Universidade Federal de Mato Grosso
Instituto de Ciências Exatas e da Terra
Departamento de Matemática

A teoria dos números na perspectiva da OBMEP

Zenilson Alves dos Santos

Mestrado Profissional em Matemática: PROFMAT/SBM

Orientador: **Prof. Dr. Martinho da Costa Araújo**

Trabalho financiado pela Capes

Cuiabá - MT

Setembro de 2020

A teoria dos números na perspectiva da OBMEP

Este exemplar corresponde à redação final da dissertação, devidamente corrigida e defendida por Zenilson Alves dos Santos e aprovada pela comissão julgadora.

Cuiabá, 25 de setembro de 2020.

Prof. Dr. Martinho da Costa Araújo
Orientador

Banca examinadora:

Prof. Dr. Martinho da Costa Araújo - UFMT
Prof. Dr. Almir Cesar Ferreira Cavalcanti - UFMT
Prof. Dr. Jose de Arimateia Fernandes - UFCG

Dissertação apresentada ao curso de Mestrado Profissional em Matemática – PROFMAT, da Universidade Federal de Mato Grosso, como requisito parcial para obtenção do título de **Mestre em Matemática**.

Dados Internacionais de Catalogação na Fonte.

S237t Santos, Zenilson Alves dos.
A teoria dos números na perspectiva da OBMEP / Zenilson Alves dos Santos. -- 2020
xi, 117 f. ; 30 cm.

Orientador: Martinho da Costa Araújo.
Dissertação (mestrado profissional) – Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação Profissional em Matemática, Cuiabá, 2020.
Inclui bibliografia.

1. Resolução de problemas. 2. ensino fundamental. 3. matemática olímpica. I. Título.

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Permitida a reprodução parcial ou total, desde que citada a fonte.

MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL DE MATO GROSSO

PRÓ-REITORIA DE ENSINO DE PÓS-GRADUAÇÃO

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

AV. FERNANDO CORRÊA DA COSTA, 2367 - BOA ESPERANÇA - 78.060-900 - CUIABÁ/MT

FONE: (65) 3615-8576 – E-MAIL: PROFMAT@UFMT.BR

FOLHA DE APROVAÇÃO

Título: **A teoria dos números na perspectiva da OBMEP**

Autor: mestrando **Zenilson Alves dos Santos**

Dissertação defendida e aprovada em **25 de setembro de 2020**.

COMPOSIÇÃO DA BANCA EXAMINADORA

1. **Doutor Martinho da Costa Araujo** (Presidente Banca/Orientador)
Instituição: Universidade Federal de Mato Grosso
2. **Doutor Almir Cesar Ferreira Cavalcanti** (Examinador Interno)
Instituição: Universidade Federal de Mato Grosso
3. **Doutor José de Arimateia Fernandes** (Membro Externo)
Instituição: Universidade Federal de Campina Grande

Cuiabá, **25/09/2020**.

Documento assinado eletronicamente por **MARTINHO DA COSTA ARAUJO**, **Docente da Universidade Federal de Mato Grosso**, em 25/09/2020, às 18:40, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **ALMIR CESAR FERREIRA CAVALCANTI**, **Docente da Universidade Federal de Mato Grosso**, em 25/09/2020, às 19:40, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **José de Arimatéia Fernandes**, **Usuário Externo**, em 29/09/2020, às 09:52, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufmt.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2815264** e o código CRC **FA4145CE**.

Referência: Processo nº 23108.067061/2020-14 SEI nº 2815264

À minha esposa Juliana e meu filho Matheus.

Aos meus pais Estelita e Florisvaldo.

Agradecimentos

Agradeço a Deus, por me dar saúde e forças para vencer as adversidades enfrentadas ao longo de toda minha trajetória profissional e acadêmica.

Aos meus pais Estelita e Florisvaldo, pela educação e valores ensinados.

À minha esposa Juliana Breciani dos Santos e ao meu filho Matheus Breciani dos Santos pelo incentivo, apoio e compreensão no decorrer dessa longa jornada de estudos.

Ao professor Dr. Martinho da Costa Araújo, meu orientador, e também professor no Profmat, que sempre esteve disponível para aconselhar e apontar direções contribuindo para que esse trabalho atingisse a sua conclusão.

Ao professor Dr. Aldi Nestor de Souza pela dedicação e pela disposição em ajudar sempre que solicitado.

À Professora Dra. Thais Silva do Nascimento, pela vontade em contribuir com o nosso crescimento enquanto profissionais da educação.

Aos demais professores que ministraram as aulas no Profmat e que compartilharam seus conhecimentos com dedicação e profissionalismo.

Ao professor Dr. Almir Cesar Ferreira Cavalcanti e o professor Dr. José de Arimateia Fernandes, integrantes da Banca Examinadora, pelas contribuições.

A todos os meus colegas de mestrado pelo companheirismo e contribuições nos momentos de estudo.

Há uma única ciência, a Matemática,
a qual ninguém se pode jactar de
conhecer porque suas conquistas são,
por natureza, infinitas; dela toda gente
fala, sobretudo os que mais a ignoram.

Malba Tahan

Resumo

Este trabalho apresenta uma proposta que possibilita inserir a teoria elementar dos números, nos anos finais do ensino fundamental. Para isso, faz-se necessária a compreensão de alguns conceitos e propriedades dos números inteiros, tais como: divisibilidade, números primos, máximo divisor comum, mínimo múltiplo comum, equações diofantinas, congruências, o pequeno teorema de Fermat e os teoremas de Euler e Wilson. Essa teoria será aplicada na resolução de problemas olímpicos, em particular da OBMEP.

Palavras chave: Resolução de problemas; ensino fundamental; matemática olímpica.

Abstract

This work presents a proposal that makes it possible to insert the elementary number theory in the final years of elementary school. For that, it is necessary to understand some concepts and properties of whole numbers, such as: divisibility, prime numbers, maximum common divisor, minimum common multiple, diophantine equations, congruences, Fermat's small theorem and the theorems of Euler and Wilson. This theory will be applied in the resolution of olympic problems, in particular OBMEP.

Keywords: Problem solving; elementary school; olympic mathematics.

Sumário

Lista de Tabelas

Introdução

> "Platão disse: "Deus é um geômetra". Jacobi mudou isso, "Deus é um aritmético". Então veio Kronecker e formulou a expressão memorável, "Deus criou os números naturais, e todo o resto é criação do homem"
>
> (Felix Klein)

Ao analisarmos o Índice de Desenvolvimento da Educação Básica (IDEB), principal indicador da qualidade da educação básica no Brasil, notamos que o resultado obtido pelos alunos dos anos finais do ensino fundamental das escola públicas, apesar de ter apresentado crescimento nos últimos anos, ainda não atingiu a meta ideal que corresponde ao de países da Organização para a Cooperação e Desenvolvimento Econômico (OCDE). E ainda, ao analisarmos o nível de proficiência em matemática, desse mesmo grupo, verificamos que aproximadamente 50% encontra-se no nível básico e no nível adequado, apenas 15%, conforme resultado do IDEB de 2017.

No entanto, vimos na Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP), uma oportunidade de fazer com que essa proficiência possa melhorar, pois a mesma favorece o ensino de matemática através de resolução de problemas olímpicos, que possuem um grau de dificuldade mais elevado se considerarmos os livros didáticos adotados pelas escolas públicas.

No capítulo 1, apresentaremos os aspectos gerais da OBMEP e a sua influência no ensino de matemática. Faremos ainda, uma análise dos indicadores educacionais do IDEB e a proficiência alcançada pelos alunos do 9° ano do ensino fundamental, tendo como referência, OBMEP (2020b), QEdu (2020a), QEdu (2020c), QEdu (2020b), Pereira (2016) e Cunha (2019).

O capítulo 2 é dedicado às definições e propriedades dos números inteiros, princípio de indução matemática, divisibilidade, divisão euclidiana, sistema de numeração deci-

mal, alguns critérios de divisibilidade, máximo divisor comum, mínimo múltiplo comum e propriedades, algoritmo de Euclides e as equações diofantinas lineares. Tomamos como referência dessa teoria, Hefez (2016), Santos (2011), POTI (2020), Araújo (2018), Domingues (1991) e Araújo (2018).

No capítulo 3, serão apresentadas e desenvolvidas as definições e propriedades dos números primos, o teorema fundamental da aritmética, o teorema de Legendre e o pequeno teorema de Fermat. Todas serão demonstradas e exemplificadas. As referências dessa teoria foram, Hefez (2016), POTI (2020), Domingues (1991) e Araújo (2018).

No capítulo 4, mostraremos as definições e propriedades de congruências, sistemas de resíduos módulo m, congruências lineares, o teorema chinês dos restos, o teorema de Wilson, o pequeno teorema de Fermat e o teorema de Euler. Para o desenvolvimento dessa das mesmas, usamos como referência, Araújo (2018).

Finalmente, no capítulo 5, apresentaremos a aplicação da teoria estudada nos capítulos 2, 3 e 4, que serão empregadas na resolução dos 40 problemas propostos que foram selecionados de competições olímpicas, em particular, das provas anteriores e do Banco de Questões da OBMEP, cujas referências são OBMEP (2020a), OBMEP (2020), Pereira (2016), Cunha (2019), Araújo (2018) e POTI (2020).

Capítulo 1

A Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP)

Neste capítulo, abordaremos alguns aspectos da OBMEP, tais como a sua origem, normas e objetivos. Faremos ainda uma breve análise de sua influência nas escola públicas, e de seus impactos na qualidade de educação. Analisaremos o resultado do IDEB das edições de 2013, 2015 e 2017, o nível de proficiência em matemática alcançado pelos alunos dos anos finais do ensino fundamental e ainda, a importância da resolução de problemas no ensino-aprendizagem de matemática.

1.1 OBMEP: Um breve histórico

A OBMEP é um projeto nacional dirigido às escolas públicas e privadas brasileiras, realizado pelo Instituto de Matemática Pura e Aplicada (IMPA), com o apoio da Sociedade Brasileira de Matemática (SBM), e promovida com recursos do Ministério da Educação (MEC) e do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) (OBMEP, 2020b).

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

- Estimular e promover o estudo da Matemática;

- Contribuir para a melhoria da qualidade da educação básica, possibilitando que um maior número de alunos brasileiros possa ter acesso a material didático de qualidade;
- Identificar jovens talentos e incentivar seu ingresso em universidades, nas áreas científicas e tecnológicas;
- Incentivar o aperfeiçoamento dos professores das escolas públicas, contribuindo para a sua valorização profissional;
- Contribuir para a integração das escolas brasileiras com as universidades públicas, os institutos de pesquisa e com as sociedades científicas;
- Promover a inclusão social por meio da difusão do conhecimento.

Essa competição vem ampliando a cada ano o seu alcance em número de escolas e alunos participantes, parte desse crescimento é devido à integração da OBMEP e OBM[1] a partir de 2017.

Desde a sua primeira edição em 2005 até a edição de 2019, o número de alunos inscritos na primeira fase saltou de 10,5 para 18,1 milhões e o percentual de municípios participantes de 93,5% para 99,7%, cobrindo assim praticamente todo território nacional. (OBMEP, 2020)

As provas são realizadas em 2 (duas) fases que por sua vez são distribuídas em 3 (três) níveis a saber:

- Nível 1: Alunos do $6^{\underline{o}}$ e $7^{\underline{o}}$ ano do ensino fundamental.
- Nível 2: Alunos do $8^{\underline{o}}$ e $9^{\underline{o}}$ ano do ensino fundamental.
- Nível 3: Alunos do ensino médio.

As duas fases são organizadas da seguinte forma:

- A primeira fase consiste em uma prova objetiva, de caráter eliminatório, composta por 20 (vinte) questões de múltipla escolha, valendo 1 (um) ponto cada, totalizando 20 (vinte) pontos, onde cada questão dispõe de 5 (cinco) opções de resposta (A, B, C, D e E), dentre as quais apenas uma delas é a correta. A prova da primeira fase é destinada a todos os alunos participantes, sendo diferenciada de acordo com o nível.

[1] A Olímpiada Brasileira de Matemática (OBM) é uma competição para estudantes dos Ensinos Fundamental (a partir do $6^{\underline{a}}$ ano), médio e Universitário das instituições públicas e privadas de todo o Brasil.

- A segunda fase se caracteriza pela aplicação de prova discursiva, de caráter classificatório, composta de 6 (seis) questões valendo até 20 (vinte) pontos cada, totalizando 120 (cento e vinte) pontos e se destina a todos os alunos participantes classificados, sendo diferenciada de acordo com o nível (OBMEP, 2020b).

1.2 A influência da OBMEP

Os números grandiosos apresentados pela OBMEP, tais como: o número de escolas e alunos participantes, a quase totalidade dos municípios brasileiros abrangidos por essa competição, dentre outros, chamam a atenção. Diante disso:

> Atualmente a OBMEP é uma política pública mundialmente reconhecida, uma das maiores iniciativas governamentais voltadas ao processo de ensino-aprendizagem em matemática, visando melhorar a motivação, o interesse e o desempenho dos alunos nas escolas públicas brasileiras (Maranhão, 2011, p. 2).

Estudos vem demonstrando que a OBMEP, além de influenciar a qualidade da educação pública, pois, de acordo com Soares e Leo (2014), as escolas que apresentam uma boa trajetória de envolvimento contínuo com a OBMEP, impacta de forma significativa a nota dos alunos em matemática na Prova Brasil, no Exame Nacional do Ensino Médio (ENEM) e ainda no Programa Internacional de Avaliação de Estudantes (PISA), ou seja, este impacto é tão maior quanto maior for o tempo de envolvimento da escola com a Olimpíada, indicando assim, a importância do envolvimento contínuo da escola com esta iniciativa. Além disso, segundo Santos e Abreu (2011), proporciona impacto positivo, trazendo benefícios futuros aos estudantes.

1.3 Indicadores educacionais

Faremos uma breve histórico do IDEB que é o principal indicador da qualidade da educação básica no Brasil.

Criado pelo Instituto Nacional de Pesquisa Educacional Anísio Teixeira (INEP) em 2007, o IDEB sintetiza em um único indicador educacional que relaciona de forma positiva informações de rendimento escolar (aprovação) e desempenho (proficiências) em exames padronizados, como a Prova Brasil e o SAEB (Fernandes, 2007, p. 1).

O seu cálculo é feito a partir dos dados sobre aprovação escolar, obtidos no Censo Escolar, e das médias de desempenho no Sistema de Avaliação da Educação Básica (SAEB). A meta para o Brasil é alcançar a média 6 (seis) até 2021, patamar educacional correspondente ao de países da OCDE, como Estados Unidos, Canadá, Inglaterra e Suécia (QEdu, 2020c).

A seguir apresentaremos os dados referentes ao aprendizado de matemática dos alunos concluintes do ensino fundamental. Para tanto tomaremos como referência os dados organizados pelo QEdu [2], que sugere uma classificação obtida a partir de discussões promovidas pelo comitê científico do movimento Todos Pela Educação[3], composto por diversos especialistas em educação, indicaram a partir de qual pontuação pode-se considerar que o aluno demonstrou o domínio da competência avaliada.

Diante do exposto acima, os alunos são distribuídos em 4 níveis em uma escala de proficiência de acordo com o número de pontos obtidos na Prova Brasil (escala SAEB), cuja classificação está descrita na tabela abaixo:

Tabela 1.1: Níveis qualitativos utilizados pelo QEdu - Matemática 9º Ano

Nível	**Pontos**
Avançado	Igual ou maior que 350
Proficiente	300 a 349 pontos
Básico	225 a 299 pontos
Insuficiente	0 a 224 pontos

Fonte: QEdu (2020a), adaptado.

- Avançado: Aprendizado além da expectativa. Recomenda-se para os alunos neste nível atividades desafiadoras.
- Proficiente: Os alunos neste nível encontram-se preparados para continuar os estudos. Recomenda-se atividades de aprofundamento.
- Básico: Os alunos neste nível precisam melhorar. Sugere-se atividades de reforço.
- insuficiente: Os alunos neste nível apresentaram pouquíssimo aprendizado. É necessário a recuperação de conteúdos.

[2]QEdu é um portal que disponibiliza informações sobre a qualidade do aprendizado em cada escola, município e estado do Brasil.

[3]É uma organização sem fins lucrativos composta por diversos setores da sociedade brasileira com o objetivo de assegurar o direito à educação básica de qualidade para todos os cidadãos até 2022, ano que se comemora o bicentenário da independência do Brasil.

A tabela abaixo mostra a distribuição do nível de aprendizagem dos alunos do 9º ano das escolas municipais e estaduais do Brasil, relativos à resolução de problemas de matemática que, de acordo com QEdu (2020b) é considerado adequado quando engloba os níveis avançado e proficiente.

Tabela 1.2: Distribuição dos alunos por nível de proficiência

Nível	**2013**	**2015**	**2017**
Avançado	1%	2%	2%
Proficiente	10%	12%	13%
Básico	52%	55%	54%
Insuficiente	37%	31%	31%

Fonte: (QEdu, 2020b), adaptado.

Considerando que esses dados são relativos ao nível Brasil, pois estamos desconsiderando aqui as variações regionais, podemos notar que o percentual de alunos que se encontram no conhecimento adequado, no qual englobam os níveis proficiente e avançado, vem aumentando gradualmente. Podemos notar esse crescimento ao analisarmos os dados coletados nos anos de 2013, 2015 e 2017 que foram respectivamente 11%, 14% e 15%.

1.4 A OBMEP no contexto educacional

A OBMEP vem contribuindo com mudanças no ensino e aprendizagem de matemática, pois além de propor situações-problemas desafiadoras, apresenta abordagem diferenciada da maioria daquelas encontradas nos livros didáticos tradicionais adotados pelas escolas públicas. Além disso, há ainda incentivos para alunos e professores através de premiações como: medalhas, certificados de menção honrosa e bolsas para participação no PIC[4], cujo objetivo é despertar o interesse pela matemática e como consequência modificar a sua prática no cotidiano das escolas.

O ensino e aprendizagem focado na resolução de problemas vem ao encontro do que se propõe e nessa perspectiva:

[4]Programa de Iniciação Científica da OBMEP

> A situação-problema é o ponto de partida da atividade matemática e não a definição. No processo de ensino e aprendizagem, conceitos, ideias e métodos matemáticos devem ser abordados mediante a exploração de problemas, ou seja, de situações em que os alunos precisem desenvolver algum tipo de estratégia para resolvê-las. Mas para que esse processo atinja os seus objetivos, é fundamental que os professores desse nível de ensino tenham uma boa formação (Brasil – MEC, 1997, p. 40-41).

E ainda:

> O elemento crucial para a transmissão do conhecimento matemático, que é o professor, não esteja recebendo uma formação adequada para exercer sua importante tarefa. Basicamente, o problema mais grave no treinamento do futuro professor é o seguinte: Quando o jovem entra na faculdade, não teve uma boa formação na escola, logo não conhece bem a matemática que vai ensinar (Lima, 2007, p. 156).

A realização da OBMEP tem contribuído de forma significativa para modificar esse cenário, pois, em um de seus objetivos está a busca pela integração das escolas com as universidades públicas, os institutos de pesquisa e as sociedades científicas.

Faz-se necessário despertar o interesse do aluno para a matemática, tornando-a atrativa e mudando alguns paradigmas usados, até hoje, no ensino da mesma. Nesse sentido:

> [...] a Matemática é a única disciplina escolar que é ensinada aproximadamente da mesma maneira e com o mesmo conteúdo para todas as crianças do mundo (D'Ambrosio, 1993, p. 7).

Deve-se então buscar estratégias de ensino adequadas e que favoreçam o ensino-aprendizagem de matemática, diante disso:

> Resolver um problema não se resume em compreender o que foi proposto e em dar respostas aplicando procedimentos adequados. Aprender a dar uma resposta correta, que tenha sentido, pode ser suficiente para que ela seja aceita e até seja convincente, mas não é garantia de apropriação do conhecimento envolvido (Brasil – MEC, 1997, p. 42).

É importante ressaltar a importância de se estudar e aprender Matemática a partir de problemas propostos e daí desenvolver gradualmente os conceitos envolvidos na sua resolução.

Nessa linha, para resolver um problema, Polya (2006) sugere 4 etapas:

- Compreensão do problema;
- Estabelecimento de um plano;
- Execução do plano;
- Retrospecto.

Essas etapas são fundamentais para que o estudante obtenha êxito na resolução de problemas, cabendo ao professor auxiliá-los nessa tarefa, propiciando condições que lhes dê a autonomia necessária.

Capítulo 2

Tópicos da teoria elementar dos números

Neste capítulo serão apresentados alguns tópicos da teoria elementar dos números que serão fundamentais para o desenvolvimento deste trabalho. Serão abordadas algumas definições e propriedades necessárias à compreensão adequada e aprofundada dos temas relativos aos números inteiros, o princípio da boa ordem e indução matemática, a divisão nos inteiros, bem como o estudo da divisibilidade, a divisão Euclidiana, a representação dos inteiros, os critérios de divisibilidade, o algoritmo de Euclides, e estudo do máximo divisor comum e do mínimo múltiplo comum e suas propriedades e as equações diofantinas lineares. Os resultados apresentados nesse capítulo foram consultados em Hefez (2016), Santos (2011), POTI (2020), Domingues (1991) e Araújo (2018).

2.1 Os números inteiros

Apresentaremos as propriedades básicas dos números inteiros que são fundamentais para o desenvolvimento da teoria e também dos problemas propostos.

A notação dos conjuntos aqui apresentadas, serão as mesmas dos livros didáticos utilizados no ensino fundamental e médio, com exceção dos números naturais $\mathbb{N}$ que não utilizaremos o elemento zero na sua composição. E quando o fizermos, indicaremos por $\mathbb{N} \cup 0$. Também não faremos uma construção axiomática dos conjuntos dos números naturais e nem dos números inteiros. As operações de adição e multiplicação, não são definidas formalmente.

Segue então que o conjunto dos números inteiros $\mathbb{Z}$, ou apenas inteiros é dado por

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

Em $\mathbb{Z}$ há um subconjunto muito importante que é o conjunto dos números naturais $\mathbb{N}$, também chamado de inteiros positivos que também representaremos por $\mathbb{Z}_+^*$, onde

$$\mathbb{Z}_+^* = \mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$$

Temos o subconjunto dos inteiros não negativos aqui representados por $\mathbb{N} \cup 0$ ou ainda por $\mathbb{Z}_+$

$$\mathbb{Z}_+ = \mathbb{N} \cup 0 = \{0, 1, 2, 3, 4, 5, \ldots\}$$

Há ainda em $\mathbb{Z}$, os subconjuntos dos inteiros negativos e não positivos que são respectivamente $\mathbb{Z}_-^*$ e $\mathbb{Z}_-$:

$$\mathbb{Z}_-^* = \{-1, -2, -3, -4, -5, \ldots\} \text{ e } \mathbb{Z}_- = \{0, -1, -2, -3, -4, -5, \ldots\}$$

2.2 Operações em $\mathbb{Z}$

2.2.1 Propriedades da adição

a_1.) $(a + b) + c = a + (b + c), \forall\ a, b, c \in \mathbb{Z}$ (associativa)

a_2.) $a + b = b + a,\ \forall\ a, b \in \mathbb{Z}$ (comutativa)

a_3.) $a + 0 = a,\ \forall\ a \in \mathbb{Z}$ (0 é o elemento neutro da adição)

a_4.) Para todo $a \in \mathbb{Z}$, existe $b \in \mathbb{Z}$ de modo que $a + b = 0$. Este elemento b, que é único, chama-se oposto de a e é indicado por $-a$.

Proposição 1. *Para quaisquer $a, b, c \in \mathbb{Z}$, se $a + c = b + c$, então $a = b$ (lei do cancelamento).*

Demonstração: $a + c = b + c \Rightarrow (a + c) + (-c) = (b + c) + (-c) \Rightarrow a + [c + (-c)] = b + [c + (-c)] \Rightarrow a + 0 = b + 0 \Rightarrow a = b$ □

Dados quaisquer $a, b \in \mathbb{Z}$, chama-se diferença entre a e b e indica-se por $a - b$, o seguinte elemento de $\mathbb{Z}$: $a - b = a + (-b)$.

2.2.2 Propriedades da multiplicação

m_1.) $(ab)c = a(bc)$, $\forall\ a, b, c \in \mathbb{Z}$ (associativa)

m_2.) $ab = ba$, $\forall\ a, b \in \mathbb{Z}$ (comutativa)

m_3.) $a \cdot 1 = a$, $\forall\ a \in \mathbb{Z}$ (1 é o elemento neutro da multiplicação)

m_4.) $ab = 0 \Rightarrow a = 0$ ou $b = 0$, (lei do anulamento do produto)

m_5.) $a(b + c) = ab + ac\ \forall\ a, b, c \in \mathbb{Z}$ (a multiplicação é distributiva em relação à adição)

Proposição 2. *Se $a, b, c \in \mathbb{Z}$, então:*

i) $a(b - c) = ab - ac$ *e* $(a - b)c = ac - bc$

ii) $a \cdot 0 = 0$ *logo* $0 \cdot a = 0$

iii) $a(-b) = (-a)b = -(ab)$

iv) $(-a)(-b) = ab$

v) $ab = ac$ *e* $c \neq 0 \Rightarrow b = c$ *(lei do cancelamento da multiplicação).*

Demonstração:

i) Como

$$a(b - c) + ac = a[(b - c) + c] = ab$$

então

$$a(b - c) = ab - ac$$

Como

$$(a - b)c + bc = [(a - b) + b]c = ac$$

então

$$(a - b)c = ac - bc$$

ii) $a \cdot 0 = a \cdot (0 - 0) = a \cdot 0 - a \cdot 0 = 0$

iii) $a(-b) = a[0 + (-b)] = a(0 - b) = a \cdot 0 - (ab) = 0 - (ab) = -(ab)$.Temos ainda que $(-a)b = (0 - a)b = 0 \cdot b - (ab) = 0 - (ab) = -(ab)$.

iv) $(-a)(-b) = -[a(-b)]$, por (iii). Mas, ainda por (iii), $a(-b) = -(ab)$. Logo $(-a)(-b) = -[-(ab)] = ab$.

v) $ab = ac \Rightarrow ab + [-(ac)] = ac + [-(ac)] \Rightarrow ab - ac = 0 \Rightarrow a(b - c) = 0$ $(a \neq 0)$ $\Rightarrow b - c = 0 \Rightarrow b = c$.

□

2.2.3 Relação de ordem em $\mathbb{Z}$

Se $a, b \in \mathbb{Z}$, diz-se que a é menor ou igual a b, e escrevemos $a \leqslant b$; ou, se $b - a \in \mathbb{Z}_+$; ou, se $b - a \in \mathbb{Z}_+^*$, então diz-se que a é menor do que b, ou seja $a < b$.

Enunciaremos a seguir as seis propriedades mais importantes envolvendo as relações $\leqslant$ e $<$ sobre $\mathbb{Z}$. Essas propriedades mostram uma relação de ordem total sobre $\mathbb{Z}$, compatível com a adição e a multiplicação.

$O_1)$ $a \leqslant a$ (reflexiva)

$O_2)$ $a \leqslant b$ e $b \leqslant a \Rightarrow a = b$ (anti-simétrica)

$O_3)$ $a \leqslant b$ e $b \leqslant c \Rightarrow a \leqslant c$ (transitiva)

$O_4)$ $a \leqslant b$ ou $b \leqslant a$

$O_5)$ $a \leqslant b \Rightarrow a + c \leqslant b + c$, $\forall\, c \in \mathbb{Z}$ ($\leqslant$ é compatível coma adição)

$O_6)$ $a \leqslant b$ e $0 \leqslant c \Rightarrow ac \leqslant bc$ ($\leqslant$ é compatível com a multiplicação)

Demonstração:

$O_1)$ $a \leqslant a \Rightarrow a - a \geqslant 0 \Rightarrow a - a = b$ para algum $b \in \mathbb{Z} \Rightarrow 0 = b \Rightarrow a = a + 0$.

$O_2)$ $a \leqslant b$ e $b \leqslant a \Rightarrow \begin{cases} b - a = u \\ a - b = v \end{cases}; u, v \in \mathbb{Z}_+ \Rightarrow \begin{cases} b = a + u \\ a = b + v \end{cases} \Rightarrow a = a + (u + v) \Rightarrow$

$u + v = 0 \Rightarrow u = v = 0$ ou $u = -v$. Portanto, $a = b$.

$O_3)$ $a \leqslant b$ e $b \leqslant c \Rightarrow \begin{cases} b-a=u \\ c-b=v \end{cases}$; $u,v \in \mathbb{Z}_+ \Rightarrow \begin{cases} b=a+u \\ c=b+v \end{cases} \Rightarrow c=a+(u+v) \Rightarrow$ $c-a=u+v$, como $u+v \in \mathbb{Z}_+$ então, $a \leqslant c$.

$O_4)$ $a \leqslant b$ ou $b \leqslant a \Rightarrow \begin{cases} b-a=u \\ a-b=v \end{cases}$; $u,v \in \mathbb{Z}_+ \Rightarrow \begin{cases} a \leqslant b, \text{ ou} \\ b \leqslant a \end{cases}$. Portanto, $a \leqslant b$ ou $b \leqslant a$.

$O_5)$ Se $a \leqslant b \Rightarrow b-a=u, u \in \mathbb{Z}_+ \Rightarrow b=a+u$, adicionando $c \in \mathbb{Z}$ nos dois lados da última igualdade, temos que

$$b+c=(a+c)+u \Rightarrow (b+c)-(a+c)=u \Rightarrow a+c \leqslant b+c, \forall\, c \in \mathbb{Z}$$

$O_6)$ $a \leqslant b \Rightarrow b-a=u, u \in \mathbb{Z}_+ \Rightarrow b=a+u$, multiplicando os dois lados da última igualdade por $c, 0 \leqslant c$, temos que $bc=(a+u)c \Rightarrow bc=ac+uc \Rightarrow bc-ac=uc$, como $uc \in \mathbb{Z}_+$. Portanto $ac \leqslant bc$.

□

As propriedades O_1 a O_4, garantem que $\leqslant$ é uma relação de ordem total sobre $\mathbb{Z}$. Delas decorre a lei da tricotomia em $\mathbb{Z}$.

Lei da tricotomia: Para quaisquer $a, b \in \mathbb{Z}$, apenas uma das situações ocorre:

i) $a=b$

ii) $a>b$, ou

iii) $a<b$

Demonstração: Por (O_4), $a \leqslant b$ ou $a \geqslant b \Rightarrow b-a=u$ ou $a-b=v$; $u,v \in \mathbb{Z}_+ \Rightarrow b=a+u$ ou $a=b+v$. Supondo $a \neq b \Rightarrow u \neq 0$ e $v \neq 0$, ou seja, $a \neq b \Rightarrow a<b$ ou $b<a$. Se ocorressem simultaneamente $a<b$ e $b<a$, então $b-a=r$ e $a-b=s$; $r,s \in \mathbb{Z}_+^* \Rightarrow b=a+r$ e $a=b+s$; $r,s \in \mathbb{Z}_+^* \Rightarrow a=a+(r+s) \Rightarrow r+s=0$ ou $r=-s$. Absurdo. Assim, se $a, b \in \mathbb{Z}$, então $a=b$ ou $a<b$. □

2.2.4 Outras propriedades

1. $a \leqslant b \Leftrightarrow -b \leqslant -a \Leftrightarrow 0 \leqslant b - a$

2. $a < b \Leftrightarrow -b < -a \Leftrightarrow 0 < b - a$

3. $a \leqslant b$ e $c \leqslant d \Rightarrow a + c \leqslant b + d$

4. $a \leqslant b$ e $c < d \Rightarrow a + c < b + d$

5. Regras de sinais:

i) $a > 0$ e $b > 0 \Rightarrow ab > 0$;

ii) $a < 0$ e $b < 0 \Rightarrow ab > 0$;

iii) $a < 0$ e $b > 0 \Rightarrow ab < 0$;

6. $a^2 \geqslant 0$ para todo $a \in \mathbb{Z}$ e $a^2 > 0$ sempre que $a \neq 0$.

7. $a < b$ e $c > 0 \Rightarrow ac < bc$.

8. $a < b$ e $c < 0 \Rightarrow ac > bc$.

9. $ac \leqslant bc$ e $c > 0 \Rightarrow a \leqslant b$.

10. $ac \leqslant bc$ e $c < 0 \Leftrightarrow a \geqslant b$.

Demonstração:

1. $a \leqslant b \Leftrightarrow -b \leqslant -a \Leftrightarrow 0 \leqslant b - a$.

i) $a \leqslant b \Leftrightarrow -b \leqslant -a$

$(\Rightarrow) a \leqslant b \Rightarrow b - a = u, u \in \mathbb{Z}_+ \Rightarrow b = a + u \Rightarrow -b = -(a + u) \Rightarrow -b = -a - u \Rightarrow$
$-b + a = -u \Rightarrow -b \leqslant -a.$

$(\Leftarrow) - b \leqslant -a \Rightarrow -a - (-b) = v, v \in \mathbb{Z}_+ \Rightarrow b - a = v \Rightarrow a \leqslant b.$

ii) $-b \leqslant -a \Leftrightarrow 0 \leqslant b - a$

$(\Rightarrow) - b \leqslant -a \Rightarrow -a - (-b) = r, r \in \mathbb{Z}_+ \Rightarrow -a + b = r \Rightarrow 0 \leqslant b - a.$

$(\Leftarrow) 0 \leqslant b - a \Rightarrow b - a = s, s \in \mathbb{Z}_+ \Rightarrow -b < -a.$

2. $a < b \Leftrightarrow -b < -a \Leftrightarrow 0 < b - a$

i) $a < b \Leftrightarrow -b < -a$

$(\Rightarrow) a < b \Rightarrow b - a = u, u \in \mathbb{Z}_+^* \Rightarrow b = a + u \Rightarrow -b = -(a + u) \Rightarrow -b = -a - u \Rightarrow$
$-b + a = -u \Rightarrow -b < -a.$

$(\Leftarrow) - b < -a \Rightarrow -a - (-b) = v, v \in \mathbb{Z}_+^* \Rightarrow -a + b = v \Rightarrow a < b.$

ii) $-b < -a \Leftrightarrow 0 < b - a$

$(\Rightarrow) - b < -a \Rightarrow -a - (-b) = r,\ r \in \mathbb{Z}_+^* \Rightarrow -a + b = r \Rightarrow 0 \leqslant b - a.$

$(\Leftarrow) 0 < b - a \Rightarrow b - a = s, s \in \mathbb{Z}_+^* \Rightarrow -b < -a.$

3. $a \leqslant b$ e $c \leqslant d \Rightarrow b - a = u$ e $d - c = v;\ u, v \in \mathbb{Z}_+ \Rightarrow b = a + u$ e $d = c + v \Rightarrow b + d =$ $(a + c) + (u + v) \Rightarrow (b + d) - (a + c) = u + v,$ como $u + v \in \mathbb{Z}_+ \Rightarrow a + c \leqslant b + d$

4. $a \leqslant b$ e $c < d \Rightarrow b - a = u$ e $d - c = v;\ u \in \mathbb{Z}_+, v \in \mathbb{Z}_+^* \Rightarrow b = a + u$ e $d = c + v \Rightarrow$ $b + d = (a + c) + (u + v) \Rightarrow (b + d) - (a + c) = u + v,$ como $u + v \in \mathbb{Z}_+^* \Rightarrow a + c < b + d$

5. Regra de sinais

i) Se $a > 0$ e $b > 0 \Rightarrow a, b \in \mathbb{Z}_+^*$; então $ab \in \mathbb{Z}_+^*$, logo $ab > 0$.

ii) De $a < 0$ e $b < 0$, temos que $0 < -a$ e $0 < -b$; então, por (i), $0 < (-a)(-b)$. Mas $(-a)(-b) = ab$. Logo $0 < ab$.

iii) De $a < 0$ e $b > 0$, temos que $0 < -a$ e $0 < b$; então, por (i), $0 < (-a)(b)$. Mas $(-a)(b) = -(ab)$. Logo $ab < 0$.

6. Se $a > 0$ ou $a < 0$, então a regra de sinais garante que $a^2 = a \cdot a > 0$; e, se $a = 0$, então $a^2 = 0$.

7. Se $a < b \Rightarrow b - a = u, u \in \mathbb{Z}_+^* \Rightarrow b = a + u \Rightarrow bc = (a + u)c = ac + uc \Rightarrow bc - ac = uc,$ como $c > 0$, então $ac < bc$.

8. Se $a < b \Rightarrow b - a = u, u \in \mathbb{Z}_+^* \Rightarrow b = a + u \Rightarrow bc = (a + u)c = ac + uc \Rightarrow bc - ac = uc,$ como $c < 0$, então $ac > bc$.

9. $ac \leqslant bc \Rightarrow bc - ac = u, u \in \mathbb{Z}_+ \Rightarrow c(b - a) = u,$ como $c > 0 \Rightarrow a \leqslant b.$

10. $ac \leqslant bc \Rightarrow bc - ac = u, u \in \mathbb{Z}_+ \Rightarrow c(b - a) = u,$ como $c < 0 \Rightarrow a \geqslant b.$

□

Definição 1. *Seja S um subconjunto não vazio de $\mathbb{Z}$. Todo elemento $k \in \mathbb{Z}$ tal que $k \leqslant x$, para todo $x \in S$, chama-se limite inferior de S. Um limite inferior de S que pertença a S chama-se menor elemento de S.*

2.2.5 Princípio da boa ordenação

Enunciaremos agora a propriedade chamada de princípio da boa ordenação.

Princípio da boa ordenação: Seja $S \neq \varnothing$ um subconjunto de $\mathbb{Z}$. Se S admite algum limite inferior em $\mathbb{Z}$, então S possui mínimo.

2.2.6 Princípio de indução matemática

O princípio de indução matemática é uma consequência imediata do princípio da boa ordenação.

Teorema 3. *(Primeiro princípio de indução) Seja a um número inteiro e suponhamos que a cada $n \geqslant a$ esteja associada uma afirmação $P(n)$. Suponha ainda que seja possível provar o seguinte:*

i) $P(a)$ é verdadeira.

ii) Para todo $r \geqslant a$, se $P(r)$ é verdadeira, então $P(r+1)$ também é verdadeira.

Nessas condições $P(n)$ é verdadeira para todo $n \geqslant a$

Demonstração: Seja $L = \{x \in \mathbb{Z};\ x \geqslant a$ e $P(x)$ é falsa$\}$. Basta provar então que $L = \varnothing$. Suponhamos que $L \neq \varnothing$ e seja $m = min\ L$. Logo $P(m)$ é falsa e como, por hipótese, $P(a)$ é verdadeira, então $m > a$. Desta última relação segue que $m > 0$; portanto $m = 1 + u$ para algum $u \in \mathbb{Z}$, e daí $u < m$.

Mas $m > a$ implica que $m \geqslant a + 1$. Assim $m = 1 + u \geqslant a + 1$, logo $u \geqslant a$.

Se $m > u \geqslant a$, $P(u)$ é verdadeira (se fosse falsa, u estaria em L, o que não é possível pois $u < m = min\ L$). Então, devido a (ii), $P(u+1) = P(m)$ é verdadeira. Absurdo. □

A afirmação $P(r)$ em (ii), é chamada de hipótese de indução.

Teorema 4. *(Segundo princípio de indução) Seja $P(n)$ uma afirmação associada a todo n maior que ou igual a um certo $a \in \mathbb{Z}$. Suponhamos que seja possível provar as duas condições a seguir:*

i) $P(a)$ *é verdadeira.*

ii) Para todo $r > a$, se $P(k)$ é verdadeira sempre que $a \leqslant k < r$ então $P(r)$ também é verdadeira.

Então $P(n)$ é verdadeira para qualquer $n \geqslant a$.

Demonstração: Seja $S = \{m \in \mathbb{Z};\ m \geqslant a$ e $P(m)$ é falsa$\}$. Devemos provar que $S = \varnothing$. Suponha que se pudesse ter $S \neq \varnothing$ e seja, segundo princípio da boa ordenação, $m_0 = min(S)$. Como $P(a)$ é verdadeira, devido à hipótese (i), então $m_0 > a$. Logo, para todo $k \in \mathbb{Z}$, $a \leqslant k < m_0$, $P(k)$ é verdadeira (pois m_0 é o mínimo dos $m \geqslant a$ para os quais $P(m)$ é falsa). Logo, pela hipótese (ii), $P(m_0)$ também é verdadeira, o que é absurdo.

Assim, $S = \varnothing$ e $P(m)$ é verdadeira para todo $m \geqslant a$. □

Exemplo 1. *Mostre que a fórmula $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ é verdadeira para todo $n \in \mathbb{N}$. Mostraremos pelo princípio da indução que a igualdade é verdadeira.*
Seja $P(n) : 1 + 3 + 5 + \cdots + (2n - 1) = n^2$.
Temos que: $P(1)$ é verdadeira, pois $1 = 1^2$.
Devemos mostrar que $P(n) \Rightarrow P(n + 1)$ é verdadeiro para todo $n \in \mathbb{N}$.
Somando $2n + 1$ nos dois lado de $P(n)$, temos

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$
$$1 + 3 + 5 + \cdots + (2n - 1) + (2n + 1) = n^2 + (2n + 1)$$
$$1 + 3 + 5 + \cdots + (2n - 1) + (2n + 1) = (n + 1)^2,$$

Com isso $P(n + 1)$ é verdadeiro.
Pelo princípio de indução matemática, $P(n)$ é verdadeiro para todo $n \in \mathbb{N}$.

2.2.7 Módulo ou valor absoluto de inteiros

Definição 2. *Seja* $a \in \mathbb{Z}$*, definimos:* $\begin{cases} |a| = a, & \text{se } a \geqslant 0 \\ |a| = -a, & \text{se } a < 0 \end{cases}$

Chamamos $|a|$ *de módulo ou valor absoluto de* a*.*

Proposição 5. *Se* a *e* b *são elementos quaisquer de* $\mathbb{Z}$*, então:*

i) $|a| = |-a|$

ii) $-|a| \leqslant a \leqslant |a|$

iii) $|ab| = |a||b|$

iv) $|a+b| \leqslant |a| + |b|$

Demonstração: Quando $a = 0$ ou $b = 0$, as afirmações são imediatas. Suponha que $a \neq 0$ e $b \neq 0$, temos que

i) Se $a > 0$, então $-a < 0$ e daí $|a| = a$ e $|-a| = -(-a) = a$. Se $a < 0$, então $|a| = -a$ e $|-a| = -a$, pois $-a > 0$.

ii) Suponhamos $a > 0$ e portanto $-a < 0$; daí $-a < a$; como neste caso $-|a| = -a$ e $|a| = a$, então $-|a| = -a < a = |a|$. Para o caso $a < 0$, o procedimento é análogo.

iii) Se $a > 0$ e $b > 0$, então $ab > 0$ e portanto $|ab| = ab = |a||b|$. Se $a < 0$ e $b > 0$, então $|a| = -a$, $|b| = b$ e $|ab| = -(ab)$ pois $ab < 0$; como $|a||b| = (-a)b = -(ab)$, então $|ab| = |a||b|$. Se $a < 0$ e $b < 0$, então $ab > 0$ e portanto $|ab| = ab$, $|a| = -a$ e $|b| = -b$; e posto que $|a||b| = (-a)(-b) = ab$, então $|ab| = |a||b|$.

iv) Devido a (ii) valem

$$-|a| \leqslant a \leqslant |a|$$

$$-|b| \leqslant b \leqslant |b|$$

Somando membro a membro essas desigualdades:

$$-(|a| + |b|) \leqslant a + b \leqslant |a| + |b|$$

Se $|a+b| = a+b$, como $a+b \leqslant |a|+|b|$, então $|a+b| \leqslant |a|+|b|$. E se $|a+b| = -(a+b)$, então $-|a+b| = a+b$; como $-(|a|+|b|) \leqslant a+b$, então $-(|a|+|b|) \leqslant -|a+b|$ logo $|a+b| \leqslant |a|+|b|$.

□

2.3 Divisão nos inteiros

Nessa seção, iremos explorar as propriedades da divisão entre dois números inteiros.

Ao efetuarmos a divisão de um número inteiro por outro, ocorrem duas possibilidades: ocorre a divisibilidade ou quando isso não acontece, é possível efetuar essa divisão, porém, com um resto. Tal divisão é chamada de divisão euclidiana.

2.3.1 Divisibilidade

Definição 3. *Dados dois números inteiros a e b, diremos que a divide b, escrevendo $a \mid b$, quando existir um número inteiro c tal que $b = ca$. Nesse caso, diremos também que a é um divisor ou um fator de b ou , ainda, que b é um múltiplo de a ou que b é divisível por a.*

Observe que $a \mid b$ não representa nenhuma operação em $\mathbb{Z}$, nem representa uma fração. Trata-se de uma sentença que diz ser verdade que existe c inteiro tal que $b = ca$. A negação dessa sentença é representada por $a \nmid b$, significando que não existe nenhum número inteiro c tal que $b = ca$.

Exemplo 2. *Pela definição, temos que:*

- $5 \mid 15$, *pois* $15 = 3 \cdot 5$;
- $-2 \mid 6$, *pois* $6 = (-3) \cdot (-2)$;
- $7 \nmid 12$, *pois não existe* $c \in Z$ *tal que* $12 = 7c$.

A divisibilidade possui algumas propriedades que serão utilizadas na resolução de problemas.

Proposição 6. *Sejam $a, b, c \in \mathbb{Z}$. Tem-se que:*

i) $1 \mid a$, $a \mid a$ *e* $a \mid 0$.

ii) $0 \mid a \Leftrightarrow a = 0$.

iii) a *divide* b *se, e somente se,* $|a|$ *divide* $|b|$

iv) se $a \mid b$ *e* $b \mid c$, *então* $a \mid c$.

Demonstração:

i) isto decorre das igualdades $a = a \cdot 1$, $a = 1 \cdot a$, $0 = 0 \cdot a$.

Note também que (i) inclui o caso $0 \mid 0$ e, portanto, todo número inteiro divide 0. Assim, 0 tem infinitos divisores.

ii) Suponhamos que $0 \mid a$; logo existe $c \in \mathbb{Z}$ tal que $a = c \cdot 0$. Pela proposição 2 $(ii.)$, conclui-se que $a = 0$.
Para a recíproca, se $a = 0 \Rightarrow 0 = c \cdot 0 \Rightarrow 0 \mid 0$.

iv) $a \mid b$ e $b \mid c$ implica que existem $f, g \in \mathbb{Z}$, tais que $b = fa$ e $c = gb$. Substituindo o valor de b da primeira equação na outra, obtemos

$$c = gb = g(fa) = (gf)a$$

o que nos mostra que $a \mid c$.

□

Dos itens (i) e (ii) obtemos que todo número inteiro a é divisível por ± 1 e por $\pm a$.

Suponha que $a \mid b$ e que $a \neq 0$. Seja $c \in \mathbb{Z}$ tal que $b = ca$. O número inteiro c, univocamente determinado, é chamado de quociente de b por a e denotado por $c = \dfrac{b}{a}$.

Exemplo 3. $\dfrac{7}{1} = 7$, $\dfrac{10}{2} = 5$, $\dfrac{3}{3} = 1$.

Proposição 7. *Se* $a, b, c, d \in \mathbb{Z}$, *então*

$$a \mid b \ \ e \ \ c \mid d \Rightarrow ac \mid bd.$$

Demonstração: Se $a \mid b$ e $c \mid d$, então existem $f, g \in \mathbb{Z}$, $b = fa$ e $d = gc$.
Portanto, $bd = (fg)(ac)$, logo, $ac \mid bd$. □

Em particular, se $a \mid b$, então $ac \mid bc$, para todo $c \in \mathbb{Z}$.

Proposição 8. *Sejam $a, b, c \in \mathbb{Z}$, tais que $a \mid (b \pm c)$. Então*

$$a \mid b \Leftrightarrow a \mid c.$$

Demonstração: Suponhamos que $a \mid (b + c)$. Logo, existe $f \in \mathbb{Z}$ tal que $b + c = fa$.
Agora, se $a \mid b$, temos que existe $g \in \mathbb{Z}$ tal que $b = ga$. Juntando as duas igualdades acima, temos

$$ga + c = fa$$

então $c = (f - g)a$, logo $a \mid c$.
A prova contrária é totalmente análoga.
Por outro lado, se $a \mid (b - c)$ e $a \mid b$, pelo caso anterior, temos $a \mid -c$, o que implica que $a \mid c$. □

Proposição 9. *Se $a, b, c \in \mathbb{Z}$, são tais que $a \mid b$ e $a \mid c$. Então para todo $x, y \in \mathbb{Z}$*

$$a \mid (xb + yc).$$

Demonstração: *$a \mid b$ e $a \mid c$, implicam que existem $f, g \in \mathbb{Z}$ tais que $b = fa$ e $c = ga$. Logo,*

$$xb + yc = x(fa) + y(ga) = (xf + yg)a,$$

o que prova o resultado. □

Proposição 10. *Dados $a, b \in \mathbb{Z}$, onde $b \neq 0$, temos que*

$$a \mid b \Rightarrow |a| \leqslant |b|$$

Demonstração: De fato, se $a \mid b$, existe $c \in \mathbb{Z}$, tal que $b = ca$. Tomando módulos, temos que $|a| \leq |c|\,|a|$. Como $b \neq 0$, temos que $c \neq 0$, logo $1 \leqslant |c|$ e, consequentemente,

$|a| \leqslant |a|\,|c| = |b|$. □

Em particular, se $a \in \mathbb{Z}$ e $a \mid 1$, então $0 < |a| \leqslant 1$, logo $|a| = 1$ e, portanto, $a \pm 1$. Como, para $b \neq 0$, temos que todo divisor de a e b é tal que $|a| \leqslant |b|$, segue-se, nesse caso, que b tem um número finito de divisores que estão no intervalo $-|b| \leqslant a \leqslant |b|$.

Proposição 11. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Tem-se que $a - b$ divide $a^n - b^n$.*

Demonstração: Por indução sobre n, tem-se:
A afirmação é verdadeira para $n = 1$, pois $a - b$ divide $a^1 - b^1 = a - b$.
Suponhamos que a afirmação $a - b \mid a^n - b^n$ seja verdadeira para algum $n \in \mathbb{N}$.
Escrevemos

$$\begin{aligned} a^{n+1} - b^{n+1} &= aa^n - ba^n + ba^n - bb^n \\ &= (a-b)a^n + b(a^n - b^n) \end{aligned}$$

Como $a - b \mid a - b$ e, pela hipótese de indução, $a - b \mid a^n - b^n$, segue da igualdade acima e da proposição 9, que $a - b \mid a^{n+1} - b^{n+1}$.
Logo, $a - b$ divide $a^n - b^n$ para todo $n \in \mathbb{N}$. □

Proposição 12. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N} \cup \{0\}$. Temos que $a + b$ divide $a^{2n+1} + b^{2n+1}$.*

Demonstração: Por indução sobre n, temos que:
A afirmação é verdadeira para $n = 0$, pois $a + b$ divide $a^1 + b^1 = a + b$. Suponhamos que a afirmação $a + b \mid a^{2n+1} + b^{2n+1}$ seja verdadeira.
Escrevemos

$$\begin{aligned} a^{2(n+1)+1} + b^{2(n+1)+1} &= a^2a^{2n+1} - b^2a^{2n+1} + b^2a^{2n+1} + b^2b^{2n+1} \\ &= (a^2 - b^2)a^{2n+1} + b^2(a^{2n+1} + b^{2n+1}) \end{aligned}$$

Como $a+b$ divide $a^2-b^2 = (a+b)(a-b)$ e, pela hipótese de indução, $a+b \mid a^{2n+1}+b^{2n+1}$, segue da igualdade acima e da proposição 9, que $a + b \mid a^{2(n+1)+1} + b^{2(n+1)+1}$. Logo, a afirmação é verdadeira para todo $n \in \mathbb{N}$. □

Proposição 13. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a+b$ divide $a^{2n} - b^{2n}$.*

Demonstração: Por indução sobre n, temos que:

A afirmação é verdadeira para $n = 1$, pois $a + b$ divide $a^2 - b^2 = (a + b)(a - b)$.

Suponhamos que a afirmação $a + b \mid a^{2n} - b^{2n}$ seja verdadeira para algum $n \in \mathbb{N}$. Escrevemos

$$\begin{aligned} a^{2(n+1)} - b^{2(n+1)} &= a^2a^{2n} - b^2a^{2n} + b^2a^{2n} - b^2b^{2n} \\ &= (a^2 - b^2)a^{2n} + b^2(a^{2n} - b^{2n}) \end{aligned}$$

Como $a+b$ divide $a^2-b^2 = (a+b)(a-b)$ e, pela hipótese de indução, $a+b \mid a^{2n}-b^{2n}$, segue da igualdade acima e da proposição 9 que $a + b \mid a^{2(n+1)} + b^{2(n+1)}$.

Logo, a afirmação é verdadeira para todo $n \in \mathbb{N}$. □

2.3.2 Divisão euclidiana

Teorema 14. *(Divisão euclidiana) Sejam a e b dois números inteiros com $b \neq 0$. Existem dois únicos inteiros q e r tais que*

$$a = bq + r, \text{ com } 0 \leq r < |b|$$

Demonstração: Considere o conjunto

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

Existência: Pela propriedade arquimediana, existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$, logo, $a - nb > 0$, o que mostra que S é não vazio. O conjunto S é limitado inferiormente por 0, logo, pelo princípio da boa ordenação, temos que S possui um menor elemento r.
Suponhamos então que $r = a - bq$. Sabemos que $r \geqslant 0$. Vamos mostrar que $r < |b|$. Suponhamos então que $r \geqslant |b|$. Portanto, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |b| + s$, logo $0 \leqslant s < r$. Mas isso contradiz o fato de r ser o menor elemento de S, pois $s = a - (q \pm 1)b \in S$, com $s < r$.
Unicidade: Suponha que $a = bq + r = bq' + r'$, onde $q, q', r, r' \in \mathbb{Z}$, $0 \leq r < |b|$ e $0 \leq r' < |b|$. Assim, temos que $-|b| < -r \leqslant r' - r \leqslant r' < |b|$. Logo, $|r - r'| < |b|$. Por

outro lado, $b(q-q') = r'-r$, o que implica que

$$|b|\,|q-q'| = |r'-r| < b,$$

o que só é possível se $q = q'$ e consequentemente, $r = r'$. □

Pelo teorema acima, os números q e r são chamados, respectivamente, de quociente, e de resto da divisão de a por b.

Da divisão euclidiana, temos que o resto da divisão de a por b é zero se ,e somente se, b divide a.

Exemplo 4. *O quociente e o resto da divisão de 17 por 5 são $q = 3$ e $r = 2$.*
O quociente e o resto da divisão de -17 por 5 são $q = -4$ e $r = 3$.

O exemplo abaixo nos permite analisar a paridade de números inteiros:

Exemplo 5. *Dado um número inteiro $n \in \mathbb{Z}$ qualquer, temos duas possibilidades:*

i) o resto da divisão de n por 2 é 0, isto é, existe $q \in \mathbb{N}$ tal que $n = 2q$; ou

ii) o resto da divisão de n por 2 é 1, ou seja, existe $q \in \mathbb{N}$ tal que $n = 2q + 1$.

Portanto, os números inteiros dividem-se em duas classes, a dos números da forma $2q$, para algum $q \in \mathbb{Z}$, chamados pares, e a dos números da forma $2q + 1$, chamados de números ímpares.

A divisão euclidiana, permite-nos obter o número de múltiplos num intervalo dado.
Temos então que, dados $a, c \in \mathbb{N}$ com $a < c$, o número de múltiplos não nulos de a menores ou iguais a c é igual ao quociente de c por a, ou o que é o mesmo, é igual a parte inteira $\left[\frac{c}{a}\right]$ do número racional $\frac{c}{a}$.

Proposição 15. *Dados os inteiros a, b e c tais que $0 < a < b < c$, então o número de múltiplos de a entre b e c é dado por*

i) $\left[\frac{c}{a}\right] - \left[\frac{b-1}{a}\right]$, *se incluirmos b na contagem.*

- *[ii)]* $\left[\frac{c}{a}\right] - \left[\frac{b}{a}\right]$, *se excluirmos b da contagem.*

Exemplo 6. *Determine quantos múltiplos de 7 há entre 1 e 400.*
Fazendo $a = 7$ *e* $c = 400$*, temos que,* $\left[\frac{400}{7}\right] = 57$*, logo, há 57 múltiplos.*

Exemplo 7. *Determine quantos múltiplos de 3 há entre 100 e 1000.*
Fazendo $a = 3$*,* $b = 100$ *e* $c = 1000$*, pelo item (ii) da proposição 15, temos que:* $\left[\frac{1000}{3}\right] - \left[\frac{100}{3}\right] = 333 - 33 = 300$*, logo, há 300 múltiplos.*

2.4 Representação dos números inteiros

A representação dos números inteiros, no cotidiano das pessoas, é feita no sistema decimal posicional. Há outros sistemas de numeração, destacando-se o sistema binário que é utilizado em computação.

Nessa trabalho vamos nos ocupar apenas com o sistema decimal.

2.4.1 Sistema de numeração decimal

No sistema de numeração decimal, todo número é representado por uma sequência formada pelos algarismos

$$1, 2, 3, 4, 5, 6, 7, 8, 9$$

acrescido do símbolo 0 (zero), que representa a ausência de algarismo.

O sistema é chamado posicional, pois cada algarismo possui um peso que é uma potência de 10, variando conforme a posição que ele ocupa no número. Assim, o algarismo mais a direita tem peso 1, o seguinte tem peso 10, o próximo tem peso 10^2 e assim por diante.

Exemplo 8. *O número 12567, na base 10 é a representação de*

$$1 \cdot 10^4 + 2 \cdot 10^3 + 5 \cdot 10^2 + 6 \cdot 10^1 + 7$$

Cada algarismo de um número possui uma ordem contada da direita para a esquerda.

Cada terna de ordens, também contada da direita para a esquerda, forma uma classe.

A seguir os nomes das primeiras classes e ordens:

$$\text{Classe das Unidades} \begin{cases} \textit{unidades} & 1^{\underline{a}} \text{ ordem} \\ \textit{dezenas} & 2^{\underline{a}} \text{ ordem} \\ \textit{centenas} & 3^{\underline{a}} \text{ ordem} \end{cases}$$

$$\text{Classe do Milhar} \begin{cases} \text{unidades de milhar} & 4^{\underline{a}} \text{ ordem} \\ \text{dezenas de milhar} & 5^{\underline{a}} \text{ ordem} \\ \text{centenas de milhar} & 6^{\underline{a}} \text{ ordem} \end{cases}$$

$$\text{Classe do Milhão} \begin{cases} \text{unidades de milhão} & 7^{\underline{a}} \text{ ordem} \\ \text{dezenas de milhão} & 8^{\underline{a}} \text{ ordem} \\ \text{centenas de milhão} & 9^{\underline{a}} \text{ ordem} \end{cases}$$

Os sistemas de numeração posicionais, baseiam-se no teorema abaixo, que é uma aplicação da divisão euclidiana.

Teorema 16. *Sejam dados os números inteiros a e b, com $a > 0$ e $b > 1$. Existem números inteiros $n \geqslant 0$ e $0 \leqslant r_0, r_1, \ldots, r_n < b$, com $r_n \neq 0$, univocamente determinados, tais que*

$$a = r_0 + r_1 b + r_2 b^2 + \ldots + r_n b^n.$$

Demonstração: Vamos demonstrar por indução completa sobre a.

Se $0 < a < b$, basta tomar $n = 0$ e $r_0 = a$. A unicidade da escrita é clara nesse caso.

Suponhamos o resultado válido para todo natural menor do que a, onde $a \geqslant b$. Vamos prová-lo para a. Pela divisão euclidiana, existem q e r, únicos, tais que

$$a = bq + r, \text{ com } 0 \leqslant r < b.$$

Como $0 < q < a$, pela hipótese de indução, segue-se que existem números inteiros $n' \geqslant 0$ e $0 \leqslant r_1, \ldots, r_{n'+1} < b$, com $r_{n'+1} \neq 0$, univocamente determinados, tais que

$$q = r_1 + r_2 b + \cdots + r_{n'+1} b^{n'}$$

Levando em consideração as igualdades acima destacadas, temos que

$$a = bq + r = b(r_1 + r_2 b + \cdots + r_{n'+1} b^{n'}) + r,$$

Daí o resultado segue-se pondo $r_0 = r$ e $n = n' + 1$ □

A representação dada no teorema acima é chamada de expansão relativa à base b. Quando $b = 10$, essa expressão é chamada expansão decimal e quando $b = 2$, ela toma o nome de expansão binária.

2.4.2 Critérios de divisibilidade

Apresentaremos os critérios de divisibilidade por 2^k, 3, 5, 6, 9, 10 e 11 e suas respectivas demonstrações. As mesmas terão como base a expansão decimal, na qual acreditamos que seja possível a sua aplicação no ensino fundamental.

Esse tema tem uma abordagem muito elementar nos livros didáticos do ensino fundamental, nos quais fica evidenciado apenas um processo de memorização, por esse motivo mostraremos como determiná-los. Deixamos a sugestão de que esses mesmos critérios podem ser obtidos ao utilizarmos congruências e suas propriedades. Assunto que veremos mais adiante.

Proposição 17. *(Critério de divisibilidade por 2^k) Seja $a = r_n \dots r_1 r_0$ um número representado no sistema decimal. Uma condição necessária e suficiente para que a seja divisível por 2^k é que o número $r_{k-1} \dots r_1 r_0$ é divisível por 2^k. Em particular, a é divisível por 2 se, e somente se, r_0 é 0,2,4,6,8; é divisível por 4 se, e somente se, $r_1 r_0$ é divisível por 4; é também divisível por 8 se, e somente se $r_2 r_1 r_0$ divisível por 8.*

Demonstração: Sendo $a = (r_n \dots r_k)10^k + r_{k-1} \dots r_0$, como $2^k \mid 10^k$, pelas proposições 8 e 9, $2^k \mid a$ se, e somente se, $2^k \mid r_{k-1} \dots r_1 r_0$. □

Proposição 18. *(Critério de divisibilidade por 5 e por 10) Seja $a = r_n \dots r_1 r_0$ um número representado no sistema decimal. Uma condição necessária e suficiente para que a seja divisível por 5 (respectivamente por 10) é que r_0 seja 0 ou 5 (respectivamente 0).*

Demonstração: Sendo $a = 10 \cdot (r_n \dots r_1) + r_0$, temos que a é divisível por 5 se, e somente se, r_0 é divisível por 5, e, portanto, $r_0 = 0$ e $r_0 = 5$. Por outro lado, a é divisível por 10, se e somente se, r_0 é divisível por 10, o que somente ocorre quando $r_0 = 0$. □

Proposição 19. *(Critério de divisibilidade por 3 e por 9) Seja $a = r_n \dots r_1 r_0$ um número representado no sistema decimal. Uma condição necessária e suficiente para que a seja divisível por 3 (respectivamente por 9) é que*
$r_n + \cdots + r_1 + r_0$ seja divisível por 3 (respectivamente 9).

Demonstração: Temos que

$$a-(r_n+\cdots+r_1+r_0) = r_n 10^n+\cdots+r_1 10+r_0-(r_n+\cdots+r_1+r_0) = r_n(10^n-1)+\cdots+r_1(10-1).$$

Como o termo à direita nas igualdades acima é divisível por 9, temos, para algum número q, que

$$a = (r_n + \cdots + r_1 + r_0) + 9q,$$

de onde se segue o resultado, em virtude das proposições 8 e 9. □

Proposição 20. *(Critério de divisibilidade por 11) Seja $a = r_n \dots r_1 r_0$ um número representado no sistema decimal. Uma condição necessária e suficiente para que a seja divisível por 11 é que $(r_0 + r_2 + r_4 + \cdots) - (r_1 + r_3 + r_5 + \cdots)$ seja divisível por 11.*

Demonstração:

Sendo,

$a = r_0 + r_1 \cdot 10 + r_2 \cdot 10^2 + r_3 \cdot 10^3 + r_4 \cdot 10^4 + \cdots + r_k \cdot 10^k$

$a = r_0+10r_1+r_1-r_1+10^2r_2+r_2-r_2+10^3r_3+r_3-r_3+10^4r_4+r_4-r_4\cdots+10^kr_k+r_k-r_k$

$a = r_0+r_1(10+1)-r_1+r_2(10^2-1)+r_2+r_3(10^3+1)-r_3+r_4(10^4-1)+r_4+\cdots+a_k(10^k-1)+a_k$

$a = r_1(10+1) + r_2(10^2-1) + r_3(10^3+1) + r_4(10^4-1) + \cdots + a_n(10^k-1) + (r_0 - r_1 + r_2 - r_3 + r_4 - \cdots + a_k \cdot (-1)^k)$

Como $11 \mid r_1(10+1) + r_2(10^2-1) + r_3(10^3+1) + r_4(10^4-1) + \cdots + a_n(10^k-1)$, pelas proposições 8 e 9, $11 \mid a$ se, e somente se, $11 \mid (r_0 - r_1 + r_2 - r_3 + r_4 - \cdots + a_k \cdot (-1)^k)$. □

Exemplo 9.

- *752 é divisível por 2, pois $r_0 = 2$.*
- *578424 é divisível por 4, pois $r_1 r_0 = 24$ e 24 é divisível por 4.*
- *65895 é divisível por 5, pois $r_0 = 5$.*
- *92370 é divisível por 5 e por 10, pois $r_0 = 0$.*
- *205101 é divisível por 3 e por 9, pois $r_5+r_4+r_3+r_2+r_1+r_0 = 2+0+5+1+0+1 = 9$ e 9 é divisível por 3 e também por 9.*

- *51634 é divisível por 11, pois* $(r_0+r_2+r_4)-(r_1+r_3) = (4+6+5)-(3+1) = 15-4 = 11$ *e 11 é divisível por 11.*

Outros critérios podem ser determinados a partir da combinação dos anteriores, como por exemplo o critério de divisibilidade por 6, no qual basta aplicar os critérios de divisibilidade por 2 e 3.

Exemplo 10. *123456789 é divisível por 9?*

Pelo critério de divisibilidade por 9, temos que $1+2+3+4+5+6+7+8+9 = 45$*,como 45 é divisível por 9, 123456789 também é.*

Exemplo 11. *211111235416 é divisível por 18?*

Como $18 = 2 \cdot 9$ *utilizaremos os critérios de divisibilidade por 2 e por 9.*

- *Note que, 211111235416 é divisível por 2, pois* $r_0 = 6$
- *Pelo critério de divisibilidade por 9,* $2+1+1+1+1+1+2+3+5+4+1+6 = 28$*, e 28 não é divisível por 9 então 211111235416 também não.*

Logo, 211111235416 não é divisível por 18.

Exemplo 12. *55682168544 é divisível por 36?*

Como $36 = 4 \cdot 9$ *utilizar os critérios de divisibilidade por 4 e por 9.*

- *Note que, 55682168544 é divisível por 4, pois* $r_1 r_0 = 44$ *e 44 é divisível por 4.*
- *Pelo critério de divisibilidade por 9,* $5+5+6+8+2+1+6+8+5+4+4 = 54$*, como 54 é divisível por 9 então 55682168544 também é.*

Logo, 55682168544 é divisível por 36.

Exemplo 13. *O inteiro* $1764x$ *é divisível por 3. Quais os valores de* x*?*

Pelo critério de divisibilidade por 3, temos que $1+7+6+4+x = 18+x$*, como* $0 \leqslant x \leqslant 9$ *e 18 é divisível por 3, então os valores possíveis para x, são 0,3,6 ou 9.*

Logo, obtemos os números 17640, 17643,17646 e 17649.

O inteiro $126x$ é divisível por 6. Quais os valores de x?

Para verificar se um número é divisível por 6, basta usar os critérios de divisibilidade por 2 e 3.

Como $0 \leqslant x \leqslant 9$, pelo critério de divisibilidade por 2, $126x$ será divisível por 2 se $x \in 0, 2, 4, 6, 8$, obtendo assim, os números 1260,1262,1264,1266 e 1268.

Pelo critério de divisibilidade por 3, $1 + 2 + 6 + x = 9 + x$, como 9 é divisível por 3 e pelo item anterior, $x = 0$ ou $x = 6$.

Logo, obtemos os números 1260 e 1266.

2.5 Algoritmo de Euclides

Nessa seção, iremos apresentar os conceitos de divisor comum, máximo divisor comum (*mdc*), o lema de Euclides, o algoritmo de Euclides, as propriedades do *mdc*, o lema de Gauss e o mínimo múltiplo comum (*mmc*).

A maioria desses resultados que usamos até hoje com pequenas variações, tem origem no Livro VII dos Elementos de Euclides escritos há aproximadamente 25 séculos.

Alguns desses conceitos, como o divisor comum, *mmc* e *mdc* são assuntos que fazem parte do currículo do ensino fundamental, porém a sua aplicação fica limitada na resolução de problemas elementares.

2.5.1 Máximo divisor comum

Definição 4. *(Divisor comum) Sejam dados dois inteiros a e b, distintos ou não. Um número inteiro d é chamado de um divisor comum de a e b quando $d \mid a$ e $d \mid b$.*

Exemplo 14. *Os números $\pm 1, \pm 2, \pm 5$ e ± 10 são os divisores comuns de 20 e 30.*

Definição 5. *(Máximo divisor comum (mdc)) Um número inteiro $d \geqslant 0$ é chamado de máximo divisor comum dos inteiros a e b, se possuir as seguintes propriedades:*

i) d é um divisor comum de a e b.

ii) d é divisível por todo divisor comum de a e b.

Temos as seguintes observações:

1. Se c é um divisor comum de a e b, então $c|d$;

2. Indicamos o máximo divisor comum de a e b, por $mdc(a, b)$ ou simplesmente por (a, b);

3. A condição (1) significa que o $mdc(a, b)$ quando existe é único;

4. O $mdc(a, b)$ não depende da ordem, ou seja, $mdc(a, b) = mdc(b, a)$;

5. Alguns casos particulares da existência do mdc: se a é um inteiro, tem-se claramente;

- $mdc(0, a) = |a|$;
- $mdc(1, a) = 1$;
- $mdc(a, a) = a$.

6. Mais ainda, para todo $b \in \mathbb{Z}$, temos que $a \mid b \Leftrightarrow mdc(a, b) = |a|$:

   De fato, se $a \mid b$, temos que $|a|$ é um divisor comum de a e b, e, se c é um divisor comum de a e b, então c divide $|a|$, o que mostra que $|a| = mdc(a, b)$.

   Reciprocamente, se $mdc(a, b) = |a|$, segue-se que $|a|$ divide b, logo $a \mid b$.

   Como todo número inteiro divide 0, o mdc de a e b, onde $a = b = 0$, é o 0, pois é um divisor comum de a e b e é o único número divisível por todos os divisores de 0. Reciprocamente, se o mdc de a e b é 0, então 0 divide a e divide b, mas o único número divisível por 0 é o próprio 0, logo $a = b = 0$.

7. Note que dados $a, b \in \mathbb{Z}$, se existir o $mdc(a, b)$, então $mdc(a, b) = mdc(-a, b) = mdc(a, -b) = mdc(-a, -b)$: Assim, para efeito do cálculo do mdc de dois números, podemos supô-los não negativos.

Exemplo 15. *O mdc de* 20 *e* 30 *é* 10.

Lema 21. *(Lema de Euclides) Sejam* $a, b, n \in \mathbb{Z}$. *Se existe* $mdc(a, b - na)$, *então* $mdc = (a, b)$ *existe e*

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

Demonstração: Seja $d = mdc(a, b - na)$, como $d \mid a$ e $d \mid (b - na)$, segue que d divide $b = b - na + na$. Logo, d é divisor comum de a e b.
Suponha agora que c seja um divisor comum de a e b. Logo, c é um divisor comum de a e $b - na$ e portanto, $c \mid d$. Isso prova que $d = mdc(a, b)$. □

2.5.2 Algoritmo de Euclides

Apresentaremos a prova construtiva do algoritmo de Euclides que também é chamado de processo de divisões sucessivas:

Dados $a, b \in \mathbb{N}$, podemos supor $b \leqslant a$. Se $b = 1$ ou $b = 0$, ou ainda, se $b \mid a$ então, $mdc(b, a) = b$. Suponhamos, então, que $1 < b < a$ e que $b \nmid a$. Logo, pela divisão euclidiana, podemos escrever

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

Temos duas possibilidades:

a) $r_1 \mid b$.

Em tal caso, $r_1 = mdc(b, r_1)$ e pelo lema de Euclides, temos que

$$r_1 = mdc(b, r_1) = mdc(b, a - q_1 b) = mdc(b, a) = mdc(a, b),$$

e o algoritmo termina.

b) $r_1 \nmid b$.

Em tal caso, podemos efetuar a divisão de b por r_1, obtendo

$$b = r_1 q_2 + r_2, \text{ com } 0 < r_2 < r_1.$$

Novamente, temos duas possibilidades:

a′) $r_2 \mid r_1$.

Nesse caso, $r_2 = mdc(r_1, r_2)$ e novamente, pelo lema de Euclides,

$$r_2 = mdc(r_1, r_2) = mdc(r_1, b - q_2 r_1) = mdc(r_1, b) = mdc(a - q_1 b, b) = mdc(a, b),$$

e paramos, pois termina o algoritmo.

b′) $r_2 \nmid r_1$.

Nesse caso podemos efetuar a divisão de r_1 por r_2, obtendo

$$r_1 = r_2 q_3 + r_3, \text{ com } 0 < r_3 < r_2.$$

Devemos continuar esse procedimento até que pare. Isto sempre ocorre, pois, caso contrário, teríamos uma sequência de números naturais $b > r_1 > r_2 > \cdots$ que não possui um menor elemento, o que não é possível pelo princípio da boa ordenação. Logo, para algum n, temos que $r_n \mid r_{n-1}$, o que implica que $mdc(a, b) = r_n$.

Podemos sintetizar o algoritmo acima, utilizando o dispositivo abaixo:

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

Exemplo 16. *Calcule o mdc de 321 e 114. Pelo algoritmo de Euclides, temos que:*

$$\begin{aligned} 321 &= 114 \cdot 2 + 93 \\ 114 &= 93 \cdot 1 + 21 \\ 93 &= 21 \cdot 4 + 9 \\ 21 &= 9 \cdot 2 + 3 \\ 9 &= 3 \cdot 3 + 0 \end{aligned}$$

Pelo dispositivo, temos

	2	1	4	2	3
321	114	93	21	9	3
93	21	9	3	0	

Portanto, $mdc(321, 114) = 3$.

2.5.3 Propriedades do mdc

Já provamos anteriormente a unicidade e a existência do $mdc(a, b)$, mas preferirmos apresentar um outro resultado que reafirmam esses fatos e vai nos ajudar a escrever de forma concreta o $mdc(a, b)$, como uma combinação linear de dois inteiros a e b.

Teorema 22. *Sejam $a, b \in \mathbb{Z}$ não simultaneamente nulos ($a \neq 0$ ou $b \neq 0$). Então, existem inteiros u e v tais que $mdc(a, b) = au + bv$.*

Demonstração: *Seja* $S = \{au + bv > 0 \text{ com } u, v \in \mathbb{Z}\}$ *o conjunto de todos os inteiros positivos. Caso* $a \neq 0$ *tem-se que um dos inteiros.*

$$a = a \cdot 1 + b \cdot 0 \text{ ou } -a = a \cdot (-1) + b \cdot 0$$

é positivo, logo $S \neq \varnothing$*. Pelo princípio da boa ordenação, existe e é único o elemento mínimo de* S*, que vamos chamar de* $d > 0$*. Por definição de* S*, existem inteiros* u, v *tais que* $d = au + bv$*. Afirmamos que* $d = mdc(a, b)$*. Com efeito, pelo algoritmo da divisão:*

$$a = df + r \text{ com } 0 \leqslant r < d$$

$$r = a - df = a - (au + bv)f = a(1 - uf) + b(-vf)$$

isto é, o resto r *é uma combinação linear de* a *e* b*. Como* $0 \leqslant r < d$ *e* $d > 0$ *é o elemento mínimo de* S*, segue que* $r = 0$ *e* $a = df$*, ou seja,* $d \mid a$*.*

Com raciocínio inteiramente análogo podemos concluir que também $d \mid b$*. Logo* d *é um divisor comum de* a *e* b*.*

Finalmente se c *é um divisor comum de* a *e* b *(*$c \mid a$ *e* $c \mid b$*), então*

$$c \mid au + bv = d \Rightarrow c \mid d \Rightarrow c \leqslant d,$$

isto é, d *é o maior divisor comum positivo de* a *e* b*, ou seja,*

$$mdc(a, b) = d = au + bv, \text{ para } u, v \in \mathbb{Z}.$$

□

Note que:

1. $mdc(a, b)$ é o menor inteiro positivo da forma $au + bv$, mas esta combinação linear de a e b não é única, pois

$$mdc(a, b) = d = a(u + bt) + b(v - at), \forall t \in \mathbb{Z}$$

2. Se $d = ar + bs$ com $r, s \in \mathbb{Z}$ então d não é necessariamente o $mdc(a, b)$.

De fato, se $mdc(a,b) = au + bv$, então para todo $t \in \mathbb{Z}$,

$$t \cdot mdc(a,b) = atu + btv = a(tu) + b(tv)$$
$$t \cdot mdc(a,b) = ar + bs, r = tu \text{ e } s = tv$$
$$t \cdot mdc(a,b) = d$$

Definição 6. *(Inteiros primos entre si) Dizemos que dois números inteiros a e b são primos entre sí ou coprimos, se $mdc(a,b) = 1$*

Exemplo 17. *São primos entre si os inteiros*

$$2 \text{ e } 3, -9 \text{ e } 16, -27 \text{ e } -35,$$

pois $mdc(2,3) = mdc(-9,16) = mdc(-27,-35) = 1$

Observe que a e b são primos entre si, se os únicos divisores comuns são ± 1.

Corolário 23. *Dois inteiros a e b são primos entre si, se e somente se, existem inteiros x e y tais que $ax + by = 1$.*
Demonstração: $\Rightarrow$) *Se $mdc(a,b) = 1$, então existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$.*
$\Leftarrow$) *Se existem inteiros x e y tais que $ax + by = 1$ e se $d = mdc(a,b)$, então $d \mid a$ e $d \mid b$, ou seja, $d \mid ax + by = 1$. Logo $d = 1$* □

Note que este corolário é o único caso em que a reciproca do teorema 22 é verdadeira.

Proposição 24. *Sejam a, b, c inteiros não simultaneamente nulos, então valem as afirmações:*

i) *se $mdc(a,b) = d$ então $mdc(na, nb) = nd, \forall n \in \mathbb{N}$;*

ii) *se $mdc(a,b) = d$ então $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$;*

iii) *(Lema de Gauss) se $a \mid bc$ e $mdc(a,b) = 1$ então $a \mid c$;*

iv) *se $a \mid c$ e $b \mid c$ então $\frac{ab}{mdc(a,b)} \mid c$;*

v) *se $mdc(a,c) = mdc(b,c) = 1$ então $mdc(ab,c) = 1$.*

Demonstração::

i) *Pelo teorema 22,* $mdc(na, nb)$ *é o menor inteiro positivo da forma* $nau+nbv = n(au+bv)$*, com* $u, v \in \mathbb{Z}$*. Por hipótese* $d = mdc(a, b)$ *é o menor inteiro positivo da forma* $au + bv$*. Assim* $mdc(na, nb) = n \cdot mdc(a, b) = n \cdot d$*.*

ii) *Se* $d = mdc(a, b)$ *então existem inteiros* a_1 *e* b_1 *tais que* $a = a_1 d$ *e* $b = b_1 d$*. Por outro lado, existem inteiros* u *e* v *tais que* $d = au + bv$*. Assim* $d = a_1 du + b_1 dv$*. Desse modo, obtemos* $1 = a_1 u + b_1 v = \left(\frac{a}{d}\right) u + \left(\frac{b}{d}\right) v$*. Pelo corolário 23, segue que* $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$*.*

iii) *Se* $a \mid bc$ *então* $bc = ra$ *para algum* $r \in \mathbb{Z}$*. Se* $mdc(a, b) = 1$ *existem inteiros* m, n *tais que* $ma + nb = 1$*, o que implica em* $mac + nbc = c$ *ou ainda* $c = mac + nra = a(mc + nr)$*. Portanto* $a \mid c$*.*

iv) *Seja* $d = mdc(a, b)$*, por hipótese* $a \mid c$ *e* $b \mid c$*, logo existem inteiros* r *e* s *tais que* $c = sa = rb$*, ou seja,* $s\frac{a}{d} = r\frac{b}{d}$*. Como* $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$*, pelo item (iii) temos que* $\frac{a}{d} \mid r$*, isto implica que* $\frac{a}{d}b \mid rb = c$*, ou seja,* $\frac{ab}{mdc(a,b)} \mid c$*. Note que a recíproca é verdadeira.*

v) *Se* $mdc(a, c) = mdc(b, c) = 1$ *então* $ax + cy = 1$*, com* $x, y \in \mathbb{Z}$ *e* $bu + cv = 1$*, com* $u, v \in \mathbb{Z}$*. Portanto*

$$\begin{aligned} 1 &= (ax + cy)(bu + cv) \\ &= axbu + axcv + cybu + cycv \\ &= ab(xu) + c(axv + ybu + ycv), \end{aligned}$$

isto implica que $mdc(ab, c) = 1$

□

Note que a recíproca de (v) também é verdadeira

2.5.4 O mdc de vários inteiros

Podemos generalizar a noção de *mdc* conforme segue:

Proposição 25. $mdc(a_1, a_2, a_3) = mdc(a_1, mdc(a_2, a_3))$

Demonstração: *Seja* $d_1 = mdc(a_1, a_2, a_3)$ *e* $d_2 = mdc(a_1, mdc(a_2, a_3))$. *Note que* d_1, d_2 *são ambos inteiros positivos. Temos que* $d_2 \mid a_1$ *e* $d_2 \mid mdc(a_2, a_3)$, *então nós realmente temos que* $d_2 \mid a_1, d_2 \mid a_2, d_2 \mid a_3$, *logo pela definição* $d_2 \mid d_1$.
Por outro lado, $d_1 \mid a_1, d_1 \mid a_2, d_1 \mid a_3$ *então por definição temos que* $d_1 \mid a_1, d_1 \mid mdc(a_2, a_3)$, *logo* $d_1 \mid d_2$.

Portanto dois inteiros positivos que são fatores um do outro devem ser iguais, segue

$$mdc(a_1, a_2, a_3) = d_1 = d_2 = mdc(a_1, mdc(a_2, a_3)).$$

□

Um número natural d será dito *mdc* de dados números inteiros $a_1, \ldots, a_n$, não todos nulos, se possuir as seguintes propriedades:

i) d é um divisor comum de $a_1, \ldots, a_n$.

ii) Se c é um divisor comum de $a_1, \ldots, a_n$, então $c \mid d$.

O *mdc*, quando existe, é certamente único e será representado por

$$mdc(a_1, \ldots, a_n).$$

Podemos estender o conceito de *mdc* para n inteiros conforme proposição abaixo.

Proposição 26. *Dados números inteiros* $a_1, \ldots, a_n$ *não todos nulos, existe o seu mdc e*

$$mdc(a_1, \ldots, a_n) = mdc(a_1, \ldots, a_{n-2}, mdc(a_{n-1}, a_n)).$$

Demonstração: Vamos provar a proposição por indução sobre n com $n \geqslant 2$.
Para $n = 2$, nada temos a provar.
Para $n = 3$ já foi provado na proposição 25.
Suponha que o resultado vale para $n > 3$. Para $n+1$, se d é o *mdc* de $a_1, \ldots, a_{n-1}, mdc(a_n, a_{n+1})$ então, pela definição, d divide $a_1, \ldots, a_{n-1}, mdc(a_n, a_{n+1})$, portanto, d é o *mdc* de $a_1, \ldots a_n, a_{n+1}$.

Por outro lado, seja c um divisor comum de $a_1, \ldots, a_n, a_{n+1}$, então c é um divisor de a_1 e c é um divisor de $a_2, \ldots a_n, a_{n+1}$. Logo pela hipótese de indução c é um divisor de $a_2, \ldots, a_{n-1}$ e c é um divisor de $mdc(a_n, a_{n+1})$. Logo $c \mid d$. □

O algoritmo e o lema de Euclides nos permitem calcular o mdc de pares de números da forma $a^n \pm b^m$, onde $a, b \in \mathbb{N}$ $mdc(a, b) = 1$, $n \in \mathbb{N} \cup 0$.

Segue abaixo um resultado importante, com $b = 1$, que usaremos na resolução de alguns problemas propostos.

Proposição 27. *Sejam $a, m, n \in \mathbb{N}$, então*

$$mdc(a^m - 1, a^n - 1) = a^d - 1, \textit{ onde } d = mdc(m, n)$$

Demonstração: Sem perda de generalidade, podemos supor que $n \geqslant m$. Pela divisão euclidiana, podemos escrever $n = mq + r$ com $0 \leqslant r < m$. Temos que $q > 0$, pois $n \geqslant m > 0$. Assim.

$$a^n - 1 = a^{mq+r} - 1 = a^r(a^m)^q - a^r + (a^r - 1) = a^r((a^m)^q - 1)) + (a^r - 1). \quad (1)$$

Como $a^m - 1$ divide $(a^m)^q - 1$, pelo lema de Euclides, temos que

$$mdc(a^m - 1, a^n - 1) = mdc(a^m - 1, a^r((a^m)^q - 1)) + (a^r - 1)) = mdc(a^m - 1, a^r - 1)$$

Se $r_1, r_2, \ldots, r_s, r_{s+1}$ são os restos parciais no algoritmo de Euclides aplicado ao par m, n com $r_s \neq 0$ e $r_{s+1} = 0$, então $r_s = mdc(m, n)$. Portanto, usando (1) repetidas vezes, temos que

$$\begin{aligned} mdc(a^m - 1, a^n - 1) &= mdc(a^m - 1, a^{r_1} - 1) = \cdots = mdc(a^{r_s} - 1, a^{r_s+1} - 1) \\ &= mdc(a^{r_s} - 1, 0) = a^{mdc(m,n)} - 1 \end{aligned}$$

□

2.5.5 Mínimo múltiplo comum (mmc)

Dizemos que um número inteiro é um múltiplo comum de dois números inteiros dados se ele é simultaneamente múltiplo de ambos os números.

Em qualquer caso, os números ab e 0 são sempre múltiplos comuns de a e b.

Definição 7. *Dizemos que um número inteiro $m \geqslant 0$ é um mínimo múltiplo comum (mmc) dos números inteiros a e b, se possuir as seguinte propriedades:*

i) m é um múltiplo comum de a e b, e

ii) se c é um múltiplo comum de a e b, então $m \mid c$.

Exemplo 18. *30 é um múltiplo comum de 3 e 5, mas não é um mmc desses números. O número 15 é o mmc de 3 e 5.*

Se m e m' são dois mínimos comuns de a e b, então, do item (ii) da definição, temos que $m \mid m'$ e $m' \mid m$. Como m e m' são números inteiros não negativos, temos que $m = m'$, o que mostra que o *mmc*, se existe é único.

Por outro lado, pelo item (ii) da definição 7, se m é o *mmc* de a e b, então $m \mid c$. Portanto, se c é positivo, temos que $m \leqslant c$, mostrando que m é o menor dos múltiplos comuns positivos de a e b

O mínimo múltiplo comum de a e b, se existe, é denotado por $mmc(a, b)$.

Caso exista $mmc(a, b)$, temos que,

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

Assim, para efeito do cálculo do mmc de dois números, podemos sempre supô-los não negativos.

Temos ainda que $mmc(a, b) = 0$ se, e somente se, $a = 0$ ou $b = 0$.

Proposição 28. *Dados dois números inteiros a e b, temos que $mmc(a, b)$ existe e*

$$mdc(a, b) \cdot mmc(a, b) = |ab|$$

Demonstração: Se $a = 0$ ou $b = 0$, a igualdade acima é trivialmente satisfeita. É também fácil verificar que a igualdade é verificada para a e b se, e somente se, ela é

verificada para $\pm a$ e $\pm b$. Então, sem perda de generalidade, podemos supor $a, b \in \mathbb{N}$. Ponhamos $m = \dfrac{ab}{mdc(a,b)}$. Como

$$m = a\frac{b}{mdc(a,b)} = b\frac{a}{mdc(a,b)},$$

temos que $a \mid m$ e $b \mid m$. Portanto, m é um múltiplo comum de a e b.

Seja c um múltiplo comum de a e b; logo, $c = na = n'b$. Segue daí que

$$n\frac{a}{mdc(a,b)} = n'\frac{b}{mdc(a,b)}.$$

Como pelo proposição 24, $\dfrac{a}{mdc(a,b)}$ e $\dfrac{b}{mdc(a,b)}$ são primos entre si, seque-se pelo Lema de Gauss, que $\dfrac{a}{mdc(a,b)}$ divide n', e, portanto, $m = \dfrac{a}{mdc(a,b)}b$ divide $n'b$ que, é igual a c. □

De acordo com a proposição acima, o *mmc* de dois inteiros a e b, ambos não nulos, pode ser obtidos da seguinte forma:

$$mmc(a,b) = \frac{|ab|}{mdc(a,b)}$$

Corolário 29. *Se a e b são números inteiros primos entre si, então $mmc(a,b) = |ab|$.*

A noção de *mmc* pode ser estendida para vários números.

Diremos que um número natural m é um *mmc* dos inteiros não nulos $a_1, \ldots, a_n$, se m é um múltiplo comum de $a_1, \ldots, a_n$, e, se para todo múltiplo comum m' desses números, tem-se que $m \mid m'$.

Proposição 30. *Sejam $a_1, \ldots, a_n$ números inteiros não nulos. Então existe o número $mmc(a_1, \ldots, a_n)$ e $mmc(a_1, \ldots, a_{n-1}, a_n) = mmc(a_1, \ldots, mmc(a_{n-1}, a_n)$.*

Demonstração: Vamos provar a proposição por indução sobre $n \geqslant 2$.

Para $n = 2$, nada temos a provar.

Suponha que o resultado vale para $n > 2$. Para $n + 1$, se m é o *mmc* de $a_1, \ldots, a_{n-1}, mmc(a_n, a_{n+1})$, pela definição, $a_1, \ldots, a_{n-1}, mmc(a_n, a_{n+1})$, dividem m, então m é o *mmc* de $a_1, \ldots, a_n, a_{n+1}$.

Por outro lado, seja m' um múltiplo comum de $a_1, \ldots, a_n, a_{n+1}$, então, m' é um múltiplo de a_1 e m' é um múltiplo de $a_2, \ldots, a_{n-1}, a_n, a_{n+1}$. Logo pela hipótese de indução,

m' é um múltiplo de $a_2, \ldots, a_{n-1}$ e m' é um múltiplo de $mmc(a_n, a_{n+1})$, portanto m' é múltiplo de m. □

Exemplo 19. *Determine* $mmc(-15, 10, 25)$

Temos que, $mmc(-15, 10, 25) = mmc(15, mmc(10, 25)) = mmc(15, 50) = 150$

2.5.6 Equações diofantinas lineares

Diversos problemas de aritmética recaem em equações do tipo

$$ax + by = c$$

onde $a, b, c \in \mathbb{Z}$ e $ab \neq 0$, essas equações são chamadas equações diofantinas lineares, nas variáveis x e y, em homenagem ao matemático grego Diofanto de Alexandria que viveu no século III d.C. e é considerado o pai da álgebra.

Todo par de inteiros (x_0, y_0) tal que $ax_0 + by_0 = c$ diz-se uma solução da equação $ax + by = c$.

Exemplo 20. *Considere* $3x + 6y = 18$. *Note que* $(x_0, y_0) = (4, 1), (-6, 6), (10, -2)$ *são soluções da equação* $3x + 6y = 18$.

Exemplo 21. *Existem equações diofantinas que não tem solução.*

Por exemplo, $2x+4y = 7$. *Pois para qualquer* x *e* y *inteiros,* $2x+4y$ *é um número par, enquanto* 7 *é um número ímpar.*

Teorema 31. *Sejam* a, b, c *inteiros com* a *e* b *não simultaneamente nulos e* $d = mdc(a, b)$*:*

i) Então a equação $ax + by = c$ *tem solução se, e somente se,* $d \mid c$*;*

ii) Além disso, se (x_0, y_0) *é uma solução particular da equação* $ax + by = c$ *então todas as outras soluções são dadas por*

$$x = x_0 + \left(\frac{b}{d}\right) t, y = y_0 - \left(\frac{a}{d}\right) t, \text{ com } t \in \mathbb{Z}.$$

Demonstração:

i) Suponha que (x_0, y_0) *é uma solução de* $ax + by = c$*, ou seja,* $ax_0 + by_0 = c$*. Como* $d = mdc(a, b)$*, temos que* $d \mid a$ *e* $d \mid b$*, ou ainda* $a = dr$ *e* $b = ds$ *para algum* $r, s \in \mathbb{Z}$.

Assim $c = drx_0 + dsy_0 = d(rx_0 + sy_0)$, *como* $rx_0 + sy_0 \in \mathbb{Z}$ *segue que* $d \mid c$.

Reciprocamente suponha que $d \mid c$, *isto é,* $c = dt$ *para algum* $t \in \mathbb{Z}$. *Como* $d = mdc(a, b)$, *existem inteiros* x_0 *e* y_0 *tais que* $d = ax_0 + by_0$, *ou seja,* $c = (ax_0 + by_0)t = a(tx_0) + b(ty_0)$ *então* $x = tx_0 = \frac{c}{d}x_0$ *e* $y = ty_0 = \frac{c}{d}y_0$ *é uma solução de* $ax + by = c$.

ii) Se (x_0, y_0) *é uma solução particular da equação* $ax + by = c$, *então*

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

para qualquer (x, y). *Logo*

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

Como $d = mdc(a, b)$, *existem* $r, s \in \mathbb{Z}$ *tais que* $a = dr$ *e* $b = ds$, *temos que* $d = mdc(dr, ds) = d \cdot mdc(r, s)$, *ou seja,* $mdc(r, s) = 1$.

Podemos escrever $r(x - x_0) = s(y_0 - y)$, *ou seja,* $r \mid s(y_0 - y) \Rightarrow r \mid y_0 - y$, *isto é,* $y_0 - y = rt$ *para algum* $t \in \mathbb{Z}$ *e de modo análogo* $x - x_0 = st$. *Portanto temos*

$$x = x_0 + \left(\frac{b}{d}\right) t \text{ e } y = y_0 - \left(\frac{a}{d}\right) t$$

Finalmente

$$ax + by = a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) = ax_0 + by_0 + \left(\frac{ab}{d} - \frac{ab}{d}\right) t = c$$

são todas as soluções

□

Observe que, se $d = mdc(a, b) = 1$ e (x_0, y_0) uma solução particular de $ax + by = c$, temos:

i) A equação sempre tem solução;

ii) Todas as soluções são da forma

$$x = x_0 + bt, y = y_0 - at, \text{ com } t \in \mathbb{Z}$$

Exemplo 22. *Determine todas as soluções inteiras da equação* $18X + 5Y = 48$.

Como $mdc(18, 5) = 1$ *e* $1 \mid 48$, *a equação* $18X + 5Y = 48$ *tem solução inteira. Por inspeção, obtemos a solução particular* $x_0 = 1$ *e* $y_0 = 6$, *então todas as soluções são dadas por* $x = 1 + 5t$ *e* $y = 6 - 18t$, *para* $t \in \mathbb{Z}$.

Capítulo 3

Números primos

Neste capítulo, faremos um estudo dos números primos, apresentaremos suas definições e propriedades, o teorema fundamental da aritmética, teorema de Legendre e o pequeno teorema de Fermat. Todas as definições serão demonstradas e acompanhadas de exemplos. Usamos como referência para o desenvolvimento da mesma, Hefez (2016), e Araújo (2018).

3.1 Teorema fundamental da aritmética

Definição 8. *(Números primos) Um inteiro p maior que 1 é um número primo se os únicos divisores positivos de p são 1 e o próprio p.*

Algumas consequências da definição:

Dados dois números primos p e q e um número inteiro a qualquer, pela definição, temos

i) Se $p \mid q$ então $p = q$.

De fato, como $p \mid q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Sendo p primo, tem-se que $p > 1$, o que acarreta $p = q$.

ii) Se $p \nmid a$, então $mdc(p, a) = 1$.

De fato, se $mdc(p, a) = d$, tem-se que $d \mid p$ e $d \mid a$. Portanto, $d = p$ ou $d = 1$. Mas, $d \neq p$, pois $p \nmid a$, e consequentemente $d = 1$.

Um número inteiro maior do que 1 e que não é primo, será dito composto. Portanto, se um número natural $n > 1$ é composto, existirá um divisor natural n_1 de n

tal que $1 < n_1 < n$. Logo, existirá um número natural n_2 tal que

$$n = n_1 n_2, \text{ com } 1 < n_1 < n \text{ e } 1 < n_2 < n$$

Exemplo 23. *São exemplos de primos os números 2, 3, 5, 7, 11 e os números 4,6,8,10 são compostos.*

Proposição 32. *(Lema de Euclides) Sejam os a, b, p inteiros a, b, p, com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração: Se $p \mid a$, então não há nada a provar. Vamos supor que $p \nmid a$, então $(a, p) = 1$. Pelo lema de Gauss $p \mid b$. □

Corolário 33. *Se $p, p_1, \ldots p_n$, são números primos e, se $p \mid p_1, p_2 \cdots p_n$, então $p = p_i$ para algum $i = 1, \ldots, n$.*

Teorema 34. *(Teorema fundamental da aritmética) Todo número inteiro n maior do que 1 ou é primo ou é um produto de números primos. Este produto é único, fora a ordem na qual os fatores ocorrem.*

Demonstração: Usaremos a segunda forma do princípio de indução. Mostraremos primeiro a existência e depois a unicidade da fatoração.
Se $n = 2$, o resultado é verdadeiro, visto que 2 é primo.

Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar.

Suponhamos, então, que n seja composto. Logo existem números naturais n_1 e n_2 tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, \ldots, p_r$ e $q_1, \ldots, q_s$ tais que $n_1 = p_1, \cdots, p_r$ e $n_2 = q_1, \cdots, q_s$. Portanto, $n = p_1 \cdots p_r q_1 \cdots q_s$.

Suponhamos que tenhamos $n = p_1 \cdots p_r = q_1 \cdots q_s$, onde os p_i e q_j são os números primos. Como $p_1 \mid q_1 \cdots q_s$, pelo corolário 33, temos que $p_1 = q_j$, para algum j, que, após reordenamento de $q_1, \ldots, q_s$, podemos supor $p_1 = q_1$. Portanto,

$$p_2 \cdots p_r = q_2 \cdots q_s.$$

Como $p_2 \cdots p_r < n$, por hipótese se de indução, segue que $r = s$ e os p_i e q_j são iguais aos pares. □

Corolário 35. *Dado um número inteiro $n \neq 0, 1, -1$, existem primos $p_1 < p_2 \cdots < p_r$ e $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$, univocamente determinados, tais que*

$$n = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

A sua demonstração é uma consequência imediata do teorema 34.

Proposição 36. *Seja $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ um número natural escrito na forma acima. Se n' é um divisor positivo de n, então*

$$n' = p_1^{\beta_1} \cdots p_r^{\beta_r},$$

onde $0 \leqslant \beta_i \leqslant \alpha_i$, para $i = 1, \ldots, r$.

Demonstração: Seja n' um divisor positivo de n e seja p^β a potência de um primo p que figura na decomposição de n' em fatores primos. Como $p^\beta \mid n$, segue que p^β divide algum $p_i^{\alpha_i}$ por ser primo com os demais $p_j^{\alpha_j}$ e consequentemente, $p = p_i$ e $0 \leqslant \beta \leqslant \alpha_i$. □

Observação 1. *Na decomposição em dois ou mais fatores primos, na qual desejamos ordená-los, poderemos usar o recurso de acrescentar fatores da forma p^0, onde p é um número primo qualquer. Assim, dados $n, m \in \mathbb{N}$ com $n > 1$ e $m > 1$ quaisquer, podemos escrever*

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \text{ e } m = p_1^{\beta_1} \cdots p_r^{\beta_r}.$$

Usando o mesmo conjunto de primos $p_1, \ldots, p_r$, desde que os expoentes $\alpha_1 \cdots \alpha_r, \beta_1 \cdots \beta_r$ variem em $\mathbb{N} \cup \{0\}$ e não apenas em $\mathbb{N}$.

Exemplo 24. *Os números $2^3 \cdot 3^2 \cdot 7$ e $3^2 \cdot 5 \cdot 7^3$, podem ser escritos respectivamente, $2^3 \cdot 3^2 \cdot 5^0 \cdot 7$ e $2^0 \cdot 3^2 \cdot 5 \cdot 7^3$*

Número de divisores

Representando por $d(n)$ o número de divisores positivos de um número natural n, segue, por contagem, que se $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, onde $p_1 \ldots, p_r$ são números primos e $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$, então

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1).$$

Exemplo 25. *A fórmula acima nos mostra que um número natural* $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$*, possui uma quantidade ímpar de divisores se, e somente se, cada* α_i *é par, ou seja, se, e somente se,* n *é um quadrado perfeito.*

Exemplo 26. *Quantos divisores naturais possui o número 60?*
Pela decomposição em fatores primos, temos que $60 = 2^2 \cdot 3 \cdot 5$ *e pela fórmula acima*

$$d(60) = (2+1)(1+1)(1+1) = 3 \cdot 2 \cdot 2 = 12$$

Concluímos que 60 tem 12 divisores.
Listando todos os divisores naturais, obtemos, $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$.

A fatoração de números naturais em primos permite determinar o *mdc* e o *mmc* de um conjunto de números.

O teorema a seguir, nos permite determinar o *mdc* e o *mmc* de um conjunto de números naturais.

Teorema 37. *Sejam* $a = \pm p_1^{\alpha_1} \cdots \pm p_n^{\alpha_n}$ *e* $b = \pm p_1^{\beta_1} \cdots \pm p_n^{\beta_n}$*. Pondo*

$$\gamma_i = min\{\alpha_i, \beta_i\}, \delta_i = max\{\alpha_i, \beta_i\}, i = 1, \ldots, n,$$

Tem-se que

$$mdc(a,b) = p_1^{\gamma_1} \cdots p_n^{\gamma_n} \text{ e } mmc(a,b) = p_1^{\delta_1} \cdots p_n^{\delta_n}.$$

Demonstração: Pela proposição 36 temos que $p_1^{\gamma_1} \cdots p_n^{\gamma_r}$ é um divisor comum de a e b. Seja c um divisor comum de a e b; logo $c = \pm p_1^{\varepsilon_1} \cdots p_n^{\varepsilon_n}$, onde $\varepsilon_i \leqslant min\{\alpha_i, \beta_i\}$ e, portanto $c \mid p_1^{\gamma_1} \cdots p_n^{\gamma_n}$.
Da definição de mínimo múltiplo comum nenhum fator primo p_i deste mínimo poderá ter um expoente que seja inferior nem a α_i e nem a β_i. Se tomarmos, pois, o maior destes dois para expoente de p_i teremos, não apenas um múltiplo comum, mas o menor possível dentre todos eles. O que conclui a demonstração. □

Exemplo 27. *Se* $a = 300$ *e* $b = 2520$*, temos que* $a = 2^2 \cdot 3 \cdot 5^2 \cdot 7^0$ *e* $b = 2^3 \cdot 3^2 \cdot 5 \cdot 7$*, pelo teorema 37 temos que* $mdc(a,b) = 2^2 \cdot 3 \cdot 5 \cdot 7^0 = 60$ *e* $mmc(a,b) = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7 = 12600$.

3.2 Expoente da maior potência de p que divide n

Se $n \in \mathbb{Z}^*$ e p é um número primo, chamaremos por $E_p(n)$ o expoente da maior potência de p que divide n.

Proposição 38. *Se m e n são dois números naturais, então*

$$m = n \Leftrightarrow E_p(m) = E_p(n) \text{ para todo número primo } p.$$

Demonstração: De fato, se $m = n$, é evidente que $E_p(m) = E_p(n)$ para todo primo p.

Reciprocamente, suponhamos que $E_p(m) = E_p(n)$ para todo primo p. Se $E_p(m) = E_p(n) = 0$, para todo primo p, então $m = n = 1$. Caso contrário, pelo teorema fundamental da aritmética, podemos escrever $m = p_a^{\alpha_1} \cdots p_r^{\alpha_r}$ e $n = q_1^{\beta_1} \cdots q_s^{\beta_s}$, onde $\{p_1, \ldots, p_r\}$ e $\{q_1, \ldots, q_s\}$ são dois conjuntos cada um deles compostos por números primos dois a dois distintos. Como

$$\{p; p \text{ é primo e } E_p(m) > 0\} = \{p_1, \ldots, p_r\}$$

e

$$\{p; p \text{ é primo e } E_p(n) > 0\} = \{q_1, \ldots, q_s\}$$

segue-se que

$$\{p_1, \ldots, p_r\} = \{q_1, \ldots, q_s\}$$

Assim $r = s$ e, após reordenarmos os elementos $q_1, \ldots, q_s$, podemos supor $q_i = p_i$ para $i = 1, \ldots, r$. Como $\alpha_i = E_{p_i}(m) = E_{p_i}(n) = \beta_i$, para $i = 1, \ldots, r$, conclui-se que $n = m$. □

Portanto, para todo primo p,

$$E_p(mmc(m,n)) = min\{E_p(m), E_p(n)\},\ E_p(mdc(m,n)) = max\{E_p(m), E_p(n)\}.$$

3.3 Distribuição dos números primos

Teorema 39. *Existem infinitos números primos.*

O matemático grego Euclides (323-283 a.C.) deu a seguinte prova:

Demonstração: Suponha que exista apenas um número finito de números primos $p_1, \ldots, p_r$. Considere o número natural $n = p_1 \cdot p_2 \cdots p_r + 1$.

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

Como existem infinitos números primos, o matemático grego Eratóstenes (276-194 a.C.), desenvolveu um método chamado de crivo de Eratóstenes, que permite determinarmos todos os números primos até um determinado valor. Descreveremos esse processo através do exemplo que segue:

Exemplo 28. *Escreva todos os números primos menores do que 140.*

- *Escreva todos os números naturais de 2 até 140;*
- *Risque todos os números múltiplos de 2 acima de 2, pois 2 é primo e os demais não;*
- *Risque todos os números múltiplos de 3 acima de 3, pois 3 é primo e os demais não;*
- *Risque todos os números múltiplos de 5 acima de 5; pois 5 é primo e os demais não;*
- *Risque todos os números múltiplos de 7 acima de 7; pois 7 é primo e os demais não;*
- *Risque todos os números múltiplos de 11 acima de 11; pois 11 é primo e os demais não;*
- *Se necessário, prossiga esse procedimento para chegar até 140.*

	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~~	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~~

Logo os números que não foram riscados, são primos menores que 140, ou seja
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.

Note que do resultado acima, alcançamos até o primo 11 para obter todos os primos menores que 140. O lema abaixo generaliza o crivo de Eratóstenes.

Lema 40. *Se um número natural $n > 1$ não é divisível por nenhum número primo p tal que $p^2 \leqslant n$, então ele é primo.*

Demonstração: Suponhamos, por absurdo, que n não seja divisível por nenhum número primo p tal que $p^2 \leqslant n$ e que não seja primo. Seja q o menor número primo que divide n; então $n = qn_1$, com $q \leqslant n_1$. Segue daí que $q^2 \leqslant qn_1 = n$. Logo, n é divisível por um número primo q tal que $q^2 \leqslant n$, absurdo. □

Note que o lema 40, nos fornece um teste de primalidade, pois para verificarmos se um dado número é primo, basta verificar que não é divisível por nenhum primo p que não supere $\sqrt{n}$.

Exemplo 29. *Verifique se 173 é um número primo. Pelo lema anterior, temos que $\sqrt{173} < 14$. Então devemos verificar se 173 é divisível pelos primos 2,3,5,7,11 e 13.*
Pelo teste de primalidade, verificamos que $2 \nmid 173$, $3 \nmid 173$, $5 \nmid 173$, $7 \nmid 173$, $11 \nmid 173$ e $13 \nmid 173$, logo 173 é um número primo.

3.4 Pequeno teorema de Fermat

O lema 40, é eficaz para testar a primalidade de números pequenos, mas não é um método prático na verificação de números grandes.

Há pelo menos 500 anos antes de Cristo, os chineses tinham conhecimento de que, se um número p é primo, então $p \mid 2^p - 2$. Somente no século XVIII, o matemático francês Pierre de Fermat generalizou esse resultado, que é chamado de pequeno teorema de Fermat.

Para demonstrar esse teorema, será necessário o seguinte lema:

Lema 41. *Seja p um número primo, os números $\binom{p}{i}$, onde $0 < i < p$, são todos divisíveis por p.*

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

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

□

Teorema 42. *(Pequeno teorema de Fermat) Dado um número primo p, tem-se que p divide o número $a^p - a$, para todo $a \in \mathbb{Z}$.*

Demonstração: Se $p = 2$, o resultado é óbvio já que $a^2 - a = a(a-1)$ é par.

Suponhamos p ímpar. Nesse caso, basta mostrar o resultado para $a \geqslant 0$.

Vamos mostrar por indução sobre a.

Para $a = 0$ temos $p \mid 0$.

Suponhamos o resultado ser válido para a, devemos provar para $a+1$. Pela

$$\begin{aligned}(a+1)^p - (a+1) &= \binom{p}{0}a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a + \binom{p}{p}a^0 \cdot 1 + (a+1) \\ &= a^p - a + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a\end{aligned}$$

Como, pelo lema anterior e pela hipótese de indução, o segundo membro da igualdade acima e divisível por p, o resultado se segue. □

O pequeno teorema de Fermat, possui uma segunda versão descrita no corolário a seguir:

Corolário 43. *Se p é um número primo e se a é um número inteiro não divisível por p, então $p \mid a^{p-1} - 1$.*

Demonstração: Como, pelo pequeno teorema de Fermat, $p \mid a(a^{p-1} - 1)$, e como $(a, p) = 1$, segue que $p \mid a^{p-1} - 1$. □

Exemplo 30. *Pelo pequeno teorema de Fermat, $7 \mid 8^7 - 8$ ou $7 \mid 8^6 - 1$.*

3.5 Decomposição do fatorial em primos

Mostraremos como obter a fatoração em primos de $n!$, com n natural.

Sejam a e b números naturais, representando pelo símbolo $\left[\frac{a}{b}\right]$ o quociente da divisão de a por b na divisão euclidiana, que é o maior inteiro menor ou igual do que o número racional $\frac{a}{b}$.

Proposição 44. *Sejam $a, b, c \in \mathbb{N}$. Temos que*

$$\left[\frac{\left[\frac{a}{b}\right]}{c}\right] = \left[\frac{a}{bc}\right].$$

Demonstração: Sejam

$$q_1 = \left[\frac{a}{b}\right] \text{ e } q_2 = \left[\frac{\left[\frac{a}{b}\right]}{c}\right].$$

Logo,

$$a = bq_1 + r_1, \text{com} 0 \leqslant r_1 \leqslant b - 1$$

e

$$\left[\frac{a}{b}\right] = q_1 = cq_2 + r_2, \text{com} 0 \leqslant r_2 \leqslant c - 1.$$

Portanto,

$$a = bq_1 + r_1 = b(cq_2 + r_2) + r_1 = bcq_2 + br_2 + r_1$$

Como

$$0 \leqslant br_2 + r_1 \leqslant b(c-1) + b - 1 = bc - 1,$$

segue-se que q_2 é o quociente da divisão de a por bc, ou seja,

$$q_2 = \left[\frac{a}{bc}\right].$$

□

Já vimos que a notação $E_p(n)$ indica a maior potência de p que divide n, em particular, $E_p(n!)$ representará a potência de p que aparece na fatoração de $n!$.

Teorema 45. *(Teorema de Legendre) Sejam n um número natural e p um número primo. Então,*

$$E_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

Demonstração: Note, inicialmente, que a soma acima é finita, pois existe um número natural r tal que $p^i > n$ para todo $i \geqslant r$; portanto, $\left[\frac{n}{p^i}\right] = 0$, se $i \geqslant r$.

A demonstração será feita por indução em n.

Para $n = 1$, a fórmula é verdadeira.

Suponha que o resultado vale para qualquer natural m com $m < n$. Note que os múltiplos de p entre 1 e n são

$$p, 2p, \ldots, \left[\frac{n}{p}\right] p.$$

Portanto,

$$E_p(n!) = \left[\frac{n}{p}\right] + E_p\left(\left[\frac{n}{n}\right]!\right)$$

Pela hipótese de indução, temos que

$$E_p\left(\left[\frac{n}{n}\right]!\right) = \left[\frac{\left[\frac{n}{p}\right]}{p}\right] + \left[\frac{\left[\frac{n}{p}\right]}{p^2}\right] + \cdots$$

O resultado decorre da proposição 44. □

Então, para calcularmos $E_p(n!)$, faremos o uso do seguinte algoritmo:

$$n = pq_1 + r_1$$

$$q_1 = pq_2 + r_2$$

$$\cdots$$

$$q_{s-1} = pq_s = r_s$$

$$\cdots$$

Como $q_1 > q_2 > \cdots$, segue que, para algum s, tem-se que $q_s < p$. Portanto, segue-se que

$$E_p(n!) = q_1 + q_2 + \cdots = q_s.$$

Exemplo 31. *Determine a maior potência de 2 que divide* 50!.

Para resolvermos o problema, deveremos achar $E_2(50!)$*, pelo teorema 45 (Legendre) temos*

$$E_2(50!) = \left[\frac{50}{2}\right] + \left[\frac{50}{2^2}\right] + \left[\frac{50}{2^3}\right] + \left[\frac{50}{2^4}\right] + \left[\frac{50}{2^5}\right] = 25 + 12 + 6 + 3 + 1 = 47$$

Logo, o expoente é 47 e ainda $2^{47} \mid 50!$.

Capítulo 4

Congruências

Neste capítulo, faremos um estudo sobre congruências, sistemas de resíduos módulo m, congruências lineares, o teorema chinês dos restos, o teoremas de Wilson, Fermat e Euler. faremos as demonstrações e exemplos dessa teoria. Para o desenvolvimento da mesma, foi consultado Araújo (2018).

Definição 9. *sejam $a, b, m \in \mathbb{Z}$ com $m > 0$, Diremos que a é congruente b módulo m, se m divide $(a - b)$.*

Observação 2. *Neste caso escrevemos:*

1. $a \equiv b \pmod{m}$ *se equivalentemente* $m \mid (a - b)$;
2. *Se* $m \nmid (a - b)$, *então* $a \not\equiv b \pmod{m}$;
3. a *e* b *deixam o mesmo resto quando divididos por* m.

Exemplo 32. *Por exemplo:*

1. $22 \equiv 1 \pmod{3}$;
2. $27 \equiv 2 \pmod{5}$;
3. $38 \not\equiv 5 \pmod{7}$.

Proposição 46. *Sejam $a, b, c, m \in \mathbb{Z}$ com $m > 0$. A congruência módulo m é uma relação de equivalência, ou seja,*

1. *Reflexiva:* $a \equiv a \pmod{m}$;
2. *Simétrica: se* $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$;

3. *Transitiva: se* $a \equiv b \pmod{m}$ *e* $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.

Demonstração:

1. $m \mid a - a = 0$;

2. $m \mid a - b \Leftrightarrow m \mid -(a - b) \Leftrightarrow m \mid b - a$;

3. $\begin{cases} m \mid a - b \\ m \mid b - c \end{cases} \Rightarrow m \mid (a - b) + (b - c) \Leftrightarrow m \mid a - c.$

□

As classes de equivalências definidas pela relação de congruência módulo m, também chamadas de classes de congruência módulo m (ou classes de resíduos módulo m) são definidas por

$$[a] = \{x \in \mathbf{Z} : x \equiv a \pmod{m}\}$$

Exemplo 33. *As classes de congruência módulo* 4 *são*

i) $[0] = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}$;

ii) $[1] = \{\ldots, -11, -7, -3, 1, 5, 9, 13, \ldots\}$;

iii) $[2] = \{\ldots, -10, -6, -2, 2, 6, 10, 14, \ldots\}$;

iv) $[3] = \{\ldots, -9, -5, -1, 3, 7, 11, 15, \ldots\}$.

Observação 3. *Logo temos que:*

1. *pela proposição anterior, o conjunto dos inteiros é dividido em* m *classes de congruência módulo* m *diferentes. Cada classe contém inteiros que são mutuamente congruentes módulo* m;

2. *dado* $a \in \mathbb{Z}$, *pelo algoritmo da divisão* $a = bm + r$ *com* $0 \leq r < m$, *ou seja,* $a \equiv r \mod m$ *então todo inteiro é congruente módulo* m *a um dos inteiros* $\{0, 1, 2, 3, \ldots, m-1\}$ *que são os restos de quando* a *é dividido por* m.

Proposição 47. *Sejam* $a, b, c, m \in \mathbb{Z}$ *com* $m > 0$. *Temos as seguintes condições:*

1. *se* $a \mid b \cdot c$ *e* $mdc(a, b) = 1$ *então* $a \mid c$;

2. *se* $a \mid c$, $b \mid c$ *e* $mdc(a, b) = 1$ *então* $a \cdot b \mid c$;

3. *se* $a \mid c$, $b \mid c$ *então* $m = mmc(a, b) \mid c$. *Vale a recíproca;*

4. *se* $mdc(a,c)=1$, $mdc(b,c)=1$ *então* $mdc(a\cdot b,c)=1$. *Vale a recíproca.*

Demonstração:

1. *De* $mdc(a,b)=1$ *temos que existem* x,y *inteiros tal que* $ax+by=1$, *multiplicando tudo por* c *temos* $acx+bcy=c$, *como* $a \mid acx$ *e de* $a \mid bc \Rightarrow a \mid bcy$, *logo* $a \mid (acx+bcy) \Rightarrow a \mid c$;

2. *De* $mdc(a,b)=1$ *temos que existem* x,y *inteiros tal que* $ax+by=1$, *multiplicando tudo por* c *temos* $acx+bcy=c$, *agora de* $a \mid c$ *e* $b \mid c$ *temos que existem* k,t *inteiros tal que* $c=ak$ *e* $c=bt$, *logo temos* $acx+bcy=abtx+baky=ab(tx+ky)$, *como* $ab \mid ab(tx+ky) \Rightarrow ab \mid c$;

3. ($\Rightarrow$) *Pelo algoritmo da divisão temos que* $c=q\cdot mmc(a,b)+r$ *para algum* q,r *inteiros e com* $0 \leq r < mmc(a,b)$. *Então de* $a \mid c$ *e* $a \mid mmc(a,b) \Rightarrow a \mid r$ *e* $b \mid c$ *e* $b \mid mmc(a,b) \Rightarrow b \mid r$, *temos que* r *é um múltiplo comum de* a *e* b *com* $r < mmc(a,b)$, *logo* $r=0$. *Portanto* $c=q\cdot mmc(a,b) \Rightarrow mmc(ab) \mid c$.
($\Leftarrow$) *Se* $mmc(a,b) \mid c$ *então* $c=q\cdot mmc(a,b)$ *para algum* q *inteiro, como* $a \mid mmc(a,b)$ *e* $b \mid mmc(a,b)$ *então* $a \mid c$ *e* $b \mid c$;

4. ($\Rightarrow$) *Se* $mdc(a,c)=1$ *então existem* x_1,y_1 *inteiros tais que* $ax_1+cy_1=1$ *e se* $mdc(b,c)=1$ *então existem* x_2,y_2 *inteiros tais que* $bx_2+cy_2=1$, *logo* $(ax_1+cy_1)(bx_2+cy_2)=1 \Rightarrow ab(x_1x_2)+c(ax_1y_2+by_1x_2+cy_1y_2)=1 \Rightarrow mdc(ab,c)=1$.
($\Leftarrow$) *Se* $mdc(ab,c)=1$ *então existem* x,y *inteiros tais que* $abx+cy=1$, *logo temos* $a(bx)+c(y)=1$ *e* $b(ax)+c(y)=1$, *portanto* $mdc(a,c)=1$ *e* $mdc(b,c)=1$.

□

Observação 4. *A proposição anterior pode ser generalizada:*

1. *se* $a \mid b_1\cdot b_2\cdot \ldots \cdot \cdots \cdot b_r\cdot c$ *e* $mdc(a,b_i)=1$ *para todo* i *com* $1 \leq i \leq r$ *então* $a \mid c$;

2. *se* $a_1 \mid c, a_2 \mid c, \ldots, a_r \mid c$ *e* $mdc(a_i,a_j)=1$ *para todo* $i \neq j$ *com* $1 \leq i,j \leq r$ *então* $a_1\cdot a_2\cdot \ldots \cdot a_r \mid c$;

3. *se* $a_1 \mid c, a_2 \mid c, \ldots, a_r \mid c$ *então* $m=mmc(a_1,a_2,\ldots,a_r) \mid c$. *Vale a recíproca;*

4. *se* $mdc(a_1,c)=mdc(a_2,c)=\ldots=mdc(a_r,c)=1$ *então* $mdc(a_1\cdot a_2\cdot \ldots \cdot a_r,c)=1$. *Vale a recíproca.*

Proposição 48. *Sejam* $a,b,c,m \in \mathbb{Z}$ *com* $m>0$. *Temos as seguintes condições:*

1. *se* $mdc(a,b)=d$ *então* $mdc\left(\frac{a}{d},\frac{b}{d}\right)=1$;

2. $mdc(a+bc,b)=mdc(a,b)$;

3. *se* $a \mid c, b \mid c$ *então* $\dfrac{ab}{mdc(a,b)} \mid c$.

Demonstração:

1. *Se* $mdc(a,b) = d$ *temos* $d \mid a$ *e* $d \mid b$ *então existem* r, s *inteiros tais que* $a = rd$ *e* $b = sd$, *como* d *contêm todos os fatores em comum de* a *e* b *temos que* r *e* s *são coprimos. Portanto* $mdc\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = mdc\left(\dfrac{rd}{d}, \dfrac{sd}{d}\right) = mdc\,(r,s) = 1$;

2. ($\Rightarrow$) *De* $mdc(a+bc, b) = d$ *temos que* $d \mid (a+bc)$ *e* $d \mid b \Rightarrow d \mid bc$ *então* $d \mid (a+bc) - bc \Rightarrow d \mid a$. *Portanto* $mdc(a,b) = d$.

   ($\Leftarrow$) *De* $mdc(a,b) = d$ *temos* $d \mid a$ *e* $d \mid b \Rightarrow d \mid bc$ *para* c *inteiro, então* $d \mid a+bc$. *Portanto* $mdc(a+bc, d) = d$.

3. *Pela proposição 47 temos que se* $a \mid c$ *e* $b \mid c$ *então* $mmc(a,b) \mid c$. *Pela proposição 28 temos que* $mmc(a,b) = \dfrac{ab}{mdc(a,b)}$, *portanto* $\dfrac{ab}{mdc(a,b)} \mid c$.

□

Proposição 49. *Sejam* $a, b \in \mathbb{Z}$ *não nulos. Então* $mdc(a,b)mmc(a,b) = |ab|$ *ou* $mdc(a,b) = \dfrac{|ab|}{mmc(a,b)}$

Demonstração: *Foi provada na proposição 28.* □

Observação 5. *A proposição anterior pode ser generalizada: se* $a_1, a_2, a_3, ..., a_n$ *são inteiros positivos dois a dois relativamente primos, então* $mmc(a_1, a_2, a_3, \ldots, a_n) = a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_n$.

Demonstração: Pela proposição 26 temos $mdc(a_1, a_2, a_3, \ldots, a_n) = mdc(a_1, \ldots, (a_{n-1}, a_n))$ e pela proposição 30 temos $mmc(a_1, a_2, a_3, \ldots, a_n) = mmc(a_1, \ldots, (a_{n-1}, a_n))$. Pela proposição 28 temos $mmc(a_1, \ldots, (a_{n-1}, a_n)) \cdot mdc(a_1, \ldots, (a_{n-1}, a_n)) = |a_1 \cdot (\ldots (a_{n-1} \cdot a_n))|$. Como $a_1, a_2, a_3, ..., a_n$ são inteiros positivos dois a dois coprimos então $mdc(a_1, \ldots, (a_{n-1}, a_n)) = 1$. Portanto $mmc(a_1, \ldots, (a_{n-1}, a_n)) \cdot 1 = a_1 \cdot (\ldots (a_{n-1} \cdot a_n)) \Rightarrow mmc(a_1, a_2, a_3, \ldots, a_n) = a_1 \cdot a_2 \cdot \ldots a_n$. □

4.1 Sistemas completos de resíduos módulo m

Definição 10. *Um sistema completo de resíduos módulo* m *é um conjunto de* m *inteiros tal que todo inteiro é congruente módulo* m *a um único inteiro desse conjunto.*

Observação 6. *Desta forma*

1. *indicamos um sistema completo de resíduos módulo* m *por* $\boldsymbol{SCR}_m$;

2. *o conjunto* $\{r_1, r_2, r_3, \ldots, r_m\}$ *é* $\boldsymbol{SCR}_m$ *módulo* m *se cada* $r_i : 1 \leq i \leq m$ *é um representante de cada classe de equivalência módulo* m*. Equivalentemente, podemos dizer que quaisquer dois desses números, diferentes entre sí, não são congruentes módulo* m*.*

Exemplo 34. *O conjunto* $\{0, 1, 2, 3, \ldots, m-1\}$ *é um* $\boldsymbol{SCR}_m$*.*

Exemplo 35. *O conjunto* $\{4, -3, 10, -9\}$ *é um* $\boldsymbol{SCR}_4$*.*

Proposição 50. *Se* $a, b, c, m \in \mathbb{Z}$ *com* $m > 0$ *e* $a \equiv b(\mod m)$*, então*

1. $a + c \equiv b + c \pmod{m}$*;*
2. $a - c \equiv b - c \pmod{m}$*;*
3. $ac \equiv bc \pmod{m}$*.*

Demonstração:

1. *De* $a \equiv b \pmod{m} \Rightarrow m \mid a - b = m \mid (a + c) - (b + c) \Rightarrow a + c \equiv b + c \pmod{m}$*;*
2. *De* $a \equiv b \pmod{m} \Rightarrow m \mid a - b \Rightarrow m \mid (a - c) - (b - c) \Rightarrow a - c \equiv b - c \pmod{m}$*;*
3. *De* $a \equiv b \pmod{m} \Rightarrow m \mid a - b \Rightarrow m \mid (a - b)c \Rightarrow m \mid ac - bc \Rightarrow ac \equiv bc \pmod{m}$*.*

□

Proposição 51. *Se* $a, b, c, m \in \mathbb{Z}$ *com* $m > 0$*,* $mdc(c, m) = d$ *e* $a \cdot c \equiv b \cdot c \mod m$*, então* $a \equiv b \pmod{\frac{m}{d}}$

Demonstração: *De* $mdc(c, m) = d$ *temos* $d \mid c$ *e* $d \mid m$ *então existem* r, s *inteiros tais que* $c = dr$ *e* $m = ds$*, com* r, s *coprimos. De* $ac \equiv bc \pmod{m}$ *então* $m \mid (a-b)c \Rightarrow ds \mid (a-b)dr \Rightarrow s \mid (a-b)s \Rightarrow a \equiv b \mod s \Rightarrow a \equiv b \pmod{\frac{m}{d}}$*.* □

Corolário 52. *Se* $a, b, c, m \in \mathbb{Z}$ *com* $m > 0$*,* $mdc(c, m) = 1$ *e* $ac \equiv bc \pmod{m}$ *então* $a \equiv b \pmod{m}$*.*

Demonstração: *Aplicação direta da proposição 51, basta fazer* $d = 1$*.* □

Exemplo 36. *Seja* m *um inteiro positivo ímpar. Mostre que o conjunto*

$$\left\{-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \frac{m-3}{2}, \frac{m-1}{2}\right\}$$

dos menores resíduos módulo m *é um* $\boldsymbol{SCR}_m$*.*

Demonstração: $m = 2k + 1$ *com* $k \in \mathbb{Z}_+$ *então temos o conjunto* $\{-k, -(k-1), \ldots, -1, 0, 1, (k-1), k\}$ *é um conjunto* $\boldsymbol{SCR}_{2k+1}$*.* □

Proposição 53. *Se $a, b, c, m \in \mathbb{Z}$ com $m > 0$, $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$ então*

1. $a + c \equiv b + d \pmod{m}$;
2. $a - c \equiv b - d \pmod{m}$;
3. $ac \equiv bd \pmod{m}$.

Demonstração:

1. $\begin{cases} a \equiv b \pmod{m} & \Rightarrow m \mid a - b \\ c \equiv d \pmod{m} & \Rightarrow m \mid c - d \end{cases}$
$\Rightarrow m \mid (a - b) + (c - d) \Rightarrow m \mid (a + c) - (b + d) \Rightarrow a + c \equiv b + d \pmod{m}$;

2. $\begin{cases} a \equiv b \pmod{m} & \Rightarrow m \mid a - b \\ c \equiv d \pmod{m} & \Rightarrow m \mid c - d \end{cases}$
$\Rightarrow m \mid (a - b) - (c - d) \Rightarrow m \mid (a - c) - (b - d) \Rightarrow a - c \equiv b - d \pmod{m}$;

3. $\begin{cases} a \equiv b \pmod{m} & \Rightarrow m \mid a - b \quad \Rightarrow m \mid (a - b)c \\ c \equiv d \pmod{m} & \Rightarrow m \mid c - d \quad \Rightarrow m \mid b(c - d) \end{cases}$
$\Rightarrow m \mid (a - b)c + b(c - d) \Rightarrow m \mid ac - bd \Rightarrow ac \equiv bd \pmod{m}$.

□

Proposição 54. *Se $\{r_1, r_2, \ldots, r_m\}$ é um $\boldsymbol{SCR}_m$ e $a > 0$ um inteiro com $mdc(a, m) = 1$ então*

$$\{ar_1 + b, ar_2 + b, \ldots, ar_m + b\}$$

também é um $\boldsymbol{SCR}_m$ para qualquer $b \in \mathbb{Z}$.

Demonstração:

- *Nenhum dos inteiros $\{ar_1 + b, ar_2 + b, \ldots ar_m + b\}$ são congruentes módulo m. De fato, se $ar_i + b \equiv ar_j + b \mod m$ pela proposição 50, temos $ar_i \equiv ar_j \mod m$. Como $mdc(a, m) = 1$ pelo corolário 52 temos que $r_i \equiv r_j \mod m$, o que não é possível, visto que por hipótese $\{r_1, r_2, \ldots, r_m\}$ é um $\boldsymbol{SCR}_m$, ou seja, $r_i \not\equiv r_j \mod m$. Portanto $i = j$.*

- *Como o conjunto de inteiros $\{ar_1 + b, ar_2 + b, \ldots, ar_m + b\}$ possui m inteiros módulo m e existem m classes de congruências módulo m, dadas por $\{[0], [1], [2], \ldots, [m - 1]\}$ segue que estes inteiros formam um $\boldsymbol{SCR}_m$*

□

Proposição 55. *Se $a, b, k, m \in \mathbb{Z}$ com $k > 0$, $m > 0$ e $a \equiv b \pmod{m}$, então $a^k \equiv b^k \pmod{m}$.*

Demonstração: *Como $a \equiv b \pmod{m} \Leftrightarrow m \mid (a-b)$. Mas*

$$a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \ldots + ab^{k-2} + b^{k-1}),$$

ou seja, $(a-b) \mid (a^k - b^k)$ o que implica que $a^k \equiv b^k \pmod{m}$. □

Proposição 56. *Se $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$, com a, b inteiros e $m_1, m_2, \ldots, m_k$ inteiros positivos, então $a \equiv b \pmod{mmc(m_1, m_2, \ldots, m_k)}$.*

Demonstração:

Por hipótese $m_1 \mid (a-b), m_2 \mid (a-b), \ldots, m_k \mid (a-b)$ pela generalização da proposição 47 temos que $mmc(m_1, m_2, \ldots, m_k) \mid (a-b)$, consequentemente $a \equiv b \pmod{mmc(m_1, m_2, \ldots, m_k)}$ □

Corolário 57. *Se $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$, com a, b inteiros e $m_1, m_2, \ldots, m_k$ inteiros positivos tai que $mdc(m_i, m_j) = 1$ para todo $i \neq j$, então $a \equiv b \pmod{m_1 \cdot m_2 \cdot \ldots m_k}$.*

Demonstração: *Como $mdc(m_i, m_j) = 1$ para todo $i \neq j$, pela generalização da proposição 49 temos $mmc(m_1, m_2, \ldots, m_k) = m_1 \cdot m_2 \cdot \ldots \cdot m_k$. Pela proposição 56 segue que $a \equiv b \pmod{m_1 \cdot m_2 \cdot \ldots \cdot m_k}$.* □

4.2 Congruências lineares

Uma congruência linear é uma equação da forma $ax \equiv b \mod m$ onde $a, b, m \in \mathbb{Z}$ com $a \neq 0, m > 0$ e x uma variável em $\mathbb{Z}$.

Seja $u \in \mathbb{Z}$ uma solução de $ax \equiv b \pmod{m}$, ou seja, $au \equiv b \pmod{m}$, pelo Algoritmo da Divisão.

$$\begin{cases} u = mq + r_0 \text{ com } 0 \leq r_0 < m \\ au = amq + ar_0, \text{ como } amq \equiv 0 \pmod{m} \\ au \equiv ar_0 \mod m \equiv b \pmod{m} \end{cases}$$

Logo r_0 também é uma solução da congruência, ou seja, representa a mesma solução de $ax \equiv b \pmod{m}$.

Exemplo 37. *Considere congruência $2x \equiv 3 \pmod{5}$. Note que $u = 4$ é uma solução, logo*

$$r_0 = -5t + 4 = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}$$

representam a mesma solução.

Proposição 58. *Se $a, b, m \in \mathbb{Z}$ com $m > 0, a \neq 0$ e $d = mdc(a, m)$:*

1. *$ax \equiv b \pmod{m}$ tem solução, se e somente se $d \mid b$;*

2. *Se $d \mid b$ e x_0 é uma solução particular de $ax + b$, então temos exatamente d soluções, as quais são duas a duas incongruentes e da forma $x = x_0 + \left(\frac{m}{d}\right) t$ para $t = 0, 1, 2, 3, \ldots, d-1$.*

Demonstração:

1. *Seja x uma solução de $ax \equiv b \pmod{m} \Leftrightarrow ax - my = b$ para algum $y \in \mathbb{Z}$. Sabemos que a equação diofantina $ax \equiv b \pmod{m}$ tem solução $\Leftrightarrow d = mdc(a, m) \mid b$.*

2. *Lembramos também que se (x_0, y_0) é uma solução particular de $ax - my = b$, então $x = x_0 + \left(\frac{m}{d}\right) t$ e $y = y_0 + \left(\frac{a}{d}\right) t$ onde, $t \in \mathbb{Z}$ são todas as soluções (infinitas soluções). Logo $x = x_0 + \left(\frac{m}{d}\right) t$ para $t \in \mathbb{Z}$ são todas as soluções $ax \equiv b \pmod{m}$. Quantas soluções incongruentes existem? Basta só descobrir sob que condições duas destas soluções $x_1 = x_0 + \left(\frac{m}{d}\right) t_1$ e $x_2 = x_0 + \left(\frac{m}{d}\right) t_2$ são congruentes módulo m, ou seja, para $x_0 + \left(\frac{m}{d}\right) t_1 \equiv x_0 + \left(\frac{m}{d}\right) t_2 \mod m$ temos que $\left(\frac{m}{d}\right) t_1 \equiv \left(\frac{m}{d}\right) t_2 \mod m$. Como $\left(\frac{m}{d}\right) \mid m$, temos $\left(\frac{m}{d}, m\right) = \frac{m}{d}$ logo $t_1 \equiv t_2 \mod \frac{m}{m/d}$, ou ainda $t_1 \equiv t_2 \mod d$. Portanto as soluções incongruente são obtidas tomando-se $x = x_0 + \left(\frac{m}{d}\right) t$ onde t percorre um sistema completo de resíduos módulo d. As soluções são da forma $x = x_0 + \left(\frac{m}{d}\right) t$ para $t = 0, 1, 2, 3, \ldots, d-1$.*

□

Exemplo 38. *Encontre todas as soluções de $9x \equiv 12 \pmod{15}$. Note que $d = mdc(15, 9) = 3 \mid 12$, logo temos 3 soluções incongruentes. Encontrando uma solução particular x_0:*

$$\begin{cases} 15 = 9 \cdot 1 + 6 \\ 9 = 6 \cdot 1 + 3 \\ 6 = 3 \cdot 2 \end{cases} ; \begin{cases} 3 = 9 - 6 \cdot 1 \\ 3 = 9 - (15 - 9 \cdot 1) \cdot 1 \\ 3 = 9 \cdot 2 - 15 \cdot 1 \\ 12 = 9 \cdot 8 - 15 \cdot 4 \end{cases} .$$

Todas as soluções são dadas por $x = 8 + \frac{15}{3} t = 8 + 5t$. Para $t = 0, 1, 2$, temos as três solões incongruentes, ou seja, $\{x = 8, x = 13, x = 18\}$, ou ainda,

$$\begin{cases} x \equiv 8 \pmod{15} \\ x \equiv 13 \pmod{15} \\ x \equiv 18 \equiv 3 \pmod{15}. \end{cases}$$

Corolário 59. *Sejam $a, m \in \mathbb{Z}$ com $m > 0$.*

1. *Se $d = mdc(a, m) = 1$ a congruência $ax \equiv 1 \pmod{m}$ tem solução única $x \pmod{m}$;*

2. *Se $d = mdc(a, m) \neq 1$ a congruência $ax \equiv 1 \pmod{m}$ não tem solução.*

Demonstração: *Segue da proposição 55* □

Definição 11. *Sejam dado $a, m \in \mathbb{Z}$ com $m > 0$ e $d = mdc(a, m) = 1$. Uma solução da congruência $ax \equiv 1 \pmod{m}$ é chamada de inverso de a módulo m.*

Exemplo 39. *Considere congruência $7x \equiv 1 \pmod{31}$ Note que esta congruência tem solução única e*

$$\begin{cases} 31 = 4 \cdot 7 + 3 \\ 7 = 2 \cdot 3 + 1 \\ 2 = 2 \cdot 1 \end{cases} ; \begin{cases} 1 = 7 - 2 \cdot 3 \\ 1 = 7 - 2 \cdot (31 - 4 \cdot 7) \\ 1 = 9 \cdot 7 - 2 \cdot 31 \end{cases}$$

Temos que $x_0 = 9$ e todas as soluções são dada por $x = 9 + 31t$ para $t = 0$, ou seja, $\{x = 9\}$ ou $x \equiv 9 \pmod{31}$. Que dizer que 9 e todos os inteiros $x \equiv 9 \pmod{31}$ são inversos de 7 módulo 31.

Proposição 60. *Seja p um número primo. O inteiro positivo a é o seu próprio inverso módulo p, se e somente se, $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$.*
Demonstração: *Se a é o seu próprio inverso módulo p, então $a^2 = a \cdot a \equiv 1 \pmod{p} \Rightarrow p \mid (a^2 - 1) = (a + 1)(a - 1) \Rightarrow p \mid (a + 1)$ ou $p \mid (a - 1) \Rightarrow a \equiv -1 \pmod{p}$ ou $a \equiv 1 \pmod{p}$. Se $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p} \Rightarrow a^2 \equiv 1 \pmod{p} \Rightarrow$ o inverso de a é o próprio a* □

Definição 12. *Um sistema reduzido de resíduos módulo m é um conjunto de inteiros formado por todos os elementos de um SCR_m que são primos com m.*

Observação 7. *Desta forma*

1. *Indicamos um sistema reduzido de resíduos módulo m por $\boldsymbol{SRR}_m$;*

2. *Um $\boldsymbol{SRR}_m$ é um conjunto de inteiros $\{r_1, r_2, r_3, \ldots, r_s\}$ tai que para todo $i = 1, 2, 3, \ldots, s$*

   (a) $r_1 \not\equiv r_j$, se $i \neq j$;

   (b) Para cada $n \in \mathbb{Z}$ existe um r_i tal que $n \equiv r_i \pmod{m}$;

   (c) $mdc(r_i, m) = 1$.

Exemplo 40. *O conjunto de inteiros $\{1, 3, 5, 7\}$ forma um $\boldsymbol{SRR}_{10}$. E conjunto de inteiros $\{1, 5, 7, 11\}$ forma um $\boldsymbol{SRR}_{12}$.*

Exemplo 41. *Encontre um* $\boldsymbol{SRR}_{15}$ *formado somente por primos. Note que* $\{1, 2, 4, 7, 8, 11, 13, 14\}$ *forma um* $\boldsymbol{SRR}_{15}$*. Trocando os primos, obtemos* $\{31, 2, 19, 7, 23, 11, 13, 29\}$*.*

4.3 Teorema chinês dos restos

Enunciaremos um importante resultado, o teorema chinês dos restos, mostraremos que é possível a sua inserção na educação básica como alternativa na resolução de problemas.

Para $a_1, a_2, a_3, \ldots, a_r, c \in \mathbb{Z}$, se $a_1 \mid c, a_2 \mid c, \ldots, a_r \mid c$, então $m = mmc(a_1, a_2, \ldots, a_r) \mid c$.

Proposição 61. *Se* $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$ *com* a, b *inteiros e* $m_1, m_2, \ldots, m_k$ *inteiros positivos, então* $a \equiv b \pmod{mmc(m_1, m_2, \ldots, m_k)}$*.*

Demonstração: *Por hipótese* $m_1 \mid (a-b), m_2 \mid (a-b), \ldots, m_k \mid (a-b)$ *pela observação anterior temos* $mmc(m_1, m_2 \ldots, m_k) \mid (a-b)$*, consequentemente* $a \equiv b \pmod{mmc(m_1, m_2 \ldots, m_k)}$*.* □

Corolário 62. *Se* $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$ *com* a, b *inteiros e* $m_1, m_2, \ldots, m_k$ *inteiros positivos, tais que* $mdc(m_i, m_j) = 1$ *para todo* $i \neq j$*, então* $a \equiv b \pmod{(m_1 \cdot m_2 \cdot \ldots \cdot m_k)}$*.*

Demonstração: *Como* $mdc(m_i, m_j) = 1$ *para todo* $i \neq j$*, temos:*

$$mmc(m_1, m_2, \ldots, m_k) = m_1 \cdot m_2 \cdot \ldots \cdot m_k.$$

Pela proposição 61 segue que $a \equiv b \pmod{(m_1 \dot{m}_2 \cdot \ldots \cdot m_k)}$*.* □

Teorema 63. *(Teorema chinês dos restos) Sejam* $m_1, m_2, \ldots, m_r$ *inteiros positivos tais que* $d = mdc(m_i, m_j) = 1$*, sempre que* $i \neq j$ *e* $a_1, a_2, \ldots, a_r$ *inteiros. Então o sistema de congruências lineares*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \qquad \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

tem solução única módulo $m = m_1 \cdot m_2 \cdot \ldots \cdot m_r$*.*

Demonstração: *Nosso objetivo é construir uma solução simultânea para o sistema de congruências. Consideremos o conjunto de r números* $M_k = \left(\frac{m}{m_k}\right) = m_1 \cdot m_2 \cdot \ldots \cdot m_{k-1} \cdot m_{k+1} \cdot \ldots \cdot m_r$

para $k = 1, 2, \ldots, r$. *Como o* $d = mdc(m_i, m_j) = 1$ *para* $i \neq j$ *temos*

$$\begin{aligned} mdc(m_1, m_k) = mdc(m_2, m_k) = \ldots = mdc(m_{k-1}, m_k) \\ = mdc(m_{k+1}, m_k) = \ldots = mdc(m_r, m_k) = 1 \end{aligned}$$

o que implica

$$mdc(m_1 \cdot m_2 \cdot \ldots \cdot m_{k-1} \cdot m_{k+1} \cdot \ldots \cdot m_r, m_k) = mdc(M_k, m_k) = 1$$

logo existem inteiros u, v *tais que* $u \cdot M_k + v \cdot m_k = 1$, *o que significa que existe* $u = s_k$ *tal que*

$$s_k \cdot M_k \equiv 1 \pmod{m_k}.$$

Como $mdc(M_k, m_k) = 1 \mid 1$ *segue que* $s_k \cdot M_k \equiv 1 \pmod{m_k}$ *tem solução única* y_k, *ou seja,*

$$M_y \cdot y_k \equiv 1 \pmod{m_k}.$$

Então

$$a_k \cdot M_k \cdot y_k \equiv a_k \pmod{m_k}$$

Uma vez que $m_k \mid M_j$ *quando* $j \neq k$, *temos*

$$M_j \equiv 0 \pmod{m_k}, \text{ então } a_j \cdot M_j \cdot y_j \equiv 0 \pmod{m_k}$$

para todos os termos, exceto o k-ésimo. Portanto $x = a_k \cdot M - k \cdot y_k \equiv a_k \pmod{m_k}$, *para* $k = 1, 2, \ldots, r$, *então a soma*

$$x = a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 + \ldots a_r \cdot M_r \cdot y_r$$

é uma solução do sistema de r congruências. A seguir mostraremos que quaisquer duas soluções do sistema de r congruências são congruentes módulo m. Sejam x_0 *e* x_1 *soluções do sistema. Então para cada k, segue que* $x_0 \equiv x_1 \equiv a_k \pmod{m_k}$ *isto implica que* $m_k \mid (x_0 - x_1)$. *Mas* $x_0 \equiv x_1 \pmod{m_1, x_0} \equiv x_1 \pmod{m_2, \ldots, x_0} \equiv x_1 \pmod{m_k}$, *então pelo corolário 62 segue que*

$$x_0 \equiv x_1 \pmod{mmc(m_1, m_2, \ldots, m_k)}.$$

Como $d = mdc(m_i, m_j) = 1$ *sempre que* $i \neq j$ *temos que*

$$mmc(m_1, m_2, \ldots, m_k) = m_1 \cdot m_2 \cdot \ldots \cdot m_k = m,$$

logo $m \mid (x_0 - x_1)$*, ou seja,* $x_0 \equiv x_1 \pmod{m}$*, o que significa que as soluções são únicas módulo* m*.* □

Exemplo 42. *Resolva o sistema*

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases}$$

Note que $m = 3 \cdot 5 \cdot 7 = 105$ *e*

$$\begin{cases} M_1 = \dfrac{105}{3} = 35 \\ M_2 = \dfrac{105}{5} = 21 \\ M_3 = \dfrac{105}{7} = 15 \end{cases} ; \begin{cases} M_1 y_1 \equiv 1 \pmod 3 \\ M_2 y_2 \equiv 1 \pmod 5 \\ M_3 y_3 \equiv 1 \pmod 7 \end{cases} ; \begin{cases} 35 y_1 \equiv 1 \pmod 3 \\ 21 y_2 \equiv 1 \pmod 5 \\ 15 y_3 \equiv 1 \pmod 7 \end{cases} ; \begin{cases} 2 y_1 \equiv 1 \pmod 3 \\ y_2 \equiv 1 \pmod 5 \\ y_3 \equiv 1 \pmod 7 \end{cases} ; \begin{cases} y_1 \equiv 2 \pmod 3 \\ y_2 \equiv 1 \pmod 5 \\ y_3 \equiv 1 \pmod 7 \end{cases}$$

$$x = a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 + a_3 \cdot M_3 \cdot y_3 = 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 = 157 \equiv 52 \pmod{105}$$

Exemplo 43. *Resolva a equação* $17x \equiv 9 \pmod{276}$ *Note que* $276 = 2^2 \cdot 3 \cdot 23 = 3 \cdot 4 \cdot 23$

$$\begin{cases} 17x \equiv 9 \pmod 3 \\ 17x \equiv 9 \pmod 4 \\ 17x \equiv 9 \pmod{23} \end{cases} ; \begin{cases} 2x \equiv 0 \pmod 3 \\ x \equiv 1 \pmod 4 \\ 17x \equiv 9 \pmod{23} \end{cases}$$

Como $d = mdc(17, 23) = 1$ *a congruência* $17x \equiv 9 \pmod{23}$ *tem uma única solução que pode ser obtida escrevendo* $d = mdc(17, 23) = 1 = -4(17) + 3(23)$*, ou seja,* $-4(17) \equiv 1 \pmod{23} \Rightarrow -36(17) \equiv 9 \pmod{23}$*, finalmente temos* $10(17) \equiv 9 \pmod{23}$*. Então basta resolver o sistema de congruências*

$$\begin{cases} x \equiv 0 \pmod 3 \\ x \equiv 1 \pmod 4 \\ x \equiv 10 \pmod{23} \end{cases}$$

$$\begin{cases} M_1 = \dfrac{276}{3} = 92 \\ M_2 = \dfrac{276}{4} = 69 \\ M_3 = \dfrac{276}{23} = 12 \end{cases} ; \begin{cases} M_1 y_1 \equiv 1 \pmod 3 \\ M_2 y_2 \equiv 1 \pmod 4 \\ M_3 y_3 \equiv 1 \pmod{23} \end{cases} ; \begin{cases} 92 y_1 \equiv 1 \pmod 3 \\ 69 y_2 \equiv 1 \pmod 4 \\ 12 y_3 \equiv 1 \pmod{23} \end{cases} ; \begin{cases} 2 y_1 \equiv 1 \pmod 3 \\ y_2 \equiv 1 \pmod 4 \\ 12 y_3 \equiv 1 \pmod{23} \end{cases} ; \begin{cases} y_1 \equiv 2 \pmod 3 \\ y_2 \equiv 1 \pmod 4 \\ y_3 \equiv 2 \pmod{23} \end{cases}$$

$$x = a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 + a_3 \cdot M_3 \cdot y_3 = 0 \cdot 92 \cdot 2 + 1 \cdot 69 \cdot 1 + 10 \cdot 12 \cdot 2 = 309 \equiv 23 \pmod 2 76$$

4.4 O teorema de Wilson

Teorema 64. *(Teorema de Wilson) Se p é um número primo, então*

$$(p-1)! \equiv -1 \pmod{p}$$

Demonstração: *Se $p = 2$, então $(2-1)! \equiv -1 \pmod 2$.*
Se $p > 2$ a congruência $ax \equiv 1 \pmod p$ possui solução única para todo $a \in \{1, 2, 3, \ldots, p-1\}$, pois $mdc(a, p) = 1$, ou seja, existe um único $z \in \{1, 2, 3, \ldots, p-1\}$ tal que $a \cdot z \equiv 1 \pmod p$, mais precisamente todo $a \in \{1, 2, 3, \ldots, p-1\}$ possui inverso. Por outro lado, para $a \in \{1, 2, 3, \ldots, p-1\}$ tal que $a^2 \equiv 1 \pmod p$ são aqueles tais que $a \equiv 1 \pmod p$ ou $a \equiv -1 \pmod p$, o que implica em $a \equiv 1 \pmod p$ ou $a \equiv p-1 \pmod p$. Logo os inversos dos elementos 1 e $p-1$ são eles próprios. Portanto agrupando os elementos $\{2, 3, \ldots, p-2\}$ em pares, onde cada par é congruente a 1 módulo p, obtemos

$$\begin{aligned}(2 \cdot 3 \cdot \ldots \cdot (p-2)) &\equiv 1 \pmod p \\ (1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-2) \cdot (p-1)) &\equiv 1 \cdot (p-1) \pmod p \\ (p-1)! &\equiv -1 \pmod p.\end{aligned}$$

□

4.4.1 Vale a reciproca do teorema de Wilson

Proposição 65. *Se n é um inteiro positivo tal que $(n-1)! \equiv -1 \pmod n$, então n é primo.*
Demonstração: *Suponha que n é composto e que $(n-1)! \equiv -1 \pmod n$ então $n = a \cdot b$ com $1 < a < n$ e $1 < b < n$ e que $(n-1)! \equiv -1 \pmod n$, ou seja, $a \mid n$ e $n \mid (n-1)! + 1$ o que implica que $a \mid (n-1)! + 1$. Por outro lado $a < n$, assim a é um dos divisores de $(n-1)!$ o que implica $(n-1)! \equiv 0 \pmod a$. Então $(n-1)! \equiv 0 \pmod a$ e $(n-1)! \equiv -1 \pmod a$, logo $1 \equiv 0 \pmod a$ o que é uma contradição, pois $a > 1$. Portanto n é primo.* □

Exemplo 44. *Para $n = 6$ temos $(6-1)! = 5! = 120 \equiv 0 \pmod 6$, logo 6 não é primo.*

4.5 O teorema de Fermat

Teorema 66. *(Pequeno teorema de Fermat) Se p é um número primo e $a \in \mathbf{Z}$ com $mdc(a,p) = 1$ então $a^{p-1} \equiv 1 \pmod{p}$.*

Demonstração: *Consideremos os $p-1$ inteiros múltiplos de a:*

$$1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a$$

i) Nenhum desses inteiros são divisíveis por p, ou seja, congruentes a $0 \mod p$. De fato, se $p \mid j \cdot a \Rightarrow p \mid j$, pois $mdc(a,p) = 1$, o que é impossível visto que $1 \leq j \leq p-1$.

ii) Quaisquer dois desses inteiros são incongruentes $\pmod{p}$. De fato, se fossem congruentes, teríamos

$$j \cdot a \equiv k \cdot a \pmod{p} \text{ com } j \neq k.$$

Digamos $1 \leq j < k \leq p-1$. Como $mdc(a,p) = 1$, teríamos $j \equiv k \pmod{p}$, o que é impossível, pois j e k são inteiros positivos menores do que p (outro modo de argumentar: se $j \cdot a \equiv k \cdot a \pmod{p}$ com $j \neq k$ nos garante que $j \equiv k \pmod{p}$ e portanto $j = k$, o que é impossível).

Por (i) e (ii) cada um dos inteiros

$$1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a$$

são congruentes módulo p a somente um dos inteiros

$$1, 2, \ldots, (p-1)$$

em uma certa ordem. O produto desses inteiros módulo p

$$1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a \equiv 1, 2, \ldots, (p-1) \pmod{p}$$
$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

Como $mdc((p-1)!, p) = 1$, pois p primo $p \nmid (p-1)!$, temos que

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

□

Exemplo 45. *Para $p = 7$ e $a = 3$, temos*

$$(1 \cdot 3) \cdot (2 \cdot 3) \cdot (3 \cdot 3) \cdot (4 \cdot 3) \cdot (5 \cdot 3) \cdot (6 \cdot 3) \equiv 3 \cdot 6 \cdot 2 \cdot 5 \cdot 1 \cdot 4 \pmod 7$$
$$3^6 \cdot (6!) \equiv 6! \pmod 7$$
$$3^6 \equiv 1 \pmod 7$$

Corolário 67. *Se p é primo e a um inteiro positivo, então $a^p \equiv a \pmod p$.*

Demonstração:

i) Se $p \nmid a$, pelo ***PTF***

$$a^{p-1} \equiv 1 \pmod p$$
$$a \cdot a^{p-1} \equiv a \cdot 1 \pmod p$$
$$a^p \equiv a \pmod p.$$

ii) Se $p \mid a$, então $a \equiv 0 \pmod p$ e $a^p \equiv 0 \pmod p$. Portanto, temos sempre $a^p \equiv a \equiv 0 \pmod p$.

□

Exemplo 46. *Mostre que $5^{38} \equiv 4 \pmod{11}$. Pelo* ***PTF*** *$5^{10} \equiv 1 \pmod{11}$.*

$$5^{38} = 5^{10 \cdot 3 + 8} = (5^{10})^3 \cdot (5^2)^4 \equiv 1^3 \cdot 3^4 \pmod{11}$$
$$\equiv 81 \pmod{11} \equiv 4 \pmod{11}.$$

Exemplo 47. *Moste que 91 não é primo. Pelo corolário anterior, basta encontrar um inteiro a tal que $a^{91} \not\equiv a \pmod{91}$ ou $a^{90} \not\equiv 1 \pmod{91}$. Note que $2^{90} = (2^{10})^9 = (1024)^9 \equiv 23^9 \equiv 64^3 \equiv 64 \pmod{91}$.*

Exemplo 48. *Prove que $(1835)^{1910} + (1986)^{2061} \equiv 0 \pmod 7$. Seja $x = (1835)^{1910} + (1986)^{2061}$. Note que $(1835) \equiv \pmod 7$ e $(1986) \equiv 5 \pmod 7$. Assim $x \equiv 1 + 5^{2061} \pmod 7$. Observe também que $(2061) \equiv 3 \pmod 6$, então $5^{2061} = 5^{6 \cdot q + 3} = 5^{6q} \cdot 5^3$. Pelo* ***PTF*** *$5^6 \equiv 1 \pmod 7$, portanto*

$$5^{2061} \equiv 1 \cdot 5^3 \pmod 7 \equiv 125 \pmod 7 \equiv 6 \pmod 7$$
$$x \equiv 1 + 6 \pmod 7 \equiv 7 \pmod 7 \equiv 0 \pmod 7$$

Exemplo 49. *Calcule* $50^{250} \pmod 6$. *Como* $83 \nmid 50$. *Pelo* ***PTF*** $50^{82} \equiv 1 \pmod{83}$, *logo*

$$50^{250} = 50^{3\cdot 82+4} = (50^{82})^3 \cdot 50^4 \equiv 1 \cdot 50^4 \pmod{83}$$
$$50^{250} \equiv 50^4 \equiv 2500^2 \equiv 10^2 \equiv 17 \pmod{83}.$$

Exemplo 50. *Resolver a equação* $16x \equiv 25 \pmod{41}$. *Pelo* ***PTF*** $16^{40} \equiv 1 \pmod{41}$, *logo*

$16^{39} \cdot 16x \equiv 16^{39} \cdot 25 \pmod{41}$, *portanto*

$$x \equiv 16^{39} \cdot 25 \pmod{41}$$
$$x \equiv (16^2)^{19} \cdot 16 \cdot 25 \pmod{41} \equiv (10)^{19} \cdot 400 \pmod{41} \equiv (10^2)^9 \cdot 10 \cdot 31 \pmod{41}$$
$$x \equiv (10^2)^9 \cdot 310 \pmod{41} \equiv (18^9) \cdot 23 \pmod{41} \equiv (18^2)^4 \cdot 18 \cdot 23 \pmod{41}$$
$$x \equiv (37)^4 \cdot 4 \pmod{41} \equiv (37)^2 \cdot (37)^2 \cdot 4 \pmod{41} \equiv 16 \cdot 16 \cdot 4 \pmod{41}$$
$$x \equiv 256 \cdot 4 \pmod{41} \equiv 10 \cdot 4 \pmod{41} \equiv 40 \pmod{41}.$$

4.6 O teorema de Euler

Definição 13. *A função* $\phi(n)$ *definida para um inteiro positivo* n *como sendo o número de inteiros positivos* k *tais que* $1 \leq k \leq n$ *e* $mdc(n,k) = 1$ *é chamada de função* ϕ *de Euler.*

Teorema 68. *Se* p *é primo, então* $\phi(p) = p - 1$. *Reciprocamente, se* p *é um inteiro positivo e* $\phi(p) = p - 1$, *então* p *é primo.*

Demonstração: Se p é primo, então $1, 2, 3, \ldots, p-1$ são primos com p, ou seja, existem $p-1$ inteiros relativamente primos com p, logo $\phi(p) = p - 1$. Suponha que p seja composto, então existe k tal que $1 < k < p$ e $k \mid p$, isto é $mdc(k,p) \neq 1$, logo pelo menos um dos $p-1$ inteiros $1, 2, 3, \ldots, p-1$ não são relativamente primos com p, logo $\phi(p) \leqslant p - 2$. Mas por hipótese $\phi(p) = p - 1$, ou seja $p - 1 \leqslant p - 2$, o que implica em $1 \leqslant 0$, o que é um absurdo. Portanto p é primo. □

Teorema 69. *Seja* p *um primo e* $a \in \mathbb{Z}_+$, *então* $\phi(p^a) = p^a - p^{a-1} = p^a\left(1 - \frac{1}{p}\right)$

Demonstração: De 1 até p^a temos p^a inteiros positivos. Basta excluir destes os que não são relativamente primos com p^a, ou seja temos que excluir os múltiplos de p que são os p^{a-1} inteiros

$$p, 2p, 3p, 4p, \ldots, p^{a-1} \cdot p$$

. Portanto $\phi(p^a) = p^a - p^{a-1} = p^a\left(1 - \frac{1}{p}\right)$. □

Exemplo 51. *Observe que:*

i) $\phi(5) = 5 - 1 = 4$; $\phi(7) = \phi(7-1) = 6$ *e* $\phi(11) = 11 - 1 = 10$.

ii) $\phi(8) = \phi(2^3) = 2^3 \cdot \left(1 - \frac{1}{2}\right) = 4$.

iii) $\phi(25) = \phi(5^2) = 5^2 \cdot \left(1 - \frac{1}{5}\right) = 20$.

Teorema 70. *Sejam m e n inteiros positivos com $mdc(m,n) = 1$, então*

$$\phi(mn) = \phi(m)\phi(n)$$

Demonstração: Formaremos uma tabela com os inteiros positivos de 1 até mn contendo os $\phi(mn)$ inteiros primos com mn:

1	$m+1$	$2m+1$	$3m+1$	$\cdots$	$(n-1)m+1$
2	$m+2$	$2m+2$	$3m+2$	$\cdots$	$(n-1)m+2$
3	$m+3$	$2m+3$	$3m+3$	$\cdots$	$(n-1)m+3$
4	$m+4$	$2m+4$	$3m+4$	$\cdots$	$(n-1)m+4$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
r	$m+r$	$2m+r$	$3m+r$	$\cdots$	$(n-1)m+r$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
m	$2m$	$3m$	$4m$	$\cdots$	mn

i) Suponha que r é um inteiro positivo tal que $1 \leqslant r \leqslant m$ e $mdc(m,r) = d > 1$. Então nenhum número da r-ésima linha é relativamente primo com mn, pois qualquer elemento desta linha é da forma $km + r$ com $1 \leqslant k \leqslant n-1$ e $d \mid km + r$, visto que $d \mid m$ e $\mid r$.

ii) Para encontrar os inteiros que são relativamente primos com mn, precisamos analisar a r-ésima linha na qual $mdc(m,r) = 1$. Se $mdc(m,r) = 1$ e $1 \leqslant r \leqslant m$ precisamos determinar quantos inteiros na linha

$$r, m+r, 2m+r, 3m+r, \ldots, (n-1)m+r$$

são relativamente primos com mn.

iii) Como $mdc(m,r) = 1$, cada um dos $r, m+r, 2m+r, 3m+r, \ldots, (n-1)m+r$ são relativamente primos com m. Logo estes n inteiros formam um sistema completo de resíduos módulo n. Então $\phi(n)$ destes inteiros são relativamente primos com n. Logo temos $\phi(n)$ inteiros relativamente primos com mn.

iv) Como existem $\phi(m)$ linhas, cada uma contendo $\phi(n)$ inteiros são relativamente primos com mn, segue que $\phi(mn) = \phi(m) \cdot \phi(n)$.

□

Teorema 71. *Seja* $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *onde* p_i *primo e* $a_i \in \mathbb{Z}_+$, *com* $1 \leqslant i \leqslant k$, *então*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Demonstração: Como $\phi(n)$ é multiplicativa, então:

$$\begin{aligned}
\phi(n) &= \phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdots \phi(p \cdot p_k^{\alpha_k}) \\
\phi(n) &= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) \\
\phi(n) &= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right) \\
\phi(n) &= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right) \\
\phi(n) &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).
\end{aligned}$$

□

Exemplo 52. *Observe que:*

i) $\phi(100) = \phi(2^2 \cdot 5^2) = 100 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 40$

ii) $\phi(720) = \phi(2^4 \cdot 3^2 \cdot 5) = 720 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 192$

Podemos agora ter outra versão da definição 12

Definição 14. *Um* $\boldsymbol{SRR}_n$ *é um conjunto de* $\phi(n)$ *inteiros tais que cada elemento do conjunto é relativamente primo com* n *e não existe quaisquer dois elementos diferentes do conjunto que sejam congruentes.*

Exemplo 53. *Observe que o conjunto de inteiros* $\{1, 3, 5, 7\}$ *forma um* $\boldsymbol{SRR}_8$.

Proposição 72. *Se* $\{r_1, r_2, \ldots, r_{\phi(n)}\}$ *é um* $\boldsymbol{SRR}_n$ *e* $a > 0$ *um inteiro com* $mdc(a, n) = 1$ *então*

$$\{a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\phi(n)},\}$$

também é um $\boldsymbol{SRR}_n$

Demonstração:

- *$mdc(ar_j, n) = 1$ para cada inteiro ar_j. De fato: Suponha que $d = mdc(ar_j, n) > 1$. Então existe um primo p tal que $p \mid d = mdc(ar_j, n) > 1$, então $p \mid ar_j \Rightarrow (p \mid a$ ou $p \mid r_j)$ e $p \mid n$, então $(p \mid a$ e $p \mid n)$ ou $(p \mid r_j)$ e $(p \mid n)$. Como $mdc(a, n) = 1$ e $mdc(r_j, n) = 1$, não podemos ter $(p \mid a$ e $p \mid n)$ e nem $(p \mid r_j$ e $p \mid n)$. Portanto $mdc(ar_j, n) = 1$ para $j = 1, 2, 3, \ldots, \phi(n)$.*

- *Nenhum dos ar_j são congruentes módulo n. Suponha que sim, ou seja, $ar_i \equiv ar_j \pmod{n}$ com $1 \leq i \leq \phi(n)$ e $1 \leq j \leq \phi(n)$. Como $mdc(a, n) = 1$, temos $r_i \equiv r_j \pmod{n}$, o que é uma contradição, pois r_i e r_j pertencem a um $\boldsymbol{SRR}_n$.*

□

Teorema 73. *Se $m > 0$ um número inteiro e $mdc(a, m) = 1$, então $a^{\phi(m)} \equiv 1 \pmod{m}$.*
Demonstração: *Seja $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ é um $\boldsymbol{SRR}_m$. Como $mdc(a, m) = 1$, pela proposição 72 $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ também é um $\boldsymbol{SRR}_m$, onde cada elemento deve ser congruente módulo m a um elemento do conjunto $\{r_1, r_2, \ldots, r_{\phi(m)}\}$, logo*

$$(ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\phi(m)}) \equiv (r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(m)}) \pmod{m}$$
$$a^{\phi(m)}(r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(m)}) \equiv (r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(m)}) \pmod{m}$$

Como $mdc(r_i, m) = 1$ para $1 \leq i \leq \phi(m)$, então $mdc(r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(m)}, m) = 1$, portanto podemos cancelar $(ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\phi(m)})$ em ambos os lados e obtemos $a^{\phi(m)} \equiv 1 \pmod{m}$. □

Nessa linha:

1. Podemos usar o teorema de Euler para encontrar inverso módulo m. Se $mdc(a, m) = 1$, então $a \cdot a^{\phi(m-1)} = a^{\phi(m)} \equiv 1 \pmod{m}$, portanto $a^{\phi(m-1)}$ é o o inverso de a módulo m.

2. Podem resolver a congruência linear $ax \equiv b \pmod{m}$ com $mdc(a, m) = 1$, é somente escrever $a^{\phi(m-1)}ax \equiv a^{\phi(m-1)}b \pmod{m}$. Portanto as soluções são os inteiros x tais que $x \equiv a^{\phi(m-1)}b \pmod{m}$.

3. Se m é primo, então $\phi(m) = m - 1$, ou seja, $a^{\phi(m-1)} \equiv 1 \pmod{m}$, que é o **PTF**.

Exemplo 54. *O conjunto de inteiros* $\{1, 3, 5, 7\}$ *forma um* $\boldsymbol{SRR}_8$ $mdc(3, 8) = 1$*, logo* $\{3, 9, 15, 21\}$ *também é um* $\boldsymbol{SRR}_8$

$$(3 \cdot 1)(3 \cdot 3)(3 \cdot 5)(3 \cdot 7) \equiv 1 \cdot 3 \cdot 5 \cdot 7 \pmod 8$$
$$(3^4)(1 \cdot 3 \cdot 5 \cdot 7) \equiv 1 \cdot 3 \cdot 5 \cdot 7 \mod 8$$
$$(3^4) \equiv 1 \pmod 8$$
$$a^{\phi(8)} \equiv 1 \pmod 8.$$

Exemplo 55. *Calcule o resto da divisão de* 33^{100} *por 40. Note que* $\phi(40) = 16$ *e* $mdc(33, 40) = 1$*, então* $33^{16} \equiv 1 \pmod{40}$*. Logo* $33^{100} = 33^{96} \cdot 33^4 = (33^{16})^6 \cdot 33^4 \equiv 1 \cdot 33^4 \pmod{40} \equiv 33^4 \pmod{40}$*. Portanto temos* $33^{100} \equiv (33^2)^2 \equiv (1089)^2 \equiv 9^2 \pmod{40} \equiv 81 \equiv 1 \pmod{40}$*.*

Exemplo 56. *Resolver a congruência* $15x \equiv 7 \pmod{32}$*. Note que* $mdc(15, 32) = 1$*. Logo* $15^{\phi(32)} \equiv 15^16 \equiv 1 \pmod{32}$*. Assim* $15^{15} \cdot 15x \equiv 15^{15} \cdot 7 \pmod{32}$*, o que implica em* $x \equiv 15^{15} \cdot 7 \pmod{32}$*. Agora observamos que* $7 \cdot 15^{15} \equiv 7 \cdot 15^{14} \cdot 15 \equiv (105)(15^2)^7 \equiv 9 \cdot (1^7) \pmod{32}$*. Portanto* $x \equiv 9 \pmod{32}$*.*

Capítulo 5

Problemas e soluções

Neste capítulo apresentaremos 40 problemas olímpicos 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 dessa importante componente curricular que é a matemática.

O critério da seleção dos problemas, levou em consideração as definições e propriedades apresentadas no capítulo 2, 3 e 4, buscando assim aliar teoria e prática.

São 17 problemas das provas anteriores da OBMEP, da primeira fase, 13 do Banco de Questões da OBMEP, e outras 10, entre problemas extraídos do POTI[1], RPM[2], entre outras.

Todas os problemas foram resolvidos indicando as definições e propriedades utilizadas, onde ainda, em alguns deles, há duas ou três soluções de modo que favoreça a construção de diversas estratégias para a resolução dos mesmos.

Sugerimos ainda ao leitor, a consulta em OBMEP (2020a), OBMEP (2020), Pereira (2016), Araújo (2018) e Cunha (2019).

5.1 Problemas e soluções

Nesta seção, serão propostos 40 problemas com diferentes graus de dificuldade. Buscamos apresentar as soluções com detalhes para tornar acessível o desenvolvimento e a compreensão dos mesmos. Diante fato de que os problemas selecionados compreendem a matemática olímpica, alguns exigem um maior grau de compreensão e abstração para o seu desenvolvimento. Por outro lado o uso adequado das propriedades podem tornar as questões apresentadas neste trabalho, mais interessantes e de certa forma acessíveis e motivadoras.

[1]Programa Polos Olímpicos de Treinamento Intensivo.
[2]Revista Professor de Matemática

Problema 1. *(OBMEP 2005 - Nível 2 - 1ª fase - Questão 8) Quantos números inteiros, múltiplos de 3, existem entre 1 e 2005?*

Este problema pode ser resolvido pelo menos de três formas diferentes. Na primeira solução, serão usados conceitos de divisibilidade e algoritmo da divisão. Na segunda, obteremos o quociente da divisão de 2005 por 3, que é equivalente a obter a parte inteira de $\left[\frac{2005}{3}\right]$. Esse cálculo nos permite obter quantos múltiplos de 3 cabem em 2005. Em outros casos que desejarmos obter o número de múltiplos num certo intervalo, sugerimos que seja consultada a proposição 15 e os exemplos 6 e 7. Na última solução, optamos pelas noções básicas de progressão aritmética, na qual, pelo critério de divisibilidade por 3 será possível obter o primeiro e o último termo dessa sequência. Mas, pelo fato de ser um assunto relativo ao ensino médio, sugerimos que seja apresentada aos alunos desse nível de ensino.

Solução: 1. *(OBMEP) Os múltiplos de 3 maiores do que 1 e menores do que 2005 são os números* $3 \times 1, 3 \times 2, 3 \times 3, \cdots, 3 \times n$ *onde* $3 \times n$ *é o maior múltiplo de 3 menor do que 2005. Usando o algoritmo da divisão, podemos escrever* $2005 = 3 \times 668 + 1$ *e segue que* $n = 668$.

Solução: 2. *Como queremos obter quantos são os múltiplos de 3 compreendidos entre 1 e 2005. Basta calcularmos a parte inteira de*

$$\left[\frac{2005}{3}\right] = 668$$

Esse resultado nos mostra que "cabem" 668 múltiplos de 3 nesse intervalo.

Solução: 3. *Pelas informações do enunciado e as definições de progressão aritmética, por ser múltiplo de 3 a razão é* $r = 3$*, o primeiro termo é facilmente obtido, onde* $a_1 = 3$*, agora para calcularmos o último, basta usarmos o critério de divisibilidade por 3, daí obtemos* $a_n = 2004$*, pois, ao somarmos os algarismos desse número, obtemos* $2 + 0 + 0 + 4 = 6$ *e* $6 \mid 3$*. Obtemos assim, a sequência* $(3, 6, \ldots, 2004)$*. Pela fórmula do termo geral da progressão aritmética,* $a_n = a_1 + (n-1)r$*, temos que* $2004 = 3 + (n-1) \cdot 3 \Rightarrow n = 668$*, onde 668 é o número de múltiplos de 3 nessa sequência.*

Problema 2. *(OBMEP 2006 - Nível 2 - 1ª fase - Questão 3) Qual é a soma dos algarismos do número* $10^{1500} + 10^{1792} + 10^{1822} + 10^{1888} + 10^{1889}$*?*

Neste problema, apresentaremos duas soluções. Na primeira, utilizaremos as noções básicas de potências de base 10 e a representação das mesmas no sistema decimal, destacando-se a importância do valor posicional dos algarismos nessa escrita. Na segunda solução mostraremos

a representação dessas potências nesse sistema e a relação que existe entre o expoente e o número de zeros seguidos de 1. Destacando-se a importância de diferenciar os termos utilizados para designar os algarismos de um número no sistema citado e usados nos livros didáticos. O valor absoluto e relativo dos algarismos na escrita decimal. Dessa forma, mostraremos que não será necessário efetuar a soma de todos esses números, pois queremos apenas o valor absoluto dos mesmos.

Solução: 1. *(OBMEP) Se n é um número natural maior que 0 então 10^n é um número da forma $1\underbrace{00\cdots00}_{n\ zeros}$.*
Logo, $10^{1500}+10^{1792}+10^{1822}+10^{1888}+10^{1889}=11\underbrace{00\cdots00}_{65\ zeros}1\underbrace{00\cdots00}_{29\ zeros}1\underbrace{00\cdots00}_{291\ zeros}1\underbrace{00\cdots00}_{1500\ zeros}$
e portanto a soma dos algarismos desse número é 5.

Solução: 2. *As potências de base 10 da forma 10^n, com $n>0$ e $n\in\mathbb{N}$. São escritas conforme os números naturais indicados no expoente conforme descreveremos abaixo:*

$$10^1=\underbrace{10}_{1\ zero},10^2=\underbrace{100}_{2\ zeros},10^3=\underbrace{1000}_{3\ zeros},\ldots,10^n=1\underbrace{000\ldots00}_{n\ zeros}$$

Segue do enunciado que:
$10^{1500}=1\underbrace{000\cdots00}_{1500\,zeros},10^{1792}=1\underbrace{000\cdots00}_{1792\,zeros},10^{1822}=1\underbrace{000\cdots00}_{1822\,zeros},10^{1888}=1\underbrace{000\cdots00}_{1888\,zeros},10^{1889}=1\underbrace{000\cdots00}_{1889\,zeros}$ *então,*

$$10^{1500}+10^{1792}+10^{1822}+10^{1888}+10^{1889}=$$
$$1\underbrace{00\cdots00}_{1500\,zeros}+1\underbrace{00\cdots00}_{1792\,zeros}+1\underbrace{00\cdots00}_{1822\,zeros}+1\underbrace{00\cdots00}_{1888\,zeros}+1\underbrace{000\cdots00}_{1889\,zeros}$$

Note que queremos apenas a soma dos algarismos dessa soma, perceba que isso pode ser feito considerando apenas o algarismo 1 em cada parcela, logo a soma é $1+1+1+1+1=5$.

Problema 3. *(OBMEP 2007 - Nível 2 - 1ª fase - Questão 17) A soma dos algarismos de um número par de nove algarismos é 79. Qual é o algarismo das unidades desse número?*

Sugerimos duas soluções para este problema. Na primeira, usaremos os conceitos de múltiplos, valor posicional no sistema de numeração decimal, paridade de inteiros e noções implícitas de combinatória. Na segunda, além dos temas citados anteriormente, faremos algumas considerações acerca da paridade de números inteiros e do critério de divisibilidade por 2.

Destacamos aqui que esse problema pode ser explorado com outras questões. Sugerimos por exemplo, calcular a quantidade de números distintos que podem ser formados considerando as restrições do enunciado. Isso pode ser proposto tanto no ensino fundamental de forma construtiva quanto no médio, através da fórmula da permutação com repetição de elementos.

Solução: 1. *(OBMEP) A maior soma possível de nove algarismos acontece quando temos nove algarismos 9 e é* $9 \times 9 = 81$. *Como* $79 = 81 - 2$ *, vemos que para que a soma de nove algarismos seja igual a 79 só há duas possibilidades*

- *sete algarismos 9 e dois algarismos 8;*
- *oito algarismos 9 e um algarismo 7.*

No primeiro caso podemos formar vários números pares com soma dos algarismos igual a 79; por exemplo, 999999988 e 899999998. No segundo caso isso não é possível pois só temos algarismos ímpares.

Solução: 2. *Pelos critérios de divisibilidade, sabemos que um número é par, quando for divisível por 2, e ainda pela paridade de números inteiros temos que:*

- *Números de mesma paridade a soma é par;*
- *Números de paridades distintas a soma é ímpar.*

Pelo fato de que a soma desses algarismos deve ser igual a 79 e esse número deve ser par, obrigatoriamente o último algarismo deve ser par. Vamos analisar, por inspeção, algumas configurações possíveis:

- *Oito algarismos 9 e o último par:* $999999998 \Rightarrow 9+9+9+9+9+9+9+9+8 = 80$*, o resultado obtido ultrapassa 1 unidade;*
- *Pelo fato anterior, devemos substituir um dos algarismos 9 para 8, daí teremos sete algarismos 9 e dois algarismos 8 sendo que um deles deve ocupar obrigatoriamente a posição das unidades e o outro em qualquer posição.*

Dessa forma podemos obtemos vários números como por exemplo: 999999988, 999998998, *dentre outros onde em qualquer uma dessas configurações a soma dos algarismos é* $9+9+9+9+9+8+9+9+8 = 79$.

Problema 4. *(OBMEP-2008 - Nível 2 - 1ª fase - Questão 9) Ana e Daniela brincam de escrever números no quadro-negro. A brincadeira começa com cada uma delas escrevendo um número natural. Depois disso:*

- *quem tiver o menor número mantém esse número;*
- *quem tiver escrito o maior número troca-o pela diferença entre seu número e o número da outra.*

Elas repetem esse procedimento até que os dois números escritos no quadro-negro fiquem iguais. Se Ana começou escrevendo 100 e Daniela 88, qual o número que vai ficar escrito no quadro-negro ao final da brincadeira?

Apresentaremos duas soluções para este problema. Na primeira, os valores dessas diferenças serão dispostos numa tabela, essa estratégia de organizar os dados permite-nos fazer análises mais detalhadas de problemas de um modo geral, e daí perceber que as operações feitas por Ana e Daniela nos remetem ao uso do algoritmo de Euclides para o cálculo do *mdc* de 100 e 88. Na outra, mostraremos que o cálculo do máximo divisor comum desses números, também podem ser obtidos pelo lema de Euclides.

Solução: 1. *(OBMEP)*

	1	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***
Ana	*100*	*12*	*12*	*12*	*12*	*12*	*12*	*12*	*12*	*8*	*4*
Daniela	*88*	*88*	*76*	*64*	*52*	*40*	*28*	*16*	*4*	*4*	*4*

Logo a resposta correta é 4. Notamos que essa brincadeira nada mais é que o algoritmo de Euclides para calcular o máximo divisor comum de dois números; no caso, a tabela pode ser interpretada como a sequência de divisões

$$100 = 1 \times 88 + 12$$
$$88 = 7 \times 12 + 4$$
$$12 = 3 \times 4 + 0$$

que nos mostra que o máximo divisor comum de 100 e 88 é 4.

Solução: 2. *O enunciado do problema nos diz que devem ser feitas subtrações sucessivas, logo sugere o cálculo do máximo divisor comum (mdc) dos números 100 e 88 e indicaremos por* $mdc(100, 88)$.

Pelo lema de Euclides, temos

$$mdc(100, 88) = mdc(100 - 88, 88) = mdc(12, 88) = mdc(12, 88 - 7 \cdot 12) = mdc(12, 4)$$
$$= mdc(4, 12 - 3 \cdot 4) = mdc(4, 0) = 4$$

Como o $mdc(100, 88) = 4$*, então, o número que ficará no final da brincadeira é 4.*

Problema 5. *(OBMEP 2008 - Nível 2 - 1ª fase - Questão 13) Os 535 alunos e os professores de uma escola fizeram um passeio de ônibus. Os ônibus, com capacidade para 46 passageiros cada, ficaram lotados. Em cada ônibus havia um ou dois professores. Em quantos ônibus havia dois professores?*

Apresentaremos três formas para resolver esse problema. Na primeira, foram usados conceitos do algoritmo da divisão e de múltiplos. Na segunda, inicialmente o problema consiste em ser modelado através de uma equação com duas variáveis e daí, por inspeção obter-se-á os resultados. E na terceira, após a modelagem do problema, usaremos as definições de equações diofantinas, que resolveremos pelas definições e propriedades de congruência linear.

Solução: 1. *(OBMEP) Como* $535 = 11 \times 46 + 29$ *, vemos que 11 ônibus são insuficientes para o passeio. Por outro lado, de* $13 \times 46 = 598$ *vemos que se o número de ônibus fosse maior ou igual a 13 o número de professores seria no mínimo* $598 - 535 = 63$ *, o que não é possível pois em cada ônibus há no máximo 2 professores. Logo o passeio foi feito com 12 ônibus e o número de professores é* $12 \times 46 - 535 = 17$*. Como cada ônibus tem 1 ou 2 professores e 17 dividido por 12 tem quociente 1 e resto 5, concluímos que o número de ônibus com 2 professores é 5.*

Solução: 2. *(OBMEP) Sejam* x *o número de ônibus com 1 professor (nesses ônibus há 45 alunos) e* y *o número de ônibus com 2 professores (nesses ônibus há 44 alunos). Logo,* $45x + 44y = 535$*. Para resolver essa equação, observe que como* x *e* y *são inteiros positivos,* y *tem que ser um múltiplo de 5 menor que 15 (porque* $15 \times 44 > 535$*), isto é,* y *vale 5 ou 10. Substituindo esses valores na equação, obtemos* $y = 5$*.*

Solução: 3. *Chamando de* x *o número de ônibus com 1 professor (nesses ônibus há 45 alunos) e por* y *o número de ônibus com 2 professores (nesses ônibus há 44 alunos), obtemos a seguinte equação diofantina:*

$$45x + 44y = 535$$

Como o $mdc(45, 44) = 1$ *e* $1 \mid 535$*, a equação tem solução. Usaremos as congruências lineares para obter soluções particulares de* x *e* y*. Assim resolveremos a congruência* $45x \equiv 535 \pmod{44}$*. Segue que:*

$$45x \equiv 535 \pmod{44} \Leftrightarrow x \equiv 7 \pmod{44}$$

Tomando $x = 7$*, temos que* $y = \dfrac{535 - 45 \cdot 7}{44} = 5$*, todas as soluções são da forma* $x = 7 + 44t$ *e* $y = 5 - 45t$*, com* $t \in \mathbf{Z}$*.*

Como x, y *devem ser inteiros positivos,*

$$\begin{array}{rcr} x > 0 & & y > 0 \\ 7 + 44t > 0 & e & 5 - 45t > 0 \\ 44t > -7 & & 47t < 5 \\ t > -0,1\ldots & & t < 0,1\ldots \end{array}$$

$$0 \leq t \leq 0$$

Logo, temos que $t = 0$ *é o único parâmetro para a solução desejada, então,*

$$x = 7 + 44 \cdot 0 = 7 \text{ e } y = 5 - 45 \cdot 0 = 5$$

Portanto, há 7 *ônibus com* 1 *professor e* 5 *ônibus com* 2 *professores.*

Problema 6. *(OBMEP 2011 - Nível 2 - 1ª fase - Questão 2) Qual é o resto da divisão de* $1 \times 2 \times 3 \times 4 \times \cdots \times 2011 + 21$ *por 8?*

Discutiremos três soluções para este problema. Na primeira, utilizaremos os conhecimentos básicos de múltiplos, divisibilidade e algoritmos da divisão. Na segunda mostraremos uma variante da primeira, na qual é possível generalizar situações que envolvem múltiplos e seus possíveis restos numa divisão. Na outra, mostraremos a possibilidade de resolvê-lo usando os conceitos de congruência modular e suas propriedades.

Apesar de que congruência modular é um tema que não faz parte do currículo da educação básica, mostraremos que e possível a sua introdução nesse nível de ensino, como alternativa na solução de problemas.

Solução: 1. *(OBMEP) Queremos dividir* $1 \times 2 \times 3 \times 4 \times \cdots \times 2011 + 21 = 1 \times 2 \times 3 \times 4 \times \cdots \times 2011 + 16 + 5$ *por 8. Como as duas primeiras parcelas do lado direito dessa expressão são múltiplos de 8, sua soma também é um múltiplo de 8. Portanto, o resto da divisão desse número por 8 é 5.*

Solução: 2. *Note que* $1 \times 2 \times 3 \times 4 \times \cdots \times 2011$ *é um múltiplo de 8 então a expressão* $\underbrace{1 \times 2 \times 3 \times 4 \times \cdots \times 2011}_{multiplo\,de\,8} + 21$*, pode ser reescrita na forma* $8k + 21 = 8k + 16 + 5 = 8(k + 2) + 5$*, onde* $k = 1 \times 3 \times 5 \times \cdots \times 2011$

Note que $8(k + 2) + 5$ *deixa resto 5 na divisão por 8.*

Solução: 3. *Seja* $N = 1 \times 2 \times 3 \times 4 \times \cdots \times 2011 + 21$*, usando congruências e suas propriedades, temos*

$$N \equiv \underbrace{1 \times 2 \times 3 \times 4 \times \cdots \times 2011}_{multiplo\,de\,8} + 21 \equiv 0 + 5 \equiv 5 \pmod 8$$

Logo $1 \times 2 \times 3 \times 4 \times \cdots \times 2011 + 21$ *deixa resto 5 na divisão por 8.*

Problema 7. *(OBMEP 2011-Nível 2 - 1ª fase - Questão 17) Mariana escreveu as decomposições em fatores primos dos números naturais de 2 a 100:* $2, 3, 2\times2, 5, 2\times3, \ldots, 3\times3\times11, 2\times2\times5\times5$. *Quantas vezes ela escreveu o algarismo 2?*

Apresentaremos duas soluções para este problema. Na primeira, serão necessários os conceitos de divisibilidade, números primos e a decomposição em fatores primos. Na outra solução, o teorema de Legendre que requer conhecimentos básicos de fatorial de um número, potências de base 2, divisibilidade e o algoritmo da divisão. Apesar de que alguns desses temas não são ensinados nesse nível de ensino, mostraremos que é possível a sua aplicação e que é uma ferramenta poderosa na resolução de problemas desse tipo.

Solução: 1. *(OBMEP)Mariana escreveu o algarismo 2:*

- *uma vez na fatoração de cada número par, isto é, 50 vezes;*
- *mais uma vez na fatoração de cada múltiplo de 4, isto é, outras 25 vezes;*
- *mais uma vez na fatoração de cada múltiplo de 8, isto é, outras 12 vezes;*
- *mais uma vez na fatoração de cada múltiplo de 16, isto é, outras 6 vezes;*
- *mais uma vez na fatoração de cada múltiplo de 32, isto é, outras 3 vezes;*
- *mais uma vez na fatoração de cada múltiplo de 64, ou seja, 1 vez;*
- *quando escreveu os números primos 23 e 29, ou seja, 2 vezes;*
- *quando escreveu 23 nas fatorações de 46, 69, 92 e quando escreveu 29 nas fatorações de 58 e 87, ou seja, 5 vezes.*

No total, Mariana escreveu $50 + 25 + 12 + 6 + 3 + 1 + 2 + 5 = 104$ *vezes o algarismo 2.*

Solução: 2. *Para determinarmos quantas vezes o fator 2 aparece na sequência dos números de 2 a 100, isso é equivalente a calcularmos a maior potência de 2 que divide* $100!$*, ou seja, devemos calcular* $E_2(100!)$*. Pelo teorema de Legendre temos*

$$E_2(100!) = \left[\frac{100}{2}\right] + \left[\frac{100}{2^2}\right] + \left[\frac{100}{2^3}\right] + \left[\frac{100}{2^4}\right] + \left[\frac{100}{2^6}\right] = 50 + 25 + 12 + 6 + 3 + 2 + 1 = 99$$

Note que $2^{99} \mid 100!$*, ou seja o fator 2 aparece 99 vezes. Porém, como desejamos obter quantas vezes o algarismo 2 parecem nos números listados, devemos observar os números 21, 23, 25, 27 e 29 que tem o algarismo 2 e não possuem o fator 2 em sua decomposição, logo há* $99 + 5 = 104$ *algarismos 2.*

Problema 8. *(OBMEP 2013 - Nível 2 - 1ª fase - Questão 17) Qual é o algarismo das dezenas da soma* $\underbrace{7}_{\text{um sete}} + \underbrace{77}_{\text{dois sete}} + \underbrace{777}_{\text{três setes}} + \underbrace{777\cdots77}_{\text{setenta e seis setes}} + \underbrace{777\cdots777}_{\text{setenta e sete setes}}$ *?*

Apresentaremos duas soluções para esse problema. Inicialmente, note que não é possível somar todas essas parcelas, porém ao usarmos as noções valor posicional no sistema de numeração decimal, podemos manipular apenas a soma dos algarismos das unidades e das dezenas desses números, facilitando assim todo o trabalho. Na outra solução, usaremos os conceitos de congruência modular. Aplicaremos congruência módulo 100 em todas as parcelas e ao final, na sua soma. Dessa forma poderemos determinar tanto o algarismo das unidades quanto das dezenas dessa soma.

Solução: 1. *(OBMEP) Ao somar os algarismos das unidades, encontramos* $77\times7 = 539$*. Logo, o algarismo das unidades da soma é 9 e 53 deve ser adicionado à casa das dezenas. A soma dos algarismos 7 que aparecem nas dezenas é* $76 \times 7 = 532$*, que somada a 53 dá 585. Logo, o algarismo das dezenas é 5. Alternativamente, podemos observar que os algarismos das dezenas e unidades da soma só dependem da soma dos algarismos das unidades e das dezenas das parcelas, ou seja, são os mesmos que os algarismos correspondentes da soma*
$7 + 77 + 77 + \cdots + 77 = 7 + 76 \times 77 = 5859$*; logo, o algarismo das dezenas da soma indicada é 5 e o das unidades é 9.*

Solução: 2. *Neste problema queremos obter os algarismos das dezenas e para que possamos obtê-lo, basta dividir a soma por 100. Perceba que, somar todos esses números é uma tarefa inviável, então nesse caso utilizaremos congruências módulo 100. Escrevendo essa soma por N, temos*

$$N = \underbrace{7}_{\text{um sete}} + \underbrace{77}_{\text{dois sete}} + \underbrace{777}_{\text{três setes}} + \underbrace{777\cdots77}_{\text{setenta e seis setes}} + \underbrace{777\cdots777}_{\text{setenta e sete setes}}$$

$$N \equiv 7 + \underbrace{77 + \cdots + 77}_{76\,vezes} \equiv 7 + 76 \times 77 \equiv 7 + 5852 \equiv 5859 \equiv 59 \pmod{100}$$

Como o resto da divisão de N por 100 é igual a 59, o algarismo das dezenas é igual a 5.

Problema 9. *(OBMEP 2017-Nível 3 - 1ª fase - Questão 15) O contrário de um número de dois algarismos, ambos diferentes de zero, é um número obtido trocando-se a ordem de seus algarismos. Por exemplo, o contrário de 25 é 52 e o contrário de 79 é 97. Qual dos números abaixo não é a soma de um número de dois algarismos com o seu contrário?*

Neste problema, faremos duas soluções. Na solução da OBMEP, serão usadas a expansão decimal de um número inteiro e noções de múltiplos de 11, na outra solução, além da

expansão decimal, faremos uso do critério de divisibilidade por 11 para obtermos a alternativa correta.

Solução: 1. *(OBMEP) Seja n um número de dois algarismos, sendo a seu algarismo das dezenas e b o das unidades; então $n = 10a + b$. Se a e b são ambos diferentes de zero, o contrário de n é $10b + a$. Desse modo, a soma de n e de seu contrário é.*

$$(10a + b) + (10b + a) = 11a + 11b = 11(a + b)$$

e portanto a soma de um número com seu contrário é sempre um múltiplo de 11. Basta agora notar que todas as opções são múltiplos de 11, com a exceção de 181.

Solução: 2. *Inicialmente vamos chamar o número de 2 algarismos por n e o seu contrário por n'. Sejam a e b os algarismos não nulos desses números e representando a sua expansão decimal, temos que $n = ab = 10a + b$ e $n' = ba = 10b + a$, cuja soma é dada por:*

$$n + n' = (ab) + (ba) = (10a + b) + (10b + a) = 11a + 11b = 11 \cdot (a + b)$$

Note que o número obtido é um múltiplo de 11. Agora, pelo critério de divisibilidade por 11, vamos verificar quais números dentre 44, 99, 121, 165, 181, são múltiplos de 11.

- *44, como $4 - 4 = 0$ e $0 \mid 11$, então 44 é divisível por 11;*
- *99, como $9 - 9 = 0$ e $0 \mid 11$, então 99 é divisível por 11;*
- *121, como $1 - 2 + 1 = 0$ e $0 \mid 11$, então 121 é divisível por 11;*
- *165, como $1 - 6 + 5 = 0$ e $0 \mid 11$, então 165 é divisível por 11;*
- *181, como $1 - 8 + 1 = -6$ e $-6 \nmid 11$, logo 181 não é divisível por 11;*

Logo, 181 não é soma de um número de dois algarismos com o seu contrário.

Problema 10. *(OBMEP 2017-Nível 3 - 1ª fase - Questão 6) Somando 1 a um certo número natural, obtemos um múltiplo de 11. Subtraindo 1 desse mesmo número, obtemos um múltiplo de 8. Qual é o resto da divisão do quadrado desse número por 88?*

Resolveremos esse problema de duas maneiras. Usaremos os conceitos básicos de divisão euclidiana e divisibilidade na solução da OBMEP, e na outra solução proposta, as definições de congruência e o teorema chinês dos restos.

Solução: 1. *(OBMEP) Lembramos primeiro que, se a e b são números naturais, dizer que a é múltiplo de b (ou b divide a) é dizer que existe outro número natural c tal que $a = bc$. O algoritmo da divisão nos diz que, se $b \neq 0$, existem únicos inteiros q e r tais que $a = qb + r$ e $0 \leqslant r < |b|$; os números q e r são ditos, respectivamente, o quociente e o resto da divisão de a por b (se $r = 0$, temos o caso em que a é múltiplo de b). Seja agora n o número natural do enunciado. Como $n + 1$ é múltiplo de 11, existe um número natural t tal que $n + 1 = 11t$; do mesmo modo, existe um número natural s tal que $n - 1 = 8s$. Multiplicando membro a membro essas expressões, temos $(n + 1)(n - 1) = n^2 - 1 = 88ts$, ou seja, $n^2 = 88ts + 1$. Essa última expressão mostra que o resto da divisão de n^2 por 88 é 1.*

Solução: 2. *Inicialmente, vamos chamar o certo número natural por x e pelas notações de congruência, o problema se resume a resolver o sistema abaixo:*

$$\begin{cases} x + 1 \equiv 0 \pmod{11} \\ x - 1 \equiv 0 \pmod{8} \end{cases} \Leftrightarrow \begin{cases} x \equiv -1 \pmod{11} \\ x \equiv 1 \pmod{8} \end{cases}$$

Como $mdc(8, 11) = 1$, o sistema tem solução. Pelas definições do teorema chinês dos restos, temos que $m = 11 \cdot 8 = 88$ e

$$\begin{cases} M_1 = \dfrac{88}{11} = 8 \\ M_2 = \dfrac{88}{8} = 11 \end{cases}; \begin{cases} M_1 y_1 \equiv 1 \pmod{11} \\ M_2 y_2 \equiv 1 \pmod{8} \end{cases}; \begin{cases} 8y_1 \equiv 1 \pmod{11} \\ 11y_2 \equiv 1 \pmod{8} \end{cases}; \begin{cases} 8y_1 \equiv 1 \pmod{11} \\ 3y_2 \equiv 1 \pmod{8} \end{cases}; \begin{cases} y_1 \equiv 7 \pmod{11} \\ y_2 \equiv 3 \pmod{8} \end{cases}$$

Então, $x = a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 = (-1) \cdot 8 \cdot 7 + 1 \cdot 11 \cdot 3 = -23 \equiv 65 \pmod{88}$, como queremos obter o resto do quadrado desse número dividido por 88, segue que $65^2 = 4225 \equiv 1 \pmod{88}$. Portanto deixa resto 1.

Problema 11. *(OBMEP 2018-Nível 2 - 1ª fase - Questão 9) Maria escolheu um número inteiro. Ela somou a esse número os três números ímpares imediatamente inferiores e os dois números pares imediatamente superiores a ele e obteve 1414 como resultado. Qual é a soma dos algarismos do número que Maria escolheu?*

Mostraremos duas soluções para este problema. Em ambas, serão necessários conhecimentos de valor posicional no sistema de numeração decimal, antecessor, sucessor, paridade de números inteiros bem como sua representação genérica. Usaremos ainda equações do primeiro grau para fazermos uma discussão mais detalhada acerca das possíveis soluções.

Solução: 1. *(OBMEP) Como 1414 é par, o número ao qual Maria somou três ímpares e dois pares é necessariamente ímpar. Escrevendo este número por n temos*

$$(n - 6) + (n - 4) + (n - 2) + n + (n + 1) + (n + 3) = 1414$$

Logo, $6n - 8 = 1414$ *e* $n = 237$*. Somando os algarismos de 237, temos:* $2 + 3 + 7 = 12$*.*

Solução: 2. *Pela paridade de números inteiros, temos dois casos a considerar:*

i) O número escolhido é par;

ii) O número escolhido é impar.

No primeiro caso, considere que o número escolhido seja par, então é da forma $2q$*, com* $q \in \mathbb{Z}$*, logo os três números imediatamente inferiores ímpares são:* $2q-1, 2q-3, 2q-5$ *e os dois pares imediatamente superiores são:* $2q+2, 2q+4$*, daí representando essa soma, temos:*

$$\begin{aligned}(2q-5)+(2q-3)+(2q-1)+(2q)+(2q+2)+(2q+4) &= 1414\\ 6\cdot(2q)-3 &= 1414\\ 2q &= \frac{1417}{6}\end{aligned}$$

Temos que $2q = \dfrac{1417}{6} \notin \mathbb{Z}$*. Logo o número escolhido não pode ser par.*

Agora suponha que o número procurado seja ímpar, ou seja da forma $2q+1$*, com* $q \in \mathbb{Z}$*. Segue que os três números imediatamente inferiores ímpares são:* $2q-1, 2q-3, 2q-5$ *e os dois pares imediatamente superiores são:* $2q+2, 2q+4$*, daí representando essa soma, temos:*

$$\begin{aligned}(2q-5)+(2q-3)+(2q-1)+(2q+1)+(2q+2)+(2q+4) &= 1414\\ 12q-2 &= 1414\\ 12q &= 1416\\ 2q+1 &= \frac{1416}{6}+1 = 237\end{aligned}$$

Logo o número procurado é ímpar igual a 237, cuja soma de seus algarismos é $2 + 3 + 7 = 12$*.*

Problema 12. *(OBMEP 2012-Nível 3 - 1ª fase - Questão 13) Para fazer várias blusas iguais, uma costureira gastou* $R\$2,99$ *para comprar botões de 4 centavos e laços de 7 centavos. Ela usou todos os botões e laços que comprou. Quantas blusas ela fez?*

Apresentaremos duas soluções para este problema. Na primeira, usaremos conceitos de divisibilidade e decomposição do números em fatores primos. Na outra, inicialmente modelaremos o problema através de um equação. Como o problema envolve duas incógnitas, obteremos então uma equação diofantina. Nesse caso, usaremos os conhecimentos acerca desse tema para resolvê-la.

Solução: 1. *A costureira gastou 299 centavos. Como as blusas são iguais, em cada uma foi gasta a mesma quantia; logo, o número n de blusas é um divisor de 299. Como* $299 = 13 \cdot 23$ *e tanto 13 quanto 23 são primos, as possibilidades para n são 1, 13, 23 e 299. O enunciado exclui a possibilidade* $n = 1$ *(são várias blusas) e a possibilidade* $n = 299$ *é excluída observando que, como um botão custa 4 centavos, a quantia gasta em qualquer blusa é maior que 1 centavo. Se* $n = 23$ *, o total em botões e laços gasto em cada blusa seria 13 centavos, o que não pode acontecer pois não é possível gastar exatamente 13 centavos com botões de 4 centavos e laços de 7 centavos. Resta a possibilidade* $n = 13$ *; nesse caso, o total gasto em botões e laços em cada blusa é de 23 centavos, que corresponde a 4 botões e 1 laço.*

Solução: 2. *Seja x o número de botões e y o número de laços utilizados para fazer as blusas, cujo custo total é de* $R\$2,99$*, obtemos a equação*

$$0,04x + 0,07y = 2,99$$

Note que, resolver a equação acima é equivalente a resolver a equação diofantina

$$4x + 7y = 299$$

Como o $mdc(4,7) = 1$ *e* $1 \mid 299$*, a equação tem solução. Usaremos as congruências lineares para obter soluções particulares de x e y. Assim resolveremos a congruência* $4x \equiv 299 \pmod 7$*. Segue que:*

$$4x \equiv 299 \pmod 7 \Leftrightarrow 4x \equiv 5 \pmod 7.$$

Como, $x_0 = 3$ *é solução da congruência, temos que,* $x \equiv 3 \pmod 7$*.*

Tomando $x = 3$*, temos que* $y = \dfrac{299 - 4 \cdot 3}{7} = 41$*. Então, todas as soluções são da forma* $x = 3 + 7t$ *e* $y = 41 - 4t$*, com* $t \in \mathbf{Z}$*.*

Como x, y devem ser inteiros positivos,

$$\begin{array}{ccc} x > 0 & & y > 0 \\ 3 + 7t > 0 & e & 41 - 4t > 0 \\ 7t > -3 & & -4t > -41 \\ t > -0,4\ldots & & t < 10,25 \end{array}$$

Logo,

$$0 \leq t \leq 10$$

Substituindo todos os valores do parâmetro t nas equações $x = 3 + 7t$ e $y = 41 - 4t$, temos:

t	0	1	2	3	4	5	6	7	8	9	10
x	3	10	17	24	31	38	45	52	59	66	73
y	41	37	33	29	25	21	17	13	9	5	1

Note que a quantidade de botões aumenta de 7 em 7 e a quantidade de laços diminui de 4 em 4 facilitando assim os cálculos.

Precisamos determinar quantas blusas ela fez. O número de botões e de laços devem ser os mesmos em cada blusa, então devemos obter o maior número d, tal que $d = mdc(x, y)$. Note que nos pares (x, y) obtidos, o maior mdc ocorre quando $d = mdc(52, 13) = 13$.

Portanto é possível fazer 13 blusas.

Problema 13. *(OBMEP 2016 - Nível 3 - 1ª fase - Questão 17) Quantos são os números naturais n tais que $\dfrac{5n-12}{n-8}$ é também um número natural?*

Mostraremos duas soluções para este problema. Na primeira, serão necessários alguns conceitos vistos anteriormente, tais como a fatoração e a divisão, divisibilidade e análise se sinais na divisão de inteiros. Numa segunda solução, usaremos a definição de divisibilidade, lema de Euclides para o cálculo do máximo divisor comum, análise de sinais da divisão de inteiros e noções básicas de inequações.

Solução: 1. *(OBMEP) Podemos reescrever a expressão somando e subtraindo 40 no denominador, como abaixo:*

$$\frac{5n-12}{n-8} = \frac{5n-40+40-12}{n-8} = \frac{5n-40}{n-8} + \frac{28}{n-8} = \frac{5(n-8)}{n-8} + \frac{28}{n-8} = 5 + \frac{28}{n-8}$$

Logo, os números inteiros n tais que $\dfrac{5n-12}{n-8}$ é um número natural são aqueles tais que $\dfrac{28}{n-8}$ é um número inteiro igual ou maior do que -5.
Para $\dfrac{28}{n-8}$ ser um número inteiro, $n-8$ deve dividir 28 e segue que $(n-8) = \pm1, \pm2, \pm4, \pm7, \pm14$ ou ±28. E, dentre esses números, para $\dfrac{28}{n-8}$ ser um número inteiro igual ou maior que -5, segue que $(n-8) = +1, +2, +4, \pm7, \pm14$ ou ±28.

Logo, os possíveis inteiros n são $n = +9, +10, +12, +15, +1, +22, -6, +36$ ou -20. Desses, sete são números naturais.

Solução: 2. *Se* $\dfrac{5n-12}{n-8}$ *é um número natural, implica que* $(n-8)|(5n-12)$. *Seja* $d = mdc(5n-12, n-8)$, *pelo lema de Euclides temos que:*

$$\begin{aligned} d &= mdc(5n-12, n-8) \\ &= mdc(5n-12-5(n-8), n-8) \\ &= mdc(5n-12-5n+40), n-8) \\ &= mdc(28, n-8) \end{aligned}$$

Pela definição, $d|28$ *e* $d|(n-8)$ *e analisando o caso em que* $d|28$, *os possíveis valores inteiros para* d *são:*$\pm 1, \pm 2, \pm 4, \pm 7, \pm 14, \pm 28$, *então como* $d|(n-8)$, *substituindo os valores obtidos anteriormente em* $n-8$, *obtemos todos os números inteiros para* n *que são:* $-6, -20, 1, 4, 6, 7, 9, 10, 12, 15, 22, 36$. *No entanto,* n *é um número natural e por isso temos que considerar duas condições em relação a* $\dfrac{5n-12}{n-8}$*:*

i) O numerador e o denominador devem ser positivos, ou seja
$5n - 12 > 0 \Rightarrow n > \dfrac{12}{5} \Rightarrow n > 2,4$ *e*
$n - 8 > 0 \Rightarrow n > 8$

Então, $n > 8$, *ou seja 9,10,12,15,22 e 36.*

ii) O numerador e o denominador devem ser negativos, ou seja
$5n - 12 < 0 \Rightarrow n < \dfrac{12}{5} \Rightarrow n < 2,4$ *e*
$n - 8 < 0 \Rightarrow n < 8$

Nesse caso $n < 2,4$, *mas n é positivo, então n=1*
Logo obtemos 7 valores naturais para n que são os números 1,9,10,12,15,22 e 36.

Problema 14. *(OBMEP 2017-Nível 3 - 1ª fase - Questão 9) A maior potência de 2 que divide o produto* $1 \times 2 \times \cdots \times 2023 \times 2024$ *é* 2^{2017}. *Qual é a maior potência de 2 que divide o produto* $1 \times 2 \times \cdots \times 4047 \times 4048$*?*

Na primeira solução proposta, abordaremos os conceitos de potências, divisibilidade, fatoração e paridade de um número inteiro. Usaremos, como solução alternativa, novamente o teorema de Legendre, para encontrarmos a maior potência de 2 que divide o número considerado.

Solução: 1. *(OBMEP) Como* 2^{2017} *é a maior potência de dois que divide o produto* $1 \times 2 \times \cdots \times 2023 \times 2024$, *podemos escrever esse produto na forma* $2^{2017} + I$, *sendo I um número ímpar.*

Já o produto $1 \times 2 \times \cdots \times 4047 \times 4048$ *pode ser escrito da seguinte maneira:*

$$1 \times (2 \times 1) \times 3 \times (2 \times 2) \times 5 \times (2 \times 3) \cdots \times (2 \times 2023) \times 4047 \times (2 \times 2024) =$$
$$(1 \times 3 \times 5 \times \cdots \times 4047) \times (2 \times 1) \times (2 \times 2) \times (2 \times 3) \times (2 \times 2023) \times (2 \times 2024) =$$
$$(1 \times 3 \times 5 \times \cdots \times 4047) \times (1 \times 2 \times \cdots \times 2023 \times 2024) \times 2^{2024} =$$
$$(1 \times 3 \times 5 \times \cdots \times 4047) \times I \times 2^{2017} \times 2^{2024}$$

O primeiro fator da última expressão também é um número ímpar, logo, $1 \times 2 \times \cdots \times 4047 \times 4048 = T \times 2^{2017+2024} = T \times 2^{2024}$*, sendo* T *um fator ímpar. Assim, o expoente da maior potência de dois que divide o produto dado é 4041.*

Solução: 2. *Queremos obter a maior potência de dois que divide* $1 \times 2 \times \cdots \times 4047 \times 4048$*, note que esse valor é equivalente a* $4048!$ *e pelo teorema de Legendre vamos encontrar* $E_2(4048!)$*.*

$$E_2(4048!) = \left[\frac{4048}{2}\right] + \left[\frac{4048}{2^2}\right] + \left[\frac{4048}{2^3}\right] + \left[\frac{4048}{2^4}\right] + \left[\frac{4048}{2^5}\right] + \left[\frac{4048}{2^6}\right] + \left[\frac{4048}{2^7}\right] + \\ + \left[\frac{4048}{2^8}\right] + \left[\frac{4048}{2^9}\right] + \left[\frac{4048}{2^{10}}\right] + \left[\frac{4048}{2^{11}}\right]$$
$$E_2(4048!) = 2024 + 1012 + 506 + 253 + 126 + 63 + 31 + 15 + 7 + 3 + 1 = 4041$$

Logo, $2^{4041} \mid 1 \times 2 \times \cdots \times 4047 \times 4048$*. Então, a maior potência de dois que divide* $1 \times 2 \times \cdots \times 4047 \times 4048$ *é 4041.*

Problema 15. *(OBMEP 2018-Nível 3 - 1ª fase - Questão 5) De quantas maneiras podemos trocar uma nota de R$20,00 por moedas de R$0,10 e R$0,25?*

Apresentaremos quatro soluções para explorar esse problema. Serão três delas propostas pela OBMEP e uma outra através de equações diofantinas. Na primeira solução, são necessários conhecimentos de paridade, múltiplos e noções elementares de combinatória. Na segunda, o problema será modelado a partir de uma equação com duas variáveis para representar a quantidade de moedas de R$0,25 e de R$0,10 centavos, ainda serão necessários conhecimentos de paridade e inequações. Na terceira, faremos conjecturas com a ideia de múltiplos, e finalmente na última, denotaremos o problema através de uma equação diofantina, cujo desenvolvimento será descrito abaixo.

Solução: 1. *(OBMEP) Não podemos usar um número ímpar de moedas de 25 centavos, mas podemos usar* $0, 2, 4, \cdots$ *até 80 dessas moedas, e cada escolha gera uma maneira diferente de fazer a troca. Logo, o número de maneiras de trocar R$ 20,00 por moedas de R$ 0,10 e R$ 0,25 é igual à quantidade de números pares entre 0 e 80, incluindo os extremos, ou seja, é 41.*

Solução: 2. *(OBMEP) Sejam x e y as quantidades de moedas de R$0,25 e R$0,10, respectivamente, usadas para formar a quantia de R$20,00. Assim,*

$$0,25x + 0,10y = 20.$$

Multiplicando a equação por 20, obtemos $5x + 2y = 400$. Como 400 e $2y$ são números pares, x também é um número par, e daí podemos escrever $x = 2z$. Uma vez que o valor do inteiro z tenha sido escolhido, teremos uma solução com $y = \frac{1}{2}(400 - 10z) = 200 - 5z$. Para que y seja um inteiro não negativo, $200 - 5z \geq 0$, ou seja, $z \leq 40$. Por outro lado, como $z \geq 0$, podemos concluir que existem exatamente 41 valores possíveis para ele, a saber: $0, 1, 2, \cdots, 40$.

Solução: 3. *(OBMEP) Pensemos no que aconteceria se usássemos moedas com valor R$0,05. Precisaríamos de 400 dessas moedas para formar a quantia de R$20,00. Podemos trocar duas dessas moedas pela moeda de R$ 0,10 e cinco delas pela moeda de R$0,25. Para que consigamos usar apenas as duas moedas (de R$0,10 e R$0,25), mencionadas no enunciado, devemos realizar todas as trocas possíveis sem sobrar nenhuma moeda de R$0,05. Para que isso seja realizável, a quantidade de moedas de R$ 0,05 convertidas em R$0,25, além de múltiplo de 5, também deve ser par, para que sobre uma quantidade par de moedas de R$0,05 que devem estar associadas às trocas por moedas de R$0,10. Os múltiplos de 5 que são pares e estão entre 0 a 400 (incluindo-os), são: $0, 10, 20, 30, \cdots, 400$. Essa lista é composta por 41 números e corresponde aos modos de usarmos as moedas de R$0,25 e R$0,10 para obtermos a quantia total de R$20,00.*

Solução: 4. *Indicamos por x e y a quantidade de moedas de R$0,10 e R$0,25 respectivamente, então de acordo com as informações do problema obtemos a equação:*

$$0,10x + 0,25y = 20,00.$$

Note que, resolver a equação acima é equivalente a resolver a equação diofantina

$$2x + 5y = 400$$

Sabemos que o $mdc(2, 5) = 1$ e $1 \mid 400$, logo a equação diofantina tem solução.Escrevendo o $mdc(2, 5) = 1$ como combinação linear de 2 e 5, temos:

$$2(-2) + 5(1) = 1$$

multiplicando tudo por 400

$$2(-800) + 5(400) = 400$$

temos então a solução geral

$$x = -800 + 5t \text{ e } y = 400 - 2t \qquad \forall t \in \mathbb{Z}$$

temos que x, y *devem ser não negativos.*

$$\begin{array}{rcl} x \geq 0 & & 0 \leq y \\ -800 + 5t \geq 0 & e & 0 \leq 400 - 2t \\ 5t \geq 800 & & 2t \leq 400 \\ t \geq 160 & & t \leq 200 \end{array}$$

$$160 \leq t \leq 200$$

Logo temos $200 - 160 + 1 = 41$ *possibilidades.*

Problema 16. *(OBMEP 2018-Nível 3 - 1ª fase - Questão 11) Qual é o maior valor possível para o máximo divisor comum de dois números naturais cujo produto é 6000?*

Proporemos duas soluções para este problema. Na primeira, serão abordados temas como a decomposição de números em fatores primos, máximo divisor comum, mínimo múltiplo comum e ainda a relação entre eles. Na segunda, além da decomposição em fatoração em primos, apresentaremos a fórmula que relaciona o *mmc* e *mdc* de dois números inteiros. Apesar dessa fórmula não ser usual no ensino fundamental, veremos que é muito útil para resolvermos problemas que relacionam os temas em questão.

Solução: 1. *(OBMEP) O mdc de dois números que estão fatorados como produto de primos é o produto dos primos comuns, cada um elevado ao menor expoente que comparece nas fatorações. Denotamos por* α *e* β *os dois números cujo produto é* $6000 = 2^4 \times 3 \times 5^3$*. Assim, os fatores primos de* α *e* β *são 2, 3 ou 5. O mdc de* α *e* β *será o maior possível, quando os fatores primos estiverem distribuídos de forma mais equânime possível. Em particular, o fator primo 2, que ocorre com expoente par na fatoração de 6000, deve ocorrer com o mesmo expoente nas fatorações de* α *e* β*, a saber, a metade do expoente (*$4 \div 2 = 2$*) que aparece na fatoração de 6000. Para o primo 5, cujo expoente é um número ímpar maior do que 2, devemos maximizar sua ocorrência nas fatorações de* α *e* β*. Para isso, subtraímos 1 de seu expoente na fatoração de 6000, ou seja, fazemos* $3 - 1 = 2$*, e depois tomamos a metade* $(2 \div 2 = 1)$*. Assim, para o caso estabelecido no*

enunciado, a fim de maximizar o mdc entre α e β, devemos ter em suas fatorações o produto $2 \times 2 \times 5 = 20$. Uma possibilidade é $\alpha = 2 \times 2 \times 5 \times 3 = 60$ e $\beta = 2 \times 2 \times 5 \times 5 = 100$. Assim, o maior valor possível para o mdc entre α e β é 20.

Solução: 2. *Sejam a e b os números naturas cujo produto é igual a 6000, pela definição temos que*

$$mdc(a,b) \cdot mmc(a,b) = |ab|$$

como a e b são números naturais, temos que

$$mmc(a,b) \cdot mdc(a,b) = ab \Leftrightarrow mdc(a,b) = \frac{ab}{mmc(a,b)}$$

Como $ab = 6000$ e a decomposição em primos de 6000 é $ab = 6000 = 2^4 \cdot 3 \cdot 5^3$.
Para que o $mdc(a,b)$ seja máximo, o $mmc(a,b)$ deve ser mínimo e para que isso ocorra, devemos distribuir $2^4 \cdot 3 \cdot 5^3$ igualmente entre a e b. Note que em 2^4 basta fazer $4 \div 2 = 2$, em 3 não tem como distribuir igualmente, ficando então, esse fator, com a ou b e ainda em 5^3 faremos $(3-1) \div 2 = 1$ então optamos por fazer a seguinte distribuição:

- $a = 2^2 \cdot 3 \cdot 5 = 60$
- $b = 2^2 \cdot 5^2 = 100$

Então, pela definição de mdc basta tomarmos o expoente mínimo das potências comuns de a e b que são 2^2 e 5, ou seja:
$mdc(a,b) = 2^2 \cdot 5 = 20$ que é a solução do problema.

Note ainda que, poderíamos resolver esse problema optando em calcular o o $mmc(a,b)$. Para isso, pela definição, basta tomar as potências máximas de a e b, ou seja

$$mmc(a,b) = 2^2 \cdot 3 \cdot 5^2 = 300$$

Então, substituindo em $mdc(a,b) = \frac{ab}{mmc(a,b)}$, obtemos

$$mdc(a,b) = \frac{6000}{300} = 20$$

Logo o maior valor possível para o mdc é 20.

Problema 17. *(OBMEP 2008-Nível 3 - 1ª fase - Questão 7) Em certo ano bissexto (isto é, um ano que tem 366 dias) o número de sábados foi maior que o número de domingos. Em que dia da semana caiu o dia 20 de janeiro desse ano?*

Nos problemas que envolvem calendário, é importante que sejam bem definidas as noções básicas do número de dias numa semana, e do número de semanas e meses em um ano, devendo ainda ser destacada a diferença do número de dias no ano comum e bissexto. Na primeira solução, serão usadas as noções de calendário citadas acima e o algoritmo da divisão. Na segunda, faremos uma abordagem do problema usando congruência modular, cujas etapas serão descritas na solução.

Solução: 1. *(OBMEP) Como a cada sábado segue um domingo, para que o número de sábados num ano seja maior que o número de domingos é necessário que o último dia desse ano seja sábado. Como* $366 = 52 \times 7 + 2$*, um ano bissexto consiste de 52 semanas e 2 dias. Logo, se 31 de dezembro foi um sábado, 2 de janeiro também foi um sábado. Contando de 7 em 7, vemos que 16 de janeiro foi um sábado, donde 20 de janeiro foi uma quarta-feira.*

Solução: 2. *Para resolver esse problema, são necessárias algumas informações:*

- *Em um ano comum há 365 dias, e num ano bissexto, 366;*
- *Uma semana tem 7 dias;*
- *Se uma determinada semana iniciar num domingo, terminará num sábado.*

Para obter quantas semanas há em um ano, usaremos congruência módulo 7, temos

$$365 \equiv 1 \pmod 7, \text{ pois } 365 = 7 \cdot 52 + 1$$
$$366 \equiv 2 \pmod 7, \text{ pois } 366 = 7 \cdot 52 + 2$$

ou seja em um ano comum há 52 semanas e 1 dia e num ano bissexto, 52 semanas e 2 dias. Isso nos diz que, se um ano comum iniciar num domingo, terminará num domingo (ou seja, no mesmo dia) e se for bissexto, terminará numa segunda.

Como queremos obter um ano bissexto em que o número de sábados é maior do que o número de domingos, o referido ano deverá terminar num sábado e seu início, numa sexta-feira.

Como são 20 dias desde o início do ano considerado até o dia 20 de janeiro, usando congruências, temos

$$20 \equiv 6 \pmod 7, \text{ pois } 20 = 7 \cdot 2 + 6$$

ou seja, são 2 semanas e 6 dias, então, o dia 20 de janeiro caiu numa quarta-feira.

Problema 18. *(OBMEP - Banco de Questões 2011 Nível 1 - Questão 1) Encontre o menor múltiplo de 9 que não possui algarismos ímpares.*

Este problema requer conceitos de múltiplos, critério de divisibilidade por 9, paridade de inteiros e a representação de números no sistema decimal.

Solução: 1. *Inicialmente note que esse número deve ser inteiro positivo e múltiplo 9, e ainda que, pelo critério de divisibilidade por 9, a soma de seus algarismos, nesse caso são pares, deve ser divisível por 9.*

Chamando esse número por $n = r_k r_{k-1} \cdots r_3 r_2 r_1 r_0$, *onde* $r_k r_{k-1} \cdots r_3 r_2 r_1 r_0$ *são os algarismos desse número e* $r_k, r_{k-1}, \ldots, r_3, r_2, r_1, r_0 \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
Analisaremos algumas possibilidades.

i) Se n tiver apenas 1 algarismo, ou seja $n = a_0$ *há uma possibilidade,* $n = 9$ *que é ímpar e não satisfaz o problema.*

ii) Se n tiver 2 algarismos, ou seja $n = r_1 r_0$, *pelo critério de divisibilidade por 9,* $r_1 + r_0 = 9$ *ou* $r_1 + r_0 = 18$. *Mas pela paridade de números inteiros,* $r_1 + r_0 = 9$ *não é possível, restando o caso* $r_1 + r_0 = 18$ *que ocorre somente se* $n = 99$ *que novamente não satisfaz o problema.*

iii) Se n tiver 3 algarismos, ou seja $n = r_2 r_1 r_0$, *então* $r_2 + r_1 + r_0 = 9$, $r_2 + r_1 + r_0 = 18$ *ou* $r_2 + r_1 + r_0 = 27$. *Mas pela paridade de inteiros, o único caso possível é* $r_2 + r_1 + r_0 = 18$. *Pelo fato de que desejamos obter o menor número possível com algarismos pares, então* $r_2 = 2$, *e para que a soma seja 18, temos que* $r_1 = 8$ *e* $r_0 = 8$, *obtendo assim* $n = 288$.

Problema 19. *(OBMEP - Banco de Questões 2011 Nível 1 - Questão 2) Uma caixa possui o formato de um bloco retangular de dimensões 102 cm, 255 cm e 170 cm. Queremos guardar nessa caixa a menor quantidade possível de pequenos cubos de aresta inteira, de forma a ocupar toda a caixa.*

a) Qual a medida da aresta de cada bloco?

b) Quantos blocos serão necessários?

Este é um problema que propicia a interação da teoria dos números com a geometria. Na solução do problema, usaremos alguns conceitos da geometria, em particular do cálculo do volume de um bloco retangular, que é dado pelo produto das três dimensões, usaremos ainda o máximo divisor comum na determinação da quantidade máxima de bloquinhos de mesma dimensão que cabem no bloco maior e nesse caso optamos por calcular o *mdc* de três números à partir da decomposição em fatores primos das medidas do mesmo.

Solução: 1. *a) Como a medida da aresta do cubo deve ser a menor possível, devemos obter um divisor comum das 3 dimensões do bloco. Então, basta calcularmos o* $mdc(102, 255, 170)$. *Pela decomposição em fatores primos temos*

$$102 = 2 \cdot 3 \cdot 17, 255 = 3 \cdot 5 \cdot 17, 170 = 2 \cdot 5 \cdot 17$$

Como o $mdc(102, 255, 170) = 17$*, a medida das das arestas do cubo é igual a 17 cm.*

b) Para calcularmos o número de cubos que cabem no bloco retangular, basta dividir o volume do bloco pelo volume de cada cubo, assim

$$\frac{102 \cdot 255 \cdot 170}{17 \cdot 17 \cdot 17} = 6 \cdot 15 \cdot 10 = 900$$

Logo, há 900 cubos no blocos retangular.

Problema 20. *(OBMEP-Banco de Questões-2011 Nível 1 - Questão 5) Dizemos que um número natural é sortudo se todos os seus dígitos são iguais a 7. Por exemplo, 7 e 7777 são sortudos, mas 767 não é. João escreveu num papel os vinte primeiros números sortudos começando pelo 7, e depois somou-os. Qual o resto da divisão dessa soma por 1000?*

Note que este problema é similar ao problema 8. Como já vimos, mostramos duas formas para resolvê-lo o que pode ser feito de maneira análoga aqui, porém, optamos por resolver este problema usando congruência modular e suas propriedades. Como desejamos encontrar o resto da divisão dessa soma por 1000, usaremos congruência módulo 1000, cujos cálculos serão descritos na solução.

Solução: 1. *Note que a soma dos 20 números sortudos corresponde à* $7 + 77 + 777 + \ldots + \underbrace{77\ldots777}_{20\,setes}$.
Para obtermos o resto da divisão dessa soma, usaremos congruência e suas propriedades. Temos que,

$$\begin{aligned}
7 &\equiv 7 \pmod{1000} \\
77 &\equiv 77 \pmod{1000} \\
777 &\equiv 777 \pmod{1000} \\
7777 &\equiv 777 \pmod{1000} \\
&\vdots \\
\underbrace{7\ldots777}_{20\,setes} &\equiv 777 \pmod{1000}
\end{aligned}$$

Note ainda que todo número sortudo a partir de 777, deixa resto 777 na divisão por 1000. Agora, escrevendo essa soma por N, temos

$$N \equiv 7 + 77 + \underbrace{777 + 777 + 777 + \cdots + 777}_{18\,vezes} \pmod{1000}$$

$$N \equiv 7 + 77 + 18 \cdot 777 \equiv 14070 \equiv 70 \pmod{1000}$$

Logo o resto da divisão de $7 + 77 + 777 + \ldots + \underbrace{77\ldots777}_{20\,setes}$ por 1000, é igual a 70.

Problema 21. *(OBMEP-Banco de Questões 2011 Nível 2 - Questão 47)*

a) Prove que o número 3999991 não é primo.

b) Prove que o número 1000343 não é primo

Neste problema, proporemos duas soluções. Na primeira, serão utilizadas as identidades $a^2 - b^2 = (a - b) \cdot (a + b)$ e $a^3 + b^3 = (a + b) \cdot (a^2 - ab + b^2)$, os conceitos de números primos e compostos. Na segunda solução, proporemos explorar o lema 40 para o teste de primalidade as proposições 11 e 12.

Solução: 1. *(OBMEP)*

a) Observe que

$$3999991 = 400000 - 9 = 4 \cdot 10^6 - 3^2 = (2 \cdot 10^3)^2 - 3^2 = (2 \cdot 10^3 - 3)(2 \cdot 10^3 + 3)$$
$$= 1997 \cdot 2003$$

b) Observe que

$$1000343 = 10^6 + 7^3 = (10^2)^3 + 7^3 = (10^2 + 7)((10^2)^2 - 10^2 \cdot 7 + 7^2)$$
$$= (10^2 + 7)((10^2)^2 - 10^2 \cdot 7 + 7^2) = 107 \cdot 9349,$$

portanto não é um número primo.

Solução: 2. *a) Inicialmente vamos verificar se 3999991 é primo. Pelo lema 40, temos que*

$$\sqrt{3999991} < 2000,$$

agora, temos que verificar se 3999991 é divisível por algum número primo menor do que 2000, mas, isso seria uma tarefa cansativa e desmotivante pois existem muitos primos menores do que 2000.

Note que $3999991 = 4000000 - 9 = 2000^2 - 3^2$ *e pela proposição 11, fazendo* $a = 2000$, $b = 3$ *e* $n = 2$, *temos que* $(2000 - 3) \mid 2000^2 - 3^2$, *ou seja* $1997 \mid 3999991$, *pois* $3999991 = 1997 \cdot 2003$. *Logo, 3999991 concluímos é um número composto.*

b) *Já vimos que o teste de primalidade em números grandes não e prático, então, como* $1000343 = 1000000 + 343 = 10^6 + 7^3 = (10^2)^3 + 7^3$ *e pela proposição 12, fazendo* $a = 10^2$, $b = 7$ *e* $n = 3$, *temos que* $(10^2 + 7) \mid 10^6 + 7^3$, *ou seja* $107 \mid 1000343$, *pois* $1000343 = 107 \cdot 9349$. *Logo, 1000343 é um número composto.*

Problema 22. *(OBMEP-Banco de Questões 2015 Nível 3 Questão 28) Em uma lousa são escritos os 2014 inteiros positivos de 1 até 2014. A operação permitida é escolher dois números a e b, apagá-los e escrever em seus lugares os números* $mdc(a, b)$*(máximo divisor comum) e* $mmc(a, b)$*(mínimo múltiplo comum). Essa operação pode ser feita com quaisquer dois números que estão na lousa, incluindo os números que resultaram de operações anteriores. Determine qual a maior quantidade de números 1 que podemos deixar na lousa.*

Para resolvermos este problema, inicialmente usaremos os conceitos de paridade o lema 21 para mostrar que dois números consecutivos são coprimos. A partir daí, com essas informações, encontraremos a quantidade máxima de números 1, conforme segue abaixo.

Solução: 1. *Representando por a e b esses números inteiros positivos e fazendo* $b = a + 1$, *ou seja o sucessor de a. Pelo lema 21 temos que:*

$$mdc(a, b) = mdc(a, a + 1) = mdc(a, a + 1 - a) = mdc(a, 1) = 1.$$

Note que, o mdc de dois números consecutivos, sempre será igual a 1, ou seja, são coprimos. Isso nos mostra que a maior quantidade de números iguais a 1 que podemos obter, ocorre quando tomamos os números consecutivos dessa sequência, ou seja devemos obter o $mdc(a, b)$ *dos pares de números* $\underbrace{(1, 2), (3, 4), \cdots, (20013, 20014)}_{1007\ pares}$, *obtendo assim 1007 números iguais a 1.*

Problema 23. *(OBMEP - Banco de Questões 2015 Nível 3 Questão 22) Seja n um número inteiro positivo. Se, para cada divisor primo p de n, o número* p^2 *não divide n, dizemos então que n é livre de quadrados. Mostre que todo número livre de quadrados tem uma quantidade de divisores que é igual a uma potência de 2.*

Neste problema, usaremos os conceitos de divisibilidade, decomposição de um número em fatores primos e a fórmula que permite encontrar o número de divisores positivos de um número inteiro. Sugerimos que seja exibido um caso para deixar mais claro o que se pede. Por

exemplo, o número $15 = 3 \cdot 5$, cujos divisores primos são 3 e 5, como $3^2 \nmid 15$ e $5^2 \nmid 15$ e a quantidade de divisores pode ser obtida por $d(15) = (1+1) \cdot (1+1) = 4$. Como os divisores positivos de 15 são 1,3,5 e 15. Note que há $2^2 = 4$ divisores livres de quadrados ou seja, uma potência de 2.

Solução: 1. *Seja n um número livre de quadrados cuja fatoração em primos é dada por:*

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

onde $p_1, p_2, \cdots, p_k$ são números primos e $\alpha_1, \alpha_2, \cdots, \alpha_k$ são os expoentes.

Como queremos que n seja livre de quadrados, então, os expoentes devem ser todos iguais a 1. Portanto,

$$n = p_1 \cdot p_2 \cdots p_k$$

Agora, para contarmos a quantidade de divisores de n, basta usarmos a fórmula

$$d(n) = \underbrace{(1+1) \cdot (1+1) \cdot \cdots \cdot (1+1)}_{k\ vezez} = \underbrace{2 \cdot 2 \cdot 2 \cdots 2}_{k\ vezes} = 2^k$$

Logo, todo número livre de quadrados tem uma quantidade de divisores igual a uma potência de 2.

Problema 24. *(OBMEP - Banco de Questões 2018 Nível 2 Questão 25) Se $A = \underbrace{111 \cdots 111}_{2m}$ e $B = \underbrace{444 \cdots 444}_{m}$, verifique a soma $A+B+1$ é um quadrado perfeito para qualquer inteiro positivo m.*

Para resolver este problema, serão necessários conhecimentos acerca dos números quadrados perfeitos, critério de divisibilidade por 3, da identidade $(a+b)^2 = a^2+2ab+b^2$ e do valor posicional dos algarismos no sistema de numeração decimal, em particular da representação de números formados apenas por algarismos iguais a 1. Note que esse tipo de número pode ser escritos na forma $\dfrac{10^n - 1}{9}$ onde n é um número inteiro positivo e representa a quantidade de dígitos iguais a 1. Esse resultado pode ser justificado de duas maneiras:

1. No ensino fundamental, sugerimos que essa representação pode ser construída através do seguinte procedimento:

$$1 = \frac{10^1 - 1}{9}$$
$$11 = \frac{10^2 - 1}{9}$$
$$111 = \frac{10^3 - 1}{9}$$
$$\vdots$$
$$\underbrace{111\ldots11}_{n\ vezes} = \frac{10^n - 1}{9}$$

2. No ensino médio, isso pode ser feito através da soma dos n termos de uma progressão geométrica.

Assim, como

$$\underbrace{111\cdots111}_{n} = 10^n + 10^{n-1} + \cdots + 10^1 + 1$$

As parcelas do segundo membro dessa igualdade formam a sequência $(1, 10^1, 10^2, \ldots, 10^{n-1}, 10^n)$, cujos termos formam uma progressão geométrica onde, o primeiro termo $a_1 = 1$ e razão $q = 10$. A soma S de seus n termos é dada pela fórmula:

$$S = a_1 \cdot \frac{q^n - 1}{q - 1} = 1 \cdot \frac{10^n - 1}{10 - 1} = \frac{10^n - 1}{9}$$

Solução: 1. *Temos que,*

$$\begin{aligned}
A + B + 1 &= \underbrace{111\cdots111}_{2m} + \underbrace{444\cdots444}_{m} + 1 = \underbrace{111\cdots111}_{2m} + 4 \cdot \underbrace{111\cdots111}_{m} + 1 \\
&= \frac{10^{2m} - 1}{9} + 4 \cdot \frac{10^m - 1}{9} + 1 = \frac{(10^m)^2 - 1}{9} + 4 \cdot \frac{10^m - 1}{9} + 1 \\
&= \frac{(10^m)^2 - 1}{9} + 4 \cdot \frac{10^m - 1}{9} + \frac{9}{9} = \frac{(10^m)^2 - 1 + 4 \cdot 10^m - 4 + 9}{9} \\
&= \frac{(10^m)^2 + 4 \cdot 10^m + 4}{9} = \frac{(10^m + 2)^2}{3^2} \\
&= \left(\frac{10^m + 2}{3}\right)^2
\end{aligned}$$

Pelo critério de divisibilidade por 3, o número $10^m + 2$ é divisível por 3, então, $A + B + 1 = \left(\frac{10^m + 2}{3}\right)^2$ é um quadrado perfeito para qualquer m inteiro positivo.

Problema 25. *(OBMEP - Banco de Questões 2018 Nível 3 Questão 6) Se* $m!$ *termina com exatamente* n *zeros, dizemos que* n *é a cauda do fatorial* $m!$ *Observe os exemplos e responda:*

- $5! = 5 \times 4 \times 3 \times 2 \times 1 = 120$*, termina em um zero, por isso, a cauda do fatorial 5! é 1; e*
- $10! = 3628800$*, termina em dois zeros, logo a cauda do fatorial 10! é igual a 2.*

a) Quais são as caudas dos fatoriais de 20! e 25!?

b) Qual o dígito das dezenas de $7! + 8! + 9! + \ldots + 2018!$*?*

Para resolver este problema, usaremos os conceitos de fatorial, potências, algoritmo da divisão e divisibilidade. No item (a), usaremos o teorema de Legendre, e como queremos encontrar o número de zeros que terminam os números 20! e 25!, devemos obter o maior potência de $10 = 2{\cdot}5$ que divide 20! e 25!. Para o item (b), além dos temas citados anteriormente, usaremos congruência modular e suas propriedades.

Solução: 1. *a) Para determinar quantos zeros termina* 20! *e* 25!*, basta usarmos o teorema de Legendre. Como* $10 = 2 \times 5$*, vamos encontrar a maior potência de 2 e de 5, ou seja* $E_2(n!)$ *e* $E_5(n!)$*.*

Vamos determinar a cauda fatorial de 20!

$$E_2(20!) = \left[\frac{20}{2}\right] + \left[\frac{20}{2^2}\right] + \left[\frac{20}{2^3}\right] + \left[\frac{20}{2^4}\right] = 10 + 5 + 2 + 1 = 18$$
$$E_5(20!) = \left[\frac{20}{5}\right] = 4$$

Temos que, $20! = 2^{18} \cdot 5^4 \cdot k = (2 \cdot 5)^4 \cdot 2^{14} \cdot k = 10^4 \cdot 2^{13} \cdot k = 10000 \cdot 2^{13} \cdot k$ *onde* $k \in \mathbb{N}$*. Logo, a cauda de 20! é 4.*

De modo análogo vamos achar a cauda fatorial de 25!*.*

$$E_2(25!) = \left[\frac{25}{2}\right] + \left[\frac{25}{2^2}\right] + \left[\frac{25}{2^3}\right] + \left[\frac{20}{2^4}\right] = 12 + 6 + 3 + 2 + 1 = 24$$
$$E_5(25!) = \left[\frac{25}{5}\right] + \left[\frac{25}{5^2}\right] = 5 + 1 = 6$$

Temos que, $25! = 2^{24} \cdot 5^6 \cdot k' = (2 \cdot 5)^6 \cdot 2^{18} \cdot k' = 10^6 \cdot 2^{13} \cdot k' = 1000000 \cdot 2^{13} \cdot k'$ *onde* $k' \in \mathbb{N}$ *logo a cauda de 25! é 6.*

Note que seria suficiente calcular apenas $E_5(n)$*, reduzindo assim os cálculos.*

b) Como queremos determinar os dígitos das dezenas dessa soma, devemos encontrar os restos da divisão dessa soma por 100. Neste caso usaremos congruência módulo 100.

$$7! = 5040 \equiv 40 \pmod{100}$$
$$8! = 40320 \equiv 20 \pmod{100}$$
$$9! = 362880 \equiv 80 \pmod{100}$$

Note que $10!$ *é divisível por 100, logo qualquer número fatorial maior do que* $10!$ *também será, isso implica que ao dividir qualquer número nessas condições por 100, deixará resto igual a 0.*

Representando por S *essa soma, ou seja,* $S = 7! + 8! + 9! + \ldots + 2018!$*, temos que*

$$S = 7! + 8! + 9! + 10! \ldots + 2017 + 2018! \equiv 40 + 20 + 80 + \underbrace{0 + 0 \ldots + 0}_{2009\ zeros} \equiv 140 \equiv 40 \pmod{100}$$

Portanto, o dígito das dezena é 4.

Problema 26. *(OBMEP - Banco de Questões 2018 Nível 3 Questão 3) Seja* $S(n)$ *a soma dos dígitos de um inteiro* n*. Por exemplo,* $S(327) = 3 + 2 + 7 = 12$*. Encontre o valor de*

$$A = S(1) - S(2) + S(3) - S(4) + \cdots - S(2016) + S(2017).$$

Na solução desse problema, serão necessários os conceitos de paridade e valor posicional do sistema de numeração decimal. Mostraremos que ao fazermos a diferença da soma dos dígitos de números consecutivos, observadas as restrições que mostraremos abaixo, o valor obtido será igual a 1.

Solução: 1. *Se* m *é par, o número* $m + 1$ *possui os mesmos dígitos que* m *com exceção do dígito das unidades, que é uma unidade maior. Portanto,* $S(m + 1) - S(m) = m + 1 - m = 1$*. Isso nos permite agrupar os termos da sequência em pares com diferença igual a 1:*

$$\begin{aligned} A &= S(1) - S(2) + S(3) - S(4) + \ldots - S(2016) + S(2017) \\ &= S(1) + (S(3) - S(2)) + (S(5) - S(4)) + \ldots + (S(2017) - S(2016)) \\ &= 1 + \underbrace{1 + 1 + \ldots + 1}_{1008\ vezes} \\ &= 1 + 1008 = 1009 \end{aligned}$$

Logo, a soma é igual a 1009.

Problema 27. *(OBMEP - Banco de Questões 2017 Nível 2 Questão 6) Determine se o número* $\underbrace{11\cdots1}_{2016}2\underbrace{11\cdots1}_{2016}$ *é um número primo ou um número composto.*

Para resolver este problema, usaremos os conceitos de números primos, compostos, a representação de um número no sistema de numeração decimal e sua decomposição. Sugerimos que sejam ilustrados casos mais simples para facilitar a compreensão dos alunos. Como exemplo, temos

$$\begin{aligned} 121 &= 110 + 11 = 11 \cdot 10^1 + 11 = 11 \cdot (10^1 + 1) \\ 11211 &= 11100 + 111 = 111 \cdot 10^2 + 111 = 111 \cdot (10^2 + 1) \\ &\vdots \\ \underbrace{111\cdots1}_{n\ uns}2\underbrace{111\cdots1}_{n\ uns} &= \underbrace{111\cdots1}_{n+1\ uns}\cdot 10^n + \underbrace{111\cdots1}_{n+1\ uns} = \underbrace{111\cdots1}_{n+1\ uns}\cdot(10^n+1) \end{aligned}$$

Solução: 1. *Para que um número seja composto, deve possuir 2 ou mais divisores maiores que 1.*

Note que

$$\begin{aligned} \underbrace{11\cdots1}_{2016}2\underbrace{11\cdots1}_{2016} &= \underbrace{11\cdots1}_{2017}\cdot 10^{2016} + \underbrace{11\cdots1}_{2017} \\ &= \underbrace{11\cdots1}_{2017}(\cdot 10^{2016}+1) \end{aligned}$$

Como $\underbrace{11\cdots1}_{2017}$ *e* $10^{2016}+1$ *são divisores do número dado e são maiores do que 1, concluímos que* $\underbrace{11\cdots1}_{2016}2\underbrace{11\cdots1}_{2016}$ *é composto.*

Problema 28. *(OBMEP - Banco de Questões 2017 Nível 2 Questão 27) Quantos divisores de* 88^{10} *deixam resto 4 quando divididos por 6?*

Usaremos os conceitos de números primos, decomposição em fatores primos, propriedades das potências, divisibilidade e a relação que permite calcular o número de divisores positivos de inteiro e as propriedades de congruências. Para facilitar a compreensão, sugerimos que inicialmente seja calculado o número de divisores positivos de 88. Isso pode ser feito pela fatoração em primos, onde $88 = 2^3 \cdot 11$, daí, o número de divisores de 88 é dado por

$$d(88) = (3+1)\cdot(1+1) = 4 \cdot 2 = 8$$

ou seja, 88 tem 8 divisores que são os números $1, 2, 4, 8, 11, 22, 44$ e 88.

Solução: 1. *A decomposição em fatores primos de 88 é dada por:*

$$88 = 2^3 \cdot 11 \Rightarrow 88^{10} = (2^3 \cdot 11)^{10} = 2^{30} \cdot 11^{10}.$$

Note que todos os divisores de 88^{10} *são da forma* $2^\alpha \cdot 11^\beta$*, com* $\alpha, \beta \in \mathbb{N}$ *e* $0 \leqslant \alpha \leqslant 30$ *e* $0 \leqslant \beta \leqslant 10$*.*
Queremos determinar todos os divisores de 88^{10} *que deixam resto 4 quando dividido por 6. Usando a notação de congruência isso é equivalente a*

$$2^\alpha \cdot 11^\beta \equiv 4 \pmod 6$$

Analisando as congruências de 2^α *para* $0 < \alpha \leqslant 30$*, temos*

$$\begin{aligned}
2 \equiv & 2 \equiv -4 \pmod 6 \\
2^2 \equiv & 4 \pmod 6 \\
2^3 \equiv & 2 \equiv -4 \pmod 6 \\
2^4 \equiv & 4 \pmod 6 \\
& \vdots \\
2^{29} \equiv & 2 \equiv -4 \pmod 6 \\
2^{30} \equiv & 4 \pmod 6
\end{aligned}$$

Observe que

$$\begin{aligned}
2^\alpha &\equiv 4 \pmod 6 \text{ se } \alpha \text{ for par} \\
2^\alpha &\equiv -4 \pmod 6 \text{ se } \alpha \text{ for ímpar}
\end{aligned}$$

Ao analisarmos as congruências de 11^β*, com* $0 \leqslant \beta \leqslant 10$*, temos que*

$$\begin{aligned}
11^\beta &\equiv (-1)^\beta \equiv 1 \pmod 6, \text{ se } \beta \text{ for par, incluindo o 0} \\
11^\beta &\equiv (-1)^\beta \equiv -1 \pmod 6, \text{ se } \beta \text{ for ímpar.}
\end{aligned}$$

Como os resultados que nos interessam são da forma

$$2^\alpha \cdot 11^\beta \equiv 2^\alpha \cdot (-1)^\beta \equiv 4 \pmod 6$$

Esse resultado ocorre apenas nas seguintes possibilidades:

i) Se α for par maior do que zero, e β for par, incluindo o zero, temos

$$2^{\alpha} \cdot 11^{\beta} \equiv 4 \cdot 1 \equiv 4 \pmod 6.$$

Então há 15 possibilidades para α e 6 para β. Logo há $15 \cdot 6 = 90$ divisores.

ii) Se α for ímpar e β for ímpar, incluindo o zero, temos

$$2^{\alpha} \cdot 11^{\beta} \equiv (-4) \cdot (-1) \equiv 4 \pmod 6.$$

Então há 15 possibilidades para α e 5 para β. Logo há $15 \cdot 5 = 75$ divisores.

Portanto, há $90 + 75 = 165$ divisores com essas características.

Problema 29. *(POTI-Nível 2) Prove que para cada primo p, a diferença $111\ldots11222\ldots22333\ldots33\ldots888\ldots88999\ldots99 - 123456789$ (onde cada digito está escrito exatamente p vezes) é múltiplo de p.*

Para resolver esse problema, usaremos o resultado do exercício 24, critérios de divisibilidade por 2 e 3, *mdc*, as definições e propriedades de congruências e o pequeno teorema de Fermat.

Solução: 1. *Pelo problema 24, temos que*

$$\underbrace{111\ldots111}_{p\ uns} = \frac{10^p - 1}{9}$$

Assim, podemos escrever o número

$$S = 111\ldots11222\ldots22333\ldots33\ldots888\ldots88999\ldots99$$

da seguinte forma:

$$S = 111\ldots11222\ldots22333\ldots33\ldots888\ldots88999\ldots99$$
$$S = \frac{10^p - 1}{9} \cdot 10^{8p} + 2 \cdot \frac{10^p - 1}{9} \cdot 10^{7p} + 3 \cdot \frac{10^p - 1}{9} \cdot 10^{6p} + \ldots + 9 \cdot \frac{10^p - 1}{9}$$

Multiplicando por 9 os 2 lados da igualdade, temos

$$9S = (10^p - 1) \cdot 10^{8p} + 2 \cdot (10^p - 1) \cdot 10^{7p} + 3 \cdot (10^p - 1) \cdot 10^{6p} + \ldots + 9 \cdot (10^p - 1)$$

Vamos verificar se é válido para os casos $p = 2$ *e* $p = 3$.

- *Se* $p = 2$, *temos que:*

$$112233445566778899 - 123456789$$

é um número múltiplo de 2, pois, pelo critério de divisibilidade por 2,

$$2 \mid 112233445566778899 - 123456789.$$

- *Se* $p = 3$, *temos que*

$$111222333444555666777888999 - 123456789$$

é múltiplo de 3, pois, pelo critério de divisibilidade por 3, $3 \mid 111222333444555666777888999$ *e* $3 \mid 123456789$, *logo* $3 \mid 111222333444555666777888999 - 123456789$.

Analisaremos os casos em que $p > 3$

Nesse caso, devemos mostrar que $9(S - 123456789)$ *é divisível por* p, *pois* $mdc(9, p) = 1$.

Pelo pequeno teorema de Fermat:

$$\begin{aligned} 9S &= (10^p - 1) \cdot 10^{8p} + 2 \cdot (10^p - 1) \cdot 10^{7p} + 3 \cdot (10^p - 1) \cdot 10^{6p} + \ldots + 9 \cdot (10^p - 1) \\ &\equiv (10 - 1) \cdot 10^{8p} + 2 \cdot (10 - 1) \cdot 10^{7p} + 3 \cdot (10 - 1) \cdot 10^{6p} + \ldots + 9 \cdot (10 - 1) \\ &\equiv 9 \cdot 123456789 \pmod{p} \end{aligned}$$

Do resultado acima, temos que

$$9S - 9 \cdot 123456789 \equiv 0 \pmod{p} \Rightarrow 9(S - 123456789) \equiv 0 \pmod{p}$$

o que prova o resultado.

Problema 30. *(OBMEP - Banco de Questões 2017 Nível 2 Questão 11) Uma fração é dita irredutível quando seu numerador e seu denominador não possuem fatores comuns, ou seja, quando o máximo divisor comum entre os dois números é 1. Por exemplo, a fração* $\frac{3}{7}$ *é irredutível, mas a fração* $\frac{10}{14}$ *não é, uma vez que 2 é um fator comum de 10 e 14.*
Para que valores de n *a fração* $\frac{5n+6}{6n+5}$ *é irredutível?*

a) *Seja* $d = mdc(5n + 6, 6n + 5)$ *o máximo divisor comum de* $5n + 6$ *e* $6n + 5$. *Verifique que* d *é um divisor de* $n - 1$.

b) *Sabendo que d é um divisor de $n-1$, conclua que d também é um divisor 11.*

c) *Verifique que se 11 divide $5n+6$, então 11 divide $6n+5$.*

d) *Para quantos inteiros positivos n, menores que 50, a fração $\dfrac{5n+6}{6n-5}$ é irredutível?*

Neste problema, utilizaremos os conceitos de divisibilidade, o lema de Euclides para verificar a irredutibilidade de uma fração, e os conceitos de congruência modular para verificar a divisibilidade.

Solução: 1. a) *Como $d = mdc(5n+6, 6n+5)$, pelo lema de Euclides, temos que:*

$$\begin{aligned} d = mdc(5n+6, 6n+5) &= mdc(5n+6, 6n+5-(5n+6)) \\ &= mdc(5n+6, n-1). \end{aligned}$$

Como $d \mid (5n+6)$ e $d \mid (n-1)$, então d é divisor de $n-1$.

b) *Pelo item (a), temos que $d = mdc(5n+6, n-1)$, então ainda pelo lema de Euclides temos que:*

$$\begin{aligned} d = mdc(5n+6, n-1) &= mdc(n-1, 5n+6-5\cdot(n-1)) \\ &= mdc(n-1, 11). \end{aligned}$$

Como $d \mid (n-1)$ e $d \mid 11$ então d é divisor de 11.

c) *Se $11 \mid 5n+6$, usando congruência módulo 11, isso é equivalente a*

$$5n+6 \equiv 0 \pmod{11}$$

Somando $6n+5$ nos dois lados da congruência, temos

$$6n+5+5n+6 \equiv 6n+5 \pmod{11} \Rightarrow 11n+11 \equiv 6n+5 \pmod{11} \Rightarrow 0 \equiv 6n+5 \pmod{11}$$

Isso é equivalente a $11 \mid 6n+5$.

d) *Pelo item (b), temos $d = mdc(n-1, 11) \Rightarrow d \mid (n-1)$ e $d \mid 11$, então $d = 1$ ou $d = 11$, se $d = 11$, temos que os $n-1 = 11k \Rightarrow n = 1+11k$ então como n são os números positivos menores que 50, temos que se $n \in \{1, 12, 23, 34, 45\}$, a fração será irredutível e nos demais casos há $50-5 = 45$ inteiros positivos n menores que 50.*

Problema 31. *(POTI-Nível 2) Encontre um número natural N que, ao ser dividido por 10, deixa resto 9, ao ser dividido por 9 deixa resto 8, e ao ser dividido por 8 deixa resto 7.*

Resolveremos esse problema de duas maneiras. Na primeira, usaremos as notações e definições do teorema chinês dos restos e na outra solução, o algoritmo da divisão e divisibilidade, máximo divisor comum e os conhecimentos de resolução de sistemas lineares que é um tema comum no ensino fundamental e médio.

Solução: 1. *Seja N número natural a ser determinado, usando as propriedades de congruência, podemos reescrever o problema da seguinte forma:*

$$\begin{cases} N \equiv 9 \pmod{10} \\ N \equiv 8 \pmod{9} \\ N \equiv 7 \pmod{8} \end{cases}$$

Podemos resolver esse sistema de congruências lineares, usando as definições do teorema chinês dos restos.

Como $mdc(10,9) = 1$, $mdc(10,8) = 2$ e $mdc(9,8) = 1$, note que nem todos os m_i são primos entre si. Assim, considerando $m_1 = 10$ e $m_3 = 8$, temos que
$mdc(10,8) = 2$ e $9 \equiv 7 \pmod 2$, então o sistema tem solução única $\pmod{mmc(10,9,8)} = \pmod{360}$. Por inspeção, analisando todas as congruências, temos que $N = -1$ é solução de todas as congruências, logo $N \equiv -1 \pmod{360}$ é equivalente a $N = 360t - 1$ com $t \in \mathbb{N}^*$, representa todas as soluções possíveis.

Listando alguns desses resultados, obtemos:

- *Para $t = 1 \Rightarrow N = 360 \cdot 1 - 1 = 359$*
- *Para $t = 2 \Rightarrow N = 360 \cdot 2 - 1 = 719$.*

Solução: 2. *Seja N número natural a ser determinado, pelo algoritmo da divisão, representaremos o problema através de um sistema de equações.*

$$\begin{cases} N = 10a + 9 & (1) \\ N = 9b + 8 & (2) \\ N = 8c + 7 & (3) \end{cases}$$

com $a, b, c \in \mathbb{N}$

Somando 1 em ambos os lados das equações (1), (2) e (3), temos :

$$\begin{cases} N+1 = 10a+10 = 10(a+1) = 10a' \\ N+1 = 9b+9 = 9(b+1) = 9b' \\ N+1 = 8c+8 = 8(c+1) = 8c' \end{cases}$$

com $a', b', c' \in \mathbb{N}$

Note que $N+1$ *é simultaneamente um múltiplo de 8,9 e 110, como o* $mdc(8,9,10) = 360$*, seque que* $N+1 = 360.t$ *com* $t \in \mathbb{N}$*, logo* $N = 360t - 1$*. Listando alguns desses resultados, obtemos:*

- *Para* $t = 1 \Rightarrow N = 360 \cdot 1 - 1 = 359$
- *Para* $t = 2 \Rightarrow N = 360 \cdot 2 - 1 = 719$*.*

Problema 32. *(RPM-80 Questão 346)*

a) Mostre que o resto da divisão de $3^{2012} - 1$ *por* $3^{12} - 1$ *é* $3^8 - 1$*.*

b) Determine o $mdc(3^{2012} - 1, 3^{12} - 1)$*.*

No item (a) desse problema, usaremos o algoritmo da divisão, e divisibilidade. Note que, podemos resolver esse problema usando a proposição 27, cujo resultado é obtido no item (b). No item (b) usaremos apenas a proposição 27, para encontrar o $mdc(3^{2012} - 1, 3^{12} - 1)$.

Solução: 1. *a) Pelo algoritmo da divisão temos que* $2012 = 12 \cdot 167 + 8$ *e somando e subtraindo* 3^8 *em* $3^{2012} - 1$*, temos*

$$\begin{aligned} 3^{2012} - 1 = 3^{12 \cdot 167 + 8} - 1 &= (3^{12})^{167} \cdot 3^8 - 3^8 + 3^8 - 1 \\ &= 3^8((3^{12})^{167} - 1) + (3^8 - 1) \\ &= 3^8(3^{12} - 1)(3^{166} + 3^{165} + \cdots + 3^{12} + 1) + (3^8 - 1) \end{aligned}$$

Como $3^{12} - 1 \mid 3^8(3^{12} - 1)(3^{166} + 3^{165} + \cdots + 3^{12} + 1)$ *e* $3^8 - 1 < 3^{12} - 1$*, então, o resto da divisão de* $3^{2012} - 1$ *por* $3^{12} - 1$ *é* $3^8 - 1$*.*

b) Para obter o $mdc(3^{2012} - 1, 3^{12} - 1)$*, vamos utilizar a proposição 27.*

Fazendo $a = 3, m = 2012, n = 12$*, temos que*

$$mdc(3^{2012} - 1, 3^{12} - 1) = 3^{mdc(2012,12)} - 1$$

Como $mdc(2012, 12) = 4$*, então,*

$$mdc(3^{2012} - 1, 3^{12} - 1) = 3^4 - 1 = 81 - 1 = 80$$

Problema 33. *Mostre que* $mdc(a, a + 2) = 1$ *ou 2 para todo inteiro* a*.*

Mais um exercício no qual aplicaremos o lema de Euclides, divisibilidade e a paridade de inteiros.

Solução: 1. *Seja* $d = mdc(a, a + 2)$*, pelo lema de Euclides temos,*

$$d = mdc(a, a + 2) = mdc(a, a + 2 - a) = mdc(a, 2)$$

isso implica que $d \mid a$ *e* $d \mid 2$*.*
Temos suas possibilidades, se a *for ímpar,* $d = 1$ *e se* a *for par,* $d = 2$*.*

Portanto $mdc(a, a + 2) = 1$ *ou* $mdc(a, a + 2) = 2$*.*

Problema 34. *(POTI-Nível 2) Encontre os três últimos dígitos de* 7^{9999}*.*

Neste problema, mostraremos que o teorema de Euler nos permite obter o resto de uma divisão envolvendo números grandes expressos na forma de potências. Note que, obter os três últimos dígitos de 7^{9999}, equivale a dividi-lo por 1000, logo usaremos congruências módulo 1000.

Solução: 1. *Como* $\phi(1000) = \phi(2^3 \cdot 5^3) = \phi(2^3) \cdot \phi(5^3) = 4 \cdot 100 = 400$*, pelo teorema de Euler, temos que*

$$7^{\phi(1000)} \equiv 7^{400} \equiv 1 \pmod{1000}, \text{pois } mdc(7, 1000) = 1. \text{ Assim,}$$

$$7^{10000} = (7^{400})^{25} \equiv 1^{25} \equiv 1 \pmod{1000}$$

Como $7 \cdot 143 = 1001 \equiv 1 \pmod{1000}$*, daí,*

$$7^{9999} \equiv 7^{9999} \cdot 7 \cdot 143 \equiv 7^{10000} \cdot 143 \equiv 143 \pmod{1000}$$

Logo, os três últimos dígitos de 7^{9999} *é 143.*

Problema 35. *Prove que se* $m = mmc(a, b)$ *e* $d = mdc(a, b)$*, então* $d \mid m$*. (O mdc sempre divide o mmc).*

Nesse problema, usaremos as definições de máximo divisor comum e de mínimo múltiplo comum para demonstrar que o *mdc* sempre divide o *mmc*. Para facilitar o entendimento, podemos exemplificar um caso particular onde essa relação ocorre. Por exemplo o $mdc(6, 9) = 3$ e o $mmc(6, 9) = 18$, no te que $3 \mid 18$, ou seja o *mdc* divide o *mmc*.

Solução: 1. *Seja $d = mdc(a, b)$, temos que $d \mid a$ e $d \mid b$, logo existem $e, f \in \mathbb{N}$ tais que $a = de$ e $b = df$.*

Temos ainda que $m = mmc(a, b)$, então $m = ag = bh$, com $g, h \in \mathbb{N}$.

Se $d \mid m$, então existe $k \in \mathbb{N}$, e único onde $m = dk$

Mas $m = ag = bh$, logo $a = \dfrac{m}{g}$ e $b = \dfrac{m}{h}$.

Pela definição, temos que

$$mdc(a, b) \cdot mmc(a, b) = ab \Rightarrow dm = (\frac{m}{g})(\frac{m}{h}) \Rightarrow m = dgh.$$

Assim, temos que $m = dk$ e $m = dgh \Rightarrow dk = dgh \Rightarrow k = gh$. Portanto, se $d \mid m$, então $mmc(a, b) = m$ e $mdc(a, b) = d$.

Problema 36. *Determine todos os números naturais a e b satisfazendo as equações $mdc(a, b) = 10$ e $mmc(a, b) = 100$.*

Neste problema, note que devemos resolver um sistema envolvendo o *mmc* e o *mdc* de dois números. Nesse caso, usaremos as definições do *mmc* e *mdc* e a fórmula que os relaciona. Esse tipo de problema não é comum no ensino básico, pois requer o conhecimento dos conceitos acerca desse assunto.

Solução: 1. *Resolver as equações $mdc(a, b) = 10$ e $mmc(a, b) = 100$, com a e b naturais, é equivalente a resolver o sistema*

$$\begin{cases} mdc(a, b) = 10 \\ mmc(a, b) = 100 \end{cases}$$

Como $mdc(a, b) = 10$ e $mmc(a, b) = 100$, pela definição,

$$mmc(a, b) \cdot mdc(a, b) = |ab| \Leftrightarrow mdc(a, b) = \frac{|ab|}{mmc(a, b)}$$

daí,

$$100 = \frac{|ab|}{10} \Rightarrow |ab| = 1000.$$

Como $mdc(a, b) = 10$ então $10 \mid a$ e $10 \mid b$, então, existem $m, n \in \mathbb{Z}$, tais que

$$a = 10m \text{ e } b = 10n$$

Como

$$mdc\left(\frac{a}{mdc(a, b)}, \frac{b}{mdc(a, b)}\right) = 1 \Rightarrow mdc\left(\frac{10m}{10}, \frac{10n}{10}\right) = mdc(m, n) = 1$$

Mas $a = 10m$, $b = 10n$ e $ab = 1000$ dessa última equação, temos que

$$10m \cdot 10n = 1000 \Rightarrow mn = 10$$

Desse resultado, segue que

i) Se $m = \pm 1$ *e* $n = \pm 10$ *então* $a = \pm 10$ *e* $b = \pm 100$.

ii) Se $m = \pm 2$ *e* $n = \pm 5$ *então* $a = \pm 20$ *e* $b = \pm 50$.

Pelo fato de que a *e* b *são números naturais, concluímos que os resultados possíveis são os pares*

$$(a, b) = (10, 100), (20, 50), (50, 20), (100, 10)$$

.

Problema 37. *Prove que* $2222^{5555} + 5555^{2222}$ *é divisível por 7.*

Temos aqui um problema envolvendo a soma de duas potências de valor elevado. Como queremos verificar se essa soma é divisível por 7, então usaremos os conceitos de divisibilidade, algoritmo da divisão e congruência modular.

Solução: 1. *Como* $2222 = 7 \cdot 317 + 3$ *e* $5555 = 7 \cdot 793 + 4$, *por congruência módulo 7 e suas propriedades, temos*

$$2222^{5555} + 5555^{2222} \equiv 3^{5555} + 4^{2222} \pmod 7$$

e,

$$3^1 \equiv 3 \pmod 7, 3^2 \equiv 2 \pmod 7, 3^3 \equiv -1 \pmod 7, 3^6 \equiv 1 \pmod 7$$
$$4^1 \equiv 4 \pmod 7, 4^2 \equiv 2 \pmod 7, 4^3 \equiv 1 \pmod 7$$

e ainda, $5555 = 6 \cdot 925 + 5$ *e* $2222 = 3 \cdot 740 + 2$, *segue que,*

$$3^{5555} = 3^{6 \cdot 925 + 5} = (3^6)^{925} \cdot 3^5 \equiv 1^{925}.3^5 \equiv 243 \equiv 5 \pmod 7 \text{ e}$$
$$4^{2222} = 4^{6 \cdot 370 + 2} = (4^6)^{370} \cdot 4^2 \equiv 1^{370} \cdot 16 \equiv 2 \pmod 7$$

Somando, temos

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

Logo $7 \mid 2222^{5555} + 5555^{2222}$.

Problema 38. *(ENQ[3] - 2019.1 Questão 02- adaptado) Prove que* $11^{n+2} + 12^{2n+1}$ *é divisível por 133, para qualquer número natural n.*

Nesse problema, assim como o anterior, usaremos congruências para verificar a divisibilidade de números com potências indefinidas. Esse problema também pode ser demonstrado pelo Princípio da Indução Matemática.

Solução: 1. *Provar que* $11^{n+2} + 12^{2n+1}$ *é divisível por 133, em congruências isso é equivalente a provar que*

$$11^{n+2} + 12^{2n+1} \equiv 0 \pmod{133}.$$

Note que

$$11^{n+2} + 12^{2n+1} = 121 \cdot 11^n + 12 \cdot 144^n$$

Usando as propriedades das congruências, temos

$$\begin{aligned} 11^{n+2} + 12^{2n+1} = 121 \cdot 11^n + 12 \cdot 144^n &\equiv 121 \cdot 11^n + 12 \cdot 11^n \pmod{133} \\ &\equiv 133 \cdot 11^n \pmod{133} \\ &\equiv 0 \pmod{133}. \end{aligned}$$

Portanto, $133 \mid 11^{n+2} + 12^{2n+1}$ *para qualquer n natural.*

Problema 39. *Prove ou dê um contra exemplo para a seguinte afirmação: se* $a = \underbrace{111\cdots111}_{m\ vezes}$ *e* $b = \underbrace{111\cdots111}_{n\ vezes}$ *então* $mdc(a,b) = \underbrace{111\cdots11}_{d\ vezes}$*, em que* $d = mdc(m,n)$*.*

Nesse problema, queremos generalizar qual é o máximo divisor comum entre dois números formados apenas por algarismos iguais a 1. Usaremos o fato de que números formados apenas por algarismos iguais a 1 podem ser representados na forma $\frac{10^n - 1}{9}$ com n inteiro positivo, as propriedades do *mdc* e a proposição 27.

Solução: 1. *Pelo problema 24, temos que*

$$\underbrace{111\cdots111}_{m\ vezes} = \frac{10^m - 1}{9} \ e$$
$$\underbrace{111\cdots111}_{n\ vezes} = \frac{10^n - 1}{9}.$$

[3]Exame Nacional de Qualificação-PROFMAT

Pelas propriedades do mdc , temos que

$$mdc(\underbrace{111\cdots111}_{m\ vezes},\underbrace{111\cdots111}_{n\ vezes}) = mdc\left(\frac{10^m-1}{9},\frac{10^n-1}{9}\right) = \frac{1}{9}\cdot mdc(10^m-1,10^n-1)$$

Pela proposição 27, onde $mdc(10^m-1,10^n-1)$*, e* $d = mdc(m,n)$ *temos que*

$$mdc(10^m-1,10^n-1) = 10^{mdc(m,n)}-1 = 10^d-1$$

Então, segue que

$$mdc(a,b) = mdc(\underbrace{111\cdots111}_{m\ vezes},\underbrace{111\cdots111}_{n\ vezes}) = mdc\left(\frac{10^m-1}{9},\frac{10^n-1}{9}\right) = \frac{1}{9}\cdot(10^d-1)$$

$$mdc(a,b) = \frac{10^d-1}{9} = \underbrace{111\cdots111}_{d\ vezes}$$

Problema 40. $mdc(\underbrace{111\cdots1111}_{80\ vezes},\underbrace{111\cdots1111}_{30\ vezes})$.

Neste problema, aplicaremos o resultado obtido no problema anterior.

Solução: 1. *Pelo problema anterior, temos que*

$$d = mdc(80,30) = 10$$

Então,

$$mdc(\underbrace{111\cdots1111}_{80\ vezes},\underbrace{111\cdots1111}_{30\ vezes}) = \underbrace{111\cdots1111}_{10\ vezes}$$

Considerações finais

.

Considerando que a OBMEP, busca incentivar o aperfeiçoamento dos professores de matemática da educação básica e como consequência a melhoria dos indicadores educacionais dessa componente curricular, foi proposta uma sequência didática, por meio de problemas oriundos da OBMEP, 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, como congruência e resultados como os teoremas de Euler e Legendre. Esses conceitos 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.

Muitas vezes o aluno tem uma ideia "pictórica"da solução de um problema, mas não tem e não conhece os meios adequados de exprimi-la de forma simbólica. Conforme a teoria de Rayond Duval pelo fato da Matemática trabalhar constantemente com objetos abstratos, para o sujeito apropriar-se de um determinado objeto abstrato, deve recorrer a algum tipo de representação, que pode ser algébrica, gráfica ou em língua materna.

Nesse sentido, a resolução de problemas ajuda o aluno a se apropriar dessas ferramentas essenciais na representação de suas ideias.

Também, se justifica inverter a lógica do ensino de matemática e, em vez de, simplesmente apresentar conceitos abstratos e cobrá-los em exercícios corriqueiros, se fazer o inverso, primeiro apresentar o problema para depois, ao tentar desenvolver a sua resolução, se chegar nos conceitos matemáticos necessários.

Esperamos que esse material possa contribuir com os professores que atuam na educação básicas, em particular nos anos finais do ensino fundamental, e demais interessados, propiciando condições para que os alunos obtenham êxito em competições como a OBMEP, bem como na melhoria dos índices educacionais de matemática.

Referências Bibliográficas

Araújo, J. E. (2018). Divisibilidade, congruência e aritmética modular em problemas olímpicos. Dissertação de Mestrado, UFCG, Campina Grande/PB.

Araújo, M. C. (2018). Notas de aula de teoria elementar dos números.

Brasil – MEC (1997). Parâmetros Curriculares Nacionais – terceiro e quarto ciclos do Ensino Fundamental. Disponível em http://portal.mec.gov.br/seb/arquivos/pdf/livro01.pdf Acesso em: 8/mar/2020.

Cunha, A. L. (2019). Aritmética na OBMEP: Uma análise de questões da primeira fase do nível 3. Dissertação de Mestrado, UFRPE, Recife/PE.

D'Ambrosio, U. (1993). Educação Matemática: Uma Visão do Estado da Arte. *Proposições, São Paulo*, 4(1):7–17.

Domingues, H. H. (1991). *Fundamentos de Aritmética-Ed.* Atual, São Paulo.

Fernandes, R. (2007). Índice de Desenvolvimento da Educação Básica (IDEB): metas intermediárias para a sua trajetória no Brasil, estados, municípios e escolas. *INEP/MEC*.

Hefez, A. (2016). *Aritmética*. Coleção Profmat. SBM, Rio de Janeiro, 2ª ed. edição.

Lima, E. (2007). *Matemática e Ensino*. Coleção do Professor de Matemática. SBM, Rio de Janeiro, 3ª ed. edição.

Maranhão, T. (2011). Avaliação de impacto da Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP-2005/2009).

OBMEP (2020). Banco de questões. Disponível em http://www.obmep.org.br/banco.htm. Acesso em: 20/mar/2020.

OBMEP (2020). OBMEP em Números. Disponível em http://www.obmep.org.br/em-numeros.htm. Acesso em: 10/mar/2020.

OBMEP (2020a). Provas e soluções. Disponível em http://www.obmep.org.br/provas.htm. Acesso em: 7/mar/2020.

OBMEP (2020b). Regulamento da OBMEP. Disponível em http://www.obmep.org.br/regulamento.htm. Acesso em: 15/mar/2020.

Pereira, M. M. (2016). A resolução de questões das olimpíadas de matemática com teoremas da aritmética. Dissertação de Mestrado, UNIR, Porto Velho/RO.

Polya, G. (2006). *A arte de resolver problemas.* Interciência, Rio de Janeiro.

POTI (2020). Material Didático. Disponível em https://poti.impa.br/index.php/site/material. Acesso em: 1/abr/2020.

QEdu (2020a). Aprendizado adequado. Disponível em https://academia.qedu.org.br/prova-brasil/aprendizado-adequado/. Acesso em: 10/mar/2020.

QEdu (2020b). Distribuição dos alunos por nível de proficiência. Disponível em https://www.qedu.org.br/brasil/proficiencia. Acesso em: 7/mar/2020.

QEdu (2020c). O que é o IDEB. Disponível em https://academia.qedu.org.br/ideb/o-que-e-o-ideb-2/. Acesso em: 8/mar/2020.

Santos, G. L. e Abreu, P. H. (2011). Avaliação de impacto da Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP): explicitação de condições de sucesso em escolas bem sucedidas.

Santos, J. P. O. (2011). *Introdução à teoria dos números.* Coleção Matemática Universitária. IMPA, Rio de Janeiro, 3ª edição.

Soares, C. M. M. e Leo, E. (2014). Impacto da Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP) no desempenho em matemática na Prova Brasil, ENEM e PISA. 2014.