incongruentes duas a duas módulo m. Essas ocorrem em um número finito e são obtidas da expressão

$$x = x_0 + \frac{m}{d}k; \text{ para } k = 0,1, \ldots\ldots, d - 1:$$

Vejamos no teorema a seguir.

Teorema 3.12.5 Consideremos a congruência $ax \equiv b(\text{mod } m)$. Se $d|b$, com $d = (a,m)$, então esta congruência possui d soluções, duas a duas incongruentes módulo m, dadas por

$$x_0,\ x_0 + \frac{m}{d},\ x_0 + 2\frac{m}{d}, \ldots, x_0 + \frac{(d-1)m}{d},$$

em x_0 é uma solução particular qualquer de $ax \equiv b(\text{mod } m)$.

Demonstração: Pelo Teorema 3.5.12, para cada inteiro k,

$$x = x_0 + \frac{m}{d}k$$

é uma solução de $ax \equiv b(\text{mod } m)$. O que devemos mostrar é que

$$(x_o + \frac{m}{d}k_1) \neq (x_0 + \frac{m}{d}k_2) \pmod{m}$$

com $0 \leq k1 < k2 \leq d - 1$. De fato, nestas condições, se

$$(x_o + \frac{m}{d}k_1) \neq (x_0 + \frac{m}{d}k_2) \pmod{m}$$

Então

$$\frac{m}{d}k_1 = \frac{m}{d}k_2$$

e pelo Teorema 3.5.7,

$$k_1 = k_2 \ (\text{mod } \frac{m}{d1}),$$

sendo $d_1 = (\frac{m}{d}, m)$. Como $m = (\frac{m}{d})d$, então $d_1 = \frac{m}{d}$, de modo que

$$\frac{m}{d1} = \frac{m}{m/d} = d$$

Portanto, $k_1 \equiv k_2(\text{mod } d)$, ou seja, $d \mid k_2 - k_1$, o que é uma contradição, desde que $0 < k_2 - k_1 < d - 1$. Por conseguinte, as soluções são duas a duas incongruentes módulo m.

Resta-nos mostrar que qualquer solução $x = x_0 + (\frac{m}{d})k$ de $ax \equiv b(\text{mod } m)$ é congruente módulo m a uma das d soluções dadas em (3.5.22). Pelo Algoritmo da Divisão, temos

$$k = dq + r, \text{ com } 0 \leq r \leq d - 1.$$

Assim,

$$x = x_0 + \frac{m}{d}k = x_0 + \frac{m}{d}(dk + r)$$

$$= x_0 + mq + r\frac{m}{d}$$

$$= x_0 + r\frac{m}{d} \ (\text{mod } m)$$

Em que $x_0 + r\frac{m}{d}$ é uma das soluções em (3.5.22).

Resumindo os resultados anteriores, podemos resolver uma congruência linear $ax \equiv b(\text{mod } m)$, com $d = (a,m)$ e $d|b$, seguindo os seguintes passos:

1. Através do Algoritmo de Euclides, obtemos inteiros r e s tais que

$$d = a.r + m.s:$$

2. Se b = dt, então $x_o = rt$ é uma solução de $ax \equiv b(\text{mod } m)$, de modo que sua solução geral é dada por

$$x = x_0 + \frac{m}{d}k \text{ com } k \in Z;$$

3.12. Sistemas de Congruências Lineares

No primeiro século da nossa era, o matemático chinês Sun-Tsu propôs o seguinte problema.

Qual é o número que deixa restos 2, 3 e 2 quando dividido, respectivamente, por 3, 5 e 7?

A resposta dada por Sun-Tsu para esse problema foi 23. Em termos de congruências, este problema consiste em resolver o seguinte sistema:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

De modo geral, estudaremos sistemas de congruências da forma:

$$\begin{cases} a1x \equiv b1 \pmod{m1} \\ a2x \equiv b2 \pmod{m2} \\ \quad\quad . \\ \quad\quad . \\ \quad\quad . \\ akx \equiv bk \pmod{mk} \end{cases}$$

Para que este sistema tenha solução, é necessário que cada uma das k congruências tenha solução, ou seja, que $d_i|b_i$, em que $d_i = (a_i,m_i)$ para cada i = 1,....,k. Entretanto, esta condição não é suficiente. Por exemplo, o sistema

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}$$

não possui solução, embora cada uma das congruências tenha solução.

O lema a seguir nos mostra como obter um sistema equivalente1 ao dado em (3.5.3), mas com os coeficientes iguais a 1.

Lema 3.13.15. A congruência linear $ax \equiv b(\text{mod } m)$, em que $d =(a,m)$, com $d|b$, é equivalente

$$a\ \ x \equiv rb_1 \ (\text{mod } n);$$

$$\text{sendo } b = b_1d,\ d = a.r + s.m \text{ e } m = nd.$$

Demonstração: Considerando $a = a_1d$, $b = b_1d$ e $m = nd$,

$$ax \equiv b(\text{mod } m) \leftrightarrow\ a_1dx \equiv b_1d(\text{mod } nd):$$

Pelo Teorema 3.13:10, temos

$$a_1x \equiv b_1(\text{mod } n).\ (5.4)$$

Dois sistemas de congruências lineares são equivalentes quando possuem as mesmas soluções. O mesmo ocorre com duas congruências lineares.

Sendo $d = a.r + s.m$, então $d = a_1d.r + s.nd$, ou seja, $1 = a_1.r + s.n$, isto é,

$$ra_1 \equiv 1(\text{mod } n):$$

Multiplicando a congruência em (3.5:.) por r, temos

$$ra_1x \equiv rb_1x\ (\text{mod } n):$$

e como $a_1 \equiv 1(\text{mod } n)$; então $x \equiv a_1rx(\text{mod } n)$, isto é,

$$x \equiv b_1r(\text{mod } n);$$

o que prova a primeira parte. Reciprocamente, se $x \equiv b_1r(\text{mod } n)$, então como $ra_1 \equiv 1(\text{mod } n)$, segue $ra_1x \equiv rb_1x\ (\text{mod } n)$.

Por outro lado, visto que $1 = a_1.r + s.n$, temos $(r,n) = 1$. Portanto, podemos cancelar o fator r da última congruência de modo a obter $xa_1 \equiv\ b_1(\text{mod } n)$, ou seja,

$$x\left(\frac{q}{d}\right) \equiv \frac{b}{d}\left(\mathrm{mod}\ \frac{m}{d}\right), \text{ onde } ax \equiv b(\mathrm{mod}\ m).$$

A vantagem de se considerar uma congruência da forma $x \equiv b(\mathrm{mod}\ m)$ é que sua solução geral é obtida de forma direta, $x = b+km$, com $k \in Z$.

De acordo como o lema anterior, o sistema dado em (3.5.3) é equivalente ao sistema

$$\begin{cases} x \equiv c1\ (\mathrm{mod}\ n1) \\ x \equiv c2\ (\mathrm{mod}\ n2) \\ \quad\vdots \\ x \equiv ck\ (\mathrm{mod}\ nk) \end{cases}$$

o qual será resolvido através do teorema a seguir com uma hipótese adicional, cujo título faz lembrar a origem desse problema.

3.13. Teorema Chinês dos Restos

Sejam $n_1, n_2, \ldots, n_k$ números naturais tais que $(n_i, n_j) = 1$ para $i \neq j$. Então, o sistema de congruências lineares dado em (3.5.5) possui uma solução, que é única módulo $n_1, n_2, \ldots, n_k$

Demonstração: Sendo $n_1, n_2, \ldots, n_k$, então

$$Ni = \left(\frac{n}{ni}\right) = n_1, n_2, \ldots, n_k;$$

ou seja, N_i é o produto de todos os inteiros $n_1, n_2, \ldots, n_k$ excluindo n_i. Desde que $(n_i, n_j) = 1$ para $i \neq j$., então $(n_i, n_j) = 1$. Assim, pela identidade de Bachet-Bézout, existem inteiros r_i e s_i tais que $r_iN_i + s_iN_i = 1$, para cada $i = 1, \ldots, k$. Vamos provar que o inteiro

$$x_0 = \sum_{i=1}^{k} c_i r_i N_i = c_1r_1N_1 + c_2r_2N_2 + \ldots + c_kr_kN_k$$

é uma solução do sistema dado. Inicialmente, se $i \neq j$, então $Nj \equiv 0(\mathrm{mod}\ n_i)$, desde que

$n_i|N_i$. Logo, $c_jr_jN_j \equiv 0(\mathrm{mod}\ n_i)$, de modo que

$$x_0 = c_ir_iN_i = c_1r_1N_1 + c_2r_2N_2 + \ldots + c_kr_kN_k \equiv c_ir_iN_i(\mathrm{mod}\ n_i)$$

Por outro lado, $r_iN_i \equiv 1(\text{mod } n_i)$ para cada i = 1,.....,k. Daí, $c_ir_iN_i \equiv c_i(\text{mod } n_i)$

e, por transitividade, $x_o \equiv c_i(\text{mod } n_i)$ para todo i. Isso mostra que x_o é uma solução do sistema.

Por fim, se y_o é outra solução do sistema, então $y_o \equiv c_i \ (\text{mod } n_i)$

para cada i = 1,.....,k. Desse modo, $x_o \equiv y_o(\text{mod } n_i)$, isto é, $n_i \mid x_o - y_o$. Desde que $(n_i, n_j) = 1$, com $i \neq j$, segue do Lema de Euclides que, $n = n_1n_2.....n_k$ divide $x_o - y_o$, ou seja, $X_o \equiv Y_O$ (mod n), o que prova a unicidade de solução módulo n. Por isso, a solução geral do sistema é

$$x = x_0 + kn;\ k \in Z:$$

Exemplo 14.1 Determine a solução do sistema

$$\begin{cases} X \equiv 2 \ (\text{mod } 3) \\ x \equiv 3 \ (\text{mod } 5) \\ x \equiv 2 \ (\text{mod } 7) \end{cases}$$

usando o Teorema Chinês dos Restos.

Solução: Como mdc(3, 5) = mdc(3, 7) = mdc(5, 7)=1, então podemos aplicar o Teorema Chinês dos Restos. Note que

$n_1 = 3$; $n_2 = 5$; $n_3 = 7$ e $N = n_1.n_2.n_3 = 3.5.7 = 105$

por outro lado

$N_1 = \frac{N}{n1} = \frac{105}{3} = 35$, $N_2 = \frac{N}{n2} = \frac{105}{5} = 21$, $N_3 = \frac{N}{n3} = \frac{105}{7} = 15$,

Agora, vamos determinar os inteiros R_i, S_i com i = 1,2,3 tais que, $R_iN_i + S_iN_i = 1$

(i) $R_1N_1 + S_1N_1 = 1 \rightarrow R_135 + S_112 = 1 \rightarrow R_1 = -1$ e $S_1 = 3$

(ii) $R_2N_2 + S_2N_2 = 1 \rightarrow R_221 + S_25 = 1 \rightarrow R_2 = 1$ e $S_2 = -4$

(iii) $R_3N_3 + S_3N_3 = 1 \rightarrow R_315 + S_37 = 1 \rightarrow R_2 = 1$ e $S_2 = -2$

Como $C_1 = 2$; $C_2 = 3$ e $C_3 = 2$, então uma solução para o sistema pode ser dada por:

$X_o = C_1R_1N_1 + C_2R_2N_2 + C_3R_3N_3 = 2.(-1).35 + 3.1.21 + 2.1.15 = 23$

Logo, a solução geral do sistema pode ser expressa da seguinte forma

$x = 23+105t;\ t \in Z:$

3.14. Equações Diofantinas Lineares

A denominação equação diofantina é uma homenagem a Diofanto de Alexandria, matemático grego do século III a.C. Diofanto viveu em uma importante cidade que era centro de atividades matemáticas da Grécia antiga. Não se sabe muito sobre a vida desse matemático. Em seu túmulo foram encontrados versos com problemas enigmáticos, pelos quais deduz-se que ele viveu 84 anos. Enigma que, segundo dizem, teria sido gravada no túmulo de Diofanto por um amigo, Metrodorus, e cujo resultado revela a idade desse matemático:

> Viajante! Aqui estão as cinzas de Diofanto. É milagroso que os números possam medir a extensão da sua vida.
> Um sexto dela foi uma bela infância.
> 2 da sua vida, a sua barba cresceu.
> Um sétimo da sua vida passou-se num casamento sem filhos.
> Mas, cinco anos após isso, nasceu o seu primeiro filho.
> Que viveu uma vida feliz durante apenas metade do tempo de vida do seu pai.
> E, em profundo pesar, o pobre velho terminou os seus dias na Terra, quatro anos após perder o seu filho, (Jornal de Mathemática Elementar no 135).

Durante toda sua vida, Diofanto escreveu vários livros, entretanto o mais importante foi Aritmética. Neste livro, ele introduz uma notação simbólica com caracteres diferentes para o quadrado de uma incógnita, cubo de uma incógnita e assim sucessivamente. Neste mesmo livro deu uma pequena introdução sobre as equações e hoje certas equações cujas soluções são números inteiros ou racionais são chamadas de Equações Diofantinas. (Carl B. Boyer,2014,p.67)

Definição 3.5.4 Uma equação diofantina linear é qualquer equação polinomial com coeficientes inteiros com uma ou mais incógnitas.

Uma equação da forma $a_1x_1 + a_2x_2 + ...+ a_nx_n = c$

é chamada equação diofantina linear, em que $a_{1,....}, a_n$ são inteiros dados, chamados coeficientes, c que também é um inteiro dado, é chamado termo constante e $x_{1,....}, x_n$ são as incógnitas.

Teorema 3.14.1 A equação diofantina ax+by = c admite solução se, e somente se, mdc(a,b) divide c.

Demonstração: Suponha que a equação admita uma solução x_o,y_o. Então vale a igualdade

$ax_o + by_o = c$. Como mdc(a,b) divide a e divide b, então divide $ax_o + by_o$, logo divide c.

Reciprocamente, suponha que mdc(a,b) divida c, ou seja, c = mdc(a,b).d, para algum inteiro d. Por outro lado, sabemos que existem inteiros r e s tais que

mdc(a,b) = a.r + b.s

Multiplicando ambos os lados da igualdade acima por d, obtemos

c = mdc(a.b).d = a.mdc(r.d) + b.mdc(s.d)

Logo, a equação diofantina ax+by = c admite pelo menos a solução

x = r.d e y = s.d

Se a equação ax+by = c admite uma solução, então o número d = mdc(a,b) divide c e, assim, é imediato verificar que x_0, y_o é uma solução da equação ax+by = c se, e somente se, é solução da equação $ax' + by' = c$, onde agora mdc(a´,b´) = 1.

Portanto, toda equação diofantina linear que possui solução é equivalente a uma equação reduzida, ou seja, uma equação da forma:

$$ax + by = c; \text{ com } mdc(a,b) = 1:$$

O próximo resultado nos dá uma fórmula para resolver a equação diofantinas linear ax + by = c, onde mdc(a,b) = 1, conhecida uma solução particular x_o, y_o da equação.

Teorema 3.14.2 Seja x_o, y_o uma solução da equação ax + by = c, onde mdc(a,b) = 1. Então, as soluções x e y em Z da equação são

$$x = x_o + tb \text{ , } y = y_o - ta \text{ , } t \in Z$$

Demonstração: Se x,y é uma solução qualquer da equação, então

$ax + by = ax_o + by_o = c$ onde

$a(x - x_o) = b(y_o - y)$ (5.7)

Daí segue que $a|b(y_o - y)$ e $b|a(x - x_o)$. Como (a,b) = 1, $a|b(y_o - y)$ e $b|a(x - x_o)$. Assim,

$y_o - y = ta$ e $x - x_o = sb$, (5.8), para alguns inteiros t e s.

Substituindo esses valores em (5:7), obtemos

$$asb = bta,$$

o que implica que s = t. Logo, de (5:8), a solução é dada por

$$x = x_o + tb;\ y = y_o - ta\ ,\ t \in Z:$$

Reciprocamente, se $x = x_o + tb$ e $y = y_o - ta$, substituindo esses valores na equação

$ax + by = c$, obtemos

$$a(x_o + tb) + b(y_o - ta) = ax_o + by_o + abt - bat = ax_o + by_o = c$$

Segue-se do teorema acima que a equação diofantina ax+by = c, com (a,b) = 1, admite infinitas soluções em Z.

Note também que as soluções da equação diofantina ax+by = c, podem ser escritas na forma

$x = x_o - tb$, $y = y_o + ta$, $t \in Z$, bastando para isso trocar t por - t no Teorema 5:18.

Exemplo 3.14.3

Deseja-se comprar 225 bolas que são vendidas em caixas que contêm 6 ou 15 bolas. Determinar as quantidades necessárias de caixas para a efetivação da compra.

Solução:

Considerando x e y os números de 6 e 15 bolas, respectivamente, o problema pode ser modelado na equação 6x+15=225. Como (6,15) = 3 e 3 divide 225, então esta equação tem solução inteira e, além disso, é equivalente à equação

$$2x + 5y = 75:$$

Por inspeção, uma solução particular para equação acima pode ser dada por $x_o = 5$ e $y_o = 13$. Logo, podemos escrever a solução geral da equação da seguinte forma:

$$\begin{cases} x = x_0 - tb \\ y = y + ta \end{cases} \qquad \begin{cases} x = 5 + 5t \\ y = 13 - 2t \text{ t} \epsilon \text{ Z} \end{cases}$$

Pela natureza do problema, apenas as soluções x ≥ 0 e y ≥ 0 são de interesse, então

$$\begin{cases} x \geq 0 \\ y \geq 0 \end{cases} \quad \begin{cases} 5 + 5t \geq 0 \\ 13 - 2t \geq 0 \end{cases} \quad \begin{cases} t \geq -1 \\ t \geq 6 \end{cases}$$

Portanto, -1 ≤ t ≤ 6, ou seja, t = {-1,......,6} são os possíveis valores de t. Por exemplo, para t = - 1, x = 0 e y = 15 (uma compra de 15 caixas com 15 bolas), t = 0, x = 5 e y = 13 (uma compra de 5 caixas com 6 bolas e de 13 caixas com 15 bolas), e assim por diante. As outras possibilidades de compras são:

* para t = 1 → x = 10 e y = 11,

* para t = 2 → x = 15 e y = 9,

* para t = 3 → x = 20 e y = 7,

* para t = 4 → x = 25 e y = 5,

* para t = 5 → x = 30 e y = 3,

* para t = 6 → x = 35 e y = 1,

O Teorema 3.5.17 pode ser estendido a equações diofantinas lineares com três ou mais variáveis e sua demonstração se faz por indução.

Teorema 3.14.4

A equação diofantina linear $a_1x_1 + a_2x_2 + ... a_nx_n = c$ possui solução se e, somente se mdc($a_{1,........,}a_n$) divide c.

Exemplo 3.14.5

Verifique se a equação 6x + 8y + 12z = 10 tem solução e caso exista encontre sua solução geral.

Solução: Como mdc(6,8,12) = 2 e 2 divide 10 a equação possui solução. Como 8y + 12z é uma combinação linear de 8 e 12, então deve ser um múltiplo de 4 = mdc(8,12), ou seja

8y + 12z = 4u (5.9)

Assim, a equação original se reduz a 6x+4u = 10, que pelo Teorema 14:4 tem solução geral da forma x = 5+2t, u = -5 - 37, com t ϵ Z. Agora substituindo em (5:9) obtemos.

8y+12z = a(-5 -3t), ou equivalentemente 2y + 3z = -5 -3t.

Agora observe que

1 = mdc(2,3) = 2.2 – 1.3 → -(10 + 6t).2 + (5 + 3t).3 = -5 -3t

o que nos dá uma solução particular e daí a solução geral é

y = -10 - 6t +3t′ e z = 5 + 3t - 2t′:

Portanto, a solução geral da equação original é

$$\begin{cases} x = 5 + 2t \\ y = -10 - 6t + 3t' \\ z = 5 + 3t - 2t' \end{cases}$$

com t; t′ ϵ Z.

Observação: O método acima pode ser aplicado a uma equação diofantina com um número qualquer de variável

O Pequeno Teorema de Fermat

Desde, pelo menos, 50 anos antes de Cristo, os chineses sabiam que, se p é um número primo, então, p | 2^p - 2. Coube a Pierre de Fermat, no século XVII, generalizar esse resultado, enunciando um pequeno, mas notável, teorema. O resultado de Pierre de Fermat, conhecido como Pequeno Teorema de Fermat, pode ser assim enunciado:

Teorema 3.15.5 (Pequeno Teorema de Fermat) Sejam p um primo e a um inteiro tal que $p \nmid$ a. Então, $A^{p-1} \equiv 1(\text{mod p})$:

Demonstração: Consideremos os primeiros p - 1 múltiplos de a, ou seja,

a,2a,3a, . . . , (p - 1)a

Observemos primeiramente que estes números são dois a dois incongruentes módulo p. De fato, se $ak_1 \equiv ak_2$ (mod p), com $1 \leq k1 < k2 \leq p - 1$, então como (a, p)=1, segue do Corolário 5:8 que $k_1 \equiv k_2$ (mod p), isto é, p | $k_2 – k1$, o que é impossível.

Além disso, se $1 \leq r \leq p - 1$ e $p|ra$, então $p|a$ ou $p|r$, o que também não é possível. Portanto, $ra \equiv 0 (\mathrm{mod}\ p)$ para todo $r = 1, \ldots, p - 1$.

De acordo com o Algoritmo da Divisão, cada inteiro é congruente módulo p a um, e somente um, número da sequência

$$1, 2, 3, \ldots, p - 1$$

Portanto, cada inteiro de (3.5.10) é equivalente a um número de (3.5.11) numa determinada ordem, digamos

$$\begin{gathered} a \equiv b_1 (\mathrm{mod}\ p), \\ 2a \equiv b_2 (\mathrm{mod}\ p), \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ (p - 1)a \equiv b_{p-1} (\mathrm{mod}\ p), \end{gathered}$$

em que $b_i \in \{1, 2, \ldots, p - 1\}$ para $i = 1, 2, \ldots, p - 1$. Multiplicando membro a membro estas congruências, temos que

$$a.2a. \ldots (p - 1)a \equiv 1.2. \ldots (p - 1)(\mathrm{mod}\ p),$$

isto é,

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

Como $((p - 1)!, p) = 1$, podemos cancelar $(p - 1)!$ desta última congruência, de modo que

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

O resultado anterior implica que para um inteiro a qualquer, divisível por p ou não,

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

Com efeito

Corolário 3.15.4 Se p é primo, então

$$a^p \equiv a(\mathrm{mod}\ p)$$

para qualquer inteiro a

Demonstração: Se $p \nmid a$, então pelo teorema anterior, $a^{p-1} \equiv 1(\mathrm{mod}\ p)$. Assim, multiplicando esta congruência por a, segue que $a^p \equiv a(\mathrm{mod}\ p)$. Se $p|a$, então $p|a^p$ e, por isso, $p|a^p - a$, ou seja, $a^p \equiv a(\mathrm{mod}\ p)$.

Note que o Pequeno Teorema de Fermat fornece-nos um teste de não P~~r~~imalidade. De fato, dado $m \in N$, com $m > 1$, se existir algum $a \in N$, com $(a,m) = 1$, tal que $m \mid a^{m-1} - 1$ então m não é primo

Exemplo 3.15.5 Determinar o resto da divisão de 2^{20017} por 7

Solução: Considerando p = 7 e a = 2, temos que $p \nmid a$. Assim, pelo Pequeno Teorema de Fermat, $2^6 \equiv 1(\mathrm{mod}\ 7)$:

Elevando ambos os membros desta congruência 288 (2017 = 7.288+1), obtemos $2^{2016} \equiv 1(\mathrm{mod}\ 7)$: Multiplicando esta congruência por 2, $2^{2017} \equiv 2(\mathrm{mod}\ 7)$: Logo, o resto da divisão é r = 2.

Seção 4. Aritméticas e seus conceitos na OBMEP: problemas, soluções e sugestões.

Nesta seção apresentamos os problemas relacionados com a Aritmética da OBMEP, com suas respectivas soluções, comentários e sugestões. Existem conceitos e teoremas que são cobrados nas provas da OBMEP, cujo quais não são ensinados na sala de aula e que não estão nos livros didáticos da educação básica, como o teorema de Euclides, teorema chinês dos restos, aritmética modular, e nós trataremos aqui desses teoremas, já expostos na seção 3, e faremos suas aplicações para resolução dos exercícios.

PROBLEMA 01 : QUESTÃO 6. (2019 – nível 1)**.** Uma festa de casamento será realizada em um salão que comporta no máximo 200 pessoas. O organizador sabe que, se distribuir 8 convidados por mesa, uma mesa ficará com apenas um convidado. O mesmo irá ocorrer se ele distribuir 6 ou 7 convidados por mesa. Se ele distribuir 9 convidados por mesa, uma mesa ficará com menos do que 9 pessoas. Quantas pessoas ficarão nessa mesa?

A) 2

B) 3

C) 4

D) 6

E) 7

Figura 1 : sala de jantar

Fonte :OBMEP

SOLUÇÕES DA OBMEP: (ALTERNATIVA E)

Vamos encontrar primeiramente o número de convidados. Chamemos esse número de n. Assim, pelo enunciado, n deixa resto 1 quando dividido por 6, 7 ou 8. Como o mínimo múltiplo comum de 6, 7 e 8 é 168, o número de convidados é $n = 169$, já que $169 < 200$. Se distribuirmos 169 pessoas em mesas com 9 lugares, restarão 7 pessoas, pois 169 dividido por 9 deixa resto 7.

SOLUÇÃO SUGERIDA:

Usando o teorema chinês do resto temos :

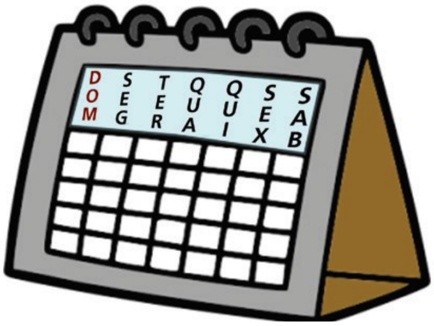
Seja p o número de convidados que foram à festa. $p \leq 200$ (capacidade) pela hipótese:

$$\left.\begin{array}{l} p = 8x+1 \Leftrightarrow p-1 \equiv 0 \bmod 8 \\ p = 6y+1 \Leftrightarrow p-1 \equiv 0 \bmod 6 \\ p = 7z+1 \Leftrightarrow p-1 \equiv 0 \bmod 7 \end{array}\right\} p-1 \equiv 0 \bmod [8,6,7]$$

Como $[8,6,7] = MMC[8,6,7] = 168$, então $p - 1 = 168t$, $t \varepsilon N$, ou seja $p = 168t + 1$ e como $p \leq 200 \rightarrow t = 1 \rightarrow p = 169$ e $169 = 9.18 + 7$ logo a resposta é 7,P

PROBLEMA 02 : QUESTÃO 02. (2019 – nível 1) Carla viajou na terça-feira e voltou 3 dias depois, na sexta-feira. Joana viajou no sábado e voltou 9 dias depois. Em que dia da semana Joana voltou?

Figura 2 : Calendário



Fonte :OBMEP

A) Domingo.

B) Segunda-feira.

C) Terça-feira.

D) Quarta-feira.

E) Quinta-feira.

SOLUÇÃO DA OBMEP: (ALTERNATIVA B)

Nove dias depois de sábado corresponde a uma semana (7 dias) mais dois dias. Uma semana depois de um sábado é novamente um sábado, oito dias depois de um sábado é um domingo, e 9 dias depois de um sábado é uma segunda-feira. Logo, Joana voltou em uma segunda-feira.

SOLUÇÃO SUGERIDA:

Observemos que a semana tem 7 dias e pelo teorema de Euclides sabemos que há 6 possíveis resultados para um número quando dividido por 7; (0,1,2,3,4,5 E 6) , fazendo 7 dias que compõem a semana temos que sobra 2 e colocando o dia de sábado como o primeiro dia, ou seja com resto 0 temos que o dia 2 é segunda feira que representa o resto 2. . Dessa maneira podemos instigar aos alunos a noção de divisibilidade e teorema dos restos, uma questão de bom proveito para o ensino da aritmética

PROBLEMA 03 : QUESTÃO 10. (2019) No Planeta Pemob as semanas têm 5 dias: Aba, Eba, Iba, Oba e Uba, nessa ordem. Os anos são divididos em 6 meses com 27 dias cada um. Se o primeiro dia de um certo ano foi Eba, qual foi o último dia desse ano?

A) Aba

B) Eba

C) Iba

D) Oba

E) Uba

Figura 3 : Planeta

Fonte :OBMEP

SOLUÇÃO DA OBMEP: (ALTERNATIVA C)

No planeta Pemob, cada ano tem 6 x 27 = 162 dias. Se, em um certo ano, o primeiro dia do ano foi Eba, então dia 5 foi Aba, dia 10 também foi Aba, e assim sucessivamente, de 5 em 5, até o dia 160, que também foi Aba. Logo, o dia 161 foi Eba e o último dia, o de número 162, foi Iba.

1	2	3	4	5	6	7	8	9	10
Eba	Iba	Oba	Ubá	Aba	Eba	Iba	Oba	Ubá	aba

SOLUÇÃO SUGERIDA:

Observemos que a semana tem 5 dias e pelo teorema de Euclides sabemos que há 4 possíveis resultados para um número quando dividido por 5; (0,1,2,3,4) , fazendo 162 dias que compõem o ano (6x27 = 162) e dividindo por 5 temos resto 2 e colocando o dia aba como o primeiro dia, ou seja com resto 0 temos que o dia 162 é iba que representa o resto 2. Dessa maneira podemos instigar aos alunos a noção de divisibilidade e teorema dos restos, uma questão de bom proveito para o ensino da matemática.

PROBLEMA 04 : QUESTÃO 9. (2019 – nível 1)**.** Um número inteiro positivo é chamado de *tetrapar* quando é divisível quatro vezes consecutivas por 2 e o resultado da última divisão é um número ímpar. Por exemplo, o número 80 é tetrapar, pois $80 \div 2 = 40$, $40 \div 2 = 20$, $20 \div 2 = 10$ e $10 \div 2 = 5$. Quantos são os números tetrapares de três algarismos?

A) 26

B) 28

C) 30

D) 56

E) 62

SOLUÇÃO DA OBMEP : (ALTERNATIVA B)

Um número, divisível quatro vezes consecutivas por 2, é divisível por . $2 \times 2 \times 2 \times 2 = 2^4 = 16$. Como o resultado, após essas divisões, deve ser ímpar, esse número é da forma $16.I$, sendo I um número ímpar. Sabendo que $16 \times 7 = 112$ é o primeiro múltiplo de 16 com 3 algarismos e que $16 \times 62 = 992$ é o último, a quantidade de números tetrapares com 3 algarismos é igual à quantidade de números ímpares de 7 a 62, incluindo o 7. Logo, $\frac{62-6}{2}$ são números tetrapares com 3 algarismos.

SOLUÇÕES SUGERIDAS

Usando conceitos de congruência modular temos pela definição o número tem que ser da forma $a = 2^4.(2k + 1)$, ou seja $a = 32k + 16$, e como o número é de 3 algarismo então resolve a inequação: $99 < a < 1000$, ou seja $99 < 32k + 16 < 1000 \rightarrow 83 < 32k < 984$, está por sua vez se resolve com a parte inteira da divisão de $[984/32] – [83/32] = 30 - 2 = 28$.

PROBLEMA 05 : QUESTÃO 19. (2019 – nível 2)**.** Marco tem dois relógios. Um deles marca as horas corretamente, e o outro atrasa 16 minutos por hora. Num certo dia os dois relógios mostravam 17:00 em seus visores. Depois de alguns dias eles voltaram a mostrar, pela primeira vez, a mesma hora. Qual é essa hora?

Figura 4 : Horário

A) 5:00

B) 11:00

C) 14:00

D) 20:00

E) 21:00

Fonte :OBMEP

SOLUÇÃO DA OBMEP : (ALTERNATIVA B)

Após X horas, um dos relógios indicará um horário de um momento futuro que poderá ser obtido do outro relógio avançando-se $16 \cdot X$ minutos. Para que eles marquem a mesma hora, esse avanço deve ser um múltiplo da quantidade de minutos de um dia, que é $24 \cdot 60$. O menor valor de X é $\frac{24.60}{16} = 90$. Como $90 = 3 \cdot 24 + 18$, após 3 dias e 18 horas eles marcarão a mesma hora em seus visores, que será 11:00.

RECOMENDAÇÃO.

Vemos aqui aplicação do algoritmo de divisão de Euclides, $90 = 3 \cdot 24 + 18$, vemos também a aplicação do mdc. Assim o professor deve ensinar aos alunos assuntos de divisões de Euclides para a resolução da questão.

PROBLEMA 06 : QUESTÃO 12. (2020 –NV1) Paulo iniciou um programa de ginástica no qual os dias do trino são separados por dois dias de descanso. Se o primeiro treino foi em uma segunda-feira, em qual dia da semana cairá o centésimo treino ?

A) sexta-feira

B) quinta-feira

C) terça-feira

D) segunda-feira

E) domingo

SOLUÇÃO OBMEP (alternativa B)

Um dia de treino e dois dias de folga formam grupos de três dias, totalizando 3x99 =297 dias até a véspera do dia do 100º treino. Como 297 = 7 x 42 + 3, esses 297 dias correspondem a 42 semanas de segunda a domingo mais 3 dias, que são segunda,terça e quarta. Logo, quarta é a véspera do 100º treino, que ocorre, então, em uma quinta.

SOLUÇÃO SUGERIDA.

Fazendo a escala de treinos temos que o treino da segunda feira , volta a ser novamente na segunda de 21 em 21 dias e ao longo desses 21 dias há 8 treinos, logo fazendo uma PA temos (8,16,24,...,96), por tanto o 96º treino é na segunda colocando mais 4 treinos caímos na quinta-feira.

PROBLEMA 07 : QUESTÃO 14. (2019 – nível 1) Paulo faz cálculos usando os números 5, 6, 7, 8 e 9, exatamente uma vez cada um. Ele somou três deles e subtraiu dessa soma a soma dos outros dois. Qual dos resultados abaixo ele pode ter obtido?

A) 0

B) 6

C) 8

D) 11

E) 15

SOLUÇÕES DA OBMEP: (ALTERNATIVA D)

A alternativa D é a correta, pois o número 11 pode ser obtido assim: 11 = (9 + 8 + 6) – (5 + 7). A alternativa A não pode ocorrer, pois o menor número que se obtém é (5 + 6 + 7) – (9 + 8) = 1. A alternativa E não pode ocorrer, pois o maior número que se obtém é (9 + 8 + 7) – (5 + 6) = 13. As alternativas B e C não podem ocorrer, pois o resultado final dos cálculos sempre será um número ímpar.

SOLUÇÃO SUGERIDA:

Pela paridade dos números e usando conceitos de aritmética e as devidas combinações temos que 5, 7 e 9 são números ímpares e 6 e 8 são números pares, há apenas três possibilidades:

(ímpar + ímpar + ímpar) – (par + par) ou

(ímpar + ímpar + par) – (ímpar + par) ou

(ímpar + par + par) – (ímpar + ímpar)

Em qualquer uma dessas possibilidades, o resultado final será sempre um número ímpar, logo só há a possibilidade de ser a D ou a A, e fazendo as contas chegamos na alternativa D pois 11 = (9 + 8 + 6) – (5 + 7) . vemos nessa questão a questão da paridade dos números, assim podemos trabalhar com alunos conceitos básicos e bem práticos da aritmética

PROBLEMA 07 : QUESTÃO 04. (2020 – NV2) Qual o resto da divisão de
1 x 2 x 3 x 4 x .....x 2011 + 21 por 8 ?

A) 7

B) 5

C) 4

D) 3

E) 2

SOLUÇÃO OBMEP (alternativa B)

Queremos dividir 1 x 2 x 3 x 4 x .....x 2011 + 21 = 1 x 2 x 3 x 4 x .....x 2011 + 16 + 5 por 8. Como as duas primeiras parcelas do lado direito dessa expressão são múltiplos de 8, sua soma também é um múltiplo de 8. Portanto, o resto da divisão desse número por 8 é 5.

SOLUÇÃO SUGERIDA

Usando congruência modular temos que podemos escrever a expressão
1 x 2 x 3 x 4 x .....x 2011 + 21 como sendo 8(1 x 2 x 3 x 4 x .....x 2011) + 21 = 8k + 21, como 8k é divisível por 8 e 21 deixa resto 5 na divisão por 8 logo nosso resultado é 5, alternativa b.

PROBLEMA 08 :QUESTÃO 02. (2020 – NV2) A soma de três números inteiros consecutivos é igual a 90. Qual é o maior desses três números ?

A) 20

B) 17

C) 14

D) 11

E) 8

SOLUÇÃO OBMEP (alternativa B).

Se n é o menor desses números, então os outros dois são n+1 e n+2. A soma dos três números é n + (n +1) + (n +2) = 90. Logo, 3n +3 = 90, donde 3n = 87 e n = 29. Logo, os números são 29,30 e 31, e o maior é 31.

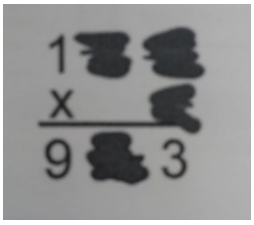
SOLUÇÃO SUGERIDA

Fazendo pelo método de tentativas temos que 90 = 30 + 30 + 30, porém como devem ser 3 números consecutivos, temos que acrescentar 1 ao primeiro e tiramos 1 do último , assim temos: 90 = 31 + 30 + 29

PROBLEMA 09 :QUESTÃO 13. (2020 –NL 1)

Tiago estava fazendo uma conta em seu caderno quando sua caneta estragou e borrou quatro algarismos, como na figura. Ele se lembra de que só havia algarismos ímpares na conta. Qual é a soma dos algarismos manchados ?

Figura 5 : borrado



Fonte :OBMEP

A) 28

B) 26

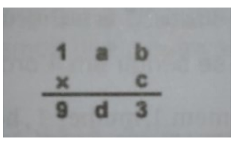
C) 20

D) 18

E) 14

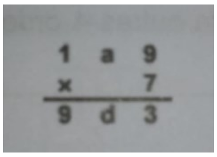
SOLUÇÃO OBMEP - (alternativa b)

Figura 6 :borrado 1

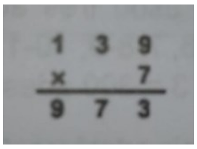


Fonte :OBMEP

Vamos chamar os algarismo borrado de a,b,c, e d, como ilustrado acima. Como o algarismo das unidades do resultado é 3, temos quatro possibilidades para b e c, nesta ordem: 1 e 3, 3 e 1, 7 e 9 ou 9 e 7. Como o multiplicador é menos que 200, podemos eliminar as duas primeiras



possibilidades, pois um número menos que 200 multiplicado por 1 ou por 3 não passa de 600. Na terceira possibilidade, o multiplicando seria no mínimo 117 e, então, o produto seria no mínimo 117 x 9 = 1053, o que não acontece.



Resta a última possibilidade, que está ilustrada acima. Como 117 x 7 = 819, tentamos 139 x 7 = 973, que está de acordo com o enunciado. Logo os algarismos manchados são 3,9,7 e 7 , e sua soma é 3 + 9 + 7 + 7 = 26.

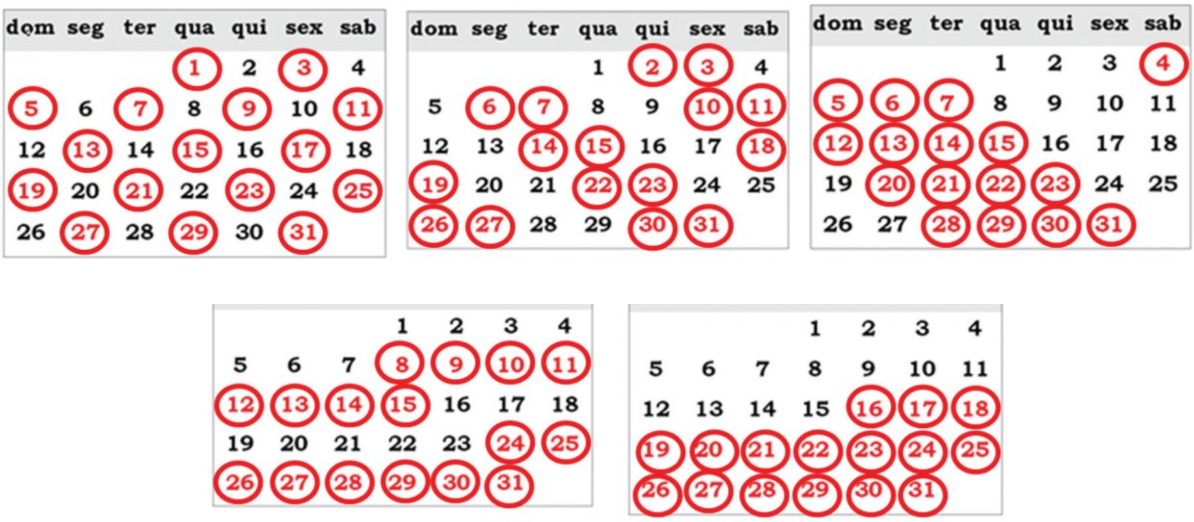
SOLUÇÃO SUGERIDA

Fazendo pelo método da tentativa temos que começamos usando 3 x 1, porém não será possível pois a casa da centena tem como resultado 9, ai então vamos para a segunda opção usando 9 x 7 porém também não é possível pois teremos que a casa da dezena fica no número 0 que é par e não pode ser usado pelo enunciado, logo só nos resta a ultima opção que é, 7x 139 = 973 cuja opção é de correta, e somando os dígitos pedidos no problema temos : 3 + 9 + 7+ 7 = 26. Que é a resposta correta.

PROBLEMA 10 : (OBMEP 2019 NIVEL 1) Mágica para adivinhar o dia do aniversário de uma pessoa

Utilizando os calendários abaixo é possível adivinhar o dia em que uma pessoa nasceu.

Figura 7 : Calendário



Fonte :OBMEP

Basta seguir as instruções:

1. Peça à pessoa que indique em quais dos calendários a data de seu nascimento aparece circulada. *(Faça um teste com o dia de seu próprio aniversário).*

2. Some os primeiros números circulados que estão nos calendários indicados pela pessoa (somente nesses) e você descobrirá a data de seu aniversário, sem que ela lhe conte. Observe que os calendários não indicados pela pessoa não entram na conta. *(No caso de seu próprio aniversário, confira se a soma que você encontrou coincide com o dia em que você nasceu).*

Veja um exemplo:

Se o dia do aniversário de uma pessoa aparece circulado apenas no primeiro e no último calendário, localize as primeiras datas circuladas nesses dois calendários: é o 1 no primeiro calendário e o 16 no último. Somando 1 + 16 você adivinha o dia em que a pessoa nasceu: é o dia 17.

O truque permite também adivinhar o mês de nascimento, desde que os meses sejam numerados:

1 – janeiro, 2 – fevereiro, 3 – março, 4 – abril, 5 – maio, 6 – junho, 7 – julho, 8 – agosto, 9 – setembro, 10 – outubro, 11 – novembro e 12 – dezembro.

Para isso, uma nova consulta aos calendários deve ser feita, e o truque funciona da mesma maneira: basta somar os primeiros números circulados que estão presentes nos calendários indicados pela pessoa (ou seja, nos calendários em que o número do mês em que a pessoa nasceu estão circulados). Por exemplo, se o número do mês estiver no segundo e no terceiro calendários, como 2 + 4 = 6, a pessoa nasceu no mês de junho. Assim, podemos adivinhar o dia e o mês em que a pessoa nasceu.

SOLUÇÃO DA OBMEP:

A adivinhação é baseada no fato de que todo número natural pode ser escrito como soma de potências de 2, e essa decomposição é única (decomposição na base 2). Isto é, se $n \varepsilon N$, então n é uma soma única de parcelas da forma $a \times 2^J$, com $a \varepsilon \{0, 1\}$ e $j \varepsilon N$. Quando um número está circulado em um calendário, a potência de 2 correspondente a esse calendário (ou seja, o primeiro número circulado nesse calendário) entra na soma, pois o algarismo que acompanha a potência de 2 correspondente é igual a 1 e, quando um número não está circulado, a potência de 2 correspondente não entra na soma.

Observe: $17 = 1 + 16 = 1 \times 2^0 + 0 \times 2^1 + 0 \times 2^2 + 0 \times 2^3 + 1 \times 2^4$, por esse motivo 17 está circulado apenas no primeiro e no último calendário.

Em outras palavras: Os calendários estão organizados de modo que cada um deles revela o algarismo que está presente na decomposição binária do número.

· O primeiro calendário nos diz se a potência $2^0 = 1$ faz parte ou não da decomposição do número na base 2.

· O segundo calendário nos diz se a potência $2^1 = 2$ faz parte ou não da decomposição do número na base 2.

· O terceiro calendário nos diz se a potência $2^2 = 4$ faz parte ou não da decomposição do número na base 2.

· O quarto calendário nos diz se a potência $2^3 = 8$ faz parte ou não da decomposição do número na base 2.

· O quinto calendário nos diz se a potência $2^4 = 16$ faz parte ou não da decomposição do número na base 2.

Como todo número tem uma decomposição única na base 2, isso permite, realizando somas de potências de 2, fazer a adivinhação.

COMENTÁRIO

Observamos nessa questão uma aplicação da decomposição em fatores primos , neste exercício lúdico que nós mostra aplicação da aritmética no ensino da matemática, podendo assim dar um exemplo prática da utilização da técnica de critérios de divisibilidade por 2 para os alunos da educação básica, sabendo que os alunos gostam muitos de jogos matemáticos é um interessante exemplo pra chamar a atenção e despertar o interesse pela matemática e introduzir conceitos matemáticos de forma lúdica.

PROBLEMA 11 :QUESTÃO 1. (2019 – nível 1)

Qual é o número que está escondido pelo borrão?

$17 - 3 = 20 - 16 +$ 

A) 10

B) 11

C) 12

D) 13

E) 14

SOLUÇÃO OBMEP - QUESTÃO 1 ALTERNATIVA A

Como 17 – 3 = 14 e 20 – 16 = 4, a conta com o borrão é a mesma que

$14 = 4 +$ 

Ora, qual é o número que somado com 4 dá 14? É o número 10. Logo, o número escondido pelo borrão é o número 10.

SOLUÇÃO SUGERIDA

Podemos usar do algoritmo mais usual entre os alunos que é jogar os números para o outro lado trocando de sinais e substituindo a mancha por “x”:

17 – 3 = 20 – 16 + x $\rightarrow$ 14 - 4 = x $\rightarrow$ 10 = x . logo a solução é 10

PROBLEMA 12 : QUESTÃO 6. (2019 – nível 1)**.** Qual das expressões abaixo tem valor diferente de $\frac{15}{4}$?

Figura 8 :Professor

Fonte :OBMEP

A) $15 \times \frac{1}{4}$

B) $\frac{15+15+15}{4+4+4}$

C) $\frac{3}{4} + 3$

D) $\frac{10}{2} + \frac{5}{2}$

E) $\frac{3}{2} \times \frac{5}{2}$

SOLUÇÃO OBMEP - QUESTÃO 6 (ALTERNATIVA D)

Os valores das expressões nas alternativas são:

A) $15 \times \frac{1}{4} = \frac{15}{4}$

B) $\frac{15+15+15}{4+4+4} = \frac{15}{4}$

C) $\frac{3}{4} + 3 = \frac{15}{4}$

D) $\frac{10}{2} + \frac{5}{2} = \frac{15}{2}$

E) $\frac{3}{2} \times \frac{5}{2} = \frac{15}{4}$

Logo, a única alternativa em que o valor da expressão não é igual a 15/4 é a alternativa D.

SOLUÇÃO SUGERIDA

Uma questão muito boa para se trabalhar as regras de operações com frações, pode-se trabalhar essa questão desde o 6º ano do ensino fundamental, detalhando e ensinando frações e tirando dúvidas de alunos mostrando que a prova da OBMEP não é um complexa como muitos pensam, esse é um ótimo exemplo para ser colocado em livros didáticos nacionais.

PROBLEMA 13 :QUESTÃO 7. (2020 – nível 1)**7.**

As casas da figura abaixo devem ser preenchidas com números primos. Em cada linha ou coluna, o produto dos números deve ser igual ao número indicado pela seta. A coluna indicada por 294 já está preenchida. Qual é o número que deve ser escrito na casa marcada com * ?

Figura 9 : Trilha

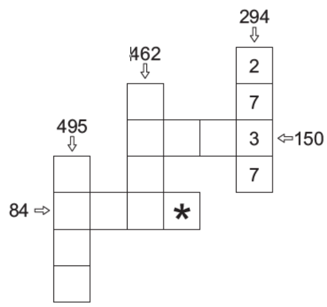
A) 2

B) 3

C) 5

D) 7

E) 11



Fonte :OBMEP

SOLUÇÃO OBMEP - QUESTÃO 7 ALTERNATIVA A

Inicialmente, observamos que as decomposições em fatores primos dos números que aparecem no enunciado são:

462 = 2.3.7.11

150 = 2.3.5.5

495 = 3.3.5.11

84 = 2.2.3.7

Na interseção de 150 com 462, deve aparecer o 2, pois o 3 já está na interseção de 150 com 294. A interseção de 495 com 84 deve ser preenchida com o 3, pois é o único fator primo comum entre esses dois números. Desta forma, sobra o 7 para a interseção de 462 com 84. Então, como a fatoração do 84 é 3 . 2 . 7 . 2, concluímos que $*$ = 2.

SOLUÇÃO SUGERIDA

Nas resoluções são explorados os conteúdos decomposição em fatores primos, divisibilidade e propriedades de potenciação muitos estudantes têm dificuldades em resolver problemas envolvendo fatores primos, apesar de pertencer a grade curricular de matemática do Ensino Fundamental. Sendo assim seria conveniente o professor fazer revisão sobre o assunto

PROBLEMA 14 : QUESTÃO 8. (2019 – nível 1**).** Os números a e b são inteiros positivos tais que $\frac{a}{11} + \frac{b}{3} = \frac{31}{33}$. Qual é o valor de $a + b$?

A) 5

B) 7

C) 14

D) 20

E) 31

SOLUÇÃO OBMEP - QUESTÃO 8 (ALTERNATIVA A)

Reescrevendo as frações da equação com um mesmo denominador comum e cancelando esse denominador, temos: $\frac{a}{11} + \frac{b}{3} = \frac{31}{33} \leftrightarrow \frac{3a}{11} + \frac{11b}{3} = \frac{31}{33} \leftrightarrow 3a + 11b = 31$

Logo, como a e b são inteiros positivos, b só pode assumir os valores 1, 2, senão o primeiro membro da última igualdade seria maior do que 31. Temos as seguintes possibilidades:

* $b = 1 \Rightarrow 3a + 11 = 31 \Rightarrow 3a = 20$, impossível, pois a é inteiro.

* $b = 2 \Rightarrow 3a + 22 = 31 \Rightarrow 3a = 9 \Rightarrow a = 3$.

Assim, $a = 3$, $b = 2$ e, portanto, $a + b = 5$.

SOLUÇÃO SUGERIDA

Vemos um ótimo exemplo de divisão para usar na educação básica, trazendo os alunos a conceitos básicos e critérios de divisibilidade aplicado nas provas, o professor deve rever conceitos de divisão nos naturais e instigar os alunos a usar métodos de tentativas, ensinando a ideia que por tentativa também é possível solucionar problemas.

PROBLEMA 15 : QUESTÃO 1. (2020 – nível 1) Os estudantes de uma escola foram divididos em equipes de 8 meninas e 5 meninos cada uma. Se nessa escola há 60 meninas a mais do que meninos, qual é o número total de estudantes?

A) 130

B) 260

C) 390

D) 520

E) 650

SOLUÇÃO OBMEP - QUESTÃO 1 (ALTERNATIVA B)

Em um grupo de 13 estudantes temos 8 meninas e 5 meninos, ou seja, 3 meninas a mais. Em 20 grupos de 13 estudantes teremos exatamente 60 meninas a mais do que meninos. Logo, no total temos $20 \times 13 = 260$ estudantes.

SOLUÇÃO SUGERIDA

Usando conceitos de proporção temos que 8 meninas e 5 meninos total 13 alunos (3 meninas a mais) 16 meninas e 10 meninos total 26 alunos (6 meninas a mais)(dobrando a quantidade). Como a quantidade de meninas dobra a cada vez que dobramos a quantidade total, temos então que para se ter 60 meninas a mais que meninos devemos dividir 60 /3 = 20 logo basta multiplicar 8x20 + 5x20 = 260 alunos.

PROBLEMA 16 : QUESTÃO 6. (2019 – nível 2)**.**

Em uma lanchonete, um pão de queijo, dois cachorros quentes e um suco de laranja custam juntos R$ 31,00; já três pães de queijo, três cachorros-quentes e dois sucos de laranja custam juntos R$ 59,00. Qual é a diferença entre os preços de um cachorro-quente e de um pão de queijo?

A) R$ 1,00

B) R$ 1,50

C) R$ 2,00

D) R$ 2,50

E) R$ 3,00

Figura 10 : Pão

Fonte :OBMEP

SOLUÇÃO OBMEP - QUESTÃO 6 (ALTERNATIVA E)

Vamos usar as letras p, c e s para denotar o preço (em reais) de um pão de queijo, de um cachorro-quente e de um suco de laranja, respectivamente. O enunciado nos diz que $p+2c+s=31$ e $3p+3c+2s=59$. Multiplicando a primeira expressão por 2 e subtraindo do resultado, pois, assim, a segunda expressão, obtemos $2(p+2c+s)-(3p+3c+2s)=c-p$ e, por outro lado, $2(p+2c+s)-(3p+3c+2s)=2\cdot 31-59=3$, ou seja, $c-p=3$.

Vamos a outra solução; ao contrário da anterior, onde o $c-p$ apareceu “por acaso”, nessa vamos sistematicamente em busca de $c-p$, escrevendo $31=p+2c+s=2(c-p)+3p+s$ e $59=3p+3c+2s=3(c-p)+6p+2s$.

Observando essas expressões, notamos que o $6p+2s$ da segunda é duas vezes o $3p+s$ da primeira, o que sugere multiplicar a primeira expressão por 2 e subtrair a segunda do resultado, pois assim os termos em p e s desaparecem, restando apenas um termo em $c-p$. Temos então $2\cdot 31-59=[4(c-p)+6p+2s]-[3(c-p)+6p+2s]=c-p$, ou seja, temos $c-p=3$ como antes.

SOLUÇÃO SUGERIDA

Usando sistemas de equações temos

$$\begin{cases} x + 2y + z = 31 \\ 3x + 3y + 2z = 59 \\ 4x + 5y + 3z = 90 \end{cases} \Rightarrow \begin{cases} x + 2y + z = 31 \\ x - y = -3 \end{cases}$$ Logo y – x = 3.

PROBLEMA 17 :QUESTÃO 10. (2020 – nível 1) Qual é a soma dos algarismos do número $\sqrt{1111111111 - 22222}$?

A) 10

B) 15

C) 18

D) 20

E) 25

SOLUÇÃO OBMEP - QUESTÃO 10 (ALTERNATIVA B)

Observando que $1111111111 = \frac{10^{10}-1}{9}$ e $11111 = 2 \text{ x } 11111 = 2 \text{ x } \frac{10^5-1}{9}$, temos $\sqrt{\frac{10^{10}-1}{9} - 2 \text{ x } \frac{10^5-1}{9}} = \frac{\sqrt{10^{10}-2.10^5+1}}{3} = \frac{\sqrt{(10^5-1)\text{^}2}}{3} = \frac{10^5-1}{3} = 3 \text{ x } \frac{10^5-1}{9} = 3\text{x}11111 = 33333.$ Logo, a soma dos algarismos do número apresentado no enunciado é $3 \times 5 = 15$

COMENTÁRIO.

Vemos aqui a necessidade de se ensinar critérios de divisibilidades, pois vemos a aplicação de divisibilidade por 9 e critérios de potenciação. Sem a mesma é impossível de resolver o problema.

EXPLANAÇÃO SOBRE OS EXERCÍCIOS

Ao analisar essa seção, vemos que a prova da OBMEP cobra conceitos que não estão presentes no dia a dia do aluno na sala de aula, como teorema chinês, algoritmo de Euclides, congruência modular, vemos ainda que na resolução das questões disponibilizadas pela OBMEP, ela usa desses teoremas para resolver suas questões, assim vemos a necessidade de se atualizar o PCC da escola e incluir esses teoremas na educação básica, para que se mantenha a coerência do que é cobrado para o que é ensinado e assim melhorar os índices de alunos ,escolas e secretárias que participam da olimpíada.

CONSIDERAÇÕES FINAIS

Concluí que os objetivos foram compridos, considerando que foram apresentados os fundamentos teóricos e conceituais da aritmética, através de demonstrações e exposições dos mesmos, abordaram-se também exercícios da OBMEP relacionados à Aritmética, mostrando comentários, exemplos, aplicações com soluções práticas e dinâmicas. Foram mostradas outras vias de solução para exercícios da OBMEP, que pode contribuir para a preparação dos alunos pelos seus professores. Pode-se observar que o uso de teoremas da aritmética como ferramentas para resolver problemas da OBMEP resulta de grande utilidade e contribui para a diminuição do tempo de resolução dos exercícios nas provas. O banco de questões da OBMEP resulta importante para auxiliar e enriquecer o conhecimento e técnicas de resolução das provas ,dando outras opções de raciocínio e discussões em sala de aula, contribuindo assim para o ensino-aprendizagem da aritmética na educação básica. Acredito que o presente trabalho possa contribuir para auxiliar professores e alunos da rede pública e privada de ensino na resolução de problemas matemáticos das provas da OBMEP. O professor pode trabalhar esses temas em sala de aula, acrescenta-los no PCC da escola, pode ainda criar grupos de estudos com alunos para prepara-los para a prova , ensinando os teoremas aqui expostos como auxilio para a resolução das questões, para assim se criar uma cultura de estudos sobre a OBMEP na escola, minimizando assim as deficiências do aluno da escola, contribuindo para a desmistificação da resolução de problemas e a melhora do desempenho dos estudantes na OBMEP e nas suas escolas. Este trabalho também foi muito importante para o desenvolvimento matemático e profissional do autor, que agradece ao PROFMAT pela sua contribuição com a formação de professores bem qualificados para enfrentar a docência nas escolas brasileiras.

REFERENÇIAS

MOREIRA, Carlos Gustavo. MOTTA, Edmilson. TEGAN,Eduardo. AMÂNCIO, Luiz. SALDANHA, Nicolau. RODRIGUES, Paulo. Olimpíadas Brasileira de Matemática. 9ª a I6ª – Problemas e Soluções. Coleção Olimpíadas de Matemática. 2ª edição. Rio de Janeiro 2009.

BRASIL, M. d. E. e. S. d. E. B. *Base Nacional Comum Curricular*. [S.l.: s.n.], 2017.

BRASIL, S. d. E. F. *Parâmetros curriculares nacionais: matemática*. [S.l.: s.n.], 1998.

NETO, Antônio Caminha Muniz. Tópicos de Matemática Elementar. *Números Reais.* Volume 1. 2ª edição 2ª impressão. SBM Coleção do Professor de Matemática. Rio de Janeiro 2014.

HEFEZ, A. *Elementos de aritmética,(Coleção do Professor de Matemática)*. Rio de Janeiro: SBM, 2011.

HEFEZ, A. *Aritmética,(Coleção Profmat)*. Rio de Janeiro: SBM, 2014.

HEFEZ, A. *Iniciação à aritmética*. Rio de Janeiro: IMPA, 2015.

OBM. *Histórico*. Disponível em: <https://www.obm.org.br/quem-somos/historico/>. Acesso em: 4 fev. 2011.

OBMEP. *Provas e Soluções*. Disponível em <http://www.obmep.org.br/provas.htm>: Olimpíada Brasileira De Matemática Das Escolas Públicas, 2021.

OBMEP EM NÚMEROS. *Olimpíada Brasileira De Matemática Das Escolas Públicas*. Disponível em: <http://www.obmep.org.br/em-numeros.htm>. Acesso em: 28 dez. 2021.

REGULAMENTO. *Olimpíada Brasileira De Matemática Das Escolas Públicas*. Disponível em: <http://www.obmep.org.br/regulamento.htm>. Acesso em: 24 jan. 2019.

OBMEP. APRESENTAÇÃO E CRONOLOGIA. Disponível em <http://www.obmep.org.br/provas.htm>: Olimpíada Brasileira De Matemática Das Escolas Públicas, 2021.

Carl B. Boyer . História da Matemática . Rio de Janeiro: estante virtual 2014