UNIVERSIDADE ESTADUAL DO CEARÁ

CENTRO DE CIÊNCIAS E TECNOLOGIA

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

FRANCISCO RUTEMBERG DA SILVA RODRIGUES

TEORIA DOS NÚMEROS: UM ESTUDO DE RESOLUÇÃO DE PROBLEMAS DA OCM DO NÍVEL 3

FORTALEZA – CEARÁ

2020

FRANCISCO RUTEMBERG DA SILVA RODRIGUES

TEORIA DOS NÚMEROS: UM ESTUDO DE RESOLUÇÃO DE PROBLEMAS DA OCM DO NÍVEL 3

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional do Programa de Pós-Graduação em Matemática do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial à obtenção do titulo de mestre em Matemática em Rede Nacional. Área de concentração: Matemática.

Orientador: Profº. Drº. Ulisses Lima Parente.

FORTALEZA – CEARÁ

20200

Dados Internacionais de Catalogação na Publicação
Universidade Estadual do Ceará
Sistema de Bibliotecas

Rodrigues, Francisco Rutemberg da Silva .
Teoria dos números: um estudo de resolução de problemas da ocm do nível 3 [recurso eletrônico] / Francisco Rutemberg da Silva Rodrigues. - 2020
Um arquivo no formato PDF do trabalho acadêmico com 75 folhas.

Dissertação (mestrado profissional) - Universidade Estadual do Ceará, Centro de Ciências e Tecnologia, Mestrado Profissional em Matemática em Rede Nacional, Fortaleza, 2020.
Área de concentração: matematica.
Orientação: Prof. Dr. Ulisses Lima Parente. .

1. Teoria dos Números. 2. OCM. 3. Problemas Olímpicos. I. Título.

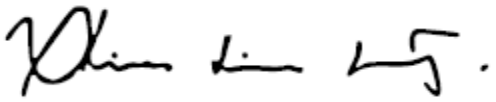
FRANCISCO RUTEMBERG DA SILVA RODRIGUES

TEORIA DOS NÚMEROS: UM ESTUDO DE RESOLUÇÃO DE PROBLEMAS DA OCM DO NÍVEL 3

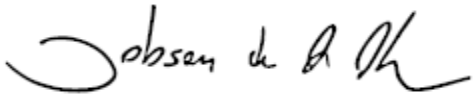
Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional do Programa de Pós-Graduação em Matemática do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial à obtenção do titulo de mestre em Matemática em Rede Nacional. Área de concentração: Matemática.

Aprovado em: 15 de dezembro de 2020

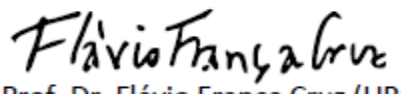
BANCA EXAMINADORA



Prof. Dr. Ulisses Lima Parente (PROFMAT/UECE/QUIXADÁ)



Prof. Dr. Jobson de Queiroz Oliveira (PROFMAT/UECE/QUIXADÁ)



Prof. Dr. Flávio França Cruz (URCA)

AGRADECIMENTOS

Agradeço primeiramente a Deus por todas bênçãos que recebi nesta longa caminhada, me dar sabedoria e força para seguir sempre em frente.

A toda a minha família, em especial minha esposa e companheira Crislândia Lima, por ter me ajudado e me encorajado a concluir o mestrado, a meus filhos, na qual, são o berço de toda minha força, minha mãe Inacia Rodrigues, meu pai Edaias Rodrigues e Minhas irmãs (Odaisa Rodrigues, Rosilene Rodrigues, Rosiane Rodrigues e Rocykelma Rodrigues), os maiores responsáveis pelos ensinamentos de vida e me fazer buscar pelo sucesso até aqui conquistado. Por todas as vezes em que compreenderam minhas ausências e me estimularam a enfrentar os obstáculos que surgiram pelo caminho.

Agradeço aos parceiros de turma do mestrado, em especial aos companheiros José e Tiago por toda aprendizagem e conhecimento compartilhado nos incansáveis momentos de estudo durante mais essa etapa concluída. Por todo o apoio, o auxílio e o incentivo a mim dedicados e por dividirem seus saberes em busca de crescimento pessoal e profissional.

Aos mestres que foram importantes para meu aprendizado. Particularmente ao meu orientador Profº. Drº. Ulisses Lima Parente, por confiar e acreditar na minha capacidade.

Agradecimento especial aos professores Jobson e Tony que participaram, contribuíram e tornaram possível a realização desse trabalho, transmitindo toda experiência e conhecimento nas aulas do PROFMAT.

Ao PROFMAT pela oportunidade de aprimoramento da minha formação.

RESUMO

Este trabalho apresenta uma proposta que possibilita inserir a teoria elementar dos números, como sugestões extracurriculares na educação básica e possibilitar uma maior participação e uma abordagem nos conteúdos relacionados à OCM. A ideia principal deste trabalho é uma ampliação na participação das escolas cearenses na OCM, tornando-lhe uma ferramenta fundamental no ensino e aprendizagem da matemática. Para isso, faz-se necessária a compreensão de alguns conceitos e propriedades dos números naturais e inteiros, tais como: divisibilidade, números primos, máximo divisor comum, mínimo múltiplo comum, equações diofantinas e congruências. Iremos também fazer um breve histórico da OCM - Olimpíada Cearense de Matemática, na qual, apresentaremos a Coluna de Matemática do Jornal O Povo e o projeto Numeratizar que tiveram um papel fundamental para preparação e incentivo dos cearenses para diversas olimpíadas nacionais e internacionais, além de sua importante contribuição para a evolução do nível da matemática no Ceará. Vamos falar também da evolução dos problemas ao longo dos anos e finalizaremos com uma lista de problemas da OCM do assunto teoria dos números.

Palavras-chave: Teoria dos Números. OCM. Problemas Olímpicos.

ABSTRACT

This work presents a proposal that makes it possible to insert the elementary number theory, as extracurricular suggestions in basic education and enable greater participation and an approach to content related to the OCM. The main idea of this work is to expand the participation of Ceará schools in the CMO, making it a fundamental tool in the teaching and learning of mathematics. For this, it is necessary to understand some concepts and properties of natural and integer numbers, such as: divisibility, prime numbers, maximum common divisor, minimum common multiple, Diophantine equations and congruences. We will also make a brief history of the OCM - Cearense Mathematics Olympiad, in which we will present the Mathematics Column of the Jornal O Povo and the Numeratizar project, which played a fundamental role in preparing and encouraging the people of Ceará for several national and international Olympics, in addition to its important contribution to the evolution of the level of mathematics in Ceará. We will also talk about the evolution of problems over the years and we will end with a list of OCM problems in the subject of number theory.

Keywords: Number Theory. OCM. Olympic problems.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

OCM	Olimpíada Cearense de Matemática
OBMEP	Olimpíada Brasileira de Matemática das Escolas Públicas
MDC	Máximo Divisor Comum
MMC	Mínimo Múltiplo Comum
UFC	Universidade Federal do Ceará
PIC	Programa de Iniciação Científica
PROFMAT	Mestrado Profissional em Matemática em Rede Nacional

SUMÁRIO

1 INTRODUÇÃO

Após ser aprovado em um concurso para professor de Matemática da Educação Básica do estado do Ceará em 2009, percebi o quanto as olimpíadas de Matemática são importantes para aprendizagem dos alunos, com isso, detiquei a orienta-los sobre olimpíadas de mátemática. Neste trabalho, irei dar enfase na Olimpíada Cearense de Matemática – OCM, levando em consideração o seu surgimento aqui no estado do Ceará em 1981 e fazendo com que alunos da rede pública e privada tenham oportunidade de participação.

Apesar de não ter participado como aluno de olimpíada, tive a oportunidade de participar do projeto OBMEP na escola desde 2015, na qual, tive meu primeiro contato com problemas olímpicos, ministrei aulas em grandes e renomadas escolas de Quixadá e Fortaleza. Essa vivência, me fez ver o quanto a Matemática em si é encantadora e faz a diferença na mente das pessoas que querem de fato criar um hábito de estudo e aprimorar seus conhecimentos.

O presente trabalho pretende contribuir com propostas extracurriculares na educação básica que possibilitem uma maior democratização de acesso e de conteúdos relacionados à OCM, pois ao serem analisados os índices de participação das escolas públicas, verifica-se um tímido percentual de unidades escolares envolvidas.

A ideia principal deste trabalho é que se consiga uma ampliação da participação das escolas cearenses na OCM, tornando-lhe uma ferramenta fundamental no ensino e aprendizagem da matemática.

Foi realizada pesquisas em livros especializados em olimpíadas de Matemática, também nos sites oficiais de cada competição na internet, contactando os respectivos coordenadores, a fim de coletar o maior número de informações.

No capítulo 5 abordaremos um breve histórico sobre as Olimpíadas Cearenses de Matemática, quais os critérios de inscrições, descrevendo o seu regulamento, elaboramos um levantamento dos municípios e escolas participantes. Mostraremos a coluna do jornal O Povo que teve papel fundamental na divulgação das olimpíadas, relatando como tais competições foram essenciais para moldar a vida de muitos ex-alunos olímpicos que se tornaram professores de Matemática, também será falado sobre o projeto Numeratizar. Também destacaremos a evolução no nível

das questões de Teoria dos Números, fazendo um comparativo do início com as questões atuais.

Os capítulos 3 a 5 são dedicados às definições e propriedades dos números naturais e inteiros, princípio de indução matemática, divisibilidade, divisão euclidiana, sistema de numeração decimal, alguns critérios de divisibilidade, máximo divisor comum, mínimo múltiplo comum e propriedades, algoritmo de Euclides, equações diofantinas lineares e artitmética dos restos, e mostraremos também alguns problemas e soluções de questões que foram abordadas na OCM desde 1981.

2 OLIMPÍADA CEARENSE DE MATEMÁTICA (OCM)

2.1 Breve Histórico da OCM

Desde 1979, segundo o site da Olimpíada Brasileira de Matemática - OBM, ver www.obm.org.br, a Sociedade Brasileira de Matemática (SBM) organizou a 1ª Olimpíadas Brasileira de Matemática (OBM), na qual, despertou nos Departamentos de Matemática das Universidades Federais a ideia da realização de Olimpíadas Regionais de Matemática. Em 1981 surgiu a ideia da criação da "Olimpíada Cearense de Matemática (OCM)".

A Olimpíada Cearense de Matemática é uma competição para estudantes do Ensino Fundamental e do Ensino Médio que é realizada anualmente desde 1981, revelando alunos, professores e escolas que têm bom desempenho na absorção e transmissão do conhecimento matemático.

As provas da OCM são realizadas na Universidade Federal do Ceará (UFC), pelo Departamento de Matemática, dividida em três níveis: nível I – sexto e sétimo anos, nível II – oitavo e nonos anos e o nível III – ensino médio. Os problemas propostos em cada competição são elaborados pelos professores da Comissão de Olimpíadas do referido departamento, grande parte deles sendo de sua própria autoria. No decorrer dos anos, a OCM tem contribuído no destaque em matemática de muitos alunos cearenses pelo mundo, na qual, a OCM é porta de entrada para competições matemáticas ao redor do mundo. Foi partindo da iniciativa desses professores e gerações seguintes que o Ceará se tornou tradicionalmente conhecido pelos excelentes resultados de seus estudantes na OBM e em diversas olimpíadas internacionais, onde devemos levar em consideração de ser uma das mais difíceis olimpíadas do Brasil. No ano de 2016, a prova da OCM foi usada também para selecionar os alunos que integrarão a equipe de Fortaleza da Olimpíada de Matemática Rio Platense[1]. Sendo que os níveis da mesma possuem uma nomenclatura diferente dos níveis da OCM e que participam dela apenas alunos de Fortaleza.

[1] Olimpíada de Matemática realizada na Argentina. A equipe brasileira é formada pelos 3 primeiros medalhistas na Olimpíada Cearense de Matemática (time de Fortaleza), e os 3 primeiros no teste de seleção realizado na Olimpíada Paulista de Matemática (equipe de São Paulo).

As primeiras Olimpíadas Cearenses de Matemática foram realizadas nas sedes de colégios das redes públicas e privadas de ensino. Sendo a partir da quarta olimpíada, as provas eram aplicadas na sede do Departamento de Matemática da Universidade Federal do Ceará, no campus do Pici. Segue, na tabela abaixo o quantitativo de inscritos nas quatro primeiras olimpíadas:

Tabela 1 - Ano, local e quantidade de inscritos na OCM

Ano	Local de prova	Inscritos
1981	Colégio Ary de Sá Cavalcante	408
1982	Colégio Juventos e Colégio Joaquim Albano	960
1983	Colégio Lourenço Filho	561
1984	Universidade Federal do Ceará – UFC	483

Fonte: elaborada pelo autor

Para uma escola participar pela primeira vez de uma OCM o representante da escola deve fazer uma solicitação formal para o coordenador da OCM e realizar um pagamento de uma taxa, em seguida receberá orientações para o preenchimento da ficha de inscrição.

A competição é disciplina pelo presente regulamento:

I - Para se inscrever na competição o candidato deve estar cursando:

• Nível 1: 6º e 7º anos do ensino fundamental I

• Nível 2: 8º e 9º anos do ensino fundamental II

• Nível 3: 1º, 2º e 3º anos do ensino médio.

II – Entregar a ficha de inscrição preenchida sem emendas e/ou rasuras.

III – Para cada Nível, haverá uma prova analítico-expositiva, baseada no programa da competição, com duração de 4 horas e composta de 5 (cinco) problemas, valendo cada um deles 10 pontos.

IV – As provas são aplicadas nas dependências do Departamento de Matemática da Universidade Federal do Ceará, no Campus do Pici.

V – As inscrições são efetuadas nos estabelecimentos de ensino fundamental e médio cadastrados.

VI – A Comissão Examinadora classifica até o máximo de 20 (vinte) candidatos de cada Nível e indicará aqueles que serão premiados com medalhas de ouro, prata e bronze, na proporção aproximada de 1:2:3 (ex: sendo x medalhas de ouro, serão 2x de prata e 3x de bronze).

VII – O total de premiados com medalhas, em cada nível, será

aproximadamente 60% dos classificados pela Comissão. Examinadora.

VIII – Será outorgado diploma de Menção Honrosa aos classificados que não forem premiados com medalhas.

IX – As decisões da Comissão Examinadora são irrecorríveis, não havendo vistas de provas nem possibilidades de revisão, nem divulgação dos critérios usados para classificação e premiação.

X – Os casos omissos deste regulamento serão resolvidos pelo Coordenador da OCM e, em última instância, pela Comissão Coordenadora da Olimpíada.

Abaixo será apresentada uma tabela com o número de alunos inscritos nas Olimpíadas Cearenses de Matemática no ano 2019, separados por níveis, na qual, a escola que leciono, EEEP Mário Alencar, participou pela primeira vez no nível 3.

Tabela 2 - Inscritos em 2019 por níveis

Ano	Nível 1	Nível 2	Nível 3	Total
2019	712	558	560	1830

Fonte: Elaborada pelo autor

Na tabela abaixo, tem-se a relação das escolas participantes do nível 3 da OCM 2019, sendo 57 escolas públicas e privadas, das cidades de Fortaleza, Sobral, Amontada e Eusébio.

Tabela 3 - Escolas participante do nível 3 da OCM (Continua)

ESCOLA	CIDADE	ADMINISTRAÇÃO
FARIAS BRITO COLEGIO CENTRAL	Fortaleza	Privada
SALESIANO DOM BOSCO COLEGIO	Fortaleza	Privada
CECILIA COLEGIO SANTA	Fortaleza	Privada
COLEGIO CHRISTUS BARAO DE STUDART	Fortaleza	Privada
EEFM PAROQUIA DA PAZ	Fortaleza	Privada
ARI DE SA CAVALCANTE COLEGIO - DUQUE DE CAXIAS	Fortaleza	Privada
ADVENTISTA PAULO CESAR AFONSO COLEGIO	Fortaleza	Privada
COLEGIO ARI DE SA CAVALCANTE WASHINGTON SOARES	Fortaleza	Privada
SANTO INACIO COLEGIO	Fortaleza	Privada
ODILON BRAVEZA COL	Fortaleza	Privada
ANTARES ATS COLEGIO	Fortaleza	Privada
ANTARES COLEGIO	Fortaleza	Privada
7 DE SETEMBRO COLEGIO - NGS	Fortaleza	Privada
7 DE SETEMBRO COLEGIO - EBS	Fortaleza	Privada
TOMAS DE AQUINO COLEGIO	Fortaleza	Privada

(Conclusão)

EEFM DOUTOR CESAR CALS	Fortaleza	Privada
TELEYOS COLEGIO	Fortaleza	Privada
COLEGIO DA POLÍCIA MILITAR DO CEARA	Fortaleza	Privada
COLEGIO MILITAR DE FORTALEZA	Fortaleza	Privada
COLEGIO MILITAR DO CORPO DE BOMBEIROS	Fortaleza	Privada
ARI DE SA CAVALCANTE COLEGIO - MAJOR FACUNDO	Fortaleza	Privada
FARIAS BRITO JOVEM SEIS BOCAS COLEGIO	Fortaleza	Privada
MASTER COLEGIO	Fortaleza	Privada
COLEGIO ANTARES ATS	Fortaleza	Privada
FARIAS BRITO COLEGIO DE APLICACAO	Fortaleza	Privada
ARI DE SA CAVALCANTE SEDE MARIO MAMEDE COLEGIO	Fortaleza	Privada
CHRISTUS COLEGIO PRE UNIVERSITARIO	Fortaleza	Privada
COLEGIO ANTARES - ATS	Fortaleza	Privada
MASTER SUL COLEGIO	Fortaleza	Privada
COLEGIO ANTARES ATS	Fortaleza	Privada
FARIAS BRITO COLEGIO PRE-VESTIBULAR CENTRAL	Fortaleza	Privada
ARI DE SA CAVALCANTE SEDE ALDEOTA COLEGIO	Fortaleza	Privada
7 DE SETEMBRO COLEGIO – EGS	Fortaleza	Privada
FARIAS BRITO PRE VESTIBULAR ALDEOTA	Fortaleza	Privada
COLEGIO CHRISTUS UNIDADE SUL	Fortaleza	Privada
COLEGIO CHRISTUS DIONISIO TORRES	Fortaleza	Privada
COLEGIO CHRISTUS UNIDADE PARQUELANDIA	Fortaleza	Privada
COLEGIO ANTARES ATS	Fortaleza	Privada
ANTARES COLEGIO PRE VESTIBULAR	Fortaleza	Privada
EEEP MARIO ALENCAR	**Fortaleza**	**Pública**
COLEGIO MILITAR DO CORPO DE BOMBEIROS	Fortaleza	Pública
EEEP MARIA ANGELA DA SILVEIRA BORGES	Fortaleza	Pública
ESCOLA MUNICIPAL PROFESSORA MARIA JOSE MACARIO COELHO	Fortaleza	Pública
OCM Avulsas Fortaleza-01 Publica	Fortaleza	Pública
COLEGIO FARIAS BRITO SOBRALENSE	Sobral	Privada
ELPIDIO RIBEIRO DA SILVA DE EI EF	Sobral	Pública
PAULO ARAGAO	Sobral	Pública
JOAQUIM BARRETO LIMA	Sobral	Pública
LEONILIA GOMES PARENTE	Sobral	Pública
JOSE INACIO GOMES PARENTE	Sobral	Pública
JOSE LEONCIO	Sobral	Pública
ARAUJO CHAVES	Sobral	Pública
MARIA DORILENE ARRUDA ARAGAO	Sobral	Pública
MARIA DE FATIMA SOUZA SILVA	Sobral	Pública
MARIA DIAS IBIAPINA	Sobral	Pública
JOSE COELHO DE MORAIS EEB	Amontada	Pública
FARIAS BRITO JUNIOR EUSEBIO COLEGIO	Eusébio	Privada

Fonte: Elaborada pelo autor

2.2 OCM e Jornal O Povo

No dia 10 de setembro de 1987, entra em cena, a Coluna Olimpíada de Matemática no cenário educacional cearense, publicada no Jornal O Povo. Inicialmente, foi pensada, segundo seus autores, apenas para veicular notícias sobre as diversas Olimpíadas de Matemática, que já aconteciam à época, na qual, terminaria por ir muito além.

Em uma quinta-feira, no dia 10 de setembro de 1987 entrou em circulação, no Jornal O Povo, o primeiro número da Coluna Olimpíada de Matemática. O espaço dedicado ocupou quase uma página inteira do primeiro caderno. E talvez poucos, ou mesmo pouquíssimos leitores, imaginariam que tal coluna se repetiria toda semana por mais de uma dezena de anos.

Recorde-se aqui o frontispício deste número:

OLIMPÍADA DE MATEMÁTICA

Universidade Federal do Ceará – Centro de Ciências – Departamento de Matemática – Ano I – n.º 1 Guilherme Ellery - João Marques Pereira – Marcondes França – Thompson Gonçalves

O formato era iniciado com o título Olimpíada de Matemática, de forma genérica. Porém, ficava claro as associações com as Olimpíadas Cearense de Matemática e Brasileira de Matemática, que ocorriam desde 1979. Em seguida, viria a informação acerca da instituição acadêmica responsável, o Departamento de Matemática, do Centro de Ciências da Universidade Federal do Ceará (UFC). E por fim, quatro nomes que indicariam a autoria da coluna.

A seguir será feita uma apresentação de uma parte do texto que foi exposto na primeira edição, no qual a coluna se inseriria, bem como sobre os principais objetivos pedagógicos da mesma.

APRESENTAÇÃO

> Iniciamos, hoje, a execução de um Projeto que visa contribuir com o aprimoramento do Ensino da Matemática nos 1º e 2 Graus, estimular o gosto por esta Ciência e suas aplicações e despertar o espírito criativo latente na nossa juventude. O Departamento de Matemática da Universidade Federal do Ceará vem se preocupando com a Iniciação à Matemática, há mais de duas décadas. Durante todo este tempo um amplo Programa vem sendo desenvolvido. Inicialmente com o Curso Mirim e com o apoio do CECINE. Posteriormente, com a realização de Cursos para professores de Fortaleza e do interior do Estado, que atuam em nossos Colégios, com a promoção da

> Olimpíada Cearense de Matemática e, agora, com a implantação do Plantão de Atendimento a alunos e professores da Rede de Ensino de 1º e 2º Graus e com a publicação semanal da Coluna Olimpíada de Matemática. (JORNAL O POVO, 10.09.1987).

Continuando essa viagem pelo número inicial da Coluna, deparamos com a reprodução do seguinte pensamento do grande matemático alemão Carl Friedrich Gauss (1777-1855), ao lado de um seu retrato pintado:

> Sempre me pareceu estranho que todos aqueles que estudam seriamente esta ciência acabam tomados de uma espécie de paixão pela mesma. Em verdade, o que proporciona o máximo prazer não é o conhecimento e sim a aprendizagem, não é a posse, mas a aquisição, não é a presença, mas o ato de atingir a meta. (JORNAL O POVO, 10.09.1987).

A escolha de Gauss, pelos autores, pode ter tido uma motivação a mais, pois o contexto socioeconômico que envolvia a família de Gauss, ao final do século XVIII na Alemanha, poderia ser muito similar a de famílias de jovens talentosos leitores da Coluna, ao final do século XX no Brasil.

Os seu autores Guilherme Ellery, João Marques Pereira, Marcondes França e Tompson Gonçalves, acreditaram que elevando o alcance dos conhecimentos matemáticos, com métodos envolventes no seu ensino, questões com suas respectivas soluções, notícias sobre eventos, fatos e comentários específicos, além de temas relacionados às Olimpíadas Matemática Estadual, Nacional e Internacionais, aumentaram o universo de leitores da coluna, obtendo reconhecimento geral, ainda disponibilizaram plantões, objetivando a aproximação com alunos, professores e interessados pela matemática.

Figura 1 - Primeira edição da Coluna Olimpíada de Matemática do Jornal O Povo


OLIMPÍADA DE MATEMÁTICA

Apresentação

Nossa Homenagem

Fonte: Jornal O Povo, Coluna Olimpíada de Matemática, nº 1 (10/09/1987).

Destacamos o Coordenador da Olimpíada Cearense de Matemática, um dos quatro autores da Coluna, na qual seria convidado pela Sociedade Brasileira de Matemática (SBM), a integrar a Coordenação Geral de Olimpíadas de Matemática no Brasil.

Figura 2 - Publicação nº 225 da Coluna Olimpíada de Matemática do Jornal O Povo

OLIMPÍADA DE MATEMÁTICA

O POVO — Fortaleza, Quinta-feira, 16 de janeiro de 1992 — Ano V - Nº 225 — (Coluna semanal)
UNIVERSIDADE FEDERAL DO CEARÁ • CENTRO DE CIÊNCIAS • DEPARTAMENTO DE MATEMÁTICA
Marcondes França • Guilherme Ellery • João Marques Pereira • Tompson Gonçalves

Professor cearense recebe convite da Sociedade Brasileira de Matemática

O Prof. César Camacho, Presidente da SBM - Sociedade Brasileira de Matemática, convidou o Prof. Marcondes Cavalcante França para fazer parte, durante dois anos, da "Comissão de Olimpíadas" daquela entidade. Esta Comissão seleciona as equipes brasileiras que participam de eventos internacionais, tais como a Olimpíada Internacional de Matemática, a Olimpíada Iberoamericana de Matemática e Olimpíada de Matemática do Cone Sul, além de organizar a Olimpíada Brasileira de Matemática nas modalidades Senior e Júnior.

Marcondes França

Prof. Marcondes é coordenador, há onze anos, da Olimpíada Cearense de Matemática e também é coordenador da equipe de professores do Departamento de Matemática da UFC, responsável pela veiculação desta Coluna. O convite da SBM ao Prof. Marcondes significa o reconhecimento daquela Sociedade ao bom desempenho dos estudantes cearenses que participaram da Olimpíada Brasileira de Matemática Senior e Júnior.

Fonte: Jornal O Povo, Coluna Olimpíada de Matemática, nº 225 (16/01/1992).

No ano de 1992 tivemos a participação de quatro estudantes selecionados pela SBM para compor a equipe brasileira na participação da Olimpíada de Matemática do Cone Sul[2], na qual, eram todos cearenses, indicando a hegemonia do nosso Estado, nesta faixa etária, à época. A equipe brasileira conquistaria um honroso segundo lugar nesta competição, ficando atrás apenas da equipe argentina.

[2] É uma competição internacional da qual participam os países meridional da América do Sul, representados por equipes de 4 estudantes que não tenham feito 16 anos de idade em 31 de dezembro do ano imediatamente anterior à celebração da Olimpíada.

Figura 3 - Publicação nº 249 da Coluna Olimpíada de Matemática do Jornal O Povo

OLIMPÍADA DE MATEMÁTICA

O POVO — Fortaleza, Domingo, 12 de julho de 1992 — Ano V - Nº 249 — (Coluna semanal)
UNIVERSIDADE FEDERAL DO CEARÁ • CENTRO DE CIÊNCIAS • DEPARTAMENTO DE MATEMÁTICA
Marcondes França • João Marques Ferreira • Tompson Gonçalves • Guilherme Ellery

Equipe do Brasil na Olimpíada de Matemática do Cone Sul é formada somente de cearenses

A Olimpíada de Matemática do Cone Sul é um concurso, anual, organizado pelos países do Cone Sul, para jovens na faixa etária de 18 anos, cujos objetivos são estimular o estudo da Matemática, descobrir talentos e vocações para esta Ciência, além de proporcionar o intecâmbio de experiências educacionais na área de Matemática e o aprofundamento da amizade entre os países participantes.

A Sociedade Brasileira de Matemática, através de concurso nacional, selecionou os jovens cearenses João Luiz Alencar Araripe Falcão (Geo), José Carlos Jucá Pompeu Filho (Farias Brito), Marcondes Cavalcante França Júnior (Colégio Militar) e Paulo José Bonfim Gomes Rodrigues (7 de Setembro) para representar o Brasil na 3ª Olimpíada de Matemática do Cone Sul que será realizada no período de 12 a 17 de julho de 1992, em Santiago, no Chile.

A expressiva vitória dos quatro jovens do Ceará é fruto do trabalho que o Departamento de Matemática da Universidade Federal do Ceará, desenvolve, há 12 anos, através do programa Olimpíada de Matemática, com os Colégios de 1º e 2º graus. Nosso programa é apoiado pelo O POVO — que oferece o espaço para esta Coluna e fomentado pelo Conselho Estadual de Desenvolvimento Científico e Tecnológico, órgão vinculado à Secretaria de Planejamento do Estado do Ceará.

A delegação de nosso País para o evento é formada pelos quatro estudantes acima referidos e pelos professores Silvio Henrique Araújo Mota (7 de Setembro), Antônio Caminha Muniz Neto (Geo) e Pedro Gilson Dantas Fernandes (Farias Brito), respectivamente, líder, vice líder e observador da delegação. Toda a equipe viajou, na terça-feira passada, para o Rio de Janeiro onde participaram de um curso de treinamento, até sexta-feira, dia 10, patrocinado pela Sociedade Brasileira de Matemática.

A outra parte da programação é a seguinte: Dia 12 (hoje) — Embarque para Santiago, 13 – Abertura da Olimpíada e passeio turístico, 14 — primeiro dia de prova (10h a 14h30min), 15 — segundo dia de prova (10h e 14h30min), 16 — passeio turístico, 17 — Encerramento da Olimpíada e premiação e 18 — retorno a Fortaleza com escala no Rio de Janeiro.

Nossos estudantes disputarão a competição com jovens da Argentina, Uruguai, Paraguai, Chile, Peru e Bolívia.

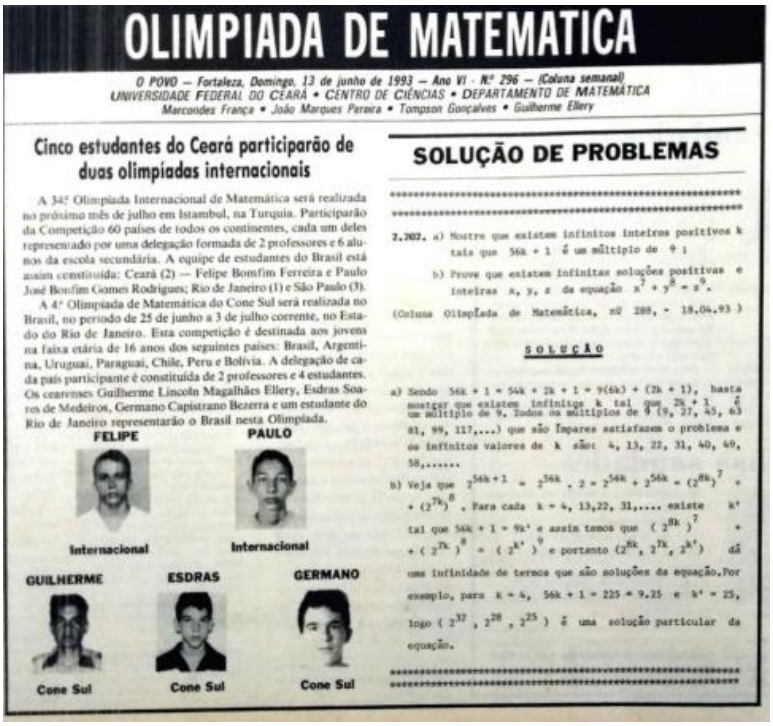
Prof. Sílvio Henrique Araújo Mota — LÍDER
Prof. Antonio Caminha Muniz Neto — VICE-LÍDER
João Luiz Alencar Araripe Falcão — ESTUDANTE
José Carlos Jucá Pompeu Filho — ESTUDANTE
Marcondes Cavalcante França Júnior — ESTUDANTE
Paulo José Bonfim Gomes Rodrigues — ESTUDANTE

Fonte: Jornal O Povo, Coluna Olimpíada de Matemática, nº 249 (12/07/1992).

O Ceará se destaca na modalidade Júnior da OBM, com 3 medalhas de ouro, 3 medalhas de prata e 2 medalhas de bronze, bem como indicariam uma evolução da participação na modalidade Sênior, com 3 medalhas de prata, 4 medalhas de bronze e 3 menções honrosas.

Pela primeira vez estudantes cearenses iriam fazer parte da equipe que representaria o Brasil na 34ª Olimpíada Internacional de Matemática em Istambul na Turquia, na qual, tiveram participação de 73 países e 413 estudantes. Da equipe de seis integrantes, dois seriam cearenses (Felipe e Paulo). E participando da 4ª Olimpíada de Matemática do Cone Sul, que se realizaria no Rio de Janeiro, estariam constituindo a delegação de cada país, 2 professores e 4 estudantes, sendo a equipe brasileira composta por 3 estudantes cearenses (Guilherme, Esdras e Germano) e 1 estudante do Rio de Janeiro.

Figura 4 - Publicação nº 296 da Coluna Olimpíada de Matemática do Jornal O Povo



OLIMPIADA DE MATEMATICA

O POVO — Fortaleza, Domingo, 13 de junho de 1993 — Ano VI - Nº 296 — (Coluna semanal)
UNIVERSIDADE FEDERAL DO CEARÁ • CENTRO DE CIÊNCIAS • DEPARTAMENTO DE MATEMÁTICA
Marcondes França • João Marques Pereira • Tompson Gonçalves • Guilherme Ellery

Cinco estudantes do Ceará participarão de duas olimpíadas internacionais

A 34ª Olimpíada Internacional de Matemática será realizada no próximo mês de julho em Istambul, na Turquia. Participarão da Competição 60 países de todos os continentes, cada um deles representado por uma delegação formada de 2 professores e 6 alunos da escola secundária. A equipe de estudantes do Brasil está assim constituída: Ceará (2) — Felipe Bomfim Ferreira e Paulo José Bomfim Gomes Rodrigues; Rio de Janeiro (1) e São Paulo (3).

A 4ª Olimpíada de Matemática do Cone Sul será realizada no Brasil, no período de 25 de junho a 3 de julho corrente, no Estado do Rio de Janeiro. Esta competição é destinada aos jovens na faixa etária de 16 anos dos seguintes países: Brasil, Argentina, Uruguai, Paraguai, Chile, Peru e Bolívia. A delegação de cada país participante é constituída de 2 professores e 4 estudantes. Os cearenses Guilherme Lincoln Magalhães Ellery, Esdras Soares de Medeiros, Germano Capistrano Bezerra e um estudante do Rio de Janeiro representarão o Brasil nesta Olimpíada.

FELIPE — Internacional
PAULO — Internacional
GUILHERME — Cone Sul
ESDRAS — Cone Sul
GERMANO — Cone Sul

SOLUÇÃO DE PROBLEMAS

2.202. a) Mostre que existem infinitos inteiros positivos k tais que $56k + 1$ é um múltiplo de 9 ;

b) Prove que existem infinitas soluções positivas e inteiras x, y, z da equação $x^7 + y^8 = z^9$.

(Coluna Olimpíada de Matemática, nº 288, - 18.04.93)

SOLUÇÃO

a) Sendo $56k + 1 = 54k + 2k + 1 = 9(6k) + (2k + 1)$, basta mostrar que existem infinitos k tal que $2k + 1$ é um múltiplo de 9. Todos os múltiplos de 9 (9, 27, 45, 63 81, 99, 117,...) que são ímpares satisfazem o problema e os infinitos valores de k são: 4, 13, 22, 31, 40, 49, 58,.....

b) Veja que $2^{56k+1} = 2^{56k} \cdot 2 = 2^{54k} + 2^{56k} = (2^{8k})^7 + (2^{7k})^8$. Para cada k = 4, 13,22, 31,.... existe k' tal que $56k + 1 = 9k'$ e assim temos que $(2^{8k})^7 + (2^{7k})^8 = (2^{k'})^9$ e portanto $(2^{8k}, 2^{7k}, 2^{k'})$ dá uma infinidade de ternos que são soluções da equação.Por exemplo, para k = 4, $56k + 1 = 225 = 9.25$ e k' = 25, logo $(2^{32}, 2^{28}, 2^{25})$ é uma solução particular da equação.

Fonte: Jornal O Povo, Coluna Olimpíada de Matemática, nº 296 (13/06/1993).

Obtendo destaque de três estudantes cearenses na competição: Exdras e Germano com medalhas de Bronze e Gulherme com medalha de Prata, na qual seriam privilegiados na edição do dia 4 de julho de 1993.

Figura 5 - Publicação nº 299 da Coluna Olimpíada de Matemática do Jornal O Povo

OLIMPIADA DE MATEMATICA

O POVO — Fortaleza, Domingo, 04 de julho de 1993 — Ano VI - Nº 299 — (Coluna semanal)
UNIVERSIDADE FEDERAL DO CEARÁ • CENTRO DE CIÊNCIAS • DEPARTAMENTO DE MATEMÁTICA
Marcondes França • João Marques Pereira • Tompson Gonçalves • Guilherme Ellery

PREMIAÇÃO DA OLIMPÍADA DO CONE SUL

A Olimpíada de Matemática do Cone Sul realizou-se, em Petrópolis, no Rio de Janeiro, no período de 26 de junho a 3 de julho com a participação de estudantes do Brasil, Uruguai, Paraguai, Chile, Peru e Bolívia. O júri internacional da competição concedeu 6 medalhas: 1 de ouro (Brasil), 1 de ouro (Argentina), 2 de prata (Brasil e Argentina) e 2 de bronze (Brasil). A equipe que representou o Brasil foi formado por 4 estudantes cearenses e 1 carioca. Os nomes dos brasileiros agraciados com medalhas são os seguintes: Andersou da Silva Almeida (ouro, Rio de Janeiro), Guilherme Lincoln Magalhães Ellery (prata, Ceará, Farias Brito), Esdras Soares de Medeiros (bronze, Ceará, 7 de Setembro) e Germano Capistrano Bezerra (bronze, Ceará, Christus).

GUILHERME — Prata
ESDRAS — Bronze
GERMANO — Bronze

Prova do 1º Grau

Na edição de hoje publicamos os enunciados das questões 5, 6 e 7 da prova do 1º Grau da 13ª Olimpíada Cearense de Matemática.

5. Considere as funções quadráticas reais $f(x) = 2x^2 + 5x + c$ e $g(x) = 2x^2 + 5x + d$. Determine a área localizada entre os gráficos de f e g no trecho de $x = n$ até $x = m$, onde m é maior que n.

6. Seja n um número natural positivo. Faça o que está solicitado em cada item:
a) Mostre que $3n + 1$ e $4n + 1$ são números primos entre si;
b) Mostre que, se k e j são números naturais primos entre si, tais que $k \cdot j = n^2$ para algum n então k e j são quadrados perfeitos;
c) Determine o menor valor de n de modo que o produto $(3n + 1) \cdot (4n + 1)$ seja um quadrado perfeito.

7. Na figura ao lado ABCDEF é um hexágono regular e PQR é um triângulo equilátero e AB = 3 e PQ = 5. Determine a área interna ao triângulo equilátero que é externa ao hexágono.

Obs.: P é o centro do círculo circunscrito ao hexágono.

Prova do 2º Grau

Iniciamos a publicação das questões da prova do 2º Grau da 13ª OCM.

1. A área de um triângulo ABC é igual a $4m^2$. Se o ângulo Â mede 30º, determine os comprimentos dos lados AB e AC de modo que o comprimento do lado BC seja o menor possível.

2. Se p e q são números complexos, com q diferente de zero e se as raízes da equação $x^2 + px + q^2 = 0$ tem o mesmo módulo, prove que $|p| \leq 2|q|$.

3. Considere duas urnas A e B, onde A contém 1.000 bolas (inicialmente todas vermelhas) e B contém 5.000 bolas (inicialmente todas brancas).
Aplique para o seguinte procedimento iterativo:
1º passo: Retira-se 100 bolas de B e coloca-se em A, passando A a contar com 1.100 bolas e B com 4.900 bolas. Em seguida, aleatoriamente, retira-se 100 bolas de A e repõe-se em B, restabelecendo os números iniciais de 1.000 bolas em A e 5.000 bolas em B;
2º Passo: Após executado o 1º passo; torna-se a retirar 100 bolas de B, aleatoriamente, e coloca-se em A. Em seguida retira-se 100 bolas de A, aleatoriamente, e devolve-se a B, novamente estabelecendo os números de 1.000 bolas na urna A e 5.000 bolas na urna B; e assim sucessivamente.
Após k passos, qual das conclusões é verdadeira?
a) Existem mais bolas brancas em A do que bolas vermelhas em B;
b) O número de bolas brancas em A é o mesmo de bolas vermelhas em B;
c) Existem mais bolas vermelhas em B do que bolas brancas em A.
Justifique sua conclusão.

Fonte: Jornal O Povo, Coluna Olimpíada de Matemática, nº 299 (04/07/1993).

Abaixo destacamos os professores responsáveis pela coluna, uma fotografia colhida no Campus do Pici, no dia 19/06/1993. Da esquerda para a direita: Marcondes Cavalcante França. Guilherme Lincoln Aguiar Ellery, Raimundo Tompson Gonçalves e João Marques Pereira.

Figura 6 - Fotografia dos Responsáveis pela Coluna Olimpíada de Matemática do Jornal O Povo

Fonte: Jornal O Povo, Coluna Olimpíada de Matemática, nº 301 (18/07/1993).

2.3 Assuntos de Teoria dos Números mais abordados na OCM

Neste capítulo apresentaremos a análise de um tema que é tradicionalmente abordado nas Olimpíadas Cearense de Matemática, listamos abaixo os assuntos mais abordados ao longo dos anos de OCM. Destacando os assuntos Teoria dos Números mais abordados e com isso ter um parâmetro para perceber a evolução dos problemas apresentados, verificando e tirando conclusões a respeito da elevação dos tópicos mais frequentes.

(Continua)

Tabela 4 - Assuntos mais abordados na OCM de Teoria dos Números

Ano	Números primos	Teorema Fundamental da Aritmética	Divisores	Algoritmo da divisão	MMC e MDC	Relação de Bézout	Equação Diofantinas Lineares	Congruências

(Conclusão)

1981	X							
1982			X	X				
1983			X	X				
1984			X	X				
1985								
1986			X	X				
1987	X							
1988								X
1989			X					
1990								X
1991			X					X
1992	X				X			X
1993					X		X	
1994	X		X					
1995								
1996	X		X					
1997			X					X
1998			X					X
1999			X		X			
2000			X		X			
2001								X
2002					X			
2003			X	X	X			
2004	X		X					
2005			X					
2006								X
2007			X					
2008								X
2009								
2010								X
2011			X					
2012			X					
2013			X					
2014							X	X
2015			X	X				
2016								
2017								
2018			X	X				
2019			X	X				X

Fonte: elaborado pelo autor

A tabela acima mostra os principais assuntos de teoria dos números que foram abordados ao longo dos anos, destacamos três: números primos, divisores e congruência.

Em seguida, serão apresentadas quatro questões com suas respectivas soluções, na qual foram escolhidos em décadas diferentes. Nessas quatro questões foi analisado a evolução dos problemas ao longo dos anos, ou seja, ao verificar as questões da primeira olimpíada (1981) e comparar com a última (2019), verifica-se

que foi exigido um conhecimento mais aguçado, na qual exige uma abstração maior na ferramenta da Teoria dos Números para resolução dos problemas, pode-se inferir que foram exigidos conhecimentos de Divisibilidade, números primos e congruência para resolução dos problemas.

Problema 2.5.1 (OCM-1981). Coloque certo (C) ou errado (E) na proposição abaixo:
01 – ( ) O número fatorial 5! – 1 é primo.

SOLUÇÃO:

O item está CORRETO.

$5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$

$5! - 1 = 120 - 1 = 119.$

Ou seja, 5! – 1 é primo.

Problema (OCM-1992 – b). Prove que o número $37^{37} + 83^{83}$ é divisível por 3.

SOLUÇÃO:

Usando que $37 \equiv 1 \pmod 3$ *e que* $83 \equiv -1 \pmod 3$ *teremos:*

$37^{37} + 83^{83} \equiv 1^{37} + (-1)^{37} \equiv 1 + (-1) \equiv 0 \pmod 3$, *ou seja,* $37^{37} + 83^{83}$ *é divisível por 3.*

Problema (OCM-2001). Se $p > 3$ é primo, prove que o resto da divisão de p^2 por 12 é igual a 1.

SOLUÇÃO:

Como p > 3, temos as seguintes possibilidades para o resto da divisão de p por 12:

$$p \equiv 1, 5, 7, 11 \pmod{12}.$$

Analisando cada uma destas possibilidades temos:

- $p \equiv 1 \pmod{12} \implies p^2 \equiv 1^2 \equiv 1 \pmod{12}.$
- $p \equiv 5 \pmod{12} \implies p^2 \equiv 5^2 \equiv 1 \pmod{12}.$
- $p \equiv 7 \pmod{12} \implies p^2 \equiv 7^2 \equiv 1 \pmod{12}.$
- $p \equiv 11 \pmod{12} \implies p^2 \equiv 11^2 \equiv 1 \pmod{12}.$

Em qualquer um dos casos temos $p^2 \equiv 1 \pmod{12}$, *ou seja, o resto da divisão de* p^2 *por 12 é 1.*

Problema (OCM-2019). Encontre os três últimos algarismos da representação decimal de 2019^{2019}. Justifique sua resposta.

Solução:

Para $n \geq 2$, *temos* $2019^n \equiv 19^n \pmod{1000}$. *Agora, módulo 1000, temos*

$$19^n = (20 - 1)^n \equiv \binom{n}{n-2} 20^2 (-1)^{n-2} + \binom{n}{n-1} 20(-1)^{n-1} + (-1)^n$$

$$\equiv (-1)^n (200n(n - 1) - 20n + 1).$$

Com n = 2019, temos (módulo 1000)

$$19^{2019} \equiv -(200 \cdot 2019 \cdot 2018 - 20 \cdot 2019 + 1)$$
$$\equiv -(200 \cdot 19 \cdot 18 - 20 \cdot 19 + 1)$$
$$\equiv -(400 - 380 + 1)$$
$$\equiv -21$$
$$\equiv 979.$$

Portanto, os últimos três algarismos de 2019^{2019} são 979.

Fazendo uma análise dos problemas abordados ao logo dos anos da OCM, percebe-se que o nível de dificuldade das questões é perceptível e com isso elas se tornaram mais abstratas, fazendo com que o aluno colocasse em pratica o raciocínio logico dedutivo, pois para chegar à solução, tem que ter uma saída mais estratégica levando em consideração todo artificio usado para aprimorarem a solução.

2.4 Alguns projetos Olímpicos cearense

Iremos apresentar alguns projetos olímpicos que se destacaram no Ceará, além do trabalho com Olimpíada Cearense de Matemática, tivemos também, o Projeto Linguagem das Letras e dos Números – Leituralizar e Numeratizar, e o Projeto Olimpíadas de Fortaleza.

O Governo do Estado do Ceará, em 2003, desenvolveu o Projeto Linguagem das Letras e dos Números – Numeratizar e Leituralizar, na qual estavam sob a supervisão da UFC. Este projeto teve como motivação os resultados obtidos nas Olimpíadas de Matemática realizadas nas escolas privadas de Fortaleza, a qual, a vertente deste projeto relativa à Matemática teve início imediato, realizando sua primeira olimpíada no segundo semestre daquele ano.

Estimulado com o sucesso do projeto, por iniciativa do Secretário Paulo de Melo Jorge Filho, a Prefeitura de Fortaleza, criou o Programa de Olimpíadas de Fortaleza, incluindo as áreas de Matemática, Português e Ciências. Olimpíadas das três áreas foram realizadas em 2004.

Figura 7 - Fotografia da premiação da Olimpíada de Fortaleza – Matemática, primeira fase

Fonte: Elaborada pelo autor.

Participaram da primeira fase do Numeratizar 110.995 alunos, provenientes de 646 escolas situadas em 190 municípios do Estado. Destes, foram para a segunda fase 5587 alunos dos quais foram selecionados 346 estudantes para premiação. Estes estudantes foram indicados para participar da fase de treinamento da olimpíada.

As olimpíadas de Fortaleza foram realizadas com 70424 alunos provenientes de 158 escolas. A inovação maior desta olimpíada foi a de que abrangeu universalmente todos os alunos da quinta a oitava série de todas as escolas municipais de Fortaleza. Destes alunos foram selecionados cerca de 11000 alunos para a segunda fase e destes 3300 para a terceira fase, sendo, ao final, selecionados 307 alunos para premiação.

As aplicações das Olimpíadas trouxeram várias vantagens, entre elas, tivemos a utilização como um sistema de avaliação da qualidade do ensino escola a escola, turma a turma. Permitiu também criar um processo de competição saudável entre as escolas. Estas vantagens associaram-se às já existentes em todas as olimpíadas que inclui a elevação da autoestima de professores, alunos e da comunidade escolar.

3 OS NÚMEROS NATURAIS

Neste tópico iremos apresentar um estudo sobre números naturais, números primos e Teorema Fundamental da Aritmética, que é um dos conceitos mais importantes de toda a matemática, além de apresentar alguns problemas, dando ferramentas necessárias aos leitores para o desenvolvimento para futuros conteúdos.

Os números naturais formam um dos conceitos mais antigos concebidos pelo ser humano. Entretanto, a sua evolução de uma noção intuitiva para um conceito mais elaborado foi muito lenta. Só no final do século 19, quando os fundamentos de toda a matemática foram questionados e intensamente repensados, é que a noção de número passou a ser baseada em conceitos da teoria dos conjuntos, considerados mais primitivos.

Neste texto, não pretendemos descrever a evolução do conceito de número natural, nem tentar explicar sua natureza, mas apenas estudar algumas das suas propriedades.

Como em tudo há sempre um ponto de partida, o nosso será o de admitir que o leitor esteja familiarizado com o conjunto dos números naturais.

$$\mathbb{N} = \{1, 2, 3, 4, 5, ...\},$$

Juntamente com as operações de adição $(a, b) \to a + b$ e de multiplicação $(a, b) \to a \cdot b$ (ou $(a, b) \to ab$).

A nossa abordagem será essencialmente axiomática; ou seja, a partir de uma lista razoavelmente pequena de propriedades básicas dos números naturais e das duas operações, iremos obter as demais propriedades.

A lista de axiomas que adotaremos não será a menor possível, pois, quanto menor for esta lista, mais demorado será chegar aos resultados mais relevantes da teoria.

Existe uma axiomática idealizada no final do século 19 pelo matemático italiano Giuseppe Peano que, com axiomas, consegue não só definir a adição e a multiplicação nos naturais, como também deduzir as propriedades que assumiremos aqui como axioma.

3.1 Adição, multiplicação, subtração e divisão

1) A adição e a multiplicação são *bem definidas*:

$$\forall\ a, b, a', b' \in \mathbb{N},\ a = a' \text{ e } b = b' \ \Rightarrow\ a + b = a' + b' \text{ e } a \cdot b = a' \cdot b'.$$

2) A adição e a multiplicação são *comutativas*:

$$\forall\ a, b \in \mathbb{N},\ a + b = b + a \text{ e } a \cdot b = b \cdot a.$$

3) A adição e a multiplicação são *associativas*:

$$\forall\ a, b, c \in \mathbb{N},\ (a + b) + c = a + (b + c) \text{ e } (a \cdot b) \cdot c = a \cdot (b \cdot c).$$

4) A adição e a multiplicação possuem *elementos neutros*:

$$\forall\ a \in \mathbb{N},\ a + 0 = a \text{ e } a \cdot 1 = a.$$

4) A multiplicação é *distributiva* com relação à adição:

$$\forall\ a, b, c \in \mathbb{N},\ a \cdot (b + c) = a \cdot b = a \cdot c.$$

A Propriedade1 é que permite somar, a ambos os lados de uma igualdade, um dado número, ou multiplicar ambos os membros por um mesmo número.

Algumas vezes, trabalharemos com outros conjuntos, diferentes dos naturais, munidos de operações de adição e multiplicação que possuem de (1) a (5) acima. Neste caso, diremos que os elementos de tais conjuntos, juntamente com as duas operações, estão sujeitos às leis básicas da aritmética. Por exemplo, sabemos que os números inteiros relativos, os números racionais, os números reais e os números complexos estão sujeitos às leis básicas da aritmética. Alertamos o leitor quanto ao fato de que estes números só serão utilizados nos exemplos e nos problemas; nunca, porém, em lugar essencial para o desenvolvimento da teoria.

6) *Integridade:* Dados $a, b \in \mathbb{N}^*$, tem-se que $a \cdot b \in \mathbb{N}$.

Equivalentemente, pela formulação contrapositiva:

$$\forall\ a, b \in \mathbb{N},\ a \cdot b = 0 \ \Rightarrow\ a = 0 \text{ ou } b = 0.$$

7) *Tricotomia:* Dados $a, b \in \mathbb{N}$, uma, e apenas uma, das seguintes possibilidades é verificada:

i) $a = b$ ii) $\exists\, c \in \mathbb{N},\ b = a + c$ iii) $\exists\, c \in \mathbb{N},\ a = b + c.$

Diremos que *a* é *menor do que b*, simbolizado por $a < b,$ toda vez que (iii) acima é verificada.

Com esta definição, temos que a propriedade (iii) acima equivale a afirmar que $b < a$. Assim, a tricotomia nos diz que, dados $a, b \in$ IN, uma, e somente uma, das seguintes condições é verificada:

i) $a = b$ *ii)* $a < b$ *iii)* $b < a$.

Utilizaremos a notação $b > a$, que se lê *b é maior do que a,* para representar $a < b$.

Decorre, das definições, que $0 < a$, para todo $a \in \mathbb{N}$. De fato, para todo $a \in \mathbb{N}$, temos que $0 + a = a$, o que implica $0 < a$.

Temos, também, que se $a + b = 0$, então $a = b = 0$. De fato, se $a \neq 0$ teríamos $b < 0$, o que é absurdo, logo $a = 0$. Analogamente, mostra-se que $b = 0$. Portanto, se $a \in \mathbb{N}$ ou $b \in \mathbb{N}$, então $a + b \in \mathbb{N}$.

Proposição 3.1.1 $a \cdot 0 = 0$ *para todo* $a \in \mathbb{N}$.

DEMONSTRAÇÃO: Temos que

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

Se $a \cdot 0 \neq 0$, então teríamos $a \cdot 0 \in \mathbb{N}$ e, portanto, seguiria, da igualdade acima, que $a \cdot 0 > a \cdot 0$, o que é absurdo. *Logo,* $a \cdot 0 = 0$.

Proposição 3.1.2 *A relação "menor do que" é transitiva:*

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

DEMONSTRAÇÃO: Supondo $a < b$ e $b < c$, temos que existem $d, f \in \mathbb{N}$ tais que $b = a + d$ e $c = b + f$. Logo, usando a associatividade da adição, temos que

$$c = b + f = (a + d) + f = a + (d + f),$$

com $d + f \in \mathbb{N}^*$, o que implica que $a < c$.

Proposição 3.1.3 *A adição é compatível e cancelativa com respeito à relação "menor do que"***:**

$$\forall\ a, b, c \in \mathbb{N},\ a < b \Leftrightarrow a + c < b + c.$$

DEMONSTRAÇÃO: Suponha que $a < b$. Logo, existe $d \in \mathbb{N}$, tal que $b = a + d$. Somando c a ambos os lados desta última igualdade, pela comutatividade e associatividade da adição, temos

$$b + c = c + b = c + (a + d) = (c + a) + d = (a + c) + d,$$

o que mostra que $a + c < b + c$.

Reciprocamente, suponha que $a + c < b + c$. Pela tricotomia, temos três possibilidades: (i) $a = b$. Isto acarretaria $a + c = b + c$, portanto, falso. (ii) $b < a$. Isto

acarretaria, pela primeira parte da demonstração, que $b + c < a + c$; também é falso. (iii) $a < b$. Esta é a única possibilidade que resta.

Proposição 3.1.4 *A multiplicação é compatível e cancelativa com respeito à relação "menor do que":*

$$\forall\ a, b, \in \mathbb{N}, \forall\ c \in \mathbb{N}, a < b \Leftrightarrow a \cdot c < b \cdot c.$$

DEMONSTRAÇÃO: Suponha que $a < b$. Logo, existe $d \in \mathbb{N}$ tal que $b = a + d$. Multiplicando por c ambos os lados dessa última igualdade, pelas propriedades comutativa e distributiva da multiplicação, decorre

$$b \cdot c = c \cdot b = c \cdot (a + d) = c \cdot a + c \cdot d = a \cdot c + c \cdot d,$$

o que mostra que $c \cdot a < b \cdot c$, pois, pela integridade, $c \cdot d \in$IN.

Reciprocamente, suponha que $a \cdot c < b \cdot c$. Pela tricotomia, temos três possibilidades a analisar:

(i) $a = b$. Isto acarretaria $a \cdot b = b \cdot c$, o que é falso. (ii) $b < a$. Isto acarretaria, pela primeira parte da demonstração, que $b \cdot c < a \cdot c$, o que também é falso. (iii) $a < b$. Esta é a única possibilidade válida.

Proposição 3.1.5 *A adição é compatível e cancelativa com respeito à igualdade:*

$$\forall\ a, b, c \in \mathbb{N}, a = b \Leftrightarrow a + c = b + c.$$

DEMONSTRAÇÃO: A implicação $a = b \Rightarrow a + c = b + c$ é consequência do fato da adição ser bem definida (Propriedade 1).

Suponha agora que $a + c = b + c$. Temos três possibilidades:

(i) $a < b$. Pela Proposição 1.1.3, temos que $a + c < b + c$, o que é um absurdo.

(ii) $b < a$. Pelo mesmo argumento acima, $b + c < a + c$, o que é também um absurdo.

(iii) $a = b$. Esta é a única alternativa válida.

Proposição 3.1.6 *A multiplicação é compatível e cancelativa com respeito à igualdade:*

$$\forall\ a, b, \in \mathbb{N}, \forall\ c \in \mathbb{N}, a = b \Leftrightarrow a \cdot c = b \cdot c.$$

DEMONSTRAÇÃO: A implicação $a = b \Rightarrow a \cdot c = b \cdot c$ decorre imediatamente do fato da multiplicação ser bem definida (Propriedade 1).

Suponha agora que $a \cdot c = b \cdot c$. Temos três possibilidades:

(i) $a < b$. Pela Proposição 1.1.4, temos que $a \cdot c < b \cdot c$, o que é um absurdo.

(ii) $b < a$. Pelo mesmo argumento acima, $b \cdot c < a \cdot c$, o que é também um absurdo.

(iii) $a = b$. Esta é a única alternativa válida.

Subtração

Dados dois números naturais *a* e *b* com $a \leq b$, sabemos que existe um número natural *c* tal que $b = a + c$. Neste caso, definimos o número *b menos a,* denotamos por $b - a$, como sendo o número *c.* Em símbolos:

$$b - a = c.$$

Proposição 3.2.1 *Sejam a, b,* $c \in \mathbb{N}$. *Se* $a \leq b$, *então*

$$c \cdot (b - a) = c \cdot b - c \cdot a.$$

DEMONSTRAÇÃO: Note que, se $a \leq b$, então $c \cdot b - c \cdot a$ está bem definida.

Suponha agora que $b - a = d$, logo $b = d + a$. Multiplicando por *c* ambos os membros desta última igualdade, obtemos $c \cdot b = c \cdot (a + d) = c \cdot a + c \cdot d$, o que implica

$$c \cdot d = c \cdot b - c \cdot a.$$

Substituindo *d* por $b - a$ na igualdade acima, obtemos

$$c \cdot (b - a) = c \cdot b - c \cdot a.$$

Os números naturais e suas propriedades que descrevemos até o presente momento não é suficiente para caracterizá-los. Contudo, podemos complementar com a teoria dos números naturais, na qual, pode ser deduzida de três axiomas, conhecidos como axiomas de Peano. Onde, podem ser, assim, formuladas:

(i) Todo número natural tem um sucessor, que ainda é um número natural; números diferentes têm sucessores diferentes.

(ii) Existe um único número natural 1 que não é sucessor de nenhum outro.

(iii) (Axioma de Indução Matemática) Se um conjunto de números naturais contém o número 1 e contém também o sucessor de cada um de seus elementos, então esse conjunto contém todos os números naturais.

O Axioma de Indução serve de base para um método de demonstração de teoremas sobre os naturais, conhecido como o *método de indução,* o qual funciona assim: “se uma propriedade *P* é válida para o número 1 e se, supondo *P* válida para um número *n* daí resultar que *P* é válida também para seu sucessor *s(n),* então *P* é válida para todos os números naturais”.

Divisão

Divisibilidade

Dados dois números inteiros *a* e *b* com $a \neq 0$, dizemos que *a* divide *b* e escrevendo $a|b$, quando existir $c \in \mathbb{N}$ tal que $b = a \cdot c$. Dizemos também que *a* é um divisor ou um fator de *b ou,* ainda, que *b* é um múltiplo de *a.* Caso *a* não divida *b,* escrevemos $a \nmid b$.

Exemplo

2 | 8, porque 8 = 2 · 4;

-4 | 20, porque 20 = (-4) · (-5);

3 | -21, porque –21 = 3 · (-7)

7 ∤ 10, porque não existe $q \in Z$ tal que 10 = 7 · *q.*

Iremos estabelecer na proposição a seguir, algumas propriedades básicas da relação de divisibilidade, as quais, usaremos em problemas futuros.

Proposição 3.3.1.1 Sejam *a, b, c* inteiros não nulos e *x, y* inteiros quaisquer.

(i) Se *b* | *a* e *a* | *b,* então $a = \pm b$.

(ii) Se *c* | *b* e *b* | *a,* então *c* | *a.*

(iii) Se *c* | *a* e *c* | *b,* então *c* | *(ax + by).*

(iv) Se *b* | *a,* então |*b*| ≤ |*a*|.

(v) Se *c* | *b,* então *c* | *ab.*

(vi) Se *b* | *a,* então *bc* | *ac.*

3.2 Representação dos Naturais

3.2.1 O Sistema Decimal

Os números naturais foram representados ao longo da história de vários modos distintos. O modo universalmente utilizado na atualidade é a representação decimal posicional. Esse sistema, variante do sistema sexagesimal utilizado pelos babilônios há cerca de 1700 anos antes de Cristo, foi desenvolvido na China e na Índia. Nesse sistema, todo número natural é representado por uma sequência formada pelos algarismos

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

Por serem 10 esses algarismos, o sistema é chamado de decimal. O sistema é também dito posicional, pois cada algarismo, além de seu valor intrínseco, possui um peso que lhe é atribuído em função de sua posição dentro da sequência. Esse peso é uma potência de 10 e varia do seguinte modo:

O algarismo da extrema direita tem peso $10^0 = 1$; o seguinte, sempre da direita para a esquerda, tem peso $10^1 = 10$; o seguinte tem peso $10^2 = 100$; o seguinte tem peso $10^3 = 1\,000$ etc. Assim, o número 1 458, no sistema decimal representa o

número

$$1 \times 10^3 + 4 \times 10^2 + 5 \times 10 + 8.$$

Os zeros à esquerda em um número são irrelevantes, pois por exemplo,

$$0231 = 0 \times 10^3 + 2 \times 10^2 + 3 \times 10 + 1 = 2 \times 10^2 + 3 \times 10 + 1 = 231.$$

Cada algarismo de um número possui uma *ordem*, contada da direita para a esquerda. Assim, no exemplo acima, o 8 é de primeira ordem, o 5 de segunda ordem, o 4 de terceira ordem e o 1 de quarta ordem.

Cada três ordens, também contadas da direita para a esquerda, constituem uma classe. As classes são usualmente separadas por um ponto. A seguir, damos os nomes das primeiras classes e ordens:

$$\text{Classe das unidades} \begin{cases} unidades\ 1ª\ ordem \\ dezenas\ 2ª\ ordem \\ centena\ 3ª\ ordem \end{cases}$$

$$\text{Classe do milhar} \begin{cases} unidades\ de\ milhar\ 4ª\ ordem \\ dezenas\ de\ milhar\ 5ª\ ordem \\ centena\ de\ milhae\ 6ª\ ordem \end{cases}$$

$$\text{Classe do milhão} \begin{cases} unidades\ do\ milhão\ 7ª\ ordem \\ dezenas\ do\ milhão\ 8ª\ ordem \\ centena\ do\ milhão\ 9ª\ ordem \end{cases}$$

3.3 Números Primos

Os números primos são números especiais que desempenham um papel importante dentro da teoria e entre outras coisas os seus produtos representam todos os números naturais.

Definição. *Um número natural diferente de 0 e de 1 e que é apenas múltiplo de 1 e de si próprio é chamado de número primo. Um número diferente de 0 e de 1 que não é primo é chamado de número composto.*

Por exemplo, 2, 3, 5 e 7 são números primos, enquanto 4, 6 e 8 são números compostos, por serem múltiplos de 2.

Mais geralmente, todo número par maior do que 2 não é primo, ou seja, é composto.

Note que a definição acima não classifica os números 0 e 1 nem como primos nem como compostos. Exceto esses dois números, todo número natural ou é primo ou é composto.

Certamente, os números compostos são em número infinito, pois já os

números pares diferentes de 2 são em número infinito.

Uma pergunta que surge espontaneamente é a seguinte: Quantos são os números primos?

Euclides de Alexandria, em 300 a.C., ou seja, há mais de 2 300 anos, mostrou que existem infinitos números primos.

Como terá Euclides feito isto? Será que ele exibiu todos os números primos? Seria isto possível? Veremos na próxima seção como ele realizou esta façanha.

Determinar se um dado número é primo ou composto pode ser uma tarefa muito árdua. Para se ter uma ideia da dificuldade, você saberia dizer se o número 241 é primo?

Muito mais difícil é decidir se o número 4 294 967 297 é primo ou composto. O matemático francês Pierre de Fermat (1601-1655) afirmou que esse número é primo, enquanto o matemático suíço Leonhard Euler (1707-1783) afirmou que é composto. Qual deles estava com a razão?

3.4 O Crivo de Eratóstenes

Um método muito antigo para se obter de modo sistemático números primos é o chamado *Crivo de Eratóstenes*[3], devido ao matemático grego Eratóstenes.

A eficiência do método é baseada na observação bem simples a seguir.

Se um número natural $a > 1$ é composto, então ele é múltiplo de algum número primo p tal que $p^2 \leq a$. Equivalentemente, é primo todo número a que não é múltiplo de nenhum número primo p tal que $p^2 < a$.

De fato, se a é composto e p é o menor número primo do qual a é múltiplo, então $a = p \times b$, onde p e b são menores do que a. De todo modo, sendo b primo ou composto, ele será múltiplo de um número primo q. Como a é múltiplo de b e b é múltiplo de q, pela transitividade da relação de ser múltiplo (Problema 1.17), temos que a é também múltiplo de q e sendo p o menor primo do qual a é múltiplo, temos $p \leq q$. Logo, $p^2 \leq p \times q \leq a$.

[3] *A palavra crivo significa peneira. O método consiste em peneirar os números naturais em um intervalo [2,n], jogando fora os números que não são primos.*

Por exemplo, para mostrar que o número 221(= 13 × 17), é composto, bastaria testar se ele é múltiplo de algum dos números primos p = 2, 3, 5, 7, 11 ou 13, já que o próximo primo 17 é tal que $17^2 = 289 > 221$.

Para se obter os números primos até uma certa ordem n, escreva os números de 2 até n em uma tabela.

O primeiro desses números, o 2, é primo, pois não é múltiplo de nenhum número anterior. Risque todos os demais múltiplos de 2 na tabela, pois esses não são primos.

O primeiro número não riscado nessa nova tabela é o 3 que é primo, pois não é múltiplo de nenhum número anterior diferente de 1. Risque todos os demais múltiplos de 3 na tabela, pois esses não são primos.

O primeiro número maior que 3 e não riscado na tabela é o 5 que é um número primo, pois não é múltiplo de nenhum número anterior diferente de 1. Risque os demais múltiplos de 5 na tabela.

O primeiro número maior do que 5 e que não foi riscado é o 7, que é primo. Risque os demais múltiplos de 7 na tabela.

Ao término desse procedimento, os números não riscados são todos os primos menores ou iguais a n.

Note que o procedimento termina assim que atingirmos um número primo p tal que $p^2 \geq n$, pois, pela observação que fizemos acima, já teríamos riscado todos os números compostos menores ou iguais a n.

Exibimos a seguir o resultado do crivo para n = 250. Note que, neste caso, o procedimento termina tão logo cheguemos ao número primo p = 17.

Consultando a tabela acima temos que o número 241 é primo, respondendo à pergunta que formulamos anteriormente.

Tabela 5 - Todos os números primos até 250 (Continua)

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

(Conclusão)

101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~
131	~~132~~	~~133~~	~~134~~	~~135~~	~~136~~	137	~~138~~	139	~~140~~
~~141~~	~~142~~	~~143~~	~~144~~	~~145~~	~~146~~	~~147~~	~~148~~	149	~~150~~
151	~~152~~	~~153~~	~~154~~	~~155~~	~~156~~	157	~~158~~	~~159~~	~~160~~
~~161~~	~~162~~	163	~~164~~	~~165~~	~~166~~	167	~~168~~	~~169~~	~~170~~
~~171~~	~~172~~	173	~~174~~	~~175~~	~~176~~	~~177~~	~~178~~	179	~~180~~
181	~~182~~	~~183~~	~~184~~	~~185~~	~~186~~	~~187~~	~~188~~	~~189~~	~~190~~
191	~~192~~	193	~~194~~	~~195~~	~~196~~	197	~~198~~	199	~~200~~
~~201~~	~~202~~	~~203~~	~~204~~	~~205~~	~~206~~	~~207~~	~~208~~	~~209~~	~~210~~
211	~~212~~	~~213~~	~~214~~	~~215~~	~~216~~	~~217~~	~~218~~	~~219~~	~~220~~
~~221~~	~~222~~	223	~~224~~	~~225~~	~~226~~	227	~~228~~	229	~~230~~
~~231~~	~~232~~	233	~~234~~	~~235~~	~~236~~	~~237~~	~~238~~	239	~~240~~
241	~~242~~	~~243~~	~~244~~	~~245~~	~~246~~	~~247~~	~~248~~	~~249~~	~~250~~

Consultando a tabela acima temos que o número 241 é primo, respondendo à pergunta que formulamos anteriormente.

Da tabela acima, extraímos todos os números primos até 250:

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241							

Fonte: elaborado pelo autor

Note que a diferença de dois números primos consecutivos, excetuando 2 e 3 (que diferem de 1) é de no mínimo 2.

Dois primos consecutivos são chamados *primos gêmeos* se eles diferem de 2.

Assim, consultando a tabela dos primos acima, os seguintes são pares de primos gêmeos:

(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), (101, 103), (107, 109), (137, 139), (149, 151), (179, 181), (191, 193), (197, 199), (227, 229), (239, 241).

O que é surpreendente é que até o presente momento os matemáticos ainda não saibam dizer se os pares de primos gêmeos formam um conjunto finito ou infinito.

Três primos consecutivos serão chamados *primos trigêmeos* se a diferença entre cada dois primos consecutivos da terna é 2.

Por exemplo, (3, 5, 7) é uma terna de primos trigêmeos. Você seria capaz de exibir outra terna de primos trigêmeos?

Ao contrário dos pares de primos gêmeos, vamos mais adiante ver que será muito fácil responder à questão da finitude ou não dessas ternas.

Outro problema muito simples de ser enunciado, mas que ainda não tem resposta, é a chamada *Conjectura de Goldbach*[4].

O matemático prussiano[5] Christian Goldbach, numa carta de 7 de junho de 1742 endereçada a Leonhard Euler, o maior matemático da época e um dos maiores matemáticos de todos os tempos, propôs que se provasse que todo número maior do que 5 é a soma de três primos.

Por exemplo, $6 = 2 + 2 + 2$, $7 = 3 + 2 + 2$, $8 = 3 + 3 + 2$, $9 = 5 + 2 + 2$, $10 = 5 + 3 + 2$, $11 = 5 + 3 + 3 = 7 + 2 + 2$, $12 = 5 + 5 + 2 = 3 + 7 + 2$ etc.

Euler respondeu que acreditava nessa conjectura, porém não sabia demonstrá-la, mas que ela era equivalente a mostrar que todo número par maior ou igual do que 4 era soma de dois números primos.

Por exemplo, $4 = 2 + 2$, $6 = 3 + 3$, $8 = 5 + 3$, $10 = 3 + 7 = 5 + 5$, $12 = 5 + 7$ etc.

Pois bem, esta conjectura, até o presente momento, não foi provada, nem desmentida.

Um outro problema proposto em 1845 pelo matemático francês Joseph Bertrand (1822-1900) foi que, dado um número natural $n > 3$, sempre existe um número primo p no intervalo $(n, 2n-2)$. Cinco anos depois, o matemático russo Pafnuti Chebyshev (1821-1894) provou de modo surpreendentemente elementar, mas não o suficiente para que o façamos aqui, que a afirmação era verdadeira.

Há uma conjectura semelhante ao Postulado de Bertrand, proposta anteriormente pelo matemático francês Adrien-Marie Legendre (1752-1833), mas que ainda não foi provada nem desmentida, que é a seguinte:

Dado um número natural n sempre existe um número primo no intervalo $(n^2, (n + 1)^2)$.

---

[4] *O termo conjectura numa linguagem mais coloquial significa* ***palpite, chute****.*

[5] *A Prússia tem uma história muito rica dentro do contexto europeu dos séculos 18, 19 e 20, marcado por guerras intermináveis. No tempo de Goldbach a Prússia era um reino muito pobre, mas que posteriormente tornou-se um potente império chegando a ocupar grande parte da Europa do Norte. Para saber mais consulte o seu professor de História.*

3.5 Teorema Fundamental da Aritmética

Nesta seção iremos apresentar mais um grande resultado da matemática que é o Teorema Fundamental da Aritmética. Antes vamos relembrar alguns conceitos.

O método do Crivo de Eratóstenes nos mostra que dado um número natural a, existe um número primo p_0 tal que ou $a = p_0$, ou a é um múltiplo não trivial de p_0; isto é, $a = p_0a_1$, com $1 < a_1 < a$.

Se a segunda possibilidade é verificada, segue que existe um número primo p_1, tal que ou $a_1 = p_1$, ou $a_1 = p_1a_2$, onde $1 < a_2 < a_1 < a$. Assim,

$$a = p_0p_1, \text{ ou } a = p_0p_1a_2.$$

Continuando a argumentação para a_2, temos $a = p_0p_1p_2$, ou $a = p_0p_1p_2a_3$, para algum primo p_2 e $1 < a_3 < a_2 < a_1 < a$.

Note que desigualdades como a acima não podem continuar indefinidamente. Logo, para algum r, o número a_r é um primo p_r, obtendo desse modo uma decomposição de a em fatores primos:

$$a = p_1p_2 \cdots p_r.$$

Obtemos, assim, o seguinte resultado que se encontra no livro *Os Elementos* de Euclides de Alexandria.

Proposição (Euclides)

Todo número natural $a > 1$, ou é primo, ou se escreve como produto de números primos.

Teorema Fundamental da Aritmética

Dado um número natural $a \geq 2$, existem um número $r > 0$, números primos $p_1 < \cdots < p_r$ e números naturais não nulos $n_1, \ldots, n_r$ tais que

$$a = p_1^{n_1} \cdots p_r^{n_r};$$

além disso, esta escrita é única[6]

[6] *Observe que ordenamos os primos que intervêm na fatoração de a por ordem crescente, daí a unicidade da escrita. Esta parte do teorema não se encontra nos Elementos de Euclides, apesar daquela obra conter todos os ingredientes para prová-la. A prova completa foi dada por Gauss mais de dois séculos depois e acredita-se que Euclides não a fez por falta de notações adequadas.*

Os números primos se distribuem dentro de $\mathbb{N}$ de modo bastante irregular. Já vimos que existem primos consecutivos cuja diferença é 2: são os primos gêmeos. Por outro lado, dado um número n arbitrário, existem dois primos consecutivos cuja diferença é maior do que n. De fato, dado n, considere o número $a = 1 \times 2 \times 3 \times \cdots \times n$. Assim,

$$a + 2,\ a + 3,\ a + 4,\ \ldots,\ a + n,$$

são inteiros consecutivos todos compostos, pois $a+2$ é múltiplo de 2, $a + 3$ é múltiplo de 3, $\ldots$, $a + n$ é múltiplo de n. Sejam p o maior primo menor do que $a + 2$ e q o menor primo maior do que $a + n$ (que existe pois os primos são infinitos); logo p e q são dois primos consecutivos, com $q - p > n$.

Alguns dos problemas mais profundos ainda por resolver estão relacionados com a distribuição dos números primos dentro da sequência dos números naturais.

3.6 Problemas

Problema 2.6.1. Determine a soma de todos os múltiplos de 6 que se escrevem no sistema decimal com dois algarismos.

Problema 2.6.2. Fixe três algarismos distintos e diferentes de zero. Forme os seis números com dois algarismos distintos tomados dentre os algarismos fixados. Mostre que a soma desses números é igual a 22 vezes a soma dos três algarismos fixados.

Problema 2.6.3. Nos tempos de seus avós não existiam as calculadoras eletrônicas e por isso eram ensinadas várias regras de cálculo mental. Uma delas era a seguinte:

Seja a um número natural cujo algarismo da unidade é 5, ou seja, $a = 10q + 5$, com q um número natural. Mostre que $a^2 = 100q(q + 1) + 25$. Com isto, ache uma regra para calcular mentalmente o quadrado de a. Aplique a sua regra para calcular os quadrados dos números; 15, 25, 35, 45, 55, 65, 75, 85, 95, 105 e 205.

Problema 2.6.4. Qual é o menor número de dois algarismos? E qual é o maior? Quantos são os números de dois algarismos? Quantos algarismos precisa-se para escrevê-los?

Problema 2.6.5. Diga quais dos seguintes números são primos e quais são

compostos:

9, 10, 11, 12, 13, 15, 17, 21, 23, 47, 49.

Problema 2.6.7 Decomponha em produtos de primos os seguintes números: 4, 6, 8, 28, 36, 84, 320 e 2 597.

Problema 2.6.8 (OCM-1981). Coloque certo (C) ou errado (E) na proposição abaixo:

01 – ( ) O número fatorial 5! – 1 é primo.

Problema 2.6.9 (OCM-1985).

(a) Mostre que, se n é um inteiro positivo, então $(n-2)n(n+1)$ é um múltiplo de 3.

(b) Mostre que, se n é um inteiro positivo, então $n^3 + 3n^2 + 5n + 3$ é divisível por 3.

Problema 2.6.10 (OCM-1986). Se p e $p + 2$ são números primos estritamente maiores que 3, prove que 6 é um divisor de $p + 1$.

Problema 2.6.11 (OCM-1988). Prove que para qualquer inteiro positivo n, $\mathbb{N} = n^2 + 1$ não é divisível por 3.

Problema 2.6.12 (OCM-1994). Se $2^k - 1\ (k \geq 2)$ é um número primo, prove que k também é primo.

Problema 2.6.13 (OCM-2015). Considere o conjunto

$B = \{a^2 + 3b^2;\ a, b \in \mathbb{Z}\}$.

Mostre que se $n \in B$ e p é um fator primo de n tal que $p \in B$, então $\frac{n}{p} \in B$.

Problema 2.6.14 (OCM-2018). Encontre, com justificativa, todos os inteiros positivos a, b e p, tais que p é primo e $1/p = 1/a^2 + 1/b^2$.

4 OS NÚMEROS INTEIROS

Dados dois números naturais a e b, até o momento, o número $b - a$ só foi definido quando $b \geq a$. Como remediar esta situação? O jeito que os matemáticos encontraram para que seja sempre definido o número $b - a$ foi o de ampliar o conjunto dos números naturais formando um novo conjunto $\mathbb{Z}$ chamado de *conjunto dos números inteiros*, cujos elementos são dados ordenadamente como segue:

$$..., -3, -2, -1, 0, 1, 2, 3, ...$$

Os números à esquerda do zero são chamados de *números negativos* e os à direita são chamados de *números positivos*. Os pares de números 1 e −1, 2 e −2, 3 e −3 etc., são chamados de *números simétricos*. O elemento 0, que não é nem positivo, nem negativo, é o seu próprio simétrico.

Em $\mathbb{Z}$ temos uma relação de ordem que estende a relação de ordem de $\mathbb{N}$, onde declaramos $a < b$ quando a se encontra à esquerda de b. Esta relação continua transitiva e total (i.e., satisfazendo à tricotomia). Os intervalos em $\mathbb{Z}$ são definidos de modo análogo aos intervalos de $\mathbb{N}$.

Representando por $-a$ o simétrico de a, seja ele positivo, negativo ou nulo, temos sempre que

$$-(-a) = a.$$

No conjunto Z, temos definida a adição como segue:

Para todo número inteiro a, definimos $a + b$ como sendo o número obtido pelo deslocamento de a para a direita de b posições, se $b \geq 0$ ou de $-b$ posições para a esquerda se $b < 0$. A adição no conjunto $\mathbb{Z}$ continua tendo as propriedades comutativa e associativa e é compatível com a relação de ordem.

Definimos a diferença $b - a$ como sendo o número obtido deslocando b para a esquerda a posições, se $a > 0$; e deslocando b para a direita $-a$ posições, se $a < 0$. Isto define uma operação em $\mathbb{Z}$, sem restrições, chamada de *subtração*. Assim, temos que a subtração é a operação inversa da adição e

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

4.1 Múltiplos Inteiros de um Número

Dado um inteiro a, consideremos o conjunto dos múltiplos inteiros de a:

$$a\mathbb{Z} = \{a \times d;\ d \in \mathbb{Z}\}.$$

Proposição 4.1.1. Os múltiplos inteiros de um elemento a possuem as seguintes propriedades:

(i) 0 é múltiplo de a.

(ii) Se m é um múltiplo de a, então $-m$ é múltiplo de a.

(iii) Um múltiplo de um múltiplo de a é um múltiplo de a.

(iv) Se m e m' são múltiplos de a, então $m + m'$ e $m - m'$ são também múltiplos de a.

(v) Se m e m' são múltiplos de a, então $e \times m + f \times m'$ é múltiplo de a, quaisquer que sejam os inteiros e e f (note que (iv) é um caso particular da presente propriedade).

(vi) Se $m + m'$ ou $m - m'$ é múltiplo de a e m é múltiplo de a, então m' é múltiplo de a.

O mesmo resultado vale para os múltiplos comuns de dois inteiros a e b. De fato, o seguinte problema lida com esta situação.

Proposição 4.1.2. Os múltiplos inteiros comuns de dois elementos a e b possuem as seguintes propriedades:

(i) 0 é múltiplo comum de a e b.

(ii) Se m é um múltiplo comum de a e b, então $-m$ é múltiplo comum de a e b.

(iii) Um múltiplo de um múltiplo comum de a e b é um múltiplo comum de a e b.

(iv) Se m e m' são múltiplos comuns de a e b, então $m + m'$ e $m - m'$ são também múltiplos comuns de a e b.

(v) Se m e m' são múltiplos comuns de a e b, então $e \times m + f \times m'$ é múltiplo comum de a e b, quaisquer que sejam os inteiros e e f (note que (iv) é um caso particular da presente propriedade).

(vi) Se $m + m'$ ou $m - m'$ é múltiplo comum de a e b e m é múltiplo comum de a e b, então m' é múltiplo comum de a e b.

Vimos que dois números naturais a e b possuem sempre um mmc que é um

número natural. Se um dos números a ou b é nulo e o outro é um inteiro qualquer, então esses números só admitem o zero como múltiplo comum, que será chamado do mínimo múltiplo comum (mmc) de a e b. Se a e b são ambos não nulos, mesmo que não sejam ambos positivos, então define-se o mínimo múltiplo comum (mmc) de a e b como sendo o menor múltiplo comum positivo; ou seja, o menor elemento positivo do conjunto

$$a\mathbb{Z} \cap b\mathbb{Z}.$$

Problema 4.1.3. Suponha que os números 216 e 144 sejam múltiplos comuns de um determinado par de números a e b. Mostre que mmc(a, b) ≤ 72.

4.2 Divisores

Nesta seção olharemos a noção de múltiplo sob outro ponto de vista.

Definição. Diremos que um número inteiro d é um *divisor* de outro inteiro a, se a é múltiplo de d; ou seja, se $a = d \times c$, para algum inteiro c. Quando a é múltiplo de d dizemos também que a é *divisível* por d ou que d *divide* a. Representaremos o fato de um número d ser divisor de um número a, ou d dividir a, pelo símbolo $d \mid a$. Caso d não divida a, escrevemos $d \nmid a$.

Assim, por exemplo, temos que $1 \mid 6$, $2 \mid 6$, $3 \mid 6$, $6 \mid 6$, $-6 \mid 6$, $-3 \mid 6$, $-2 \mid 6$, $-1 \mid 6$.

Além disso, se $d \in \{-6, -3, -2, -1, 1, 2, 3, 6\}$, então $d \nmid 6$. Temos também que $1 \mid a$ e $d \mid 0$, para todo d, inclusive quando $d = 0$, pois 0 é múltiplo de qualquer número[7]. Note também que se $d \mid a$, então $-d \mid a$, $d \mid -a$ e $-d \mid -a$.

Note que se a e d são números naturais, com $a \neq 0$, e se $d \mid a$, então $d \leq a$. De fato, sendo a um múltiplo natural não nulo do número natural d, sabemos que $a \geq d$.

Problema 4.2.1. Mostre que das duas propriedades acima segue que, se a é um inteiro não nulo, os divisores de a são em número finito.

Proposição 4.2.2. Se a e b são números naturais não nulos, então $a \mid b$ e $b \mid a$ se, e somente se, $a = b$.

Os critérios de multiplicidade podem ser reenunciados como critérios de

[7] Isto absolutamente não quer dizer que podemos dividir zero por zero, pois como $0 = c \times 0$ para todo c, o "quociente" de 0 por 0 poderia ser qualquer número, logo não estaria bem definido.

divisibilidade.

Por exemplo, dado um número $n = n_r \ldots n_1 n_0$ na sua representação decimal, temos o resultado:

n é divisível por 2 (*ou seja múltiplo de* 2) *se e somente se* n_0 *é um número par.*

Problema 4.2.3. Enuncie critérios de divisibilidade por 3, 4, 5, 8, 9 e 10.

Utilizando a noção de divisor, podemos também redefinir a noção de número primo como sendo um número $p > 1$ que só possui 1 e o próprio p como divisores positivos.

A divisibilidade possui várias propriedades importantes decorrentes das propriedades dos múltiplos e cuja utilização vai nos facilitar a vida.

A relação de divisibilidade é transitiva, ou seja, se $a \mid b$ e $b \mid c$, então $a \mid c$.

De fato, isto é o mesmo que a transitividade da relação de ser múltiplo (veja Problema 1.17).

Proposição 4.2.4. As seguintes propriedades importantes da divisibilidade:

(a) Se $d \mid a$ e $d \mid b$, então $d \mid (b + a)$ e $d \mid (b - a)$.

(b) Se $d \mid (b + a)$ ou $d \mid (b - a)$ e $d \mid a$, então $d \mid b$.

(c) Conclua que d é um divisor comum de a e de b se e somente se d é um divisor comum de a e de $b - a$.

Definição. Dados dois números inteiros a e b não simultaneamente nulos, o maior divisor comum de a e b será chamado de *máximo divisor comum* de a e b e denotado por mdc(a, b).

Note que mdc(a, b) = mdc(b, a).

O problema de determinar o mdc de dois números é bem simples quando os números são pequenos, pois neste caso podemos listar todos os divisores comuns desses números e escolher o maior deles, que será o seu mdc.

Por exemplo, para calcular mdc(12, 18), determinamos os divisores de 12, que são:

±1, ±2, ±3, ±4, ±6, ±12; e os divisores de 18, que são: ±1, ±2, ±3, ±6, ±9, ±18.

Tomando o maior divisor comum, obtemos: mdc(12, 18) = 6.

No entanto, quando um dos dois números for grande, esse método fica impraticável, pois achar os divisores de um número grande é muito complicado. O que fazer então? Euclides, três séculos antes de Cristo, nos dá uma solução para este

problema descrevendo um algoritmo muito eficiente para fazer este cálculo. O Algoritmo de Euclides, como é conhecido o método por ele desenvolvido, será descrito e generalizado mais na frente, na qual recordamos abaixo:

Um número *d* é divisor comum de *a* e *b*, não ambos nulos, se, e somente se, ele é um divisor comum de *a* e *b* − *a*.

Tomando o máximo divisor comum, obtemos a seguinte identidade: mdc(*a, b*) = mdc(*a, b* − *a*), que permite ir reduzindo sucessivamente o cálculo do mdc de dois números ao cálculo do mdc de números cada vez menores.

Como exemplo de aplicação, vejamos como isto vai permitir o cálculo de mdc(3 264, 1 234):

mdc(3 264, 1 234) = mdc(1 234, 3 264 − 1 234) =
mdc(1 234, 2 030) = mdc(1 234, 2 030 − 1 234) =
mdc(1 234, 796) = mdc(796, 1 234 − 796) =
mdc(796, 438) = mdc(796 − 438, 438) =
mdc(358, 438) = mdc(358, 438 − 358) =
mdc(358, 80) = mdc(358 − 80, 80) =
mdc(278, 80) = mdc(198, 80) =
mdc(118, 80) = mdc(38, 80) =
mdc(38, 42) = mdc(38, 4) =
mdc(34, 4) = mdc(30, 4) =
mdc(26, 4) = mdc(22, 4) =
mdc(18, 4) = mdc(14, 4) =
mdc(10, 4) = mdc(6, 4) = 2.

As contas anteriores serão abreviadas de modo drástico com o algoritmo de Euclides para o cálculo do mdc que iremos apresentar na Seção 3.8.

Proposição 4.2.5. Sejam *a* e *b* dois números com um divisor comum *d*. Então *d* divide $a \times n + b \times m$, quaisquer que sejam os números inteiros *n* e *m*.

Dois números inteiros, não ambos nulos, serão ditos *primos entre si* se não forem múltiplos de um mesmo número diferente de 1 e de −1.

Portanto, dois inteiros *a* e *b*, não ambos nulos, são primos entre si se os únicos divisores comuns de *a* e *b* são 1 e −1, o que equivale a dizer que mdc(*a, b*) = 1.

Exemplos de pares de inteiros primos entre si são: 2 e 3; 4 e 15; 9 e 7. Não são primos entre si os pares: 2 e 4; 3 e 6; 9 e 12.

Dois números primos distintos são sempre primos entre si.

Dois números consecutivos são sempre primos entre si. De fato, podemos escrever os dois números na forma n e $n + 1$, logo

$$\text{mdc}(n,\ n + 1) = \text{mdc}(n,\ n + 1 - n) = \text{mdc}(n,\ 1) = 1.$$

Problema 4.2.6.

(a) Mostre que dois números inteiros da forma n e $2n + 1$ são sempre primos entre si.

(b) Mostre que se n é um número ímpar, então $\text{mdc}(n,\ 2n + 2) = 1$.

(c) Mostre que se n é um número par, então $\text{mdc}(n,\ 2n + 2) = 2$.

Proposição 3.2.7. Sejam a e b dois números naturais não ambos nulos e seja $d = \text{mdc}(a, b)$. Se a' e b' são os dois números naturais tais que $a = a' \times d$ e $b = b' \times d$, então $\text{mdc}(a', b') = 1$.

4.3 Algoritmo da Divisão

Uma das propriedades mais importantes dos números naturais é a possibilidade de dividir um número por outro com resto pequeno. Essa é a chamada divisão euclidiana.

Sejam dados dois números naturais a e b, com $a > 0$ e b qualquer. Queremos comparar o número natural b com os múltiplos do número a. Para isto, considere todos os intervalos da forma $[na,(n + 1)a)$, para n um número natural qualquer. Isto nos dá uma partição de N, ou seja,

$$N = [0, a) \cup [a, 2a) \cup [2a, 3a) \cup \cdots \cup [na,(n + 1)\ a) \cup \cdots$$

e os intervalos acima são dois a dois sem elementos em comum.

Portanto, o número b estará em um e apenas um dos intervalos acima. Digamos que b pertença ao intervalo

$$[qa,(q + 1)a).$$

Logo, existem dois números naturais q e r, unicamente determinados, tais que

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

O número b é chamado dividendo, o número a divisor, os números q e r são chamados, respectivamente, quociente e resto da divisão de b por a.

Note que dados dois números naturais a e b, nem sempre b é múltiplo de a, este será o caso se, e somente se, $r = 0$.

Como determinar os números q e *r* na divisão euclidiana?

Caso $b < a$ Como $b = 0 \times a + b$, temos que $q = 0$ e $r = b$.

Caso $b = a$ Neste caso, tomamos $q = 1$ e $r = 0$.

Caso $b > a$ Podemos considerar a sequência:

$$b - a,\ b - 2a,\ \ldots,\ b - na,$$

até encontrar um número natural q tal que $b - (q + 1)a < 0$, com $b - qa \geq 0$. Assim, obtemos $b = qa + r$, onde $r = b - qa$ e, portanto, $0 \leq r < a$.

Por exemplo, para dividir o número 54 por 13, determinamos os resultados da subtração de 54 pelos múltiplos de 13:

$54 - 13 = 41$,

$54 - 2 \times 13 = 28$,

$54 - 3 \times 13 = 15$,

$54 - 4 \times 13 = 2$

$54 - 5 \times 13 = -11 < 0$.

Assim, a divisão euclidiana de 54 por 13 se expressa como:

$$54 = 4 \times 13 + 2.$$

Problema 4.3.1. Efetue a divisão euclidiana nos seguintes casos:

(a) de 43 por 3

(b) de −43 por 3

Proposição 4.3.2. Mostre o chamado Algoritmo da Divisão Euclidiana nos inteiros:

Dados inteiros a e b, com $a > 0$, existe um único par de inteiros q e r tal que

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

Sugestão: Considere os intervalos da forma $[na,(n + 1) a)$, com n em Z.

Pela proposição 4.3.2, se $a > 0$, os possíveis restos da divisão de um número qualquer por a são os números $0, 1, \ldots, a - 1$.

Por exemplo, os possíveis restos da divisão de um número inteiro por 2 são $r = 0$ *ou* $r = 1$.

Se um dado número quando divido por 2 deixa resto $r = 0$, ele é divisível por 2, ou seja, ele é par.

Se, ao contrário, esse número deixa resto 1 quando dividido por 2, ele é ímpar.

Assim, um número é par se é da forma $2q$ e é ímpar se é da forma $2q + 1$, para algum inteiro q.

Proposição 4.3.3. Dentre dois inteiros consecutivos um deles é par e o outro ímpar.

Proposição 4.3.4. Um número *n* escrito no sistema decimal como $n_r \ldots n_1 n_0$ deixa resto n_0 quando dividido por 10. Como se relacionam os restos da divisão de *n* por 2 ou 5 com os restos da divisão de n_0 por 2 ou 5?

Um número quando dividido por 3 pode deixar restos $r = 0$, $r = 1$ ou $r = 2$.

Proposição 4.3.5. Três inteiros consecutivos um e apenas um deles é múltiplo de 3.

Demonstração: Suponha que os três inteiros consecutivos sejam a, $a + 1$ e $a + 2$. Temos as seguintes possibilidades: a deixa resto 0, 1 ou 2 quando dividido por 3.

1) Suponha que a deixe resto 0 quando dividido por 3, ou seja, $a = 3q$. Logo, $a + 1 = 3q + 1$ e $a + 2 = 3q + 2$. Assim, um e apenas um dos três números é múltiplo de 3, a saber, a.

2) Suponha que a deixe resto 1 quando dividido por 3, ou seja, $a = 3q + 1$. Logo, $a + 1 = 3q + 2$ e $a + 2 = 3q + 3 = 3(q + 1)$. Assim, um e apenas um dos três números é múltiplo de 3, a saber, a + 2.

3) Suponha que a deixe resto 2 quando dividido por 3, ou seja, $a = 3q+2$. Logo, $a+1 = 3q+3 = 3(q+1)$ e $a+2 = 3q+4 = 3(q+1)+1$. Assim, um e apenas um dos três números é múltiplo de 3, a saber, a + 1.

Problema 4.3.6. Mostre que dados três números a, $a + 2$ e $a + 4$, um e apenas um deles é múltiplo de 3. Usando este fato, mostre que a única terna de primos trigêmeos é (3, 5, 7).

Problema 4.3.7. Mostre que dados três números $2a$, $2(a + 1)$ e $2(a + 2)$, um e apenas um deles é múltiplo de 3.

Problema 4.3.7.

(a) Mostre que a soma de três inteiros consecutivos é sempre múltiplo de 3.

(b) Dados três inteiros consecutivos, mostre que um deles é múltiplo de 3 e a soma dos outros dois também.

Dividir por $a > 0$ é agrupar em conjuntos com a elementos. Por exemplo, para saber quantas dúzias de ovos temos no quintal, temos que dividir o número de ovos por 12, a divisão podendo ser exata ou não. Se tivermos 36 ovos, teremos 3 dúzias exatas, mas se tivermos 38 ovos, teremos ainda 3 dúzias de ovos e sobrariam

2 ovos.

Problema 4.3.8. Uma fábrica produz chicletes que são embalados em pacotes de cinco unidades cada. Quantos pacotes serão produzidos com 3 257 unidades?

4.4 Mínimo Múltiplo Comum

Sabemos que todo múltiplo do mmc de dois inteiros é um múltiplo comum desses inteiros. Mostraremos no próximo resultado que vale a recíproca desse fato.

Teorema 4.4.1. *Todo múltiplo comum de dois inteiros a e b é múltiplo de mmc(a,b).*

Demonstração. Seja $m = mmc(a,b)$. Suponha que m' seja um múltiplo comum de a e b. Se $m' = 0$, nada temos a provar, pois 0 é múltiplo de qualquer inteiro, inclusive de m. Suponha que $m' \neq 0$, logo $a \neq 0$ e $b \neq 0$, o que mostra que $m = mmc(a,b) > 0$. Pelo algoritmo da divisão euclidiana, podemos escrever

$$m' = mq + r, \text{ com } 0 \leq r < m.$$

Logo, $r = m' - mq$ e, sendo m' e mq múltiplos comuns de a e b, segue que r é múltiplo de comum de a e b. Mas então $r = 0$, pois caso contrário teríamos um múltiplo comum r de a e b, tal que $0 < r < m$, contradizendo a definição de mmc.

O Teorema acima nos fornece a seguinte relação:

$$a\mathbb{Z} \cap b\mathbb{Z} = mmc(a,b)\mathbb{Z}.$$

Problema 4.4.2. Sendo n um número inteiro qualquer, mostre que o número $n(n + 1)(2n + 1)$ é sempre múltiplo de 6.

Dados três números inteiros a, b e c, não nulos, podemos nos perguntar como calcular o seu mínimo múltiplo comum $mmc(a,b,c)$, ou seja, o menor elemento positivo do conjunto dos múltiplos comuns de a, b e c.

Portanto, queremos determinar o menor elemento positivo do conjunto

$$a\mathbb{Z} \cap b\mathbb{Z} \cap c\mathbb{Z} = (a\mathbb{Z} \cap b\mathbb{Z}) \cap c\mathbb{Z} = mmc(a, b)\,\mathbb{Z} \cap c\mathbb{Z}.$$

Isto nos mostra que

$$mmc(a,b,c) = mmc\,(mmc(a,b),c).$$

Assim, para calcular o mmc de três números recai-se no cálculo de dois mmc de dois números.

Problema 4.4.3. Calcule mmc(4,6,9).

Você deve ter notado que calcular o mmc de dois números é ainda uma

tarefa muito trabalhosa, pois o que aprendemos até o momento foi escrever ordenadamente os múltiplos de cada um dos números até encontrarmos o menor múltiplo comum positivo. Com este método, é praticamente impossível calcular o mmc de dois números quando um deles for bastante grande. Na próxima seção finalizaremos um método muito mais eficiente para se determinar o mmc, baseado no Algoritmo do mdc de Euclides e no teorema a seguir.

Problema 4.4.4. Sejam a, b, d e m quatro inteiros positivos tais que $a \times b = m \times d$. Mostre que m é um múltiplo comum de a e b se, e somente se, d é um divisor comum de a e b.

Teorema 4.4.5. *Sejam a e b dois inteiros positivos. Tem-se a seguinte identidade:*

$$mmc(a,b) \times mdc(a,b) = a \times b.$$

Demonstração. Como a é um múltiplo de $mdc(a,b)$, segue que $a \times b$ é múltiplo de $mdc(a,b)$. Logo, $a \times b = m \times mdc(a,b)$, para algum inteiro positivo m. Temos que m é um múltiplo comum de a e b e, consequentemente, temos que $m = mmc(a,b) \times c$, para algum c positivo. Assim,

$$a \times b = mmc(a,b) \times (c \times mdc(a, b)). \quad (1)$$

Segue que $c \times mdc(a,b)$ é um divisor comum de a e b, logo sendo o mdc o maior dentre esses divisores, segue que

$$c \times mdc(a,b) \leq mdc(a,b). \quad (2)$$

Como $c \geq 1$, temos que

$$mdc(a,b) \leq c \times mdc(a,b),$$

o que juntamente com a desigualdade (2) implica que $c = 1$. Agora, o resultado segue da equação (1).

O mmc de dois números é igual ao seu produto se, e somente se, os dois números são primos entre si.

Proposição 4.4.6. Suponha que n seja um número natural divisível por a e por b. Sabendo que $mdc(a,b) = 1$, então n é divisível por $a \times b$.

4.5 Algoritmo do mdc de Euclides

O Lema de Euclides: *Dados inteiros a e b, os divisores comuns de a e b são os mesmos que os divisores comuns de a e b − c × a, para todo número inteiro c fixado.*

Demonstração. Se d é um divisor comum de a e b, é claro que d é divisor comum de a e de $b - c \times a$.

Reciprocamente, suponha que d seja divisor comum de a e de $b - c \times a$. Logo, d é divisor comum de $b - c \times a$ e de $c \times a$ e, portanto, tem-se que d é divisor de b. Assim, d é divisor comum de a e b.

O Lema de Euclides nos diz que os divisores de comuns de a e b são os mesmos divisores comuns de a e $b - a \times c$, logo tomando o maior divisor comum em ambos os casos, obtemos a fórmula:

$$mdc(a,b) = mdc(a,b - a \times c),$$

o que permite ir diminuindo passo a passo a complexidade do problema, até torná-lo trivial.

Algoritmo de Euclides para o cálculo do mdc

Nada melhor do que um exemplo para entender o método.

Vamos calcular $mdc(a,b)$, onde $a = 162$ e $b = 372$.

Pelo Lema de Euclides, sabemos que o mdc de a e b é o mesmo que o de a e de b menos um múltiplo qualquer de a. Otimizamos os cálculos ao tomarmos o menor dos números da forma b menos um múltiplo de a e isto é realizado pelo algoritmo da divisão:

$$372 = 162 \times 2 + 48.$$

Assim,

$$mdc(372, 162) = mdc(372 - 162 \times 2, 162) = mdc(48, 162).$$

Apliquemos o mesmo argumento ao par $a_1 = 48$ e $b_1 = 162$:

$$162 = 48 \times 3 + 18.$$

Assim,

$$\begin{aligned} mdc(372, 162) &= mdc(162, 48) \\ &= mdc(162 - 48 \times 3, 48) \\ &= mdc(18, 48). \end{aligned}$$

Apliquemos novamente o mesmo argumento ao par $a_2 = 18$ e $b_2 = 48$:

$$48 = 18 \times 2 + 12.$$

Assim,

$$mdc(372, 162) = mdc(48, 18) = mdc(48 - 18 \times 2, 18) = mdc(12, 18).$$

Novamente, o mesmo argumento para o par $a_3 = 18$ e $b_3 = 12$ nos dá:

$$18 = 12 \times 1 + 6.$$

Assim,

$$mdc(372, 162) = mdc(18, 12) = mdc(18 - 12 \times 1, 12) = mdc(6, 12).$$

Finalmente, obtemos

$$mdc(372, 162) = mdc(12, 6) = mdc(12 - 6 \times 2, 6) = mdc(0, 6) = 6.$$

Logo,

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

O procedimento acima pode ser sistematizado como segue:

	2	3	2	1	2
372	162	48	18	12	6=mdc
48	18	12	6	0	

O Algoritmo de Euclides usado de trás para frente nos dá uma informação adicional fundamental.

Das igualdades acima podemos escrever:

$\boxed{6} = 18 - 12 \times 1$

$12 = 48 - 18 \times 2$

$18 = 162 - 48 \times 3$

$48 = 372 - 162 \times 2$

Donde,

$$\begin{aligned}\boxed{6} &= 18 - 12 \times 1 = 18 - (48 - 18 \times 2)\\ &= 18 \times 3 - 48\\ &= (162 - 48 \times 3) \times 3 - 48\\ &= 162 \times 3 - 48 \times 10\\ &= 162 - (372 - 162 \times 2) \times 10\\ &= 162 \times 23 - 372 \times 10.\end{aligned}$$

Assim, podemos escrever:

$$\boxed{6} = mdc(372, 162) = 162 \times 23 + 372 \times (-10).$$

Este método sempre se aplica conduzindo ao seguinte importante resultado:

Teorema 4.5.1. (Relação de Bézout). *Dados inteiros a e b, quaisquer, mas não ambos nulos, existem dois inteiros n e m tais que mdc(a, b) = a × n + b × m.*

4.6 Aplicações da Relação de Bézout

Uma propriedade notável do máximo divisor comum que decorre da Relação de Bézout é a seguinte:

Se d é um divisor comum de dois números a e b, não simultaneamente nulos, então d divide $mdc(a, b)$.

De fato, sendo d um divisor de a e de b, temos que d é um divisor de todo número da forma $a \times n + b \times m$, logo, em particular, de $mdc(a, b)$.

Definindo

$$a\mathbb{Z} + b\mathbb{Z} = \{a \times n + b \times m;\ n, m \in \mathbb{Z}\},$$

temos o seguinte resultado:

Proposição 4.6.1. *Dados dois inteiros a e b, não ambos nulos, o menor elemento positivo do conjunto* $a\mathbb{Z} + b\mathbb{Z}$ *é* $mdc(a, b)$.

Demonstração. De fato, ponhamos $d = mdc(a, b)$. Como $d \mid a$ e $d \mid b$, temos que d divide todo elemento de $aZ + bZ$, logo d é menor ou igual do que qualquer elemento positivo de $a\mathbb{Z} + b\mathbb{Z}$. Pela Relação de Bézout, temos que $d \in a\mathbb{Z} + b\mathbb{Z}$, logo d é o menor elemento positivo do conjunto $a\mathbb{Z} + b\mathbb{Z}$.

Daí decorre um importante critério para que dois números sejam primos entre si.

Proposição 4.6.2. *Dois números inteiros a e b são primos entre si se, e somente se, existem inteiros m e n tais que* $a \times n + b \times m = 1$.

Demonstração. Suponhamos que a e b sejam primos entre si, isto é, $mdc(a, b) = 1$. Como, pela Relação de Bézout, existem inteiros n e m tais que $a \times n + b \times m = mdc(a, b)$, segue que $a \times n + b \times m = 1$.

Reciprocamente, se existem n e m tais que $a \times n + b \times m = 1$, segue que 1 é o menor elemento positivo do conjunto $aZ + bZ$, logo ele é o mdc de a e b. Portanto, a e b são primos entre si.

Proposição 4.6.3. Se a e b dois números naturais não ambos nulos e c um terceiro número natural não nulo, então $mdc(c \times a, c \times b) = c \times mdc(a, b)$.

Proposição 4.6.4. Se a, b e c três números naturais não nulos, então $mmc(c \times a, c \times b) = c \times mmc(a, b)$.

Outra propriedade fundamental que decorre da Relação de Bézout é o resultado a seguir:

Proposição 4.6.5. Sejam a, b e c três inteiros tais que a divide $b \times c$ e a e

b são primos entre si, então a divide c.

Demonstração. Como $a \mid b \times c$, então existe um inteiro e tal que $b \times c = a \times e$. Como a e b são primos entre si, então existem inteiros n e m tais que $a \times n + b \times m = 1$. Multiplicando esta última igualdade por c obtemos

$$a \times n \times c + b \times m \times c = c.$$

Substituindo aí $b \times c$ por $a \times e$, temos que

$$c = a \times n \times c + a \times e \times m = a \times (n \times c + e \times m),$$

mostrando que $a \mid c$.

A série de problemas a seguir nos permitirá deduzir a unicidade referida no Teorema Fundamental da Aritmética.

Proposição 4.6.6. Se a um número inteiro qualquer e p um número primo, então uma das seguintes possibilidades acontece: $p \mid a$ ou $mdc(a, p) = 1$.

Proposição 4.6.7. Sejam a e b dois inteiros e p um número primo. Se $p \mid a \times b$, então $p \mid a$ ou $p \mid b$.

Proposição 4.6.8. Sejam p, p_1 e p_2 três números primos. Se $p \mid p_1 \times p_2$, então $p = p_1$ ou $p = p_2$.

A propriedade acima pode se generalizar como segue:

Se $p, p_1, p_2, \ldots, p_r$ são números primos e se $p \mid p_1 \times p_2 \times \cdots \times p_r$, então para algum índice i tem-se que $p = pi$.

Proposição 4.6.9. Se $p_1, \ldots, p_r$ e $q_1, \ldots, q_s$ são duas coleções de números primos e se

$$p_1 \times \cdots \times p_r = q_1 \times \cdots \times q_s,$$

então $r = s$ e reordenando $q_1, \ldots q_r$, se necessário, tem-se que $p_1 = q_1, \ldots, p_r = q_r$.

Este último problema é a prova da unicidade da escrita como produto de primos de qualquer número natural maior do que 1, contida no enunciado do Teorema Fundamental da Aritmética.

Seja n um número natural escrito na sua decomposição em fatores primos como

$$n = p_1^{a_1} \times \cdots \times p_r^{a_r},$$

e seja n' um divisor positivo de n. Logo na decomposição de n' em fatores primos só podem aparecer os fatores primos $p_1, \ldots, p_r$, com expoentes $b_1, \ldots, b_r$, respectivamente, satisfazendo

$$0 \leq b_1 \leq a_1, \ldots, 0 \leq b_r \leq a_r. \quad (3.3)$$

Note que permitimos que alguns dos b_i sejam nulos, pois o correspondente primo p_i pode não constar da fatoração de n' .

Por exemplo, os divisores positivos de 60 = 22 × 3 × 5 são:

$2^0 \times 3^0 \times 5^0 = 1$, $2^0 \times 3^1 \times 5^0 = 3$, $2^0 \times 3^0 \times 5^1 = 5$,

$2^0 \times 3^1 \times 5^1 = 15$, $2^1 \times 3^0 \times 5^0 = 2$, $2^1 \times 3^1 \times 5^0 = 6$,

$2^1 \times 3^0 \times 5^1 = 10$, $2^1 \times 3^1 \times 5^1 = 30$, $2^2 \times 3^0 \times 5^0 = 4$,

$2^2 \times 3^1 \times 5^0 = 12$, $2^2 \times 3^0 \times 5^1 = 20$, $2^2 \times 3^1 \times 5^1 = 60$.

O número de divisores de é $n = p_1^{a_1} \times \cdots \times p_r^{a_r}$, exatamente o número de números inteiros $b_1, \ldots, b_r$ satisfazendo às desigualdades (3.3), logo esse número é

$$(a_1 + 1) \times \cdots \times (a_r + 1).$$

Problema 4.6.10. Ache os divisores positivos de 40 e de 120. Quais são todos os divisores?

Problema 4.6.11. Quantos divisores positivos tem o número 63 × 25?

É fácil determinar o mdc e o mmc de dois números decompostos em fatores primos. Por exemplo, se

$$a = 2^3 \times 3^5 \times 7^3 \times 17 \text{ e } b = 3^4 \times 7^5 \times 19,$$

temos que mdc(a, b) = $2^0 \times 3^4 \times 7^3$, enquanto

$$mmc(a, b) = 2^3 \times 3^5 \times 7^5 \times 17 \times 19.$$

Os números a e b acima podem ser representados como produtos de potências dos mesmos primos, com o artifício de introduzir fatores extras da forma p^0 (= 1) para certos números primos p. Mais precisamente, podemos escrever

$$a = 2^3 \times 3^5 \times 7^3 \times 17 \times 19^0 \text{ e } b = 2^0 \times 3^4 \times 7^5 \times 17^0 \times 19.$$

$$a = p_1^{a_1} \times \cdots \times p_r^{a_r} \text{ e } b = p_1^{b_1} \times \cdots \times p_r^{b_r}$$

Proposição 4.6.12. Dados dois números decompostos em fatores primos, escritos ambos como produtos de potências dos mesmos primos, onde $a^1 \geq 0, \ldots, a^r \geq 0$ e $b^1 \geq 0, \ldots, b^r \geq 0$,

temos que,

$$\text{mdc}(a, b) = p_1^{c_1} \times \cdots \times p_r^{c_r} \quad \text{e} \quad \text{mmc}(a, b) = p_1^{d_1} \times \cdots \times p_r^{d_r},$$

onde

$$c_i = min\{a_i , b_i\} \text{ e } d_i = max\{a_i , b_i\}, i = 1, \ldots, r.$$

Mostre como obter disto uma nova prova da igualdade

$$mdc(a, b)mmc(c, b) = ab.$$

O leitor não deve se iludir sobre a facilidade em calcular o mdc e o mmc com o método acima, pois para utilizá-lo é necessário que os dois números estejam decompostos em fatores primos. Se os dois números são grandes e não são dados na forma fatorada, é muito trabalhoso fatorá-los para calcular o mdc ou o mmc, sendo, nesse caso, muito mais eficiente o Algoritmo de Euclides.

4.7 Equações Diofantinas Lineares

A resolução de muitos problemas de aritmética e olimpíadas de matemática depende da resolução de equações do tipo $ax + by = c$, onde a, b e c são números inteiros dados e x e y são incógnitas a serem determinadas em Z. Um exemplo típico de um problema modelado por este tipo de equação é o seguinte:

Problema 4.7.1. De quantos modos podemos comprar selos de cinco e de três reais, de modo a gastar cinquenta reais?

Dada uma equação, as perguntas naturais que se colocam são as seguintes:

1) Quais são as condições para que a equação possua solução?

2) Quantas são as soluções?

3) Como calcular as soluções, caso existam?

Daremos a seguir respostas a essas perguntas no caso das equações em questão.

A primeira pergunta admite a resposta a seguir.

Teorema 4.7.1. *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_0, y_0. Então vale a igualdade $ax_0 + by_0 = c$. Como $mdc(a, b)$ divide a e divide b, segue que ele divide $ax_0 + by_0$, logo divide c.

Reciprocamente, suponha que $mdc(a, b)$ divida c, ou seja $c = mdc(a, b) \times d$, para algum inteiro d. Por outro lado, sabemos que existem inteiros n e m tais que

$$mdc(a, b) = a \times n + b \times m.$$

Multiplicando ambos os lados da igualdade acima por d, obtemos

$$c = mdc(a, b) \times d = a \times (n \times d) + b \times (m \times d).$$

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

$$x = n \times d \text{ e } y = m \times d.$$

Problema 4.7.3. Diga quais são as equações diofantinas a seguir que possuem pelo menos uma solução:

(a) 3x + 5y = 223

(b) 5x + 15y = 33

Problema 4.7.4. Mostre que se *a* e *b* são números inteiros tais que *mdc(a, b) = 1*, então toda equação diofantina *ax + by = c* possui solução, independentemente do valor de *c*.

Problema 4.7.5. Para quais valores de *c*, onde *c* é inteiro, a equação *30x + 42y = c* admite soluções inteiras?

Se a equação *ax + by = c* admite uma solução, então o número *d = mdc(a, b)* divide *c* e, portanto, temos que $a = a' \times d$, $b = b' \times d$ e $c = c' \times d$, onde $mdc(a', b') = 1$

Assim, é imediato verificar que x_0, y_0 é uma solução da equação $ax+by = c$ se, e somente se, é solução da equação $a'x+b'y = c'$, onde agora $mdc(a', b') = 1$.

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

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

O próximo resultado nos dará uma fórmula para resolver a equação diofantina linear *ax + by = c*, onde *mdc (a, b) = 1*, conhecida uma solução particular x_0 e y_0 da equação.

Teorema 4.7.6. Seja x_0 e y_0 uma solução particular, arbitrariamente dada, da equação *ax + by = c*, onde *mdc(a, b) = 1*. Então as soluções da equação são da forma $x = x_0 + tb$ e $y = y_0 - ta$, para *t* variando em $\mathbb{Z}$.

Demonstração. Se *x*, *y* é uma solução qualquer da equação, temos que

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

donde

$$a(x - x_0) = b(y_0 - y). \quad (3)$$

Daí segue que $a \mid b(y_0 - y)$ e $b \mid a(x - x_0)$. Como *mdc(a, b) = 1*, segue que $a \mid (y_0 - y)$ e $b \mid (x - x_0)$. Assim,

$$y_0 - y = ta \text{ e } x - x_0 = sb, \quad (4)$$

para alguns inteiros *t* e *s*. Substituindo esse valores em (3), obtemos

$$asb = bta,$$

o que implica que *s = t.* Logo, de (4), temos que a solução é dada por $x = x_0 + tb$ e $y = y_0 - ta$.

Reciprocamente, se $x = x_0 + bt$ e $y = y_0 - at$, substituindo esses valores na equação $ax + by = c$, obtemos

$$a(x_0 + bt) + b(y_0 - at) = ax_0 + by_0 + abt - bat = ax_0 + by_0 = c.$$

Por exemplo, a equação $3x + 5y = 50$ admite a solução particular $x_0 = 0$ e $y_0 = 10$. Assim, a solução geral dessa equação é dada por $x = 0 + 5t$ e $y = 10 - 3t$. Se estivermos à procura de soluções não negativas então deveríamos ter $10 - 3t \geq 0$, o que implica que $t = 0, 1, 2$ ou 3. Assim, o *Problema 3.7.1* admite as seguintes soluções:

(a) 10 selos de 5 reais.

(b) 5 selos de 3 reais e 7 selos de 5 reais.

(c) 10 selos de 3 reais e 4 selos de 5 reais.

(d) 15 selos de 3 reais e um selo de 5 reais.

O único verdadeiro trabalho que se tem para resolver uma equação diofantina linear $ax + by = c$ é calcular $mdc(a, b)$ para verificar se divide ou não c e descobrir uma solução particular x_0, y_0. O primeiro problema se resolve utilizando o algoritmo de Euclides para o cálculo do *mdc*. Quanto ao segundo, o de determinar uma solução particular da equação, procede-se por inspeção se a e b são números pequenos. Caso a ou b seja grande, podemos usar o algoritmo de Euclides de trás para a frente para determinar inteiros n e m tais que

$$an + bm = mdc(a, b) = 1,$$

e depois multiplicar ambos os membros da equação acima por c, obtendo $a(nc) + b(mc) = c$, dando-nos a solução particular $x_0 = nc$ e $y_0 = mc$.

4.8. Problemas

Problema 4.8.1. Mostre que em $\mathbb{Z}$ continua valendo que $(b - a) + a = b$ e que $(a + b) - b = a$.

Problema 4.8.2. Mostre com exemplos que a subtração não é uma operação nem comutativa nem associativa.

Problema 4.8.3. Mostre que em $\mathbb{Z}$ um intervalo $[a, b]$, onde $a \leq b$, tem $b - a + 1$ elementos.

A multiplicação nos inteiros é definida como segue: Se $a, b \geq 0$, sabemos o que é $a \times b$. Definimos

$$(-a) \times b = a \times (-b) = -(a \times b), \text{ e } (-a) \times (-b) = a \times b.$$

Assim, $a \times b$ está definido para quaisquer inteiros a e b. A mul- tiplicação em $\mathbb{Z}$ continua sendo comutativa, associativa e distributiva com relação à adição e à

subtração.

Tem-se também que se $a \times b = 0$, com a e b inteiros, então $a = 0$ ou $b = 0$.

Problema 4.8.4. Mostre que se $a \times c = b \times c$, com $c \neq 0$, então $a = b$.

A multiplicação também continua compatível com a ordem, no seguinte sentido:

Se $a < b$ e $c > 0$, então $c \times a < c \times b$.

Problema 4.8.5. Mostre com um exemplo que em Z não vale a propriedade:

Se $a < b$, então $a \times c < b \times c$, qualquer que seja c.

Nem a sua recíproca:

Se $a \times c < b \times c$, então $a < b$, qualquer que seja c.

Problema 4.8,6. Determine *mdc(a, b), mmc(a, b)* e inteiros n e m tais que $mdc(a, b) = a \times n + b \times m$ para os seguintes pares de números a e b.

(a) $a = 728$ e $b = 1\,496$

Problema 4.8.7. De que maneiras podemos comprar selos de cinco e de sete reais, de modo a gastar cem reais?

Problema 4.8.8. Se um macaco sobe uma escada de dois em dois degraus, sobra um degrau; se ele sobe de três em três degraus, sobram dois degraus. Quantos degraus a escada possui, sabendo que o número de degraus é múltiplo de sete e está compreendido entre 40 e 100.

Problema 4.8.9. Mostre que nenhum número pode deixar resto 5 quando dividido por 12 e resto 4 quando dividido por 15.

Problema 4.8.10. Ache todos os números naturais que quando divididos por 18 deixam resto 4 e quando divididos por 14 deixam resto 6.

Problema 4.8.11 (OCM-1981). Prove que não existem inteiros m e n tais que $m^2 = n^2 + 1954$.

Problema 4.8.12 (OCM-1991).

(a) Se n é um inteiro divisível por 3, mostre que $2^n - 1$ é divisível por 7.

(b) Se n não é divisível por 3, mostre que $2^n - 1$ não é divisível por 7

Problema 4.8.13 (OCM-1997). Seja n um inteiro positivo tal que $3n + 7$ é um quadrado perfeito. Prove que $n + 3$ é a soma de três quadrados perfeitos, com possível repetição.

Problema 4.8.14 (OCM-2003). Mostre que a diferença entre um número racional, suposto distinto de zero e um, e seu inverso, nunca é um número inteiro.

Problema 4.8.15 (OCM-2004). Qual o menor inteiro positivo com o mesmo número de divisores de 2004.

Problema 4.8.16 (OCM-2005). Determinar os inteiros $n > 1$ que são divisíveis por todos os primos menores do que n.

Problema 4.8.17 (OCM-2016). A sequência de Fibonacci (F_1, F_2, F_3, . . .) é definida de seguinte forma: $F_1 = 1$, $F_2 = 1$ e, para $m \geq 3$, $F_m = F_{m-1} + F_{m-2}$. Seja k um inteiro positivo. Mostre que existe um inteiro positivo n tal que o n´umero de Fibonacci F_n é divisível por k.

Problema 4.8.18 (OCM-2017). Um inteiro positivo q é dito um quadrado perfeito quando existe um inteiro positivo k tal que $q = k^2$. Por exemplo, 9 e 64 são quadrados perfeitos, pois $9 = 3^2$ e $64 = 8^2$. Mostre que não existe quadrado perfeito de oito algarismos cujos quatro algarismos de mais alta ordem (os quatro primeiros da esquerda para a direita) são todos iguais a 9.

Problema 4.8.19 (OCM-2019). Tem-se várias peças com o formato de um retângulo 1 × 5 e várias peças com o formato de um quadrado 3×3. Qual o menor inteiro positivo n tal que é possível cobrir totalmente um tabuleiro $n \times n$ utilizando pelo menos uma peça de cada um desses tipos e sem que haja sobreposição de peças? Justifique sua

resposta.

5 A ARITMÉTICA DOS RESTOS

Iremos apresentar conceitos de conguências e suas propriedades, conceitos esses muito importantes para dar base ao leitor da pesquisa além de ser importante para um futuro aprofundamento em Teoria dos Números. No entanto, espera-se que esses conceitos sejam ferramentas úteis para um melhor desenvolvimento nas soluções de problemas de olimpíadas de matemáticos.

5.1 Congruências

Definição 5.1.1. Sejam *a* e *b* dois inteiros quais quer e *m* um número inteiro maior do que 1. Diz-se *a* é congruente a *b* módulo *m, e denota-se* $a \equiv b \bmod m$, *se* $m \mid (a - b)$.

Proposição 5.1.2. *Dados a e b dois inteiros quaisquer e m um inteiro positivo maior do que 1, tem-se que* $a \equiv b \bmod m$ *se, e somente se, a e b deixam o mesmo resto quando divididos por m.*

Demonstração. Pela simplicidade do argumento, inicialmente disponibiliza-se a prova de que se *a* e *b* deixam o mesmo resto quando divididos por *m*, então $a \equiv b \bmod m$. Ora, por hipótese existem q_1, q_2 e r inteiros tais que $a = mq_1 + r$ e $b = mq_2 + r$, com $0 \leq r < m$. Daí, $a - b = m(q_1 - q_2) \therefore m \mid (a - b) \therefore a \equiv b \bmod m$. Agora, suponha que existam inteiros q_1, q_2, r_1 e r_2 tais que $a = mq_1 + r_1$ e $b = mq_2 + r_2$, com $0 \leq r_1, r_2 < m$. Como $m \mid (a - b) = m(q_1 - q_2) + r_1 - r_2$, segue que $m \mid (r_1 - r_2) \therefore m \mid |r_1 - r_2|$. Porém, $0 \leq |r_1 - r_2| < m$, assim a única alternativa é $|r_1 - r_2| = 0 \therefore r_1 = r_2$.

Proposição 5.1.3. *Sejam* a_1, a_2, b_1, b_2 *inteiros quaisquer e seja m um inteiro maior do que 1. são válidos os seguintes resultados:*

(i) $a_1 \equiv a_1 \bmod m$.

(ii) $a_1 \equiv b_1 \bmod m \Rightarrow b_1 \equiv a_1 \bmod m$.

(iii) $a_1 \equiv b_1 \bmod m$ e $b_1 \equiv a_2 \bmod m \Rightarrow a_1 \equiv a_2 \bmod m$.

(iv) $a_1 \equiv b_1 \bmod m$ *e* $a_2 \equiv b_2 \bmod m \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \bmod m$.

(v) $a_1 \equiv b_1 \bmod m$ *e* $a_2 \equiv b_2 \bmod m \Rightarrow a_1 \times a_2 \equiv b_1 \times b_2 \bmod m$.

(vi) $a \equiv b \bmod m \Rightarrow a^n \equiv b^n \bmod m$, $\forall a, b \in N$ *e* $n \in Z_+$.

Demonstração:

(iv) De fato, como $a_1 \equiv b_1 \bmod m$ e $a_2 \equiv b_2 \bmod m$, então *m* divide $b_1 - a_1$ e

divide $b_2 - a_2$. Logo

$$m \text{ divide } (b_1 - a_1) \pm (b_2 - a_2) = (b_1 \pm b_2) - (a_1 \pm a_2),$$

mostrando que $b_1 \pm b_2 \equiv a_1 \pm a_2 \ mod\ m$.

Conclui-se que as congruências de mesmo módulo somam-se e subtraem-se membro a membro tal qual as igualdades.

(v) De fato, como $a_1 \equiv b_1 \ mod\ m$ e $a_2 \equiv b_2 \ mod\ m$, então m divide $a_1 - b_1$ e $a_2 - b_2$. Por outro lado, como

$$a_1 \times a_2 - b_1 \times b_2 = a_1 \times (a_2 - b_2) + b_2 \times (a_1 - b_1),$$

segue que m divide $a_1 \times a_2 - b_1 \times b_2$, o que prova o resultado.

Conclui-se que as congruências de mesmo módulo multiplicam-se membro a membro tal qual as igualdades.

(vi) Vamos ultilizar indução sobre n.

$$a \equiv b \ mod\ m, \text{ então}$$

$$a \cdot a \equiv b \cdot b \ mod\ m \Rightarrow a^2 \equiv b^2 \ mod\ m$$

$$a \cdot a^2 \equiv b \cdot b^2 \ mod\ m \Rightarrow a^3 \equiv b^3 \ mod\ m$$

Se $a^k \equiv b^k \ mod\ m$, por hipótese de indução.

Então, $a^{k+1} = a^k \cdot a \equiv b^k \cdot b = b^{k+1} \ mod\ m$.

Pela definição, as congruências módulo m tem tudo a ver com os restos da divisão por m. Segue-se, da definição de congruência módulo m e das propriedades das proposicões acima, o seguinte fato:

Todo número inteiro a é congruente módulo m a um e somente um dos números 0, 1, . . ., m − 1.

De fato, os possíveis restos da divisão de a por m são precisamente os números $0, 1, \ldots, m - 1,$ cujos restos da divisão por m são eles próprios, logo dois a dois não congruentes módulo m.

Exemplos:

1) $15 \equiv 8 \bmod 7$, pois o restos das divisões de 15 e de 8 por 7 são os mesmos (iguais a 1).

2) $27 \equiv 32 \bmod 5$, pois os restos das divisões de 27 e 32 por 5 são os mesmos (iguais a 2).

3) $31 \not\equiv 29 \bmod 3$, pois o resto da divisão de 31 por 3 é 1, enquanto o resto da divisão de 29 por 3 é 2.

5.2 Critérios de Divisibilidade e Restos

O resto da divisão de um inteiro *n* por 2, pois esse é 0 ou 1, dependendo de *n* ser par ou ímpar.

Para facilitar a determinação do resto da divisão de um inteiro *n* por 3 ou por 9, podemos utilizar os conhecimentos já adquiridos, evitando o trabalho de efetuar a divisão em questão.

De fato, sabemos que se $n_r \ldots n_1 n_0$ é a escrita de *n* no sistema decimal, então

$$n - (n_r + \cdots + n_1 + n_0) = (10^r - 1)n_r + \cdots + (10 - 1)n_1.$$

Como o segundo membro da igualdade acima é divisível por 3 e por 9, o mesmo ocorre com o primeiro membro, logo

$$n \equiv (n_r + \cdots + n_1 + n_0) \bmod 3; \text{ e } \bmod 9.$$

Assim, pela definição de congruência, temos os seguintes fatos:

O resto da divisão por 3 (respectivamente por 9) de um número $n = n_r \ldots n_1 n_0$*, escrito no sistema decimal, é igual ao resto da divisão por 3 (respectivamente por 9) do número* $n_r + \cdots + n_1 + n_0$.

5.3 Problemas

Problema 5.3.1. Verifique se são verdadeiras ou falsas as seguintes afirmações: 3

5 ≡ 27 mod 4; 72 ≡ 32 mod 5; 83 ≡ 72 mod 5; 78 ≡ 33 mod 9.

Problema 5.3.2. Se $a \equiv b \bmod 4$, mostre que $a \equiv b \bmod 2$.

Problema 5.3.3. Mostre que $10^n \equiv 1 \bmod 9$, para todo número natural *n*.

Problema 5.3.4. Sejam *a* um número inteiro qualquer e *m* um inteiro maior do que 1. Suponha que *r* seja um número inteiro tal que $0 \leq r < m$ e $a \equiv r \bmod m$. Mostre que *r* é o resto da divisão de *a* por *m*.

Sugestão: Utilize a unicidade da escrita no Algoritmo da Divisão.

Problema 5.3.5. Determine os restos da divisão por 3 e por 9 dos números: 325 e 548.

Sabemos que todo número *n* é da forma $n = n_0 + 10m$, onde n_0 é o algarismo das unidades de *n*. Assim, $n \equiv n_0 \bmod 5$ e $n \equiv n_0 \bmod 10$. Isto acarreta que:

Os restos da divisão de n por 5 e por 10 são, respectivamente, os restos

da divisão de n_0 por 5 e por 10.

Problema 5.3.6. Determine os restos da divisão por 5 e por 10 dos números: 3 254, 127, 54 827, 33 875 435.

Problema 5.3.7. Descreva critérios semelhantes aos estabelecidos acima para determinar os restos da divisão de um número por 4, 8, 25 e 125.

Problema 5.3.8. Determine os restos da divisão por 4, 8, 25 e 125 dos números: 3 254, 12 736, 54 827, 33 875 435, 57 612 510.

As congruências possuem propriedades operatórias notáveis que exploraremos a seguir.

Problema 5.3.9. Suponha que $a \equiv b \bmod m$. Mostre que

$$a \pm c \equiv b \pm c \bmod m,$$

qualquer que seja o inteiro c.

Problema 5.3.10. Sejam a e b dois números inteiros cujos restos da divisão por 7 são respectivamente 6 e 2. Determine os restos da divisão de $a + b$, $a - b$ e de $b - a$ por 7

Sugestão: Para o último resto, observe que $-4 \equiv 3 \bmod 7$.

Problema 5.3.11. Sem efetuar as somas e subtrações indicadas, determine os restos da divisão por 2, 3, 5, 9, 10 e 25 do número 3 534 785 + 87 538 − 9 535 832.

Problema 5.3.12. Suponha que $a \equiv b \bmod m$. Mostre que

$$a \times c \equiv b \times c \bmod m,$$

qualquer que seja o inteiro c.

Problema 5.3.13. Sejam a e b dois números inteiros cujos restos da divisão por 7 são respectivamente 6 e 2. Determine o resto da divisão de $a \times b$ por 7.

Problema 5.3.14. Sem efetuar as multiplicações indicadas, determine os restos da divisão por 2, 3, 5, 9, 10 e 25 do número $5\,327\,834^3 \times 3\,842\,536^2 \times 9\,369\,270\,001^{20}$.

Note que $2 \times 3 \equiv 2 \times 6 \bmod 6$, mas no entanto $3 \neq 6 \bmod 6$. Portanto, no caso das congruências não vale um cancelamento análogo ao caso da igualdade.

Problema 5.3.15. Sejam a, b, c e m números inteiros e com $m > 1$. Mostre que se $a \times c \equiv b \times c \bmod m$ e se $mdc(c, m) = 1$, então $a \equiv b \bmod m$.

Problema 5.3.16 (OCM-1992). Prove que o número $37^{37} + 83^{83}$ é divisível por 3.

Problema 5.3.17 (OCM-1998). Prove que entre números inteiros quaisquer podemos escolher dois, digamos a e b, tais que $ab^3 - ba^3$ seja divisível por 10.

Problema 5.3.18 (OCM-2001). Se $p > 3$ é primo, prove que o resto da divisão de $p2$ por 12 é igual a 1.

Problema 5.3.19 (OCM-2001). Achar o menor natural n tal que 2001 é a soma dos quadrados de n inteiros ímpares. Justifique sua solução.

Problema 5.3.20 (OCM-2014). Faça os seguintes itens:

(a) Prove que existem $x, y, z \in N$ tais que $13x^4 + 3y^4 - z^4 = 2013$.

(b) Prove que não existem $x, y, z \in N$ tais que $13x^4 + 3y^4 - z^4 = 2014$.

Problema 5.3.21 (OCM-2019). Encontre os três últimos algarismos da representação decimal de 2019^{2019}. Justifique sua resposta.

5.4 Problemas e soluções

Neste tópico apresentaremos 22 problemas que foram apresentados na OCM ao longo dos anos sobre a teoria elementar dos números, também conhecida por aritmética. O nosso intuito é que os mesmos sirvam como banco de questões para consulta e possível aplicação na educação básica, buscando assim promover mudanças no ensino desse importante componente curricular. O critério da seleção dos problemas, levou em consideração as definições e propriedades apresentadas nos capítulos 2, 3 e 4, buscando assim aliar teoria e prática.

Busca-se apresentar as soluções o mais detalhada possível, para tornar acessível o desenvolvimento e a compreensão dos mesmos. Diante do fato de que os problemas selecionados exigem um maior grau de compreensão e abstração para o seu desenvolvimento.

Problema 5.4.1 (OCM-1981). Coloque certo (C) ou errado (E) na proposição abaixo:

01 – ( ) O número fatorial 5! – 1 é primo.

SOLUÇÃO:

O item está CERTO.

$5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$

$5! - 1 = 120 - 1 = 119$

$121 = 11 \cdot 11.$

Ou seja, 5! – 1 é primo.

Problema 5.4.2 (OCM-1981). Prove que não existem inteiros m e n tais que $m^2 = n^2 + 1954$.

SOLUÇÃO:

$$m^2 = n^2 + 1954 \iff m^2 - n^2 = 1954 \iff (m + n)(m - n) = 1954$$

Observe agora que, se m, n tiverem paridade distintas (ou seja, um par e outro ímpar) teremos (m + n) e (m – n) ambos ímpares e seu produto será ímpar, logo não poderá ser 1954.

Por outro lado, se m e n tiverem a mesma paridade (ambos pares ou ambos ímpares), teremos (m + n) e (m – n) pares o que implica que o produto (m + n)(m – n) será múltiplo de 4, e com isto também não poderá ser 1954.

Problema 5.4.3 (OCM-1985).

(a) Mostre que, se n é um inteiro positivo, então $(n – 2)n(n + 1)$ é um múltiplo de 3.

(b) Mostre que, se n é um inteiro positivo, então $n^3 + 3n^2 + 5n + 3$ é divisível por 3.

SOLUÇÃO:

(a) Basta observar que dentre três números consecutivos há sempre um que é múltiplo de três.

(b) Observe que:

$$n^3 + 3n^2 + 5n + 3 = (n – 1)n(n + 1) + 3(n^2 + 2n + 1).$$

Pelo item (a) já sabemos que $3 \mid (n – 1)n(n + 1)$ e também $3 \mid 3(n^2 + 2n + 1)$. Segue portanto o item (b).

Problema 5.4.4 (OCM-1986). Se p e $p + 2$ são números primos estritamente maiores que 3, prove que 6 é um divisor de $p + 1$.

SOLUÇÃO:

Como p é um primo maior que 3, p deve ser ímpar, o que já implica que p + 1 é par. Por outro lado, não podemos ter $p \equiv 0 \pmod 3$, pois p é primo maior que três. Também não podemos ter $p \equiv 1 \pmod 3$, pois nesse caso p + 2 seria divisível por 3. Logo $p \equiv 2 \pmod 3$, de modo que $p + 1 \equiv 0 \pmod 3$. Com isso provamos que p + 1 é múltiplo de 6.

Problema 5.4.5 (OCM-1988). Prove que para qualquer inteiro positivo n, $N = n^2 + 1$ não é divisível por 3.

SOLUÇÃO:

Temos as seguintes possibilidades:

- $n \equiv 0 \pmod 3 \implies n^2 \equiv 0 \pmod 3 \implies n^2 + 1 \equiv 1 \pmod 3$;
- $n \equiv 1 \pmod 3 \implies n^2 \equiv 1 \pmod 3 \implies n^2 + 1 \equiv 2 \pmod 3$;
- $n \equiv 2 \pmod 3 \implies n^2 \equiv 1 \pmod 3 \implies n^2 + 1 \equiv 2 \pmod 3$;

Deste modo, $n^2 + 1$ sempre deixa resto 1 ou 2 quando dividido por 3.

Problema 5.4.6 (OCM-1991).

(a) Se *n* é um inteiro divisível por 3, mostre que $2^n - 1$ é divisível por 7.

(b) Se *n* não é divisível por 3, mostre que $2^n - 1$ não é divisível por 7.

SOLUÇÃO:

Seja $n = 3k + r$, em que $r = 0, 1$ ou 2. Teremos portanto:

$$2^n \equiv 2^{3k} \cdot 2^r \equiv (2^3)^k \cdot 2^r \equiv 8^k \cdot 2^r \equiv 1 \cdot 2^r \equiv 2^r \pmod 7.$$

(a) Se $r = 0$, concluímos que:

$$2^n \equiv 2^0 \equiv 1 \pmod 7 \implies 7 \mid 2^n - 1.$$

(b) Se $r = 1$ ou 2, teremos:

$$2^n \equiv 2^r \equiv 2, 4 \pmod 7,$$

O que nos diz que $2^n - 1$ não é divisível por 7.

Problema 5.4.7 (OCM-1992 – b). Prove que o número $37^{37} + 83^{83}$ é divisível por 3.

SOLUÇÃO:

Usando que $37 \equiv 1 \pmod 3$ e que $83 \equiv -1 \pmod 3$ teremos:

$37^{37} + 83^{83} \equiv 1^{37} + (-1)^{37} \equiv 1 + (-1) \equiv 0 \pmod 3$, ou seja, $37^{37} + 83^{83}$ é divisível por 3.

Problema 5.4.8 (OCM-1994). Se $2^k - 1$ $(k \geq 2)$ é um número primo, prove que *k* também é primo.

SOLUÇÃO:

Suponha que k não seja primo. Logo, $k = pq$ com $p, 1 > 1$.

Usando a factoração:

$$x^q - 1 = (x - 1)(x^{q-1} + x^{q-2} + \cdots + x + 1)$$

aplicada a $x = 2p$ temos:

$$2^{pq} - 1 = (2^p)^q - 1 = (2^p - 1)(2^{p(q-1)} + \cdots + 2^p + 1).$$

Daí o número $2^{pq} - 1$ não seria primo, pois foi escrito como produto de dois fatores claramente maiores que 1. Absurdo

Conclusão: k deve ser primo.

Note que a recíproca deste resultado não é verdadeira. Veja por exemplo que:

$$2^{11} - 1 = 2047 = 23 \cdot 89.$$

Problema 5.4.9 (OCM-1997). Seja *n* um inteiro positivo tal que $3n + 7$ é um quadrado perfeito. Prove que $n + 3$ é a soma de três quadrados perfeitos, com possível repetição.

SOLUÇÃO:

Seja $3n + 7 = x^2$, para algum $x \in \mathbb{N}$. Daí, podemos concluir que x não é múltiplo de 3. Portanto, $x = 3k \pm 1$, que substituído na expressão nos dá:

$$3n + 7 = (3k \pm 1)^2 \Longrightarrow 3(n + 3 - 2 = 9k^2 \pm 6k + 1$$

$$\Longrightarrow \quad 3(n + 3) = 9k^2 \pm 6k + 3 \Longrightarrow n + 3 = 3k^2 \pm 2k + 1$$

$$\Longrightarrow \quad n + 3 = k^2 + k^2 + (k \pm 1)^2,$$

O que encerra nossa demonstração.

Problema 5.4.10 (OCM-1998). Prove que entre números inteiros quaisquer podemos escolher dois, digamos *a* e *b*, tais que $ab^3 - ba^3$ seja divisível por 10.

SOLUÇÃO:

Inicialmente, note que:

$$S = ab^3 - ba^3 = ab(b^2 - a^2) = ab(b + a)(b - a).$$

Assim, se a ou b for par, teremos S par, e se a e b forem ímpares, (b + a) será par e S será par. De qualquer forma, S é sempre par.

Precisamos então em escolher dois dos três números para garantir que S será múltiplo de 5.

I. *Se houver $a \equiv 0 \pmod 5$, basta escolhermos este a para tornar $S \equiv 0 \pmod 5$.*
II. *Se nenhum $a \equiv b \pmod 5$, basta escolhermos este a e b, e teremos $(b - a) \equiv 0 \pmod 5$, o que torna $S \equiv 0 \pmod 5$.*

Se nenhuma destas duas possibilidades ocorre, os números a, b e c serão distintos módulos 5 e congruentes a 1, 2, 3 ou 4. É fácil ver que um dos pares (1, 4) ou (2, 3) vai aparecer, e se o escolhermos, teremos $(b + a) \equiv 0 \pmod 5$, o que torna $S \equiv 0 \pmod 5$.

Problema 5.4.11 (OCM-2001). Se $p > 3$ é primo, prove que o resto da divisão de p^2 por 12 é igual a 1.

SOLUÇÃO:

Como p > 3, temos as seguintes possibilidades para o resto da divisão de p por 12:

$$p \equiv 1, 5, 7, 11 \pmod{12}.$$

Analisando cada uma destas possibilidades temos:

- $p \equiv 1 \pmod{12} \Longrightarrow p^2 \equiv 1^2 \equiv 1 \pmod{12}$.
- $p \equiv 5 \pmod{12} \Longrightarrow p^2 \equiv 5^2 \equiv 1 \pmod{12}$.
- $p \equiv 7 \pmod{12} \Longrightarrow p^2 \equiv 7^2 \equiv 1 \pmod{12}$.
- $p \equiv 11 \pmod{12} \Longrightarrow p^2 \equiv 11^2 \equiv 1 \pmod{12}$.

Em qualquer um dos casos temos $p^2 \equiv 1 \pmod{12}$, ou seja, o resto da divisão de p^2 por 12 é 1.

Problema 5.4.12 (OCM-2001). Achar o menor natural *n* tal que 2001 é a soma dos quadrados de *n* inteiros ímpares. Justifique sua solução.

SOLUÇÃO:

Como 2001 não é um quadrado perfeito, $n \geq 2$. Observe agora que, se x é um número ímpar, temos $x^2 \equiv 1 \pmod{8}$. Portanto, se $2001 = a_1^2 + a_2^2 + \cdots + a_n^2$ com os a_{is}' ímpares teremos:

$$2001 = a_1^2 + a_2^2 + \cdots + a_n^2 \equiv 1 + 1 + \cdots \equiv n \pmod{8}.$$

Daí $n \equiv 2001 \equiv 1 \pmod{8}$, donde concluímos que $n \geq 9$. Para n = 9 podemos montar um exemplo, veja:

$$2001 = 43^2 + 11^2 + 5^2 + 1^2 + 1^2 + 1^2 + 1^2 + 1^2 + 1^2.$$

Problema 5.4.13 (OCM-2003). Mostre que a diferença entre um número racional, suposto distinto e zero e um, e seu inverso, nunca é um número inteiro.

SOLUÇÃO:

Há uma correção a ser feita no enunciado: devemos também excluir o caso x = -1. Seja $x = \frac{p}{q}$ o número racional, onde $p \neq 0$e MDC(p,q) = 1. A diferença a ser analisada é:

$$\mathrm{d} = \frac{p}{q} - \frac{\mathrm{q}}{p} = \frac{p^2 - q^2}{pq}.$$

Suponha que d seja inteiro. Temos portanto:

$$p \mid p^2 - q^2 \implies p \mid q^2,$$

e como mdc(p,q) = 1, devemos ter $p = \pm 1$. De modo análogo prova-se que $q = \pm 1$, o que é uma contradição, pois nesse caso $x = \pm 1$.

Problema 5.4.14 (OCM-2004). Qual o menor inteiro positivo com o mesmo número de divisores de 2004.

SOLUÇÃO:

Fatorando em primos, obtemos $2004 = 2^2 \cdot 3 \cdot 167$. Logo 2004 tem (2 + 1)(1 + 1)(1 + 1) = 12 divisores. Os números que têm 12 divisores podem ter as seguintes factorações em primos:

$$p^{11},\ p^5q,\ p^3q^2,\ p^2qr.$$

Os menores números de cada uma destas formas são os seguintes:

$$2^{11} = 2048;\quad 2^5 \cdot 3 = 96;\quad 2^3 \cdot 3^2 = 72;\quad 2^3 \cdot 3 \cdot 5 = 60.$$

A resposta é portanto 60.

Problema 5.4.15 (OCM-2005). Determinar os inteiros $n > 1$ que são divisíveis por todos os primos menores do que n.

SOLUÇÃO:

Para n = 2 o problema admite solução por vacuidade, ou seja, por não existirem primos menores que n = 2 que não dividam n.

Para n > 2, considere um fator primo p de n – 1. Então, p divide n – 1, de modo que p ≤ n – 1 < n, mas p não divide n, já que n – 1 e n são primos entre si. Logo, o problema não admite solução para n > 2.

Problema 5.4.16 (OCM-2014). Faça os seguintes itens:

(a) Prove que existem $x, y, z \in N$ tais que $13x^4 + 3y^4 - z^4 = 2013$.

(b) Prove que não existem $x, y, z \in N$ tais que $13x^4 + 3y^4 - z^4 = 2014$.

SOLUÇÃO.

(a) Fazendo z = 2x, obtemos $y^4 - x^4 = 671$ ou, ainda, $(y^2 - x^2)(y^2 + x^2) = 11 \cdot 61$. Portanto, $y^2 - x^2 = 11$ e $y^2 + x^2 = 61$, de forma que x = 5, y = 6 e z = 10.

(b) Suponha que haja uma solução. Como $a^4 \equiv 0$ ou $1 (\text{mod. } 8)$, temos $13x^4 + 3y^4 - z^4 \equiv 0, 2, 4, 5$ ou $7 (\text{mod. } 8)$. Mas, como $2014 \equiv 6 (\text{mod. } 8)$, chegamos a uma contradição.

Problema 5.4.17 (OCM-2015). Considere o conjunto

$$B = \{a^2 + 3b^2; a, b \in Z\}.$$

Mostre que se $n \in B$ e p é um fator primo de n tal que $p \in B$, então $\frac{n}{p} \in B$.

SOLUÇÃO.

Suponha que n e p são elementos de B. Sejam $a, b, x, y \in Z$ tais que

$$n = a^2 + 3b^2 \text{ e } p = x^2 + 3y^2 .$$

Temos

$$y^2n - b^2p = (y^2a^2 + 3y^2b^2) - (b^2x^2 + 3b^2y^2) = y^2a^2 - b^2x^2.$$

Portanto,

$$p|(ya - bx)(ya + bx).$$

Trocando b por −b se necessário, podemos assumir que

$$p|(ya - bx).$$

Temos também

$$x^2n - 3b^2p = (a^2x^2 + 3b^2x^2) - (3b^2x^2 + 9b^2y^2) = a^2x^2 - 9b^2y^2.$$

Portanto,

$$p|(ax - 3by)(ax + 3by).$$

Trocando a por −a se necessário, podemos assumir que

$$p|(ax + 3by).$$

Sejam

$$c = \frac{ax+3by}{p} \text{ e } d = \frac{ya-bx}{p}.$$

Uma conta simples nos dá

$$c^2 + 3d^2 = \left(\frac{x^2+3y^2}{p}\right)\left(\frac{a^2+3b^2}{p}\right) = \frac{n}{p}.$$

Portanto, $\frac{n}{p} \in B.$

Problema 5.4.18 (OCM-2016). A sequência de Fibonacci (F_1, F_2, F_3, . . .) é definida de seguinte forma: $F_1 = 1$, $F_2 = 1$ e, para $m \geq 3$, $F_m = F_{m-1} + F_{m-2}$. Seja k um inteiro positivo. Mostre que existe um inteiro positivo n tal que o número de Fibonacci F_n é divisível por k.

Problema 5.4.19 (OCM-2017). Um inteiro positivo q é dito um quadrado perfeito quando existe um inteiro positivo k tal que $q = k^2$. Por exemplo, 9 e 64 são quadrados perfeitos, pois $9 = 3^2$ e $64 = 8^2$. Mostre que não existe quadrado perfeito de oito algarismos cujos quatro algarismos de mais alta ordem (os quatro primeiros da esquerda para a direita) são todos iguais a 9.

Problema 5.4.20 (OCM-2018). Encontre, com justificativa, todos os inteiros positivos *a, b e p*, tais que *p* é primo e

$$\frac{1}{p} = \frac{1}{a^2} + \frac{1}{b^2}.$$

SOLUÇÃO.

Se $\frac{1}{p} = \frac{1}{a^2} + \frac{1}{b^2}$ *, então* $a^2b^2 = (a^2 + b^2)p$ *e, daí, p | a ou | b. Se a = pc (o caso em que p | b pode ser tratado de modo análogo), então* $pc^2b^2 = p^2c^2 + b^2$ *, de modo que p | b. Sendo b = pd, obtemos* $c^2 + d^2 = pc^2d^2$ *ou, ainda,* $p = \frac{1}{c^2} + \frac{1}{d^2}$ *. Mas aí,*

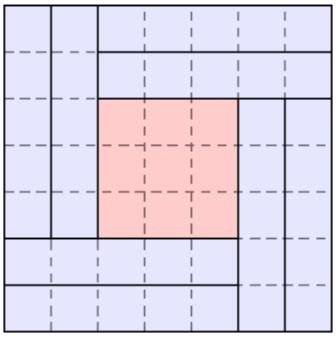
$$2 \leq p = \frac{1}{c^2} + \frac{1}{d^2} \leq \frac{1}{1^2} + \frac{1}{1^2} = 2,$$

o que força termos p = 2 e c = d = 1. Então, a = b = 2.

Problema 5.4.21 (OCM-2019). Tem-se várias peças com o formato de um retângulo 1 × 5 e várias peças com o formato de um quadrado 3×3. Qual o menor inteiro positivo *n* tal que é possível cobrir totalmente um tabuleiro *n*×*n* utilizando pelo menos uma peça de cada um desses tipos e sem que haja sobreposição de peças? Justifique sua resposta.

SOLUÇÃO.

Sendo a e b os números de peças de formato 1 × 5 e 3 × 3, respectivamente, temos $5a + 9b = n^2$. *Agora, é claro que* $5 \times 8 + 9 \times 1 = 7^2$, *e uma configuração com 8 peças 1 × 5 e 1 peça 3 × 3 é mostrada na figura abaixo:*



Por outro lado, como $5a + 9b \geq 14$, *se* $n < 7$ *teremos* $5a + 9b = 16, 25$ *ou* 36. *Mas, claramente* $5a + 9b = 16$ *não tem solução. Também, se* $5a + 9b = 25$, *então* $5 \mid b$, *logo,* $b \geq 5$ *e* $5a + 9b \geq 5 \cdot 1 + 9 \cdot 5 = 50$, *um absurdo. Por fim, se* $5a + 9b = 36$, *então* $9 \mid a$, *de forma que* $a \geq 9$ *e, daí,* $5a + 9b \geq 5 \cdot 9 + 9 \cdot 1 = 54$, *um novo absurdo.*

Problema 5.4.22 (OCM-2019). Encontre os três últimos algarismos da representação decimal de 2019^{2019}. Justifique sua resposta.

SOLUÇÃO

Para $n \geq 2$, *temos* $2019^n \equiv 19^n \pmod{1000}$. *Agora, módulo 1000, temos*

$$19^n = (20 - 1)^n \equiv \binom{n}{n-2} 20^2 (-1)^{n-2} + \binom{n}{n-1} 20(-1)^{n-1} + (-1)^n$$

$$\equiv (-1)^n (200n(n - 1) - 20n + 1).$$

Com $n = 2019$, *temos (módulo 1000)*

$$19^{2019} \equiv -(200 \cdot 2019 \cdot 2018 - 20 \cdot 2019 + 1)$$

$$\equiv -(200 \cdot 19 \cdot 18 - 20 \cdot 19 + 1)$$

$$\equiv -(400 - 380 + 1)$$

$$\equiv -21$$

$$\equiv 979.$$

Portanto, os últimos três algarismos de 2019^{2019} *são 979.*

6 CONCLUSÃO

Pode-se entender que as Olimpíadas de Matemática são uma disputa saudável entre os estudantes da Educação Básica, que utilizam seu lado intelectual, num torneio onde suas ferramentas são disciplina mental, imaginação e criatividade. Os participantes concorrem resolvendo problemas desafiadores. Diante disso, desenvolvem uma atividade intelectual, valoriza o saber e a competência, um avanço cultural. Também gera um processo de competição saudável entre as escolas, eleva a autoestima de alunos, professores e da comunidade escolar em geral.

Deve-se considerar que a OCM, busca incentivar professores a encontrar talentos em matemática, e como consequência a melhoria dos indicadores educacionais. Foi proposta uma sequência didática, por meio de problemas oriundos da OCM, que pode ser trabalhada em sala de aula para complementar os conceitos de aritmética, tradicionalmente vistos no ensino fundamental. Essa sequência didática explora todos os conceitos fundamentais da teoria elementar dos números. Podem ser estudados com um enfoque elementar nos algoritmos que envolvem o cálculo do mmc e do mdc, além da divisibilidade entre dois inteiros, sem necessariamente se ter uma preocupação com as provas e demonstrações dos resultados e teoremas envolvidos.

Também merece destaque no ramo das olimpiadas de matemática as publicações feitas na Coluna Olimpíada de Matemática do Jornal O Povo, na qual, contribuíram fundamentalmente com o ensino da Matemática no Ceará. No período de suas publicações, foi disponibilizado aos leitores conceitos, teoremas, problemas e biografias de grandes matemáticos. A Coluna disponibilizava, também, informativos de olimpíadas nacionais e internacionais.

Merece destacar neste trabalho, um projeto desenvolvido no Estado do Ceará em 2003, em parceria com a Universidade Federal do Ceará, “Projeto Linguagem dos Números – NUMERATIZAR, motivado pelos resultados obtidos nas Olimpíadas de Matemática realizadas nas escolas privadas de Fortaleza, cujos alunos se destacavam em várias Olimpíadas de Matemática. Seus idealizadores o definem como um projeto matemático de inclusão social, caracterizado por um conjunto de 94 atividades que visa encontrar jovens talentos em Matemática em todas as classes sociais. E segundo alguns autores, esse projeto foi o precursor para a criação da OBMEP.

O trabalho que vem sendo realizado no Estado do Ceará, no decorrer dos anos, vem se refletindo aos dias atuais, ou seja, os cearenses tornaram-se referencias na educação Matemática para olimpíadas. As questões olimpicas foram se tornando mais elaboradas, elevando o seu nível e fazendo com que os alunos tenham um “treinamento” mais especifico, com isso, os alunos cearenses também foram ganhando destaques nas principais olimpíadas brasileiras e compondo as equipes para representar o Brasil em olimpíadas internacionais.

Entretanto, vale salientar que a Olimpíada Cearence de Matemática ainda precisa ser realizado um trabalho de divulgação mais abrangente, pois, ela ainda está limitada na capital cearense, não abrange todos os municípios cearenses. O ideal seria expandir a OCM para todo o Estado do Ceará, pois, poderia ser descobertos novos talntos em outros lugares do Estado.

Por fim, esperamos que esse material possa contribuir com os professores e alunos, em particular no ensino médio, e demais interessados, propiciando condições para que obtenham desempenho satisfatório competições olímpicas, assim como, melhoria dos índices educacionais de matemática.

REFERÊNCIAS

ARAÚJO, J. E. **Divisibilidade, congruência e aritmética modular em problemas olímpicos**. 2018. 135f. Dissertação (Mestrado profissional em Matemática) - Universidade Federal de Campina Grande, Campina Grande, 2018.

CARNEIRO, E. A. de S.; CAMPOS, O.; PAIVA, F. A. M. **Olimpíadas Cearenses de Matemática 1981 – 2005:** Nível Médio. Rio de Janeiro: SBM, 2014.

CUNHA, A. L. **Aritmética na OBMEP:** Uma análise de questões da primeira fase do nível 3. 2019. 137f. Dissertação (Mestrado em Matemática) - Universidade Federal Rural de Pernambuco Recife, 2019.

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

HEFEZ, A. **Elementos de Aritmética.** [S.l.: s.n.], 2012. (Série Textos Universitários, Sociedade Brasileira de Matemática.)

HEFEZ, A. **Indução Matemática.** Disponível em: http://www.obmep.org.br. Acesso em: 3 set. 2020.

HEFEZ, A. **Iniciação à Aritmética.** Disponível em: http://www.obmep.org.br. Acesso em: 3 set. 2020.

SILVA, N. U. **Introdução à Teoria dos Números:** Uma Nova Proposta para Educação Básica. 2019. 97f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) – Universidade Federal de Alagoas, Alagoas, 2019.

NOGUEIRA FILHO, C. **A Coluna Olimpíada de Matemática do Jornal O Povo (1987-1996):** entre documentos e narrativas. 2016. 205 f. Tese (Doutorado em Educação) – Programa de Pós-graduação em Educação Brasileira, Universidade Federal do Ceará, Fortaleza, 2016.

OLIMPÍADA BRASILEIRA DE MATEMÁTICA. **Historico.** Disponível em: http://www.obm.org.br/opencms/quem_somos/breve_historico/. Acesso em: 08 maio 2019.

PROJETO cearense tem 133 alunos premiados este ano em olimpíadas. **O Povo Online,** Fortaleza, 07 dez. 2018. Disponível em: https://empregosecarreiras.opovo.com.br/estudantes/projeto-cearense-tem-mais-de-100-alunos-premiados-em-olimpiadas-nacionais-neste-ano/. Acesso em: 10 jun. 2019.

VICTOR, C.A.S. **A Olimpíada de Matemática:** Que preciosidades que envolvem os problemas desta competição e qual o impacto para o professor de matemática sem experiência em olimpíadas e a sua importância para o estudante? 2013. 103 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) – Universidade Federal Rural do Rio de Janeiro, Rio de Janeiro, 2013.