

Ciências Exatas e da Terra: Aprendizado, Integração e Necessidades do País 2

Américo Junior Nunes da Silva
André Ricardo Lucas Vieira
(Organizadores)

Ciências Exatas e da Terra: Aprendizado, Integração e Necessidades do País 2

Américo Junior Nunes da Silva
André Ricardo Lucas Vieira
(Organizadores)

Editora Chefe

Profª Drª Antonella Carvalho de Oliveira

Assistentes Editoriais

Natalia Oliveira

Bruno Oliveira

Flávia Roberta Barão

Bibliotecária

Janaina Ramos

Projeto Gráfico e Diagramação

Natália Sandrini de Azevedo

Camila Alves de Cremo

Luiza Alves Batista

Maria Alice Pinheiro

Imagens da Capa

Shutterstock

Edição de Arte

Luiza Alves Batista

Revisão

Os Autores

2021 by Atena Editora

Copyright © Atena Editora

Copyright do Texto © 2021 Os autores

Copyright da Edição © 2021 Atena Editora

Direitos para esta edição cedidos à Atena Editora pelos autores.



Todo o conteúdo deste livro está licenciado sob uma Licença de Atribuição *Creative Commons*. Atribuição-Não-Comercial-NãoDerivativos 4.0 Internacional (CC BY-NC-ND 4.0).

O conteúdo dos artigos e seus dados em sua forma, correção e confiabilidade são de responsabilidade exclusiva dos autores, inclusive não representam necessariamente a posição oficial da Atena Editora. Permitido o *download* da obra e o compartilhamento desde que sejam atribuídos créditos aos autores, mas sem a possibilidade de alterá-la de nenhuma forma ou utilizá-la para fins comerciais.

Todos os manuscritos foram previamente submetidos à avaliação cega pelos pares, membros do Conselho Editorial desta Editora, tendo sido aprovados para a publicação com base em critérios de neutralidade e imparcialidade acadêmica.

A Atena Editora é comprometida em garantir a integridade editorial em todas as etapas do processo de publicação, evitando plágio, dados ou resultados fraudulentos e impedindo que interesses financeiros comprometam os padrões éticos da publicação. Situações suspeitas de má conduta científica serão investigadas sob o mais alto padrão de rigor acadêmico e ético.

Conselho Editorial

Ciências Humanas e Sociais Aplicadas

Prof. Dr. Alexandre Jose Schumacher – Instituto Federal de Educação, Ciência e Tecnologia do Paraná

Prof. Dr. Américo Junior Nunes da Silva – Universidade do Estado da Bahia

Prof. Dr. Antonio Carlos Frasson – Universidade Tecnológica Federal do Paraná

Prof. Dr. Antonio Gasparetto Júnior – Instituto Federal do Sudeste de Minas Gerais
Prof. Dr. Antonio Isidro-Filho – Universidade de Brasília
Prof. Dr. Carlos Antonio de Souza Moraes – Universidade Federal Fluminense
Prof. Dr. Crisóstomo Lima do Nascimento – Universidade Federal Fluminense
Prof^ª Dr^ª Cristina Gaio – Universidade de Lisboa
Prof. Dr. Daniel Richard Sant’Ana – Universidade de Brasília
Prof. Dr. Deyvison de Lima Oliveira – Universidade Federal de Rondônia
Prof^ª Dr^ª Dilma Antunes Silva – Universidade Federal de São Paulo
Prof. Dr. Edvaldo Antunes de Farias – Universidade Estácio de Sá
Prof. Dr. Elson Ferreira Costa – Universidade do Estado do Pará
Prof. Dr. Eloi Martins Senhora – Universidade Federal de Roraima
Prof. Dr. Gustavo Henrique Cepolini Ferreira – Universidade Estadual de Montes Claros
Prof^ª Dr^ª Ivone Goulart Lopes – Instituto Internazionele delle Figlie de Maria Ausiliatrice
Prof. Dr. Jadson Correia de Oliveira – Universidade Católica do Salvador
Prof. Dr. Julio Candido de Meirelles Junior – Universidade Federal Fluminense
Prof^ª Dr^ª Lina Maria Gonçalves – Universidade Federal do Tocantins
Prof. Dr. Luis Ricardo Fernandes da Costa – Universidade Estadual de Montes Claros
Prof^ª Dr^ª Natiéli Piovesan – Instituto Federal do Rio Grande do Norte
Prof. Dr. Marcelo Pereira da Silva – Pontifícia Universidade Católica de Campinas
Prof^ª Dr^ª Maria Luzia da Silva Santana – Universidade Federal de Mato Grosso do Sul
Prof^ª Dr^ª Paola Andressa Scortegagna – Universidade Estadual de Ponta Grossa
Prof^ª Dr^ª Rita de Cássia da Silva Oliveira – Universidade Estadual de Ponta Grossa
Prof. Dr. Rui Maia Diamantino – Universidade Salvador
Prof. Dr. Urandi João Rodrigues Junior – Universidade Federal do Oeste do Pará
Prof^ª Dr^ª Vanessa Bordin Viera – Universidade Federal de Campina Grande
Prof. Dr. William Cleber Domingues Silva – Universidade Federal Rural do Rio de Janeiro
Prof. Dr. Willian Douglas Guilherme – Universidade Federal do Tocantins

Ciências Agrárias e Multidisciplinar

Prof. Dr. Alexandre Igor Azevedo Pereira – Instituto Federal Goiano
Prof^ª Dr^ª Carla Cristina Bauermann Brasil – Universidade Federal de Santa Maria
Prof. Dr. Antonio Pasqualetto – Pontifícia Universidade Católica de Goiás
Prof. Dr. Cleberton Correia Santos – Universidade Federal da Grande Dourados
Prof^ª Dr^ª Daiane Garabeli Trojan – Universidade Norte do Paraná
Prof^ª Dr^ª Diocléa Almeida Seabra Silva – Universidade Federal Rural da Amazônia
Prof. Dr. Écio Souza Diniz – Universidade Federal de Viçosa
Prof. Dr. Fábio Steiner – Universidade Estadual de Mato Grosso do Sul
Prof. Dr. Fágner Cavalcante Patrocínio dos Santos – Universidade Federal do Ceará
Prof^ª Dr^ª Girlene Santos de Souza – Universidade Federal do Recôncavo da Bahia
Prof. Dr. Jael Soares Batista – Universidade Federal Rural do Semi-Árido
Prof. Dr. Júlio César Ribeiro – Universidade Federal Rural do Rio de Janeiro
Prof^ª Dr^ª Lina Raquel Santos Araújo – Universidade Estadual do Ceará
Prof. Dr. Pedro Manuel Villa – Universidade Federal de Viçosa
Prof^ª Dr^ª Raissa Rachel Salustriano da Silva Matos – Universidade Federal do Maranhão
Prof. Dr. Ronilson Freitas de Souza – Universidade do Estado do Pará
Prof^ª Dr^ª Talita de Santos Matos – Universidade Federal Rural do Rio de Janeiro
Prof. Dr. Tiago da Silva Teófilo – Universidade Federal Rural do Semi-Árido

Prof. Dr. Valdemar Antonio Paffaro Junior – Universidade Federal de Alfenas

Ciências Biológicas e da Saúde

Prof. Dr. André Ribeiro da Silva – Universidade de Brasília

Prof^ª Dr^ª Anelise Levay Murari – Universidade Federal de Pelotas

Prof. Dr. Benedito Rodrigues da Silva Neto – Universidade Federal de Goiás

Prof^ª Dr^ª Débora Luana Ribeiro Pessoa – Universidade Federal do Maranhão

Prof. Dr. Douglas Siqueira de Almeida Chaves – Universidade Federal Rural do Rio de Janeiro

Prof. Dr. Edson da Silva – Universidade Federal dos Vales do Jequitinhonha e Mucuri

Prof^ª Dr^ª Elizabeth Cordeiro Fernandes – Faculdade Integrada Medicina

Prof^ª Dr^ª Eleuza Rodrigues Machado – Faculdade Anhanguera de Brasília

Prof^ª Dr^ª Elane Schwinden Prudêncio – Universidade Federal de Santa Catarina

Prof^ª Dr^ª Eysler Gonçalves Maia Brasil – Universidade da Integração Internacional da Lusofonia Afro-Brasileira

Prof. Dr. Ferlando Lima Santos – Universidade Federal do Recôncavo da Bahia

Prof. Dr. Fernando Mendes – Instituto Politécnico de Coimbra – Escola Superior de Saúde de Coimbra

Prof^ª Dr^ª Gabriela Vieira do Amaral – Universidade de Vassouras

Prof. Dr. Gianfábio Pimentel Franco – Universidade Federal de Santa Maria

Prof. Dr. Helio Franklin Rodrigues de Almeida – Universidade Federal de Rondônia

Prof^ª Dr^ª Iara Lúcia Tescarollo – Universidade São Francisco

Prof. Dr. Igor Luiz Vieira de Lima Santos – Universidade Federal de Campina Grande

Prof. Dr. Jefferson Thiago Souza – Universidade Estadual do Ceará

Prof. Dr. Jesus Rodrigues Lemos – Universidade Federal do Piauí

Prof. Dr. Jônatas de França Barros – Universidade Federal do Rio Grande do Norte

Prof. Dr. José Max Barbosa de Oliveira Junior – Universidade Federal do Oeste do Pará

Prof. Dr. Luís Paulo Souza e Souza – Universidade Federal do Amazonas

Prof^ª Dr^ª Magnólia de Araújo Campos – Universidade Federal de Campina Grande

Prof. Dr. Marcus Fernando da Silva Praxedes – Universidade Federal do Recôncavo da Bahia

Prof^ª Dr^ª Maria Tatiane Gonçalves Sá – Universidade do Estado do Pará

Prof^ª Dr^ª Mylena Andréa Oliveira Torres – Universidade Ceuma

Prof^ª Dr^ª Natiéli Piovesan – Instituto Federaci do Rio Grande do Norte

Prof. Dr. Paulo Inada – Universidade Estadual de Maringá

Prof. Dr. Rafael Henrique Silva – Hospital Universitário da Universidade Federal da Grande Dourados

Prof^ª Dr^ª Regiane Luz Carvalho – Centro Universitário das Faculdades Associadas de Ensino

Prof^ª Dr^ª Renata Mendes de Freitas – Universidade Federal de Juiz de Fora

Prof^ª Dr^ª Vanessa Lima Gonçalves – Universidade Estadual de Ponta Grossa

Prof^ª Dr^ª Vanessa Bordin Viera – Universidade Federal de Campina Grande

Ciências Exatas e da Terra e Engenharias

Prof. Dr. Adélio Alcino Sampaio Castro Machado – Universidade do Porto

Prof. Dr. Carlos Eduardo Sanches de Andrade – Universidade Federal de Goiás

Prof^ª Dr^ª Carmen Lúcia Voigt – Universidade Norte do Paraná

Prof. Dr. Cleiseano Emanuel da Silva Paniagua – Instituto Federal de Educação, Ciência e Tecnologia de Goiás

Prof. Dr. Douglas Gonçalves da Silva – Universidade Estadual do Sudoeste da Bahia

Prof. Dr. Eloi Rufato Junior – Universidade Tecnológica Federal do Paraná
Prof^ª Dr^ª Érica de Melo Azevedo – Instituto Federal do Rio de Janeiro
Prof. Dr. Fabrício Menezes Ramos – Instituto Federal do Pará
Prof^ª Dra. Jéssica Verger Nardeli – Universidade Estadual Paulista Júlio de Mesquita Filho
Prof. Dr. Juliano Carlo Rufino de Freitas – Universidade Federal de Campina Grande
Prof^ª Dr^ª Luciana do Nascimento Mendes – Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
Prof. Dr. Marcelo Marques – Universidade Estadual de Maringá
Prof. Dr. Marco Aurélio Kistemann Junior – Universidade Federal de Juiz de Fora
Prof^ª Dr^ª Neiva Maria de Almeida – Universidade Federal da Paraíba
Prof^ª Dr^ª Natiéli Piovesan – Instituto Federal do Rio Grande do Norte
Prof^ª Dr^ª Priscila Tessmer Scaglioni – Universidade Federal de Pelotas
Prof. Dr. Takeshy Tachizawa – Faculdade de Campo Limpo Paulista

Linguística, Letras e Artes

Prof^ª Dr^ª Adriana Demite Stephani – Universidade Federal do Tocantins
Prof^ª Dr^ª Angeli Rose do Nascimento – Universidade Federal do Estado do Rio de Janeiro
Prof^ª Dr^ª Carolina Fernandes da Silva Mandaji – Universidade Tecnológica Federal do Paraná
Prof^ª Dr^ª Denise Rocha – Universidade Federal do Ceará
Prof. Dr. Fabiano Tadeu Grazioli – Universidade Regional Integrada do Alto Uruguai e das Missões
Prof. Dr. Gilmei Fleck – Universidade Estadual do Oeste do Paraná
Prof^ª Dr^ª Keyla Christina Almeida Portela – Instituto Federal de Educação, Ciência e Tecnologia do Paraná
Prof^ª Dr^ª Miranilde Oliveira Neves – Instituto de Educação, Ciência e Tecnologia do Pará
Prof^ª Dr^ª Sandra Regina Gardacho Pietrobon – Universidade Estadual do Centro-Oeste
Prof^ª Dr^ª Sheila Marta Carregosa Rocha – Universidade do Estado da Bahia

Conselho Técnico Científico

Prof. Me. Abrãao Carvalho Nogueira – Universidade Federal do Espírito Santo
Prof. Me. Adalberto Zorzo – Centro Estadual de Educação Tecnológica Paula Souza
Prof. Dr. Adaylson Wagner Sousa de Vasconcelos – Ordem dos Advogados do Brasil/Seccional Paraíba
Prof. Dr. Adilson Tadeu Basquerote Silva – Universidade para o Desenvolvimento do Alto Vale do Itajaí
Prof. Dr. Alex Luis dos Santos – Universidade Federal de Minas Gerais
Prof. Me. Aleksandro Teixeira Ribeiro – Centro Universitário Internacional
Prof^ª Ma. Aline Ferreira Antunes – Universidade Federal de Goiás
Prof. Me. André Flávio Gonçalves Silva – Universidade Federal do Maranhão
Prof^ª Ma. Andréa Cristina Marques de Araújo – Universidade Fernando Pessoa
Prof^ª Dr^ª Andreza Lopes – Instituto de Pesquisa e Desenvolvimento Acadêmico
Prof^ª Dr^ª Andrezza Miguel da Silva – Faculdade da Amazônia
Prof^ª Ma. Anelisa Mota Gregoleti – Universidade Estadual de Maringá
Prof^ª Ma. Anne Karynne da Silva Barbosa – Universidade Federal do Maranhão
Prof. Dr. Antonio Hot Pereira de Faria – Polícia Militar de Minas Gerais
Prof. Me. Armando Dias Duarte – Universidade Federal de Pernambuco
Prof^ª Ma. Bianca Camargo Martins – UniCesumar

Profª Ma. Carolina Shimomura Nanya – Universidade Federal de São Carlos
Prof. Me. Carlos Antônio dos Santos – Universidade Federal Rural do Rio de Janeiro
Prof. Me. Christopher Smith Bignardi Neves – Universidade Federal do Paraná
Prof. Ma. Cláudia de Araújo Marques – Faculdade de Música do Espírito Santo
Profª Drª Cláudia Taís Siqueira Cagliari – Centro Universitário Dinâmica das Cataratas
Prof. Me. Clécio Danilo Dias da Silva – Universidade Federal do Rio Grande do Norte
Prof. Me. Daniel da Silva Miranda – Universidade Federal do Pará
Profª Ma. Daniela da Silva Rodrigues – Universidade de Brasília
Profª Ma. Daniela Remião de Macedo – Universidade de Lisboa
Profª Ma. Dayane de Melo Barros – Universidade Federal de Pernambuco
Prof. Me. Douglas Santos Mezacas – Universidade Estadual de Goiás
Prof. Me. Edevaldo de Castro Monteiro – Embrapa Agrobiologia
Prof. Me. Eduardo Gomes de Oliveira – Faculdades Unificadas Doctum de Cataguases
Prof. Me. Eduardo Henrique Ferreira – Faculdade Pitágoras de Londrina
Prof. Dr. Edwaldo Costa – Marinha do Brasil
Prof. Me. Eliel Constantino da Silva – Universidade Estadual Paulista Júlio de Mesquita
Prof. Me. Ernane Rosa Martins – Instituto Federal de Educação, Ciência e Tecnologia de Goiás
Prof. Me. Euvaldo de Sousa Costa Junior – Prefeitura Municipal de São João do Piauí
Prof. Dr. Everaldo dos Santos Mendes – Instituto Edith Theresa Hedwing Stein
Prof. Me. Ezequiel Martins Ferreira – Universidade Federal de Goiás
Profª Ma. Fabiana Coelho Couto Rocha Corrêa – Centro Universitário Estácio Juiz de Fora
Prof. Me. Fabiano Eloy Atilio Batista – Universidade Federal de Viçosa
Prof. Me. Felipe da Costa Negrão – Universidade Federal do Amazonas
Prof. Me. Francisco Odécio Sales – Instituto Federal do Ceará
Profª Drª Germana Ponce de Leon Ramírez – Centro Universitário Adventista de São Paulo
Prof. Me. Gevair Campos – Instituto Mineiro de Agropecuária
Prof. Me. Givanildo de Oliveira Santos – Secretaria da Educação de Goiás
Prof. Dr. Guilherme Renato Gomes – Universidade Norte do Paraná
Prof. Me. Gustavo Krahl – Universidade do Oeste de Santa Catarina
Prof. Me. Helton Rangel Coutinho Junior – Tribunal de Justiça do Estado do Rio de Janeiro
Profª Ma. Isabelle Cerqueira Sousa – Universidade de Fortaleza
Profª Ma. Jaqueline Oliveira Rezende – Universidade Federal de Uberlândia
Prof. Me. Javier Antonio Albornoz – University of Miami and Miami Dade College
Prof. Me. Jhonatan da Silva Lima – Universidade Federal do Pará
Prof. Dr. José Carlos da Silva Mendes – Instituto de Psicologia Cognitiva, Desenvolvimento Humano e Social
Prof. Me. Jose Elyton Batista dos Santos – Universidade Federal de Sergipe
Prof. Me. José Luiz Leonardo de Araujo Pimenta – Instituto Nacional de Investigación Agropecuaria Uruguay
Prof. Me. José Messias Ribeiro Júnior – Instituto Federal de Educação Tecnológica de Pernambuco
Profª Drª Juliana Santana de Curcio – Universidade Federal de Goiás
Profª Ma. Juliana Thaisa Rodrigues Pacheco – Universidade Estadual de Ponta Grossa
Profª Drª Kamilly Souza do Vale – Núcleo de Pesquisas Fenomenológicas/UFPA
Prof. Dr. Kárpio Márcio de Siqueira – Universidade do Estado da Bahia
Profª Drª Karina de Araújo Dias – Prefeitura Municipal de Florianópolis
Prof. Dr. Lázaro Castro Silva Nascimento – Laboratório de Fenomenologia & Subjetividade/UFPR

Prof. Me. Leonardo Tullio – Universidade Estadual de Ponta Grossa
Prof^ª Ma. Lillian Coelho de Freitas – Instituto Federal do Pará
Prof^ª Ma. Liliansi Aparecida Sereno Fontes de Medeiros – Consórcio CEDERJ
Prof^ª Dr^ª Lívia do Carmo Silva – Universidade Federal de Goiás
Prof. Dr. Lucio Marques Vieira Souza – Secretaria de Estado da Educação, do Esporte e da Cultura de Sergipe
Prof. Dr. Luan Vinicius Bernardelli – Universidade Estadual do Paraná
Prof^ª Ma. Luana Ferreira dos Santos – Universidade Estadual de Santa Cruz
Prof^ª Ma. Luana Vieira Toledo – Universidade Federal de Viçosa
Prof. Me. Luis Henrique Almeida Castro – Universidade Federal da Grande Dourados
Prof^ª Ma. Luma Sarai de Oliveira – Universidade Estadual de Campinas
Prof. Dr. Michel da Costa – Universidade Metropolitana de Santos
Prof. Me. Marcelo da Fonseca Ferreira da Silva – Governo do Estado do Espírito Santo
Prof. Dr. Marcelo Máximo Purificação – Fundação Integrada Municipal de Ensino Superior
Prof. Me. Marcos Aurelio Alves e Silva – Instituto Federal de Educação, Ciência e Tecnologia de São Paulo
Prof^ª Ma. Maria Elanny Damasceno Silva – Universidade Federal do Ceará
Prof^ª Ma. Marileila Marques Toledo – Universidade Federal dos Vales do Jequitinhonha e Mucuri
Prof. Me. Pedro Panhoca da Silva – Universidade Presbiteriana Mackenzie
Prof^ª Dr^ª Poliana Arruda Fajardo – Universidade Federal de São Carlos
Prof. Me. Ricardo Sérgio da Silva – Universidade Federal de Pernambuco
Prof. Me. Renato Faria da Gama – Instituto Gama – Medicina Personalizada e Integrativa
Prof^ª Ma. Renata Luciane Polsaque Young Blood – UniSecal
Prof. Me. Robson Lucas Soares da Silva – Universidade Federal da Paraíba
Prof. Me. Sebastião André Barbosa Junior – Universidade Federal Rural de Pernambuco
Prof^ª Ma. Silene Ribeiro Miranda Barbosa – Consultoria Brasileira de Ensino, Pesquisa e Extensão
Prof^ª Ma. Solange Aparecida de Souza Monteiro – Instituto Federal de São Paulo
Prof^ª Ma. Taiane Aparecida Ribeiro Nepomoceno – Universidade Estadual do Oeste do Paraná
Prof. Me. Tallys Newton Fernandes de Matos – Faculdade Regional Jaguaribana
Prof^ª Ma. Thatianny Jasmine Castro Martins de Carvalho – Universidade Federal do Piauí
Prof. Me. Tiago Silvio Dedoné – Colégio ECEL Positivo
Prof. Dr. Welleson Feitosa Gazel – Universidade Paulista

Ciências exatas e da terra: aprendizado, integração e necessidades do país 2

Editora Chefe: Profª Drª Antonella Carvalho de Oliveira
Bibliotecária: Janaina Ramos
Diagramação: Maria Alice Pinheiro
Correção: Kimberlly Elisandra Gonçalves Carneiro
Edição de Arte: Luiza Alves Batista
Revisão: Os Autores
Organizadores: Américo Junior Nunes da Silva
André Ricardo Lucas Vieira

Dados Internacionais de Catalogação na Publicação (CIP)

C569 Ciências exatas e da terra: aprendizado, integração e necessidades do país 2 / Organizadores Américo Junior Nunes da Silva, André Ricardo Lucas Vieira. – Ponta Grossa - PR: Atena, 2021.

Formato: PDF

Requisitos de sistema: Adobe Acrobat Reader

Modo de acesso: World Wide Web

Inclui bibliografia

ISBN 978-65-5706-961-5

DOI 10.22533/at.ed.615211404

1. Ciência. 2. Tecnologia. I. Silva, Américo Junior Nunes da (Organizador). II. Vieira, André Ricardo Lucas (Organizador). III. Título.

CDD 500

Elaborado por Bibliotecária Janaina Ramos – CRB-8/9166

Atena Editora

Ponta Grossa – Paraná – Brasil

Telefone: +55 (42) 3323-5493

www.atenaeditora.com.br

contato@atenaeditora.com.br

DECLARAÇÃO DOS AUTORES

Os autores desta obra: 1. Atestam não possuir qualquer interesse comercial que constitua um conflito de interesses em relação ao artigo científico publicado; 2. Declaram que participaram ativamente da construção dos respectivos manuscritos, preferencialmente na: a) Concepção do estudo, e/ou aquisição de dados, e/ou análise e interpretação de dados; b) Elaboração do artigo ou revisão com vistas a tornar o material intelectualmente relevante; c) Aprovação final do manuscrito para submissão.; 3. Certificam que os artigos científicos publicados estão completamente isentos de dados e/ou resultados fraudulentos; 4. Confirmam a citação e a referência correta de todos os dados e de interpretações de dados de outras pesquisas; 5. Reconhecem terem informado todas as fontes de financiamento recebidas para a consecução da pesquisa.

APRESENTAÇÃO

O desenvolvimento da ciência e da tecnologia tem acarretado diversas transformações na sociedade contemporânea, refletindo em mudanças nos níveis econômico, político e social. É comum considerarmos ciência e tecnologia motores do progresso que proporcionam não só desenvolvimento do saber humano, mas, também, uma evolução real para o homem.

Sendo assim, precisamos de uma imagem de ciência e tecnologia que possa trazer à tona a dimensão social do desenvolvimento científico–tecnológico, entendido como produto resultante de fatores culturais, políticos e econômicos. Seu contexto histórico deve ser analisado e considerado como uma realidade cultural que contribui de forma decisiva para mudanças sociais, cujas manifestações se expressam na relação do homem consigo mesmo e os outros.

Hoje, estamos vivendo um período, por conta do contexto da Pandemia provocada pelo Novo Coronavírus, onde os olhares se voltam a Ciência e a Tecnologia. Antes de tudo isso acontecer os conhecimentos produzidos em espaços acadêmicos, centros de pesquisa e laboratórios, por exemplo, tem buscado resposta para problemas cotidianos, em busca de melhorar a vida da população de uma forma geral.

É nesse ínterim que este livro, intitulado “Ciências Exatas e da Terra: Aprendizado, Integração e Necessidades do País 2”, em seu segundo volume, reúne trabalhos de pesquisa e experiências em diversos espaços, com o intuito de promover um amplo debate acerca das diversas áreas que o compõe.

Por fim, ao levar em consideração todos esses elementos, a importância desta obra, que aborda de forma interdisciplinar pesquisas, relatos de casos e/ou revisões, reflete-se nas evidências que emergem de suas páginas através de diversos temas evidenciando-se não apenas bases teóricas, mas a aplicação prática dessas pesquisas.

Nesse sentido, desejamos uma boa leitura a todos e a todas.

Américo Junior Nunes da Silva
André Ricardo Lucas Vieira

SUMÁRIO

CAPÍTULO 1..... 1

STABILITY EVALUATION OF SEQUENTIAL ESTIMATORS APPLIED TO ORBIT DETERMINATION: SIGMA-POINT AND EXTENDED KALMAN FILTERS

Paula Cristiane Pinto Mesquita Pardal

Rodolpho Vilhena de Moraes

Helio Koiti Kuga

DOI 10.22533/at.ed.6152114041

CAPÍTULO 2..... 16

VARIAÇÃO DO NÍVEL DA ÁGUA E DA SUPERFÍCIE POTENCIOMÉTRICA EM POÇOS DE MONITORAMENTO NA ÁREA DE UM ATERRO SANITÁRIO

Willian Fernando de Borba

José Luiz Silvério da Silva

Edner Baumhardt

Éricklis Edson Boito de Souza

Pedro Daniel da Cunha Kemerich

Gabriel D'ávila Fernandes

Mateus Guimarães da Silva

Fernando Ernesto Ucker

DOI 10.22533/at.ed.6152114042

CAPÍTULO 3..... 30

DESENVOLVIMENTO E IMPLANTAÇÃO DE UM TERMÔMETRO DE SENSAÇÃO TÉRMICA NO IFSC CAMPUS URUPEMA

Glauco Cardozo

Marcos Roberto Dobler Stroschein

Enzzo Comassetto

DOI 10.22533/at.ed.6152114043

CAPÍTULO 4..... 33

DESIGN REGENERATIVO E DIREITO AMBIENTAL: CONSTRUÇÃO DE PONTE PARA A ECONOMIA CIRCULAR

Marcos Paulo Marques Araújo

DOI 10.22533/at.ed.6152114044

CAPÍTULO 5..... 49

O QUE ESTAMOS PRODUZINDO DE CONHECIMENTO CIENTÍFICO SOBRE TECNOLOGIA ASSISTIVA NO BRASIL?

Fernanda do Nascimento Maia

Renan Carvalho

Clara Ribeiro

DOI 10.22533/at.ed.6152114045

CAPÍTULO 6.....	56
TREINAMENTOS EM REALIDADE VIRTUAL VOLTADOS PARA ORGANIZAÇÕES DE ALTA CONFIABILIDADE	
Diego de Jesus Penaforte Parreiras	
André Ribeiro de Oliveira	
DOI 10.22533/at.ed.6152114046	
CAPÍTULO 7.....	68
ANÁLISE DA INFLUÊNCIA DAS SIMPLIFICAÇÕES REALIZADAS NAS EQUAÇÕES CINEMÁTICAS DO SATÉLITE CBERS	
Roberta Veloso Garcia	
Hugo Henrique Valim de Lima Campos	
Hélio Koiti Kuga	
DOI 10.22533/at.ed.6152114047	
CAPÍTULO 8.....	77
A ENGENHARIA AMBIENTAL NO ESTUDO DA EROSIÃO DE PRAIAS ASSOCIADOS AOS IMPACTOS DAS CONSTRUÇÕES NA ZONA COSTEIRA NO ESTADO DO CEARÁ, BRASIL	
Glacianne Gonçalves de Oliveira Maia	
Márcio Roberto de Paula da Fonseca	
Luis de Carvalho Feitosa Neto	
Lucas Barbosa Fernandes	
Vitória Lima Tavares	
DOI 10.22533/at.ed.6152114048	
CAPÍTULO 9.....	84
GÊNESE DE LINHAS DE PEDRA ATRAVÉS DE INFERÊNCIAS PALEOAMBIENTAIS NO MÉDIO VALE DO RIO PARAÍBA DO SUL, SUDESTE DO BRASIL	
Heloisa Helena Gomes Coe	
André Luiz Carvalho da Silva	
Amanda Pacheco Seixas	
Igo Fernando Lepsch	
Mauro Parolin	
Kita Macario	
DOI 10.22533/at.ed.6152114049	
CAPÍTULO 10.....	103
CARACTERIZAÇÃO DE FOLHAS DE ALUMÍNIO DE USO DOMÉSTICO POR EDXRF	
Carlos Augusto da Mata Bittencourt Junior	
Joaquim Teixeira de Assis	
Marcelino José dos Anjos	
DOI 10.22533/at.ed.61521140410	
CAPÍTULO 11.....	110
CARACTERIZAÇÃO BIOMÉTRICA E PRODUTIVA DA VINAGREIRA VERDE COM DIFERENTES ADUBAÇÕES NPK	
Vinícius Junqueira Minjoni	

Luis Felipe Lima e Silva
José Ricardo Mantovani

DOI 10.22533/at.ed.61521140411

CAPÍTULO 12..... 120

**MONITORAMENTO DA QUALIDADE DO AR EM AMBIENTES COM FOTOCOPIADORAS
UTILIZANDO *TRADESCANTIA PALLIDA***

Ana Luisa Santos de Carvalho
André Búrigo Leite
Luciano da Silva Lima

DOI 10.22533/at.ed.61521140412

CAPÍTULO 13..... 135

**REAPROVEITAMENTO DE RESÍDUOS TÊXTEIS PROVENIENTES DO POLO DA MODA
DO MUNICÍPIO DE NOVA FRIBURGO NO DESENVOLVIMENTO DE COMPÓSITOS DE
POLIPROPILENO**

Nancy Isabel Alvarez Acevedo
Rafael Gelson Ismério Cler
Marisa Cristina Guimarães Rocha

DOI 10.22533/at.ed.61521140413

CAPÍTULO 14..... 148

**AVALIAÇÃO DA AADIÇÃO DO TALCONAS PROPRIEDADES TÉRMICAS E MORFOLÓGICAS
DE MISTURAS DE POLIPROPILENO COM ELASTÔMERO TERMOPLÁSTICO**

Carlos Ivan Ribeiro de Oliveira
Marisa Cristina Guimarães Rocha
Joaquim Teixeira de Assis
Ana Lúcia Nazareth da Silva

DOI 10.22533/at.ed.61521140414

CAPÍTULO 15..... 160

**SOLUÇÃO DE UM PROBLEMA DE MULTICAMADAS DE CONDUÇÃO DE CALOR
UTILIZANDO O MÉTODO QUADRUPOLO**

Guilherme Ramalho Costa
José Aguiar dos Santos Júnior
José Ricardo Ferreira Oliveira
Gilmar Guimarães

DOI 10.22533/at.ed.61521140415

CAPÍTULO 16..... 167

PLANO REAL, UMA MUDANÇA NA SOCIEDADE BRASILEIRA

Felipe Matheus Rodrigues
Rita de Cassia Araújo

DOI 10.22533/at.ed.61521140416

CAPÍTULO 17..... 180

PREVIDÊNCIA COMPLEMENTAR: A IMPORTANCIA DA PREVIDÊNCIA COMPLEMENTAR

Bruna Larissa dos Santos Pereira

Rita de Cassia Araujo

DOI 10.22533/at.ed.61521140417

CAPÍTULO 18..... 192

O USO DA GEOMETRIA ANALÍTICA NA CONSTRUÇÃO DO GPS

Raimundo Eugênio da Silva Filho

Iarla Antunes de Matos Arrais

José Augusto Pereira Nogueira

Líliã Santos Gonçalves

Francisco Ronald Feitosa Moraes

DOI 10.22533/at.ed.61521140418

CAPÍTULO 19..... 203

A ESSÊNCIA ENTRE A DIVISÃO EUCLIDIANA E A CONGRUÊNCIA MODULAR

Marcos Garcia de Souza

Paulo Sérgio da Silva Pantoja

DOI 10.22533/at.ed.61521140419

CAPÍTULO 20..... 219

ESTÁGIO CURRICULAR SUPERVISIONADO DE OBSERVAÇÃO: CONJECTURANDO SOBRE ESSE ESPAÇO DE FORMAÇÃO

Lucas Gabriel Gonçalves da Silva

Américo Junior Nunes da Silva

DOI 10.22533/at.ed.61521140420

SOBRE OS ORGANIZADORES 227

ÍNDICE REMISSIVO..... 228

A ESSÊNCIA ENTRE A DIVISÃO EUCLIDIANA E A CONGRUÊNCIA MODULAR

Data de aceite: 01/04/2021

Marcos Garcia de Souza

Professor do Instituto Federal do Pará-Campus
Marabá industrial, Marabá-Pará
<http://lattes.cnpq.br/3074811984365865>

Paulo Sérgio da Silva Pantoja

Professor do Instituto Federal do Pará-Campus
Marabá industrial, Marabá-Pará
<http://lattes.cnpq.br/6779419284218288>

RESUMO: A divisão euclidiana com resto é caracterizada quando se determina um único par de números inteiros - quociente e resto. Esse resultado possibilita abstrair diversas propriedades sobre o resto. Em especial, conceber o conceito de congruência modular. Nesse sentido, propomos investigar a relação da divisão euclidiana com a definição de congruência modular. Além disso, apresentar algumas propriedades de congruência no conjunto dos números inteiros e construir a definição de classe residual (ou de restos) e a propriedade de números inteiros pertencerem à classe de restos. E, com isso, decidir quando dois números inteiros são ou não congruentes, módulo, um número inteiro positivo fixado. Destacar, ainda, que os possíveis restos da divisão de dois inteiros geram o conjunto de todas as classes residuais e, por meio da relação de congruência modular, determinam uma partição no conjunto dos números inteiros. Apresentaremos, também, o Pequeno Teorema de Fermat na aplicação

de problemas relacionados com a congruência modular e a divisão euclidiana de dois inteiros.

PALAVRAS - CHAVE: Divisão euclidiana; Congruência modular; Classe residual.

THE ESSENCE BETWEEN THE EUCLIDIAN DIVISION AND THE MODULAR CONGRUENCE

ABSTRACT: The Euclidean division with remainder is characterized when a single pair of an integer is determined- quotient and remainder. This result makes it possible to abstract several properties over the remainder and, specially, the construction of the modular congruence concept. In this sense, we propose to investigate the relationship between the Euclidean division with the modular congruence concept, as well as to present some properties of congruence in the integers set and to construct the residue class definition with the property that two integers belongs to the residue class. Based on that, we try to decide if these two integers are congruent or not, a module or a prefixed number. The possible remains of the two integers division generate the set of the all residual classes and, through the relation of modular congruence, a partition in the set of integer numbers is determined. As part of the resolution of some examples, the Fermat's Little Theorem will also be used throughout this paper.

KEYWORDS: Euclidean division; Modular congruence; Residual class.

1 | INTRODUÇÃO

A divisão euclidiana é uma *operação* estruturada na *existência* e *unicidade* de um par de números inteiros relacionados por meio das *operações* de *multiplicação* e *adição* (ou *subtração*).

O conceito de congruência modular de dois números inteiros relaciona a *operação* de *subtração* com a *relação* “*divide*”.

Diante disso, analisaremos a estrutura da divisão euclidiana e a caracterização da congruência modular no conjunto dos números inteiros.

Essa análise será feita por abstrações na equação da divisão euclidiana e a iniciaremos considerando o Postulado de Eudoxo¹ para compreender a existência do quociente e do resto na estrutura dessa divisão.

2 | POSTULADO DE EUDOXO E DIVISÃO EUCLIDIANA EM $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

Uma *propriedade fundamental* dos números naturais é que **não existe número natural entre dois números naturais consecutivos**. De fato, dado $n \in \mathbb{N}$, suponha o contrário, ou seja, que *existe* $a \in \mathbb{N}$, tal que $n < a < n + 1$. Isto equivale a $n < a$ e $a < n + 1$. Logo, existem $r, s \in \mathbb{N}^*$, tais que:

$$n < a \Rightarrow a = n + r \dots (I) \quad \text{e} \quad a < n + 1 \Rightarrow n + 1 = a + s \dots (II)$$

Substituindo (I) em (II), temos:

$$n + 1 = a + s = (n + r) + s \quad \text{e, portanto,} \quad r + s = 1.$$

Porém, $r + s = 1$, com $r, s \in \mathbb{N}^*$, é um absurdo! Isto ocorreu porque supomos o número a entre n e $n + 1$. Assim, segue a propriedade fundamental.

A partir desse fato, sejam os números $a, b \in \mathbb{N}$, com $0 < b \leq a$. Multiplicando os números naturais por b (“*tabuada de multiplicação*” do número b), obtemos:

$$0 \times b = 0; \quad 1 \times b = b; \quad 2 \times b = 2b; \quad 3 \times b = 3b; \quad \dots; \quad k \times b = kb; \quad \dots, \quad \text{onde } k \in \mathbb{N}.$$

Note que os números $0, b, 2b, 3b, \dots, kb, \dots$ formam uma sequência e, à medida que o número natural k aumenta, o produto kb se aproxima do número a , de modo que, para algum $k = n$, teremos: $nb = a$ ou $nb < a < (n + 1)b$.

Isso equivale a $bn \leq a < b(n + 1)$, onde $n \in \mathbb{N}$. Com isso, estabelecemos a *existência* do número natural n .

Perceba, também, que $(n + 1)$ é o *menor* número natural, tal que $bn \leq a < b(n + 1)$, com $n \in \mathbb{N}$. De fato, considere o conjunto $M = \{n \in \mathbb{N} ; a < bn\}$. Assim, $M \neq \emptyset$, pois: $0 < b \in \mathbb{N}$ implica $b^3 > 1$ e, por conseguinte, $nb^3 > n$, onde $n \in \mathbb{N}$. Somando b nessa última

¹ Eudoxo (408 – 355? a.C.), discípulo de Platão, foi um eminente matemático da sua época. Criou a Teoria das Proporções que compõe o Livro V de Os elementos de Euclides. (BOYER, 1996, p. 62)

desigualdade, obtemos: $nb + b^3 n + b$, que implica $b(n + 1)^3 n + b > n$ e, portanto, $b(n + 1) > n$. Logo, $M \neq \emptyset$ e $n + 1$ é o menor elemento do conjunto $M = \{n \in \mathbb{N} ; a < bn\}$. Com isso, segue o postulado:

Postulado (ou Axioma) de Eudoxo. Dados $a, b \in \mathbb{N}$, com $0 < b \leq a$, existe um número $n \in \mathbb{N}$, tal que $bn \leq a < b(n + 1)$.

Outra maneira de justificar esse Axioma é por meio de uma *partição* no conjunto dos números naturais. Em outras palavras, dado um número natural $b > 0$, o conjunto $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ pode ser escrito na forma:

$$\mathbb{N} = \{0, 1, 2, 3, \dots\} \cup \\ \cup \{b, b + 1, b + 2, \dots, 2b - 1\} \cup \dots \cup \\ \cup \{bq, bq + 1, bq + 2, \dots, b(q + 1) - 1\} \cup \dots$$

Assim, qualquer que seja $a \in \mathbb{N}$ implica $bq \leq a < b(q + 1)$, para algum $q \in \mathbb{N}$.

A partir do Postulado de Eudoxo, segue o teorema:

Teorema 1 (Divisão euclidiana). Dados a e b naturais, com $b \neq 0$, existe um único par de números naturais q e r , tal que $a = bq + r$ (ou $r = a - bq$), com a condição $0 \leq r < b$.

Demonstração: Sejam $a, b \in \mathbb{N}$, com $0 < b < a$. Pelo axioma de Eudoxo, existe $n \in \mathbb{N}$, tal que $bn \leq a < b(n + 1)$. Daí:

$$nb \leq a < (n + 1)b \Leftrightarrow nb \leq a < nb + b \Leftrightarrow 0 \leq a - nb < b.$$

Definindo $r = a - bq$ e fazendo $n = q$, conclui-se que **existem** dois números naturais q e r , com a condição de $0 \leq r < b$ (ou $0 \leq r < b - 1$)

Os números q e r são **únicos**. De fato, suponha que existem outros dois números naturais q' e r' . Assim:

$$a = bq + r = bq' + r', \text{ com } 0 \leq r < r' < b \Leftrightarrow bq - bq' = r' - r \Leftrightarrow \\ b(q - q') = r' - r.$$

Como $0 \leq r < r' < b$, então, $r' - r$ é múltiplo de b se, e somente se, $r' - r = 0$, ou seja, $r' = r$.

Por outro lado, sendo $r' - r = 0$ e $b > 0$, temos: $b(q - q') = r' - r = 0$ se, e somente se, $q - q' = 0$ e, portanto, $q = q'$.

Os números a, b, q e r na equação $a = bq + r$, com a condição de $0 \leq r < b$, têm *nomenclaturas especiais*, a saber: a é o *dividendo*, b é o *divisor*, q é o *quociente (máximo)* e r é o *resto (mínimo)*.

Observações: 1) A divisão euclidiana vale no conjunto dos números inteiros. Basta tomar o *valor absoluto* de b , isto é: $|b| = b$, se $b \geq 0$ e $|b| = -b$, se $b < 0$. Assim, dados dois números inteiros a e $|b|$, existe um único par de inteiros q e r , tal que $a = |b|q + r$, com $0 \leq r$

$< |b|$; **2)** A condição $0 \leq r < |b|$ permite listar *todos os possíveis restos* da divisão euclidiana de a por $|b| \neq 0$, a saber: $0, 1, 2, \dots, |b| - 1$, e também identificar o *maior resto possível* (ou *resto máximo*), ou seja, o número inteiro positivo $r_{\max} = |b| - 1$.

Exemplo 1. Considerando os possíveis restos da divisão de n por 7 , determinar os possíveis restos da divisão de n^2 por 7 ,

Resolução: Na divisão de n por 7 , o **Teorema 1** garante que existe um único par de números inteiros q e r , tais que: $n = 7q + r$, com $0 \leq r < 7$ (ou $r = 0, 1, 2, \dots, 6$). Logo, $n^2 = (7q + r)^2 = 7^2q^2 + 2 \cdot 7qr + r^2 = 7(7q^2 + 2qr) + r^2$ e, portanto, $n^2 = 7p + r^2$, onde $p = 7q^2 + 2qr$. Para $r = 0, 1, 2, \dots, 6$ segue, respectivamente, que: $r^2 = 0^2, 1^2, 2^2, \dots, 6^2$.

Exemplo 2. Seja $r_b(m)$ o resto da divisão de m por b . Mostre que:

a) $r_b(m + n) = r_b(r_b(m) + r_b(n))$.

b) $r_b(m \cdot n) = r_b(r_b(m) \cdot r_b(n))$.

Resolução: a) Na divisão euclidiana de m por b , temos: $m = bk + r_b(m)$ ou $r_b(m) = m - bk$. Agora, sejam $r_b(m + n) = m + n - bk_2$ e $n = bk_1 + r_b(n)$. Então:

$$\begin{aligned} r_b(m + n) &= m + n - bk_2 = bk + r_b(m) + bk_1 + r_b(n) - bk_2 \\ &= r_b(m) + r_b(n) + b(k + k_1 - k_2) \\ &= r_b(m) + r_b(n) + bq. \end{aligned}$$

Note que $r_b(m + n)$ é o resto da divisão de $(m + n)$ por b , ou seja:

$$r_b(m + n) = r_b(r_b(m) + r_b(n)).$$

b) Por analogia ao item a), temos: $r_b(m) = m - bk$. Além disso:

$$m = bk + r_b(m), \quad n = bk_1 + r_b(n) \quad \text{e} \quad r_b(m \cdot n) = m \cdot n - bk_2.$$

Assim:

$$\begin{aligned} r_b(m \cdot n) &= m \cdot n - bk_2 = [bk + r_b(m)] \cdot [bk_1 + r_b(n)] - bk_2 \\ &= b^2kk_1 + bkr_b(n) + bk_1r_b(m) + r_b(m)r_b(n) - bk_2 \\ &= b(bkk_1 + kr_b(n) + k_1r_b(m) - k_2) + r_b(m)r_b(n) \\ &= bq + r_b(m)r_b(n). \end{aligned}$$

Observe que $r_b(m \cdot n)$ é o resto da divisão de $m \cdot n$ por b . Então, $r_b(m \cdot n) = r_b(r_b(m) \cdot r_b(n))$.

2.1 Múltiplos e divisores

Considere a equação $a = bq + r$, com $0 \leq r < b$. Então, para $r = 0$, temos: $a = bq$. Assim, seguem as definições 1 e 2:

Definição 1. Dados dois números naturais a e b , dizemos que a é um *múltiplo de b*

(ou b é um *divisor de* a) se existe $k \in \mathbb{N}$, de modo que $a = bk$.

A equação $a = bk$, onde k é natural, enseja definir a *relação “divide”* com os números naturais a e b .

Definição 2. Dados dois números naturais a e $b \neq 0$, diz-se que b *divide* a (e denotamos por $b \mid a$) se, e somente se, *existe* $k \in \mathbb{N}$, tal que $a = bk$.

Em símbolos, escrevemos: $\forall a, b \in \mathbb{N}$, com $b \neq 0$, $b \mid a \Leftrightarrow \exists k; a = bk$, onde $k \in \mathbb{N}$.

Em outras palavras, a é *múltiplo* (ou *divisível por*) de b . Neste caso, b é um *fator* (ou um *divisor*) de a .

A *negação* da relação “ b divide a ” escreve-se “ b não divide a ” e, em símbolos, escreve-se $b \nmid a$.

Nesse contexto, para $n \in \mathbb{N}^*$, **se $n \mid a$, então $n \leq a$, para todo $a \in \mathbb{N}$** (*Propriedade da Limitação*). De fato, como $n \mid a$, então existe $q \in \mathbb{N}^*$, de modo que $a = nq$, com $q \geq 1$. Daí, multiplicando esta desigualdade por n , obtém-se: $nq \geq n$ implica $a = nq \geq n$ e, portanto, $a \geq n$, para todo $a \in \mathbb{N}$.

Assim, os *divisores positivos* de um número natural a são, *pelo menos*, 1 e a . Quando os divisores positivos um número natural a são, *apenas*, 1 e a , dizemos que a é um *número primo*.

O numeral 1 chama-se *divisor universal*, pois, $1 \mid a$, para todo $a \in \mathbb{N}$. Além disso, $a \mid a$, com $a \neq 0$, pois, $a = 1 \times a$ e, portanto, $a \mid a$.

A partir da relação “*divide*”, podemos elaborar diversas propriedades, no entanto, isso não será objeto de reflexão neste texto.

2.2 Máximo Divisor Comum

No Livro VII, de *Os elementos* de Euclides, a Proposição 2 permite calcular o *máximo divisor comum* de dois números naturais. Atualmente, sua aplicação é conhecida como “*algoritmo de Euclides*”.

Dados dois números naturais a e b , não simultaneamente nulos, um número natural $d \neq 0$ chama-se *divisor comum* de a e b se: $d \mid a$ e $d \mid b$.

Um número natural $d \neq 0$ é o *máximo divisor comum* de dois números naturais a e b se as duas condições a seguir forem satisfeitas:

i) d é divisor comum de a e b ; e

ii) se existir um $c \in \mathbb{N}$ que seja também divisor comum de a e b , então $c \mid d$ (ou seja, d é divisível por *todo* divisor comum de a e b) e, por consequência, $c \leq d$.”

Denotaremos o máximo divisor comum de a e b por $d = (a, b)$.

O máximo divisor comum é *único*. Pois, se $d = (a, b)$ e $d' = (a, b)$, então, $d \leq d'$ e $d' \leq d$. Logo, $d = d'$. Portanto, quando existe o máximo divisor comum de dois números naturais, ele é único.

Proposição 1. Sejam dois números naturais a e b . Se $b \mid a$, então $b = (a, b)$.

Demonstração: i) Temos: $b \mid b$ e, se $b \mid a$, então b é divisor comum de a e b .

ii) se existir um $c \in \mathbb{N}$ que é divisor comum de a e b , então, $c \mid b$ e, portanto, $c \leq b$.

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

Lema de Euclides. Sejam dois números naturais a e b . Se existe $(a, b - na)$, para algum $n \in \mathbb{N}$, então, existe (a, b) , tal que $(a, b - na) = (a, b)$.

Demonstração: i) Seja $d = (a, b - na)$, para algum $n \in \mathbb{N}$. Então, $d \mid a$ e $d \mid (b - na)$ e, portanto, $d \mid b = (b - na) + na$. Logo, d é um divisor comum de a e b .

ii) Agora, suponha que $c \in \mathbb{N}$ é divisor comum de a e b . Então, c é divisor comum de a e $(b - na)$. Logo, $c \mid d$. Portanto, $d = (a, b) = (a, b - na)$.

O método para mostrar a existência do máximo divisor comum de dois números naturais é um processo iterativo utilizando o algoritmo e o Lema de Euclides. Vejamos: dados dois naturais a e b , com $0 < b \leq a$, suponha que b não divide a . Então, pelo algoritmo de Euclides, temos: $a = bq + r$ ou $a - bq = r$, com $0 \leq r < b$.

Assim, há dois casos:

- se r divide b , então, pelo Lema de Euclides: $r = (a, r) = (a, b - na) = (a, b)$.
- se r não divide b , segue, pelo algoritmo de Euclides, que:

$$b = rq_1 + r_1 \text{ ou } b - rq_1 = r_1, \text{ com } 0 \leq r_1 < r.$$

Assim, de modo análogo, temos duas possibilidades:

- se r_1 divide r , novamente pelo Lema de Euclides:

$$r_1 = (r, r_1) = (r, b - rq_1) = (a - bq, b) = (a, b).$$

- se r_1 não divide r , podemos efetuar a divisão de r por r_1 , obtendo:

$$r = r_1q_2 + r_2 \text{ ou } r - r_1q_2 = r_2, \text{ com } 0 \in \mathbb{N} \ r_2 < r_1.$$

Como $b > r > r_1 > r_2 > \dots$, então esse procedimento não pode continuar indefinidamente.

De fato: se fosse possível continuar esse processo, o conjunto $\{b, r, r_1, r_2, \dots\} = \{b, b - 1, \dots, 2, 1, 0\}$ não teria um mínimo, o que é impossível. Logo, para algum $n \in \mathbb{N}$, teremos: $r_n \mid r_{n-1}$.

Assim, pelo Lema de Euclides:

$$r_n = (r_n, r_{n-1}) = (r, b - rq_1) = (a - bq, b) = (a, b).$$

Na prática, o máximo divisor comum dois números naturais a e b pode ser calculado pelo diagrama a seguir:

	q	q_1	q_2	\dots	q_{n-1}	q_n	
a	b	\swarrow	\swarrow	\swarrow	\swarrow	\swarrow	$r_n = (a, b)$
r	r_1	r_2	r_3	\dots	r_n	0	

Exemplo 3. Determinar o máximo divisor comum entre 325 e 450.

Resolução: Temos:

	1	2	1	1	2
450	325	125	75	50	25
125	75	50	25	0	

Portanto, $(325, 450) = 25$. Note que, fazendo $450 = a$ e $325 = b$, segue que: $125 = a - b$. E, no diagrama acima, temos: $75 = b - 2(a - b) = 3b - 2a$; $50 = a - b - (3b - 2a) = 3a - 4b$; e $25 = 3b - 2a - (3a - 4b) = 7b - 5a$.

Assim, $7b - 5a = 25$, ou seja: $(7) \cdot 325 + (-5) \cdot 450 = (450, 325)$. Isso significa que, aplicando o *processo inverso* do cálculo do máximo divisor comum de dois números, é possível determinar dois números inteiros relacionados com o máximo divisor comum. Em outras palavras, o máximo divisor comum de dois números naturais é *uma combinação linear* desses números, conforme segue o teorema:

Teorema 2. (Bézout) Se $d = (a, b)$, então, *existem* m e n inteiros, tais que $m.a + n.b = d$.

Demonstração: Supondo que $a > b$. Então, pelo algoritmo de Euclides, temos: $a = bq_1 + r_1$, com $r_1 < b$. Assim:

$$\begin{aligned} r_1 &= a - bq_1, & r_1 < b. \\ r_2 &= b - r_1q_2, & r_2 < r_1. \\ r_3 &= r_1 - r_2q_3 + r_3, & r_3 < r_2. \\ &\vdots \\ r_{k-1} &= r_{k-3} - r_{k-2}q_{k-1}, & r_{k-1} < r_{k-2}. \\ r_k &= r_{k-2} - r_{k-1}q_k, & r_k < r_{k-1}. \\ r_{k-1} &= r_kq_{k+1}. \end{aligned}$$

Aplicando o processo de substituição, a partir da equação de r_1 até a equação de r_k , obtemos:

$$\begin{aligned} r_1 &= 1.a + (-q_1)b = m_1a + n_1b. \\ r_2 &= 1.b + (-r_1)q_2 = 1.b - (m_1a + n_1b)q_2 = (-m_1)a + (1 - n_1q_2)b = m_2a + n_2b. \\ &\vdots \\ r_k &= m_ka + n_kb. \end{aligned}$$

Na equação $r_k = m_ka + n_kb$, temos: $m = m_k$, $n = n_k$ e $r_k = d = (a, b)$.

Corolário 1. Se a e b são primos entre si, isto é, $(a, b) = 1$, então, existem m e n inteiros, tais que $m.a + n.b = 1$.

3 I CONGRUÊNCIA MODULAR EM $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$

Em 1801, Gauss publicou um dos grandes clássicos da matemática: “*Disquisitiones arithmeticae*”. Nesse livro, ele trata dos conceitos de congruência modular e classe de restos.

Dados dois números inteiros a e $m > 1$, por meio da divisão euclidiana, é garantida a *existência* e a *unicidade* de um par de número inteiros q e r , tal que $a = mq + r$ (ou $mq = a - r$), com $0 \leq r < m$.

A igualdade $mq = a - r$, com $0 \leq r < m$, permite escrever a relação “ m divide $a - r$ ”. Fixando $m > 1$, concebe-se um novo objeto matemático: a *relação de congruência, módulo m* , conforme definição a seguir:

Definição 3. Fixado um número inteiro $m > 1$, dizemos que um número inteiro a é *congruente* a um número inteiro b , módulo m (e denota-se por $a \equiv b \pmod{m}$), se, e somente se, m divide $a - b$.

Em símbolos, escrevemos: $a \equiv b \pmod{m} \Leftrightarrow m \mid a - b$, com $a, b, m \in \mathbb{Z}$, sendo $m > 1$.

Quando a não é congruente a b , módulo m , escrevemos $a \not\equiv b \pmod{m}$. Isto equivale a $m \nmid a - b$.

Para $m = 1$, segue que $a \equiv b \pmod{1}$ se, e somente se, $1 \mid a - b = k$, onde $k \in \mathbb{Z}$ e, portanto, $a = b + k$, ou seja, $a \geq b$ ($a > b$ ou $a = b$) implica $a \equiv b$.

Daqui por diante, usaremos a notação simplificada $a \equiv b \pmod{m}$, para dizer que a é congruente a b , módulo m .

Por definição, sabemos que $a \equiv b \pmod{m}$ equivale a $m \mid a - b$ e, por conseguinte, existe $k \in \mathbb{Z}$, tal que $a - b = mk$. Esta equação permite dizer que: “Dois números inteiros a e b são congruentes, módulo $m > 1$, se, e somente se, a diferença de a e b é um múltiplo de m .”

A expressão $a - b = mk$ (ou $a = b + mk$) tem semelhança com divisão euclidiana de dois números inteiros e, portanto, com a relação “*divide*”.

Nesse sentido, a divisão euclidiana e a relação de congruência modular de dois números inteiros têm compatibilidade, de acordo com as equivalências a seguir:

Operação de divisão euclidiana	Relação de congruência, módulo $m > 1$
Dados a e $m \neq 0$, existem únicos q e r , tais que $a = mq + r \Leftrightarrow 0 \leq r < m$.	Dados a e $m > 1$, temos: $a = mq + r$, com $0 \leq r < m \Leftrightarrow a - r = mq \Leftrightarrow m \mid a - r \Leftrightarrow a \equiv r \pmod{m}$, com $0 \leq r < m$.

Note que, por um lado, a *divisão euclidiana* fica estabelecida quando se determina um único par de inteiros q (quociente) e r (resto) restrito. Por outro lado, todo inteiro a é congruente, módulo $m > 1$, ao resto r obtido pela divisão de a por m , ou seja, $a \equiv r \pmod{m}$, com

$$0 \leq r < m.$$

Assim, para determinar o resto da divisão de a por $m > 1$, basta encontrar um inteiro r , tal que $a \equiv r \pmod{m}$, com $0 \leq r < m$. Além disso, a *relação* de congruência entre dois números inteiros, módulo $m > 1$, fica caracterizada pelo resto dessa divisão, conforme o teorema a seguir:

Teorema 3. Dois números inteiros a e b são congruentes, módulo $m > 1$, se, e somente se, deixam o *mesmo resto* na divisão por m .

Demonstração: (\Rightarrow) Suponha que $a \equiv b \pmod{m}$. Então, por definição, temos: $m \mid a - b$, ou seja, $a = mk + b$, para algum inteiro k .

Agora, pela divisão euclidiana, segue que $b = mq + r_b$, com $0 \leq r_b < m$, onde r_b é o resto da divisão de b por $m > 1$. Assim:

$$a = mk + b = mk + (mq + r_b) = (k + q)m + r_b \text{ e, portanto, } a = mp + r_b, \text{ onde } p = k + q.$$

Isso significa que r_b é, também, o resto da divisão de a por m .

(\Leftarrow) Reciprocamente, sejam r_a e r_b são, respectivamente, os restos da divisão de a , b por m , com $0 < r_a \leq r_b < m$. Então, $a = mp + r_a$ e $b = mq + r_b$. Assim:

$$a - b = mp + r_a - (mq + r_b) = m(p - q) + r_a - r_b = mk + r_a - r_b, \text{ onde } k = p - q.$$

Como $r_a = r_b$ ou $r_a - r_b = 0$, segue que $a - b = mk$. Logo, $m \mid a - b$, ou seja, $a \equiv b \pmod{m}$.

A proposição seguinte mostra que a relação “ \equiv ” (congruência) modular é *compatível*, em relação à “ $=$ ” (igualdade), com as operações de *adição*, *subtração* e *multiplicação*.

Proposição 2. Sejam $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$. Então, valem as seguintes afirmações: **i)** $a \pm c \equiv b \pm d \pmod{m}$; e **ii)** $ac \equiv bd \pmod{m}$.

Demonstração: i) Temos: $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$ implicam $m \mid a - b$ e $m \mid c - d$. Logo, $m \mid (a - b) \pm (c - d) = (a - c) - (b - d)$. Portanto, $a \pm c \equiv b \pm d \pmod{m}$.

ii) Por hipótese, temos: $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$. Logo, $m \mid a - b$ e $m \mid c - d$. Mas: $ac - bd = ac - ad + ad - bd = a(c - d) + d(a - b)$. Logo, $m \mid ac - bd$ e, portanto, $ac \equiv bd \pmod{m}$.

Proposição 3. Sejam as congruências $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$. Então, para todo número natural n : **i)** $na \equiv nb \pmod{m}$; e **ii)** $a^n \equiv b^n \pmod{m}$.

Demonstração: i) Como $a \equiv b \pmod{m}$, então, $m \mid a - b$. Para todo $n \in \mathbb{N}$, segue que:

$$m \mid n(a - b) = na - nb \Leftrightarrow na \equiv nb \pmod{m}.$$

ii) Para justificar essa propriedade, com n um número natural, usaremos um método para demonstrar proposições referentes a números naturais – *Princípio (ou Axioma) de Indução Matemática*.

Princípio (ou Axioma) de Indução Matemática

Dada uma *sentença aberta* $P(n)$, com $n \in \mathbb{N} = \{0, 1, 2, 3, \dots\}$. Suponha que $a \in \mathbb{N}$, tal que: **i)** $P(a)$ é verdadeira (*verificar*); e **ii)** Para todo $n \in \mathbb{N}$, $P(n)$ implica $P(n + 1)$ é verdadeira (*demonstrar*). Então, segue que $P(n)$ é verdadeira, para todo $n \geq a$.

Demonstração: Seja um subconjunto $S = \{n \in \mathbb{N}; P(n)\}$ de \mathbb{N} , tal que $P(n)$ é uma *sentença aberta* verdadeira. Considere o conjunto $E_m = \{m \in \mathbb{N}; (a + m) \in S\}$. Então: $a + E_a = \{a \in \mathbb{N}; a + a = 2a = n \in S\}$. Logo, $a + E_a$ é subconjunto de S . Assim, para todo $k \in (a + E_a)$ implica $k \in S$. Em particular, **i)** para $m = 0$, temos:

$$a + m = a + 0 = a = n \in S \text{ e, portanto, } 0 \in E_m.$$

Por outro lado, **ii)** se $m \in E_m$, então $a + m \in S$. Daí, $(a + m) + 1 \in S$. Logo, $m + 1 \in E_m$.

Assim, pelo Princípio de Indução Matemática, segue que $E_m = \mathbb{N}$. Portanto, para todo $m \geq a$, o conjunto $\{a \in \mathbb{N}; m \geq a\} = a + \mathbb{N} \subset S$.

Nota: Para dar um sentido preciso a sentenças abertas referentes a números naturais, utilizando o Princípio de Indução Matemática, escreve-se, por recorrência, uma expressão E_n , com $n \in a + \mathbb{N}$, da seguinte forma: define-se E_a , para $a \in \mathbb{N}$, e demonstra-se, a partir E_n , como obter E_{n+1} , para todo $n \in a + \mathbb{N}$.

No item **ii)** $P(n): a^n \equiv b^n (m)$, para todo $n \in \mathbb{N}$, temos: para $n = 1$, $a^1 \equiv b^1 (m)$ é verdadeiro. Suponha, por hipótese de indução, que $a^k \equiv b^k (m)$ é verdadeira, para algum $k \in \mathbb{N}$. Devemos mostrar que para $k + 1$ também é verdadeira, isto é, $a^{k+1} \equiv b^{k+1} (m)$. Com efeito: $a^{k+1} = a^k \cdot a^1 \equiv b^k \cdot b^1 (m) \equiv b^{k+1} (m)$. Logo, por indução, $a^n \equiv b^n (m)$, para todo $n \in \mathbb{N}$.

Exemplo 4. Determinar o resto da divisão de 2^{100} por 17.

Resolução: Seja o resto r da divisão de 2^{100} por 17. Então, $2^{100} \equiv r (17)$. Agora, note que $2^4 = 16 \equiv -1 (17)$, ou seja, $2^4 \equiv (-1) (17)$. Além disso, $100 = 4q$, onde $q \in \mathbb{Z}$. Assim, $2^{100} = 2^{4q} = (2^4)^q \equiv (-1)^q (17)$. Como o resto r é um número inteiro positivo ($0 \leq r < 17$), segue que $r = (-1)^q$, onde q é inteiro *par*. Portanto, $r = 1$.

Observação: Em geral, não vale a recíproca da propriedade do item **i)** da **Proposição 3**, ou seja, *não* é verdade que $na \equiv nb (m)$ implica $a \equiv b (m)$, Lei do Cancelamento.

As propriedades operacionais de somar, subtrair e multiplicar na relação de congruência modular funcionam de modo semelhante à relação de igualdade. Entretanto, a operação de divisão (Lei do Cancelamento) só pode ser efetivada, caso cumpra a condição da proposição a seguir.

Proposição 4. Sejam $n, m \in \mathbb{Z}$, tais que $(n, m) = 1$ (restrição). Então, $na \equiv nb \pmod{m}$ se, e somente se, $a \equiv b \pmod{m}$.

Demonstração: Temos: $na \equiv nb \pmod{m}$ se, e somente se, $m \mid na - nb = n(a - b)$. Como $(n, m) = 1$, segue que m não divide n . Logo, $m \mid a - b$. Isto equivale a $a \equiv b \pmod{m}$.

Portanto, a Lei do Cancelamento só pode ser aplicada na congruência $na \equiv nb \pmod{m}$ se, e somente se, n e m forem primos entre si, ou seja, se, e só se, $(n, m) = 1$.

O teorema a seguir apresenta uma propriedade importante em \mathbb{Z} .

Teorema 4. A relação de congruência modular é uma relação de equivalência sobre \mathbb{Z} .

Demonstração: Devemos mostrar que “ \equiv ”, módulo $m > 1$, é: **i) reflexiva**, **ii) simétrica** e **iii) transitiva**. Com efeito:

i) reflexiva: $m \mid 0 = a - a$ e, portanto, $a \equiv a \pmod{m}$.

ii) simétrica: $a \equiv b \pmod{m}$ implica $m \mid a - b = -(b - a)$ implica $b \equiv a \pmod{m}$.

iii) transitiva: $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$ implicam $a = b + mp$ e $b = c + mq$ e, por conseguinte, temos: $a = (mq + c) + mp = (p + q)m + c$ implica $a - c = km$, onde $k = p + q$. Logo, $a \equiv c \pmod{m}$.

Agora, seja $a \equiv r \pmod{m}$, onde r é o resto da divisão de a por $m > 0$. Logo, $a = mk + r$, com $0 \leq r < m$. Considere o conjunto formado por todos os números inteiros congruentes a r , módulo $m > 1$: $\{x \in \mathbb{Z}; x \equiv r \pmod{m}, \text{ com } 0 \leq r < m\}$. Assim:

$$\begin{aligned} \{x \in \mathbb{Z}; x \equiv r \pmod{m}, \text{ com } 0 \leq r < m\} &= \{x \in \mathbb{Z}; m \mid x - r, \text{ com } 0 \leq r < m\} \\ &= \{x \in \mathbb{Z}; x = mk + r, \text{ com } 0 \leq r < m\}. \end{aligned}$$

Isso sugere a seguinte definição:

Definição 4. Seja um número $r \in \mathbb{Z}$. Chama-se *classe de restos* (ou *residual*), módulo $m > 1$, do número inteiro r , o conjunto r_m de todos os números inteiros congruentes a r , módulo m .

Em símbolos, a *classe de restos*, módulo $m > 1$, de $r \in \mathbb{Z}$ é:

$$r_m = \{x \in \mathbb{Z}; x \equiv r \pmod{m}\} = \{x \in \mathbb{Z}; x = mk + r, k \in \mathbb{Z}\}.$$

Note que a classe de restos, módulo $m > 1$, é concebida a partir de cada um dos possíveis restos na divisão de um inteiro x por m .

Proposição 5. Para cada $a \in \mathbb{Z}$, existe um, e somente um, $r \in \mathbb{Z}$, com $0 \leq r \leq m - 1$, tal que $a_m = r_m$.

Demonstração: Seja $a \in \mathbb{Z}$. Então, na divisão euclidiana de a por um inteiro $m > 1$, existe um único inteiro r , tal que $a = mq + r$, com $0 \leq r \leq m - 1$, para algum $q \in \mathbb{Z}$.

Como r é único, tal que $a \equiv r(m)$, com $0 \leq r \leq m - 1$, segue que r é o único, de modo que $a_m = r_m$, com $0 \leq r \leq m - 1$.

Proposição 6. Se a e b pertencem a mesma classe de restos r_m , então, $a \equiv b(m)$.

Demonstração: Temos: $a, b \in r_m$ implica $a \equiv r(m)$ e $b \equiv r(m)$. Por simetria, $b \equiv r(m)$ implica $r \equiv b(m)$. Daí, por transitividade, $a \equiv r(m)$ e $r \equiv b(m)$ implicam $a \equiv b(m)$.

Proposição 7. Seja um inteiro $m > 1$. Dados os números inteiros r e s , considere as classes residuais r_m e s_m . Então: **i)** $r_m = s_m$ se, e somente se, $r \equiv s(m)$; e **ii)** $r_m \neq s_m$ implica $r_m \cap s_m = \emptyset$ (ou, de modo equivalente, $r_m \cap s_m \neq \emptyset$ implica $r_m = s_m$).

Demonstração: Sejam $r_m = \{x \in \mathbb{Z}; x \equiv r(m)\}$ e $s_m = \{y \in \mathbb{Z}; y \equiv s(m)\}$. Então:

$$\text{i) } r_m = s_m \Leftrightarrow x = y \Leftrightarrow r + mk_1 = s + mk_2 \Leftrightarrow r - s = m(k_2 - k_1) = mq \Leftrightarrow r \equiv s(m).$$

$$\text{ii) } r_m \neq s_m \Leftrightarrow x \neq y \Leftrightarrow r + mk_1 \neq s + mk_2 \Leftrightarrow r - s \neq m(k_2 - k_1) = mq \Leftrightarrow r \not\equiv s(m) \text{ implica } r_m \cap s_m = \emptyset. \quad \blacksquare$$

Seja r é o resto da divisão de um inteiro x por $m > 1$. Então, $0 \leq r < m$. Daí, os possíveis valores de r são: $0, 1, 2, \dots, m - 1$.

Agora, considere a correspondência $\equiv : r \rightarrow r_m$ que, a cada resto r , associa um conjunto r_m , ou seja:

$$0 \rightarrow 0_m, \quad 1 \rightarrow 1_m, \quad 2 \rightarrow 2_m, \quad \dots, \quad m - 1 \rightarrow (m - 1)_m.$$

ou

$$r = 0 \rightarrow 0_m = \{x \in \mathbb{Z}; x \equiv 0(m)\} = \{mk; k \in \mathbb{Z}\} = \{\dots, -2m, -m, 0, m, 2m, \dots\}.$$

$$r = 1 \rightarrow 1_m = \{x \in \mathbb{Z}; x \equiv 1(m)\} = \{mk + 1; k \in \mathbb{Z}\} = \{\dots, -2m + 1, -m + 1, 1, m + 1, 2m + 1, \dots\}.$$

⋮

$$r = m - 1 \rightarrow (m - 1)_m = \{x \in \mathbb{Z}; x \equiv (m - 1)(m)\} = \{mk + (m - 1); k \in \mathbb{Z}\}.$$

Com isso, a correspondência $\equiv : r \rightarrow r_m$ permite destacar dois conjuntos, a saber: 1) o conjunto dos possíveis restos r , na divisão de x por m , com $0 \leq r < m$:

$$\{0, 1, 2, \dots, m - 1\}.$$

2) o conjunto de todas as classes de restos (ou resíduos), módulo m , que denotamos por \mathbb{Z}_m (ou $\mathbb{Z}/(m)$):

$$\mathbb{Z}/(m) = \mathbb{Z}_m = \{0_m, 1_m, 2_m, \dots, (m-1)_m\}.$$

Em especial, o conjunto $\mathbb{Z}/(m)$ tem a seguinte propriedade:

Proposição 8. O conjunto \mathbb{Z}_m tem exatamente m elementos, para $m > 1$.

Demonstração: Sejam $a, m \in \mathbb{Z}$, com $m > 1$. Então, dividindo-se a por m , obtemos: $a = mq + r$, com $0 \leq r < m$. Assim, existem m possíveis restos.

Como $a = mq + r$ equivale $a - r = mq$ e, por conseguinte, $m \mid a - r$, então, $a \equiv r \pmod{m}$, com $0 \leq r < m$. E, pela Proposição 7, segue que $a_m = r_m$.

Por outro lado, $r \in \{0, 1, 2, \dots, m-1\}$ implica $r_m \in \mathbb{Z}_m = \{0_m, 1_m, 2_m, \dots, (m-1)_m\}$.

Agora, suponha, por absurdo, que existem duas classes $r_m, s_m \in \mathbb{Z}_m$, tais que $r_m = s_m$, com $0 \leq r < s < m$. Neste caso, $r_m = s_m$ implica $r \equiv s \pmod{m}$ e, portanto, $m \mid r - s$. Mas, $0 < r - s < m$ é impossível! Logo, para restos distintos implicam classes residuais distintas. Assim, \mathbb{Z}_m tem exatamente m elementos.

Proposição 9. O número inteiro $m > 1$, por meio da relação de congruência, módulo m , determina uma *partição* em \mathbb{Z} . Em outras palavras, as classes residuais de \mathbb{Z}_m têm as seguintes propriedades: **i)** $\forall r_m \in \mathbb{Z}_m, r_m \neq \emptyset$; **ii)** $\forall r_k, r_j \in \mathbb{Z}_m$ implicam $r_k \cap r_j = \emptyset$, se $k \neq j$; e $r_k \cap r_j = \emptyset$, se $k \neq j$; e **iii)** $\bigcup_{i=0}^{m-1} r_i = \mathbb{Z}$.

Demonstração: i) Seja $r_m = \{x \in \mathbb{Z}; x \equiv r \pmod{m}\}$. Fazendo $x = r$, temos:

$$r_m = \{r \in \mathbb{Z}; r \equiv r \pmod{m}\} = \mathbb{Z}. \text{ Logo, } r_m \neq \emptyset.$$

ii) Suponha, por absurdo, que $r_k \cap r_j \neq \emptyset$, para $k \neq j$. Então, existe $c \in r_k \cap r_j$. Isto implica $c \in r_k$ e $c \in r_j$, logo, $c \equiv r \pmod{m}$ e $c \equiv r' \pmod{m}$. Daí, $k \mid c - r$ e $j \mid c - r'$, ou seja, $k = j$. Mas isto é um absurdo! Isto ocorreu em supor que $r_k \cap r_j \neq \emptyset$. Então, $r_k \cap r_j = \emptyset$, se $k \neq j$.

iii) Neste caso, devemos mostrar que: **a)** $\bigcup_{i=0}^{m-1} r_i \subset \mathbb{Z}$ e **b)** $\mathbb{Z} \subset \bigcup_{i=0}^{m-1} r_i$. Com efeito:

a) $c \in \bigcup_{i=0}^{m-1} r_i$ implica $c \in r_i = \{x \in \mathbb{Z}; x \equiv r(i)\}$, para $i = 0, 1, \dots, m-1$. Então, $c \equiv r(i)$, com $i = 0, 1, \dots, m-1$ e, portanto, $c \in \mathbb{Z}_m$. Assim, $\bigcup_{i=0}^{m-1} r_i \subset \mathbb{Z}_m$.

b) $c \in \mathbb{Z}_m$ implica $c \in r_i$, para todos $i \in \{0, 1, \dots, m-1\}$. Daí, $c \in \bigcup_{i=0}^{m-1} r_i$. Logo, $\mathbb{Z}_m \subset \bigcup_{i=0}^{m-1} r_i$. ■

Teorema 5. Seja um número primo p . Então, $a^p \equiv a \pmod{p}$, para todo $a \in \mathbb{Z}^*$.

Demonstração: Por indução sobre a , temos: para $a = 1$, segue que $1^p \equiv 1 \pmod{p}$ é

verdadeiro.

Agora, por hipótese de indução, suponha que $k^p \equiv k \pmod{p}$, para algum $a = k$. Assim, para $a = k + 1$, segue que:

$$\begin{aligned} (k+1)^p &= k^p + \binom{p}{1}k^{p-1} + \dots + \binom{p}{i}k^{p-i} + \dots + 1 \\ &= k^p + p(k^{p-1} + \dots + \frac{(p-1)\cdot(p-2)\cdot\dots\cdot 2\cdot 1}{(p-1)!}k^{p-1}) + \dots + 1 \\ &= k^p + n\cdot p + 1, \text{ onde } n = k^{p-1} + \dots + \frac{(p-1)\cdot(p-2)\cdot\dots\cdot 2\cdot 1}{(p-1)!}k^{p-1} \\ &\equiv k^p + 1 \pmod{p}. \end{aligned}$$

Mas, por hipótese de indução, $k^p \equiv k \pmod{p}$. Logo, $(k+1)^p \equiv k^p + 1 \pmod{p}$ implica $(k+1)^p \equiv k+1 \pmod{p}$.

Assim, por indução, $a^p \equiv a \pmod{p}$, para todo $a \in \mathbb{Z} \setminus \{0\}$, com p primo.

Uma das consequências de $a^p \equiv a \pmod{p}$ ocorre quando temos a restrição $\text{mdc}(a, p) = 1$, ou seja, que os números a e p são primos entre si ou, mais especificamente, quando o primo p não divide o inteiro a . Neste caso, podemos aplicar a Lei do Corte (ou Cancelamento), dividindo $a^p \equiv a \pmod{p}$ por a . O resultado dessa divisão dá origem ao *Pequeno Teorema de Fermat*.

Teorema 6. (Pequeno Teorema de Fermat) Se o número primo p não divide o número inteiro a , então, $a^{p-1} \equiv 1 \pmod{p}$.

Demonstração: Como p é primo, segue que $a^p \equiv a \pmod{p}$, para todo $a \in \mathbb{Z}$. Mas, por hipótese, p não divide a . Logo, pela lei do cancelamento, podemos dividir $a^p \equiv a \pmod{p}$ pelo inteiro a . Daí:

$$a^p \equiv a \pmod{p} \text{ implica } a^p \div a \equiv a \div a \pmod{p} \text{ e, portanto, } a^{p-1} \equiv 1 \pmod{p}.$$

Por meio desse Teorema, o **Exemplo 4** é facilmente resolvido. Vejamos: o problema consiste em determinar o menor número positivo r , tal que $2^{100} \equiv r \pmod{17}$. Como $p = 17$ é primo e não divide $a = 2$, segue, pelo Pequeno Teorema de Fermat, que:

$$2^{17-1} = 2^{16} \equiv 1 \pmod{17} \text{ implica } 2^{4q} \equiv 1 \pmod{17}, \text{ onde } q \in \mathbb{Z} \text{ e, portanto, } 2^{100} \equiv 1 \pmod{17}.$$

Logo, $r = 1$.

Exemplo 5. Determine o resto da divisão de 2^{2001} por 101.

Resolução: Devemos achar o menor número positivo r , tal que $2^{2001} \equiv r \pmod{101}$. Como $p = 101$ é primo e não divide $a = 2$, então, pelo Pequeno Teorema de Fermat, segue que que: $2^{101-1} = 2^{100} \equiv 1 \pmod{101}$.

Como $2^{2001} = (2^{100})^{20} \cdot 2$, segue que: $2^{2001} = 1^{20} \cdot 2 \equiv 2 \pmod{101}$. Portanto, $r = 2$.

Exemplo 6. Qual é a menor solução positiva e a solução geral da equação $x \equiv 7 \pmod{3}$?

Resolução: Pelo **Teorema 3**, x e 7 deixam o *mesmo resto* na divisão por $m = 3$. O algoritmo da divisão permite escrever: $7 = m3 + 1$, onde 1 o menor resto. Logo, o resto da divisão de x por 3 é, também, 1 , ou seja, $x \equiv 7 \pmod{3}$ equivale a $x \equiv 1 \pmod{3}$. Então, a menor solução positiva da equação $x \equiv 1 \pmod{3}$ é $x_0 = 1$.

Por outro lado, $x \equiv 1 \pmod{3}$ equivale a $3 \mid x - 1$. Assim, a solução geral da equação $x \equiv 7 \pmod{3}$ é $x = 3q + 1$, onde $q \in \mathbb{Z}$.

Exemplo 7. a) Mostre que $x \equiv 7 \pmod{12}$ implica $x \equiv 3 \pmod{4}$. **b)** Seja um número primo p . Mostre que $x^2 \equiv 1 \pmod{p}$ implica $x \equiv \pm 1 \pmod{p}$.

Resolução: a) Por definição, $x \equiv 7 \pmod{12}$ implica $x = 7 + 12k = (3 + 4) + 3 \cdot 4k = 3 + 4(1 + 3k)$ e, portanto, $x = 3 + 4q$ ou $x - 3 = 4q$. Daí, $4 \mid x - 3$, ou seja, $x \equiv 3 \pmod{4}$.

b) Temos: $x^2 \equiv 1 \pmod{p}$ é equivalente a $p \mid x^2 - 1 = (x - 1)(x + 1)$. Como p é primo, segue que $p \mid (x - 1)$ ou $p \mid (x + 1)$ e, por conseguinte, $x \equiv 1 \pmod{p}$ ou $x \equiv -1 \pmod{p}$ se, e somente se, $x \equiv \pm 1 \pmod{p}$.

Proposição 10. Sejam a congruência $a \equiv b \pmod{m}$ e um número $n \in \mathbb{Z}$. Então, valem as seguintes afirmações:

- i) $a \equiv b \pmod{m}$ e $n \mid m$ implicam $a \equiv b \pmod{n}$.
- ii) $a \equiv b \pmod{m}$ e $a \equiv b \pmod{n}$ se, e somente se, $a \equiv b \pmod{\text{mmc}(m, n)}$.
- iii) $na \equiv nb \pmod{m}$ e $d = \text{mdc}(m, n)$ se, e somente se, $a \equiv b \pmod{\frac{m}{d}}$.

Demonstração: i) Temos: $a \equiv b \pmod{m}$ e $n \mid m$ implicam $n \mid m \mid a - b$ e, portanto, $n \mid a - b$ implica $a \equiv b \pmod{n}$.

ii) (\Rightarrow) Suponha $a \equiv b \pmod{m}$ e $a \equiv b \pmod{n}$. Então, $m \mid a - b$ e $n \mid a - b$. Pela definição de $\text{mmc}(m, n)$, temos: $\text{mmc}(m, n) \mid a - b$ e, portanto, $a \equiv b \pmod{\text{mmc}(m, n)}$.

(\Leftarrow) Temos: $a \equiv b \pmod{\text{mmc}(m, n)}$ implica $\text{mmc}(m, n) \mid a - b$. Como $m \mid \text{mmc}(m, n)$ e $n \mid \text{mmc}(m, n)$, então, $m \mid a - b$ e $n \mid a - b$ e, portanto, $a \equiv b \pmod{m}$ e $a \equiv b \pmod{n}$.

iii) (\Rightarrow) Temos: $na \equiv nb \pmod{m}$ implica $m \mid na - nb = n(a - b)$. Então, para algum $k \in \mathbb{Z}$, temos: $n(a - b) = mk$. Mas, $d = \text{mdc}(m, n)$, daí:

$$n(a - b) = mk \text{ implica } \left(\frac{n}{d}\right)(a - b) = \left(\frac{m}{d}\right)k, \text{ onde } \text{mdc}\left(\frac{n}{d}, \frac{m}{d}\right) = 1.$$

Como $\left(\frac{n}{d}\right)a \equiv \left(\frac{n}{d}\right)b \pmod{\left(\frac{m}{d}\right)}$ e $\text{mdc}\left(\frac{n}{d}, \frac{m}{d}\right) = 1$, então, vale a lei do cancelamento, ou seja, $a \equiv b \pmod{\left(\frac{m}{d}\right)}$.

(\Leftarrow) Temos: $d = \text{mdc}(m, n)$ implica $d \mid m$ e $d \mid n$, logo, existem m_0 e n_0 , tais que m

$= dm_0$ e $n = dn_0$. Por hipótese, $a \equiv b \pmod{m_0}$, logo, $a - b = m_0k$, para algum $m_0 \in \mathbb{Z}$. Daí:
 $a - b = m_0k$ implica $n(a - b) = m_0kn = m_0kdn_0 = mkn_0 = mq$, onde $q = kn_0$.
Portanto, $n(a - b) = m.q$ implica $m \mid n.a - n.b$, ou seja, $n.a \equiv n.b \pmod{m}$.

4 | CONCLUSÃO

A aritmética elementar possui imensa variedade de definições, proposições e teoremas. Dessa forma, ela possibilita discutir diversos conceitos e suas relações intrínsecas. Em particular, o conceito de congruência modular de dois números inteiros com a divisão euclidiana.

O resto dessa divisão caracteriza o conceito de congruência modular de dois números inteiros. Além disso, encaminha a definição de classe residual (ou restos), com a propriedade de que se dois números inteiros pertencem a mesma classe de restos, então estes dois números inteiros são congruentes módulo a um número pré-fixado. E todos os possíveis restos da divisão de dois inteiros geram o conjunto de todas as classes residuais que, por meio da relação de congruência modular, determina uma partição no conjunto dos números inteiros.

Em essência, é o resto da divisão de dois números inteiros que relaciona a divisão euclidiana e o conceito de congruência modular.

Portanto, nesse contexto, a congruência modular de dois números inteiros tem como essencial a teoria dos restos, oriunda da divisão euclidiana.

REFERÊNCIAS

- ALENCAR FILHO, Edgard de. **Teoria Elementar dos Números**. São Paulo, 1992.
- AYRES, Frank Jr. **Álgebra Moderna**. São Paulo, 1973.
- BOYER, Carl B. **História da Matemática**. São Paulo, 1996.
- DOMINGUES, H.H. **Fundamentos de Aritmética**. São Paulo, 1991.
- ENZO R. Gentile. **Aritmética Elemental**. Buenos Aires, Argentina, 1985.
- HEFEZ A. **Curso de Álgebra, vol. 1**. Rio de Janeiro – SBM, 2002.
- MUNIZ NETO. **Tópicos de Matemática Elementar: teoria dos números**. Rio de Janeiro – SBM, 2013.
- SHINE, Calos Yuzo. **21 Aulas de Matemática Olímpica**. Rio de Janeiro – SBM, 2009.
- SCHEINERMAN, E.R. **Matemática Discreta: uma introdução**. São Paulo, 2003.

ÍNDICE REMISSIVO

A

Acessibilidade 49

Água subterrânea 16, 17, 23, 27, 28

Algorithm Stability 1, 14

Alimentos Funcionais 110

Alumínio 7, 90, 103, 104, 105, 107, 108, 109

Aposentadoria 180, 181, 182, 183, 184, 185, 186, 187

B

Biomonitoramento 120, 122, 124, 125, 130, 131, 132, 133, 134

C

Câmbio 167, 170

CBERS-2B 68, 73, 74

Cenário econômico 167

Classe residual 203, 218

CoDesign 33

Compósitos 8, 135, 136, 137, 138, 140, 141, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158

Compósitos Ternários 148, 150

Congruência Modular 9, 203, 204, 210, 213, 218

Consumidor 34, 35, 37, 39, 167, 173, 174, 176

D

Dados Reais 68, 73, 74, 76

Design de interação 56

Design e tecnologia 49, 56

Design Regenerativo 6, 33, 34, 36, 37, 38, 39, 41, 42, 44, 45, 46

Direito ambiental 6, 33

Divisão Euclidiana 9, 203, 204, 205, 206, 210, 211, 214, 218

E

Economia circular 6, 33, 34, 36, 41, 42, 43, 44, 45, 46

Elastômero Termoplástico 8, 148, 150, 152, 158, 159

Equação Cinemática 68

Extended Kalman Filter 1, 3, 14

F

Fitólitos 84, 87, 89, 90, 92, 94, 96, 97, 98, 99, 100, 101

Fluorescência de raios X 103

Folhas de Alumínio 7, 103, 104, 105

Fotocopiadoras 8, 120, 121, 122, 123, 124, 126, 127, 128, 129, 130, 131, 132, 133

Função de Transferência 160

G

Geometria Analítica 9, 192, 193, 194

H

Hibiscus sabdariffa L. 110, 111, 118, 119

Hortaliça não convencional 110, 111, 112

I

Inflação 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177

L

Linhas de pedra 7, 84, 86, 87, 88, 89, 90, 91, 92, 97, 98, 101

M

Matemática 28, 192, 193, 194, 195, 197, 201, 202, 210, 212, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227

Médio Vale do Rio Paraíba do Sul 7, 84, 88, 98

N

Nível estático 16

Nutrição Humana 110

Nutrição Vegetal 110, 112

O

Orbit Determination 6, 1, 2, 3, 7, 8, 9, 14, 15

Organizações de alta complexidade 56, 58, 59, 61

P

Pesquisa e metodologia do design 49

Planos de Previdência Privada 180, 189

Poliéster 135, 136, 137, 139, 144

Polipropileno 8, 135, 137, 142, 144, 145, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159

políticas públicas 33, 34, 42, 123

Prevenção de acidentes 56

Previdência Complementar Aberta 180, 190

Previdência Complementar Fechada 180

Propriedades 8, 18, 104, 112, 135, 137, 138, 142, 143, 145, 146, 147, 148, 149, 150, 154, 158, 159, 161, 194, 203, 207, 213, 215

R

Realidade virtual 7, 56, 57, 58, 59, 61, 63, 64, 65

Reconstituição Paleoambiental 84

Resíduos sólidos 16, 18, 27, 35, 37, 38, 40, 41, 42, 43, 135

Resíduos têxteis 8, 135, 136, 137, 139, 145, 146

S

Saúde 34, 40, 43, 49, 50, 54, 61, 105, 120, 121, 122, 123, 124, 125, 132, 134, 183

Sensação Térmica 6, 30, 31, 32

Sigma-Point Kalman Filter 1

Sistema Aquífero Serra Geral 16, 18, 28

Sistema de Posicionamento Global 192, 193, 195

Suavizador de Estado 68

T

Talco 8, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158

Taxa Selic 167, 173, 177

Tecnologia Assistiva 6, 49, 50, 51, 54, 55

Termômetro 6, 30, 31, 32

Teste de micronúcleos 120

Tradescantia Pallida 8, 120, 121, 122, 125, 128, 130, 131, 133, 134

Transferência de calor 160, 161, 165

Transformada de Laplace 160

Ciências Exatas e da Terra: Aprendizado, Integração e Necessidades do País 2

www.atenaeditora.com.br 

contato@atenaeditora.com.br 

[@atenaeditora](https://www.instagram.com/atenaeditora) 


www.facebook.com/atenaeditora.com.br 


 **Atena**
Editora

Ano 2021

Ciências Exatas e da Terra: Aprendizado, Integração e Necessidades do País 2

www.atenaeditora.com.br 

contato@atenaeditora.com.br 

[@atenaeditora](https://www.instagram.com/atenaeditora) 

www.facebook.com/atenaeditora.com.br 