



UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA
Mestrado Profissional em Matemática em Rede Nacional



Maria Aparecida da Silva Barbosa

**Aritmética nas Olimpíadas de Matemática: uma proposta para
estudantes do Ensino Médio**

RECIFE
2026



UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA
Mestrado Profissional em Matemática em Rede Nacional



Maria Aparecida da Silva Barbosa

Aritmética nas Olimpíadas de Matemática: uma proposta para estudantes do Ensino Médio

Dissertação de mestrado apresentada ao Departamento de Matemática da Universidade Federal Rural de Pernambuco como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Clessius Silva

RECIFE
2026

Dados Internacionais de Catalogação na Publicação
Sistema Integrado de Bibliotecas da UFRPE
Bibliotecário(a): Auxiliadora Cunha – CRB-4 1134

B238a Barbosa, Maria Aparecida da Silva.
Aritmética nas olimpíadas de matemática: uma proposta para estudantes do Ensino médio / Maria Aparecida da Silva Barbosa. – Recife, 2026.
164 f.; il.

Orientador(a): Clessius Silva.

Dissertação (Mestrado) – Universidade Federal Rural de Pernambuco, Programa de Mestrado Profissional em Matemática (PROFMAT), Recife, BR-PE, 2026.

Inclui referências e apêndice(s).

1. Aritmética. 2. Matemática - Olimpíadas. 3. Resolução de problemas. 4. Didática 5. Educação básica. I. Silva, Clessius, orient. II. Título

CDD 510

MARIA APARECIDA DA SILVA BARBOSA

**"Aritmética nas Olimpíadas de Matemática: Uma proposta para
estudantes do Ensino Médio"**

*Trabalho apresentado ao Programa de
Mestrado Profissional em Matemática –
PROFMAT do Departamento de Matemática da
UNIVERSIDADE FEDERAL RURAL DE
PERNAMBUCO, como requisito parcial para
obtenção do grau de Mestre em Matemática.*

Aprovado em 18/06/2026

BANCA EXAMINADORA

Prof. Dr. Clessius Silva (Orientador) – UFRPE

Prof. Dr. Felipe Wergete Cruz - UFPE

Prof. Dr. Marcelo Pedro dos Santos– PROFMAT/UFRPE

À minha família

Agradecimentos

Agradeço primeiramente a Deus pelo dom da vida e pela força que me sustentou em cada etapa desta caminhada. À minha mãe, Maria José da Silva, agradeço por ter concebido a minha vida e por ter me incentivado a estudar durante toda a minha trajetória. Cada conquista alcançada nasceu do apoio, do cuidado e do estímulo que recebi dela. Tudo o que realizei até aqui, e o que ainda construirei, carrega a marca do seu amor e da sua dedicação.

Ao meu parceiro de vida, Adson Sarinho Gomes, deixo minha gratidão mais profunda. Ele é o amor que me sustenta com paciência, confiança e presença constante. Acreditou no meu potencial desde o início, apoiou cada escolha e compreendeu todos os momentos em que o mestrado exigiu grande parte do meu tempo e energia. A sua confiança em mim foi essencial para que eu seguisse até aqui.

Agradeço à EREM Dr. Mota Silveira, ambiente onde vivenciei crescimento e amadurecimento profissional. À gestora Elza de Souza Interaminense, agradeço pela compreensão e pela sensibilidade em viabilizar minha trajetória acadêmica. Sou grata aos meus companheiros de trabalho pelo incentivo à continuidade dos meus estudos. Registro também meu reconhecimento ao professor Douglas de Souza, pelas conversas produtivas e pelas idas à universidade que sempre renderam aprendizado. Agradeço também a Pedro Henrique, pelas leituras atentas e contribuições essenciais na revisão desta dissertação.

Aos meus colegas de turma, agradeço pela parceria nas noites de estudo, nas semanas de provas e nas preparações para o ENQ. Crescemos juntos, compartilhando desafios, descobertas e muito aprendizado. À minha amiga Nataly Maria, agradeço pela troca constante e pelo apoio mútuo desde o ingresso no PROFMAT, mesmo estudando em polos distintos. Agradeço também a Bruno Glasses, pelos materiais de estudo que contribuíram significativamente para minha preparação ao longo do curso.

Ao PROFMAT, registro minha gratidão pela oportunidade de formação e aprimoramento profissional. À CAPES, pelo apoio financeiro concedido ao longo do curso, que possibilitou minha permanência e dedicação ao programa. Aos professores do PROFMAT/UFRPE, deixo meu reconhecimento pelos ensinamentos, pela dedicação e pela construção conjunta de saberes. Ao meu orientador, Prof. Dr. Clessius Silva, pela orientação atenta, o diálogo constante e os direcionamentos oferecidos para o desenvolvimento desta pesquisa.

A todos que contribuíram para esta trajetória, expresso minha sincera gratidão.

*“Sei que meu trabalho é uma gota no oceano,
mas sem ele o oceano seria menor.”
(Santa Teresa de Calcutá)*

Resumo

A preparação olímpica é pouco presente na rotina das escolas públicas, o que faz com que muitos estudantes percebam as provas como excessivamente difíceis. Essa percepção é compreensível, pois, sem momentos específicos de estudo, lidar com os problemas matemáticos torna-se realmente mais desafiador. Além disso, grande parte dos conteúdos explorados nas olimpíadas de matemática não integra o currículo da educação básica, o que amplia ainda mais a distância entre o estudante e as competições olímpicas. Diante desse cenário, este estudo apresenta uma proposta de sequência didática em aritmética voltada à preparação de estudantes do ensino médio para olimpíadas de matemática. Embora essas olimpíadas mobilizem milhões de participantes e desempenhem papel formativo relevante, a ausência de preparação sistemática e de material preparatório nas escolas limita o desempenho dos estudantes. Para enfrentar esse problema, realizou-se uma revisão dos principais conteúdos aritméticos, devido à sua recorrência nas provas olímpicas, apoiada em referências consolidadas na área. A partir desse estudo, foram selecionadas e analisadas questões de edições anteriores, com atenção às estratégias de resolução e aos padrões conceituais envolvidos. Com base nesse material, elaborou-se uma sequência didática composta por sete encontros, destinada a apoiar professores na preparação dos estudantes e a estimular o interesse pela matemática e pela participação em competições olímpicas. A proposta integra teoria, resolução de problemas e atividades investigativas, favorecendo o desenvolvimento do raciocínio lógico, da autonomia intelectual e da confiança dos participantes. Espera-se que o material produzido contribua para fortalecer projetos de preparação olímpica no ambiente escolar e incentivar o interesse pela matemática.

Palavras-chave: Aritmética. Olimpíadas de matemática. Resolução de problemas. Sequência didática. Educação básica.

Abstract

Olympic preparation is usually not part of the routine in public schools, so many students end up seeing these exams as overly difficult. This perception is understandable, since without dedicated study time, tackling mathematical problems becomes much more challenging. Furthermore, much of the content explored in Mathematics Olympiads is not included in the basic education curriculum, which widens the gap between students and these competitions. Given this context, this study presents a proposed didactic sequence in arithmetic aimed at preparing high school students for mathematics Olympiads. Although these Olympiads engage millions of participants and play an important educational role, the lack of systematic preparation and instructional materials in schools limits students' performance. To address this issue, a review of the main arithmetic topics was conducted, given their frequent presence in Olympiad exams, supported by well-established references in the field. Based on this study, questions from previous editions were selected and analyzed, with attention to the problem-solving strategies and the conceptual patterns involved. From this corpus, a didactic sequence consisting of seven sessions was developed, designed to support teachers in preparing students and to foster interest in mathematics and in participating in Olympiad competitions. The proposal integrates theory, problem-solving, and investigative activities, promoting the development of logical reasoning, intellectual autonomy, and students' confidence. It is expected that the material produced will contribute to strengthening Olympiad preparation initiatives in schools and to encouraging greater interest in mathematics.

Keywords: Arithmetic. Mathematics Olympiads. Problem Solving. Didactic Sequence. Basic Education.

Lista de ilustrações

Figura 1 – Tabuleiro do jogo trilha dos restos	94
Figura 2 – Simulação da equação diofantina do caixa eletrônico no GeoGebra. . .	113
Figura 3 – Tabuleiro Trilha dos Restos	134
Figura 4 – Cartas Escova Diofantina - Frente	152
Figura 5 – Cartas Escova Diofantina - Verso	153
Figura 6 – Distribuição dos papéis.	161

Lista de tabelas

Tabela 1	–	Exemplos representativos de soluções da equação $ax + by = 15$	111
Tabela 2	–	Soluções inteiras não negativas para $2x + 5y = 50$	113

Lista de abreviaturas e siglas

SAEB	Sistema de Avaliação da Educação Básica
INEP	Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira
BNCC	Base Nacional Comum Curricular
OBMEP	Olimpíada Brasileira de Matemática das Escolas Públicas
OPEMAT	Olimpíada Pernambucana de Matemática
TMM ²	Torneio Meninas na Matemática
IMO	International Mathematical Olympiad
OBM	Olimpíada Brasileira de Matemática
SBM	Sociedade Brasileira de Matemática
IMPA	Instituto Nacional de Matemática Pura e Aplicada
CNPq	Conselho Nacional de Desenvolvimento Científico e Tecnológico

Sumário

	Introdução	14
1	OLIMPÍADAS DE MATEMÁTICA NA EDUCAÇÃO BÁSICA	16
2	FUNDAMENTOS DA ARITMÉTICA	21
2.1	Divisibilidade	21
2.2	Sistemas de Numeração	23
2.3	Máximo divisor comum	27
2.4	Mínimo múltiplo comum	33
2.5	Equações Diofantinas Lineares	35
2.6	Números primos	38
2.7	Congruência	44
2.8	Teorema Chinês dos Restos	55
3	RESOLUÇÃO DE PROBLEMAS	58
3.1	Problemas	60
4	SEQUÊNCIA DIDÁTICA	88
4.1	Orientação Docente	88
4.2	Proposta Didática	89
4.3	Encontros e questões propostas	92
4.3.1	Encontro 01 – Divisibilidade	92
4.3.2	Encontro 02 - Sistema de Numeração	99
4.3.3	Encontro 03 - Máximo divisor comum	103
4.3.4	Encontro 04 - Equações Diofantinas	109
4.3.5	Encontro 05 - Números Primos	116
4.3.6	Encontro 06 - Congruências	120
4.3.7	Encontro 07 - Teorema chinês dos restos	125
	Conclusão	129
	REFERÊNCIAS	130
	APÊNDICES	132
	APÊNDICE A – DIVISIBILIDADE	133

APÊNDICE B – SISTEMAS DE NUMERAÇÃO	138
APÊNDICE C – MÁXIMO DIVISOR COMUM E MÍNIMO DIVISOR COMUM	147
APÊNDICE D – EQUAÇÕES DIOFANTINAS	151
APÊNDICE E – NÚMEROS PRIMOS	156
APÊNDICE F – CONGRUÊNCIA	160
APÊNDICE G – TEOREMA CHINÊS DOS RESTOS	164

Introdução

As olimpíadas científicas têm ganhado cada vez mais espaço e incentivo no Brasil, especialmente aquelas voltadas para a área da matemática. Os resultados obtidos ao longo dos anos mostram que essas competições podem ser um caminho promissor para a descoberta de jovens talentos brasileiros. No entanto, ao analisar os conteúdos necessários para um bom desempenho nessas olimpíadas e a realidade cotidiana da sala de aula, percebe-se que o currículo, como a BNCC (1), não está alinhado aos objetivos dessas competições. Diante disso, torna-se essencial proporcionar momentos de preparação que permitam ao estudante vivenciar experiências formativas, despertar o interesse pela área e desenvolver as competências necessárias para enfrentar desafios matemáticos de forma satisfatória.

Entre as áreas da matemática presentes na trajetória escolar, destaca-se a Aritmética como tema central deste trabalho. A aritmética está entre as primeiras áreas com as quais o estudante tem contato ao iniciar sua vida escolar, constituindo-se como uma das bases do desenvolvimento do raciocínio lógico. Normalmente, muitos problemas desse campo podem ser resolvidos de maneira intuitiva, por meio de tentativas, verificações e ajustes no pensamento matemático, permitindo que o estudante proponha estratégias iniciais mesmo sem dominar completamente o conteúdo envolvido. Em diversas situações, ele consegue simplificar a questão para compreender o que está sendo solicitado e identificar o padrão presente no problema. Assim, trabalhar com problemas aritméticos pode ser um caminho eficaz para despertar o interesse, estimular a criatividade e fortalecer a base necessária para enfrentar desafios mais complexos.

Nessa perspectiva, a resolução de problemas assume papel essencial. É preciso oferecer ao estudante oportunidades de compreender problemas, formular estratégias de resolução, planejamento e execução de ações que o conduzam a uma solução consistente. Parte desse processo envolve verificar se a resposta encontrada condiz com o que foi proposto e tal julgamento é uma habilidade que tende a se desenvolver com mais facilidade quando o problema possui uma estrutura simples. Entretanto, diante de problemas mais complexos, o estudante necessita de suporte teórico que o auxilie na tomada de decisões fundamentadas. Daí surge a importância de trabalhar esses temas na Educação Básica, permitindo que os estudantes desenvolvam repertório, estratégias e confiança para lidar com situações desafiadoras. A utilização de questões olímpicas de edições anteriores contribui para esse processo, pois possibilita ao estudante adquirir experiência, compreender o estilo das avaliações, desenvolver postura investigativa e aprender a enfrentar questões inéditas com autonomia.

Diante desse cenário e considerando a necessidade de oferecer suporte teórico e prático aos docentes, emerge a seguinte questão orientadora desta pesquisa: que fundamentos e atividades devem compor uma sequência didática de aritmética capaz de apoiar professores na preparação de estudantes para olimpíadas de matemática?

A partir dessas reflexões, os objetivos desta pesquisa envolvem promover, no ambiente da escola pública, a criação de um espaço formativo, considerando as dificuldades enfrentadas nesse contexto, como a falta de recursos, de estrutura adequada e de tempo específico para a preparação de estudantes para olimpíadas. Nesse cenário, essa preparação, em muitos casos, ocorre por meio de ações complementares desenvolvidas pelo professor, para além das atividades previstas na rotina escolar. Pretende-se despertar nos estudantes o interesse pelas olimpíadas de matemática por meio de um curso de aritmética, fortalecendo sua confiança, desenvolvendo habilidades matemáticas e ampliando suas perspectivas acadêmicas. Busca-se também estudar os principais conteúdos recorrentes em aritmética nas competições de forma acessível e significativa, analisando e resolvendo questões das edições passadas, apresentar soluções alternativas quando possível, além de estimular a leitura, a escrita e a argumentação matemática, favorecendo o raciocínio necessário para provas discursivas. A proposta inclui ainda incentivar o raciocínio lógico-dedutivo, promover o desenvolvimento matemático por meio de atividades desafiadoras e produzir um material didático acessível e adaptável, que possa ser utilizado por outros professores da educação básica.

Com esse propósito, foi elaborada uma sequência didática voltada a professores da educação básica, oferecendo subsídios para o trabalho com estudantes que desejam ampliar seus conhecimentos matemáticos. A sequência apresentada nesta dissertação serve como material didático de apoio, reunindo sugestões de conteúdos, atividades motivadoras e problemas de edições anteriores de Olimpíadas de Matemática. Espera-se que esse material possa contribuir para a implementação ou o fortalecimento de projetos olímpicos no ambiente escolar, estimulando a participação dos estudantes em clubes de matemática. Mais que focar na conquista de medalhas, pretende-se aproximar os estudantes da matemática e promover um vínculo significativo com a área. Assim, espera-se contribuir para a formação de estudantes mais autônomos, curiosos e capazes de pensar matematicamente.

Este trabalho está organizado em quatro capítulos. O Capítulo 1 apresenta um panorama sobre as olimpíadas de matemática no Brasil. O Capítulo 2 reúne os fundamentos teóricos da Aritmética necessários à compreensão dos problemas selecionados. O Capítulo 3 trás uma coletânea de questões olímpicas acompanhadas de estratégias de resolução. No Capítulo 4, descreve-se a sequência didática proposta e suas possibilidades de utilização no ambiente escolar.

1 Olimpíadas de Matemática na Educação Básica

As olimpíadas de matemática configuram-se como importantes iniciativas educacionais que visam estimular o interesse dos estudantes e aproximá-los da linguagem e do raciocínio matemático. Em todo o Brasil, instituições promovem competições voltadas a diferentes níveis de ensino com o propósito de despertar talentos e desenvolver habilidades cognitivas e criativas. Em geral, essas competições são estruturadas em etapas sucessivas, nas quais o avanço do estudante depende de seu desempenho na fase anterior.

De modo mais amplo, as olimpíadas científicas abrangem diversas áreas do conhecimento, como Matemática, Biologia, Robótica, História e Meio Ambiente, contribuindo para a formação científica e cidadã dos participantes. Segundo o Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), essas iniciativas promovem o interesse pela investigação, fortalecem vínculos entre escolas, universidades e centros de pesquisa, e se configuram como instrumentos de democratização do acesso ao conhecimento científico (2, 3). Além de despertar o espírito de cooperação e o pensamento crítico, as olimpíadas têm desempenhado papel relevante na descoberta de jovens talentos e na valorização da cultura científica no país.

As olimpíadas científicas tiveram origem no final do século XIX com as primeiras edições realizadas na Hungria, em 1894, voltadas para a área da Matemática. Em 1959, foi criada a International Mathematical Olympiad (IMO), realizada pela primeira vez na Romênia, reunindo sete países do leste europeu. Desde então, a IMO consolidou-se como a principal competição mundial de Matemática voltada para estudantes do ensino médio e atualmente conta com a participação de mais de cem países (4, 5).

Inspirado nesse movimento internacional, o Brasil criou, em 1979, a *Olimpíada Brasileira de Matemática* (OBM), organizada pela *Sociedade Brasileira de Matemática* (SBM), em parceria com o *Instituto Nacional de Matemática Pura e Aplicada* (IMPA) com o apoio do *Conselho Nacional de Desenvolvimento Científico e Tecnológico* (CNPq). A OBM tem por objetivo identificar talentos e selecionar estudantes para representar o país em competições internacionais, além de estimular os estudos em Matemática entre estudantes do ensino fundamental, médio e superior (6, 7).

A partir da experiência bem-sucedida da OBM, foi criada, em 2005, a *Olimpíada Brasileira de Matemática das Escolas Públicas* (OBMEP), uma iniciativa do IMPA e da SBM com apoio do governo federal. Esta tem como propósito popularizar o acesso às competições científicas, incentivar o estudo da Matemática e contribuir para a melhoria

da educação básica no país (6).

Nos últimos anos, as olimpíadas de matemática vêm ganhando destaque no cenário educacional brasileiro, mobilizando milhões de estudantes e professores em todo o país. A OBMEP, em particular, é atualmente a competição mais abrangente em nível nacional. Em sua 20ª edição, realizada em 2025, contou com a participação de mais de 18 milhões de estudantes de 99,93% dos municípios brasileiros (8).

No âmbito regional, destaca-se a *Olimpíada Pernambucana de Matemática* (OPEMAT), uma atividade de extensão promovida pelo Departamento de Matemática da Universidade Federal Rural de Pernambuco (UFRPE). Assim como a OBMEP, a OPEMAT busca despertar o raciocínio lógico e o pensamento criativo, envolvendo estudantes do ensino fundamental e médio, de escolas públicas e particulares do estado.

Diante desse alcance, observamos o quanto que as olimpíadas estão presentes nas escolas brasileiras e conseqüentemente vemos a importância de incentivar ainda mais estudantes a participarem das competições. Apesar da ampla participação nas olimpíadas de matemática, observa-se que muitas escolas públicas ainda não dispõem de espaços e momentos para preparação dessas competições. Ao analisarmos os documentos norteadores da educação básica (1, 9, 10), vemos que o currículo escolar não dialoga de maneira direta com o tipo de conteúdo, linguagem e nível de raciocínio exigidos nas provas olímpicas. Como consequência, os estudantes participam das competições olímpicas sem preparação prévia, o que contribui para a percepção de que se trata de avaliações difíceis e desconectadas.

Normalmente, as escolas/professores realizam as inscrições para as olimpíadas, mas não dispõem de encontros preparatórios com tais finalidades, e então o trabalho do professor se restringe a alertar os estudantes sobre a proximidade da prova poucos dias antes da aplicação. Quando algum conteúdo coincide com o currículo, algumas questões são eventualmente discutidas em sala; entretanto, essas práticas são pontuais e não fazem parte da rotina escolar. Além disso, como apenas alguns estudantes demonstram interesse pelas olimpíadas, as ações voltadas à preparação ficam, geralmente, restritas a momentos isolados, sem continuidade ao longo do ano letivo.

Perante esse cenário, torna-se fundamental oferecer suporte específico aos estudantes interessados em participar das competições olímpicas, especialmente para aqueles que avançam para as fases seguintes. Muitos alunos chegam à segunda etapa da OBMEP, por exemplo, sem conhecer adequadamente a estrutura da prova, os tipos de raciocínio envolvidos e os conteúdos que costumam ser cobrados. Compreender a lógica por trás das questões em edições anteriores pode ser decisiva para que possam enfrentar as questões com maior segurança.

Preparar estudantes para as olimpíadas de matemática não se resume a solucionar problemas isolados, mas envolve apresentar a dinâmica das provas, discutir estratégias,

promover o estudo progressivo de conteúdos recorrentes e proporcionar o desenvolvimento do raciocínio lógico. A criação de espaços de estudo, oficinas e momentos de resolução de questões, especialmente fundamentados na análise de edições anteriores, representa uma ação pedagógica que contribui para o engajamento, a confiança e a formação matemática dos estudantes.

Dentre as áreas abordadas nessas olimpíadas, a aritmética ocupa uma posição de destaque por conta da frequência em que problemas aritméticos aparecem nas provas. Embora temas como sistema de numeração, números primos e compostos, divisibilidade, MDC e MMC não sejam objetos de conhecimento no ensino médio, são pré-requisitos para o trabalho de diversos temas desta etapa escolar, de modo que o domínio dessas habilidades torna-se fundamental. Pelo fato destes conteúdos não estarem previstos como objetos de conhecimento para o Ensino Médio na Base Nacional Comum Curricular (BNCC) e, conseqüentemente, no Currículo de Pernambuco, algumas definições e propriedades deixam de ser retomadas ou aprofundadas, o que pode gerar lacunas conceituais em conhecimentos necessários para a resolução de problemas em contextos olímpicos.

Além disso, conteúdos como equações diofantinas, congruências e o teorema chinês dos restos não aparecem nos currículos escolares, o que torna os problemas olímpicos distantes da realidade dos alunos e/ou excessivamente difíceis por não dominarem ou nem conhecerem estratégias eficientes para resolver os problemas.

É comum que algumas questões de aritmética possam ser resolvidas por inspeção, intuição ou tentativa e erro; às vezes, a própria questão guia a solução do problema, onde o item “a” auxilia na elaboração da estratégia necessária para solucionar o item “b”, por exemplo, e assim sucessivamente. Contudo, quando o estudante conhece propriedades necessárias que envolvem o problema em si, é possível desenvolver uma visão mais ampla dos padrões e das relações envolvidas. Isso facilita o processo de resolução e amplia a autonomia intelectual, permitindo que elabore estratégias mais rápidas, adequadas, eficientes e elegantes.

Dessa forma, incluir a aritmética de maneira intencional no Ensino Médio, especialmente no contexto da preparação para olimpíadas, contribui não apenas para o domínio conceitual, mas também para a construção de uma base sólida que favoreça a compreensão de conteúdos mais avançados da Matemática e fortaleça o desempenho escolar como um todo.

Para estudantes interessados em aprofundar seus estudos em Matemática ou em áreas afins, a participação em competições científicas constitui um importante estímulo acadêmico e pode abrir portas para oportunidades futuras, como bolsas de iniciação científica, programas de formação, premiações e até mesmo o ingresso em universidades públicas. Proporcionar momentos de preparação olímpica para os estudantes pode transformar a relação do estudante com a Matemática, promovendo autoconfiança e um senso de

pertencimento ao universo científico.

Apesar de muitos estudantes demonstrarem afinidade e aptidão com a Matemática, por vezes, falta-lhes, ao longo da trajetória escolar, um olhar atento que incentive o desenvolvimento pleno de suas habilidades. Por isso, é importante oferecer aos estudantes a oportunidade de ampliar seus horizontes, explorando suas capacidades e reconhecendo seu potencial enquanto indivíduos capazes de pensar matematicamente de forma criativa, lógica e estratégica.

Ao oferecer atividades voltadas à preparação para as olimpíadas, a escola amplia as possibilidades de aprendizagem e favorece o desenvolvimento de competências essenciais para o pensamento matemático. Tais experiências contribuem para formar estudantes capazes de pensar de maneira crítica e estratégica, desenvolver autonomia intelectual e compreender a Matemática como uma prática ativa, dinâmica e profundamente conectada à resolução de problemas.

Dessa forma, as olimpíadas de matemática assumem um papel formativo que vai além do caráter competitivo. Inseridas no cotidiano escolar, elas tornam-se instrumentos de ensino capazes de despertar o interesse, fortalecer a autoestima, promover o pensamento lógico e ampliar o repertório conceitual dos estudantes. Ao estimular o contato constante com problemas de aritmética e outras áreas, contribui-se para a construção de uma experiência de aprendizagem significativa, prazerosa e transformadora.

A Base Nacional Comum Curricular (BNCC) enfatiza o desenvolvimento de competências como a argumentação lógica e a resolução de problemas complexos, contribuindo assim com habilidades diretamente relacionadas às exigidas nas olimpíadas de matemática. Ao trabalhar com esse tipo de desafio, os estudantes são convidados a desenvolver autonomia intelectual, pensamento criativo, perseverança e raciocínio dedutivo (1).

Ao propor uma variedade de problemas relacionados a um mesmo tema, busca-se ampliar o repertório do estudante para que futuramente ele possa reconhecer estratégias previamente utilizadas em situações análogas. Essa familiaridade contribui para a construção de uma bagagem conceitual e estratégica que favorece a aprendizagem e o desempenho mesmo diante de questões inéditas em futuras olimpíadas e também no próprio aprendizado escolar.

Ainda que nem todos os problemas apresentados se repitam em formato ou conteúdo, é provável que surjam avaliações futuras com questões cujo raciocínio seja semelhante. Desenvolver no estudante a sensibilidade para padrões e conexões entre problemas é uma forma eficaz de prepará-los para enfrentar desafios com maior autonomia e segurança, fomentando seu interesse e fortalecendo seu potencial cognitivo ao mesmo tempo que promove o ato de fazer matemática.

Por vezes, as questões olímpicas de aritmética podem ser resolvidas por meio do

raciocínio lógico-dedutivo, mesmo sem conhecimento teórico aprofundado; para tal, é importante entender e compreender os conhecimentos prévios dos estudantes e analisar até onde conseguem resolver problemas propostos com base em conceitos já estudados. Ao propor situações-problema instigantes, pretende-se estimular o pensamento matemático autêntico, a curiosidade e a criatividade. Conforme os problemas se tornam mais complexos, surgirá naturalmente a necessidade de sistematizar o conhecimento, aprofundar a teoria e treinar estratégias. Assim, a aprendizagem ocorre de forma significativa, pois parte da experiência concreta, desperta o desejo de compreender mais e fortalece o raciocínio lógico enquanto habilidade essencial para outras áreas da Matemática e para a vida.

Desta forma, as olimpíadas de matemática configuram-se como uma importante ferramenta pedagógica, capaz de ir além do caráter competitivo e assumir um papel formativo no processo de ensino e aprendizagem. Elas representam um espaço de descoberta, em que o estudante é desafiado a pensar e ao serem inseridas no cotidiano escolar, tornam-se instrumentos de ensino capazes de despertar o interesse, fortalecer a autoestima e desenvolver o raciocínio lógico. Os conceitos e propriedades da aritmética estão presentes de forma recorrente nas provas olímpicas e oferecem diversas possibilidades para o desenvolvimento de habilidades matemáticas. Assim, compreender e valorizar o ensino da aritmética no contexto das olimpíadas é também reconhecer que aprender Matemática pode ser uma experiência significativa, prazerosa e transformadora e há a necessidade de incluir as olimpíadas enquanto ferramentas essenciais e sempre presentes no ensino escolar.

2 Fundamentos da Aritmética

Este capítulo apresenta os principais resultados da Aritmética que servirão de base tanto para a resolução dos problemas olímpicos propostos quanto para a construção da sequência didática desenvolvida neste trabalho. Os conteúdos aqui abordados foram selecionados por sua relevância conceitual e por seu potencial em desenvolver o raciocínio lógico e o pensamento algébrico dos estudantes.

A fundamentação teórica baseia-se, principalmente, nas obras de *Hefez* (11, 12) e *Domingues* (13), que apresentam de forma rigorosa e estruturada os conceitos essenciais da Aritmética. O conteúdo desenvolvido neste capítulo busca consolidar tais fundamentos, servindo de suporte teórico para as discussões e propostas apresentadas nos capítulos seguintes.

2.1 Divisibilidade

A divisão é um conceito apresentado aos estudantes no ensino fundamental, quando se iniciam os estudos das quatro operações básicas. Nesse contexto, o ato de dividir costuma ser associado a procedimentos algorítmicos já conhecidos, frequentemente executados de forma mecânica. No entanto, por trás dessa operação existe uma estrutura aritmética rica, cuja compreensão é essencial para que o estudante desenvolva autonomia em resolução de problemas.

Em muitas situações, não nos interessa apenas o resultado final da divisão, mas sim características estruturais dela, como a análise dos múltiplos envolvidos ou a determinação do resto. A capacidade de traduzir o algoritmo da divisão para a linguagem algébrica, isto é, representar uma divisão como uma igualdade entre inteiros, permite generalizar procedimentos, reconhecer padrões e resolver problemas que vão muito além da execução do algoritmo em si.

A partir dessa perspectiva, estudar a divisão no conjunto dos inteiros é mais do que dominar um cálculo, é compreender uma ferramenta conceitual que fundamenta diversos raciocínios matemáticos.

Nesse sentido, torna-se importante formalizar a ideia de dividir números inteiros de modo a descrever, em linguagem matemática precisa, quando uma divisão pode ser realizada sem resto e quais propriedades se preservam nesse processo.

Dados dois números inteiros a e b , dizemos que a divide b quando existe um número inteiro c tal que $b = c \cdot a$. Nesse caso, escrevemos $a \mid b$. Se tal número c não existe, dizemos que a não divide b e representamos por $a \nmid b$.

Quando $a \mid b$, dizemos que a é um *divisor* de b e que b é um *múltiplo* de a .

Alguns exemplos simples ilustram a definição: $1 \mid 6$, $2 \mid 6$, $3 \mid 6$ e $6 \mid 6$, pois em todos os casos é possível encontrar um inteiro c tal que $6 = a \cdot c$. Por outro lado, $4 \nmid 6$ e $0 \nmid 6$, já que nenhuma multiplicação inteira envolvendo esses valores produz 6.

A relação de divisibilidade apresenta algumas propriedades diretas da definição: ela é *reflexiva* ($a \mid a$ para todo a), *transitiva* (se $a \mid b$ e $b \mid c$, então $a \mid c$) e todo inteiro divide o zero ($a \mid 0$ para todo a). Quando restringimos a relação ao conjunto dos números naturais, incluindo o zero, ela também é *antissimétrica*: se $a \mid b$ e $b \mid a$, então necessariamente $a = b$. No entanto, essa última propriedade não vale em $\mathbb{Z}$, pois $2 \mid (-2)$ e $(-2) \mid 2$, mas $2 \neq -2$. Consequentemente, embora a divisibilidade seja reflexiva e transitiva em $\mathbb{Z}$, a ausência da propriedade de antissimetria impede que ela seja caracterizada como uma relação de ordem nesse conjunto.

Entre os resultados que derivam diretamente da definição, destaca-se o fato de que, se um número divide dois inteiros, então ele também divide qualquer combinação linear desses inteiros.

Proposição 2.1. *Sejam $a, b, c \in \mathbb{Z}$. Se $a \mid b$ e $a \mid c$, então*

$$a \mid (xb + yc) \quad \text{para todos } x, y \in \mathbb{Z}.$$

Demonstração. Se $a \mid b$, então existe $r \in \mathbb{Z}$ tal que $b = ra$. Analogamente, se $a \mid c$, existe $s \in \mathbb{Z}$ tal que $c = sa$.

Substituindo essas expressões na combinação linear dada, obtemos:

$$xb + yc = x(ra) + y(sa) = (xr + ys)a.$$

Portanto, $a \mid (xb + yc)$, pois $xb + yc$ é um múltiplo de a . □

A operação de divisão $a \mid b$ no conjunto dos números inteiros não é sempre possível dados $a, b \in \mathbb{Z}$, pois nem sempre existe um número inteiro c tal que $b = a \cdot c$. Por exemplo, 5 não é divisor de 7, pois não existe inteiro que multiplicado por 5 resulte em 7. Entretanto, mesmo quando a divisão exata não é possível, podemos realizar a chamada divisão euclidiana, na qual admitimos um pequeno resto. Essa possibilidade, garantida para quaisquer inteiros, é fundamental na estrutura aritmética de $\mathbb{Z}$.

O resultado a seguir garante que, mesmo quando b não divide a , é sempre possível decompor a em termos de b com um pequeno resto.

Teorema 2.2. (*Divisão Euclidiana*) *Sejam a e b dois números inteiros com $b \neq 0$. Existem dois únicos números inteiros q e r tais que*

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

em que $|b|$ representa o valor absoluto de b , pois o divisor pode ser positivo ou negativo. Dessa forma, a condição $0 \leq r < |b|$ garante que o resto seja sempre não negativo e estritamente menor que o módulo do divisor.

A demonstração a seguir é a apresentada em (11).

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 implica que $S \neq \emptyset$. O conjunto S é limitado inferiormente por 0, logo, pelo *Princípio da Boa Ordenação*, temos que S possui um menor elemento r . Logo, r é escrito na forma $r = a - bq$, para algum $q \in \mathbb{Z}$. Sabemos que $r \geq 0$.

Vamos mostrar que $r < |b|$. Suponhamos, por absurdo, que $r \geq |b|$. Portanto, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |b| + s$, logo $0 \leq s < r$. Mas isso contradiz o fato de r ser o menor elemento de S , pois $s = a - (q \pm 1)b \in S$, com $s < r$.

Unicidade. Suponha que $a = bq + r$ e $a = bq' + r'$, onde $q, q', r, r' \in \mathbb{Z}$, $0 \leq r < |b|$ e $0 \leq r' < |b|$. Assim, $-|b| < -r \leq r' - r \leq r' < |b|$. Logo, $|r' - r| < |b|$.

Por outro lado, $b(q - q') = r' - r$, o que implica que $|b| |q - q'| = |r' - r| < |b|$, o que só é possível se $q = q'$ e, conseqüentemente, $r = r'$. $\square$

Nas condições do teorema, os inteiros q e r são chamados, respectivamente, de quociente e resto da divisão de a por b . Em particular, quando o resto é igual a 0, então b divide a , ou seja, $b \mid a$. Assim, o *Teorema da Divisão Euclidiana* generaliza a noção de divisibilidade ao garantir que qualquer inteiro a pode ser escrito na forma $a = bq + r$, mesmo quando b não divide a , com um resto estritamente menor que $|b|$.

As ideias de divisibilidade e divisão euclidiana aparecem com grande frequência na resolução de problemas aritméticos, sendo, portanto, ferramentas essenciais para a definição e a compreensão de diversos conceitos da aritmética.

2.2 Sistemas de Numeração

Escrever um número em diferentes representações pode ser bastante útil na resolução de diversas situações-problema. Em nossa trajetória escolar, estudamos principalmente o sistema de numeração decimal, que será o nosso ponto de partida nesta seção.

Desde os anos iniciais do *Ensino Fundamental*, é comum a realização de atividades nas quais o professor apresenta um número e solicita que os estudantes o escrevam por extenso. Essa prática permite que os alunos identifiquem as classes numéricas (unidades,

dezenas, centenas etc.), favorecendo a compreensão do valor posicional. Embora possa parecer uma atividade de menor relevância, trata-se de um recurso fundamental para desenvolver diferentes formas de representação de um mesmo número.

Por exemplo, ao escrevermos o número 2345 por extenso, temos: dois mil, trezentos e quarenta e cinco. A partir dessa escrita, é possível destacar a decomposição do número no sistema decimal:

- dois mil = $2000 = 2 \cdot 1000 = 2 \cdot 10^3$;
- trezentos = $300 = 3 \cdot 100 = 3 \cdot 10^2$;
- quarenta = $40 = 4 \cdot 10 = 4 \cdot 10^1$;
- cinco = $5 = 5 \cdot 1 = 5 \cdot 10^0$.

Portanto,

$$2345 = 2 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10^1 + 5 \cdot 10^0.$$

Atividades como essa proporcionam ao estudante compreender que, no sistema de numeração decimal, o valor de cada algarismo depende da posição que ele ocupa (14).

O sistema de numeração decimal é o mais comum e o mais utilizado para representar os números (11). No entanto, ele não é o único possível, pois existem diversas formas de representação, denominadas sistemas de numeração. Muitos desses sistemas seguem o princípio do valor posicional, que explicamos a seguir.

De modo geral, dizemos que um sistema de numeração é posicional quando, dada uma base $b > 1$, cada algarismo pode assumir valores entre 0 e $b - 1$, e a posição que ele ocupa representa uma potência de b . Assim, em qualquer base b , um número pode ser escrito com potências de b .

A compreensão desse tema é útil na resolução de diversos problemas e em muitas situações, a solução de um problema pode ficar mais simples quando representamos o número em outra base. Formalizamos essa ideia a seguir.

Teorema 2.3. *Sejam $a, b \in \mathbb{Z}$, com $a > 0$, e $b > 1$. Então, existem inteiros $n \geq 0$ e $0 \leq r_0, r_1, \dots, r_n < b$, com $r_n \neq 0$, tais que*

$$a = r_0 + r_1b + r_2b^2 + \dots + r_nb^n.$$

Além disso, essa representação é única.

Demonstração. Vamos demonstrar o teorema por *Indução Completa* sobre a .

Se $0 < a < b$, então basta tomar $n = 0$ e $r_0 = a$. Assim, $a = r_0$, o que já é da forma desejada. A unicidade é imediata, pois não há outra forma de escrever a com potências de b sem ultrapassar o valor de a .

Suponhamos que todo natural menor do que a , onde $a \geq b$ possui representação na forma do teorema. Vamos provar que a também possui tal representação. Pela divisão euclidiana, existem inteiros q e r tais que

$$a = bq + r, \quad 0 \leq r < b.$$

Da igualdade anterior, $bq = a - r$. Como $0 \leq r < b$, temos $a - r \leq a$, e portanto $bq \leq a$. Como $b > 1$, resulta que $q < a$. Além disso, como $a \geq b$, segue que $q \geq 1$. Logo, $0 < q < a$. Isso permite aplicar a hipótese de indução a q .

Como $q < a$, pela hipótese de indução existem inteiros $r_1, r_2, \dots, r_{n+1}$ tais que

$$q = r_1 + r_2b + \dots + r_{n+1}b^n,$$

com $0 \leq r_i < b$ para todo i e $r_{n+1} \neq 0$.

Substituindo a expansão de q , obtemos $a = b(r_1 + r_2b + \dots + r_{n+1}b^n) + r$. Distribuindo o fator b , obtemos

$$a = r + r_1b + r_2b^2 + \dots + r_{n+1}b^{n+1}.$$

Basta agora definir

$$r_0 = r.$$

Assim,

$$a = r_0 + r_1b + r_2b^2 + \dots + r_{n+1}b^{n+1},$$

o que prova a existência da representação para a .

A unicidade decorre do fato de que o resto r_0 e o quociente q são únicos pela divisão euclidiana e a expansão de q é única pela hipótese de indução. Portanto, toda a representação de a , na forma acima, é única. $\square$

Observe que o procedimento de divisões sucessivas apresentado a seguir é exatamente o processo construído na demonstração do Teorema 2.3, que garante que esse método sempre funciona, termina e produz uma única representação. Assim, para determinarmos a expansão de um número qualquer relativa à base b , aplicamos sucessivamente a divisão euclidiana, como apresentado a seguir:

Dado $a > 0$ e $b > 1$:

1. Divida a por b : escreva $a = q_0b + r_0$ com $0 \leq r_0 < b$.
2. Se $q_0 = 0$, pare. Caso contrário, divida q_0 por b : $q_0 = q_1b + r_1$, com $0 \leq r_1 < b$.

3. Repita até obter $q_n = 0$. Os restos formam os algarismos da representação de a na base b . Assim,

$$a = [r_n r_{n-1} \cdots r_1 r_0]_b,$$

em que a notação $[\cdot]_b$ indica que o número está escrito na base b , isto é,

$$[r_n r_{n-1} \cdots r_1 r_0]_b = r_0 + r_1 b + r_2 b^2 + \cdots + r_n b^n.$$

Os algarismos devem ser lidos de baixo para cima (do último resto para o primeiro).

Exemplo 2.4. Exemplos de conversão [com $a = 2345$]

(a) Base $b = 2$.

$$\begin{aligned} 2345 &= 2 \cdot 1172 + \boxed{1}, \\ 1172 &= 2 \cdot 586 + \boxed{0}, \\ 586 &= 2 \cdot 293 + \boxed{0}, \\ 293 &= 2 \cdot 146 + \boxed{1}, \\ 146 &= 2 \cdot 73 + \boxed{0}, \\ 73 &= 2 \cdot 36 + \boxed{1}, \\ 36 &= 2 \cdot 18 + \boxed{0}, \\ 18 &= 2 \cdot 9 + \boxed{0}, \\ 9 &= 2 \cdot 4 + \boxed{1}, \\ 4 &= 2 \cdot 2 + \boxed{0}, \\ 2 &= 2 \cdot 1 + \boxed{0}, \\ 1 &= 2 \cdot 0 + \boxed{1}. \end{aligned}$$

Lendo os restos de baixo para cima: $2345 = [100100101001]_2$.

(b) Base $b = 5$.

$$\begin{aligned} 2345 &= 5 \cdot 469 + \boxed{0}, \\ 469 &= 5 \cdot 93 + \boxed{4}, \\ 93 &= 5 \cdot 18 + \boxed{3}, \\ 18 &= 5 \cdot 3 + \boxed{3}, \\ 3 &= 5 \cdot 0 + \boxed{3}. \end{aligned}$$

Logo, $2345 = [33340]_5$.

(c) Base $b = 16$.

$$\begin{aligned} 2345 &= 16 \cdot 146 + \boxed{9}, \\ 146 &= 16 \cdot 9 + \boxed{2}, \\ 9 &= 16 \cdot 0 + \boxed{9}. \end{aligned}$$

Em hexadecimal, 9, 2, 9 correspondem aos dígitos 9, 2, 9, portanto $2345 = (929)_{16}$.

Dessa forma, o procedimento de divisões sucessivas fornece a representação de qualquer número inteiro positivo em qualquer base $b > 1$. Compreender e manipular números em diferentes bases ou em sua forma posicional permite analisar sua estrutura de maneira mais clara, fornecendo ferramentas úteis para a resolução de problemas de teoria dos números e questões matemáticas desafiadoras.

2.3 Máximo divisor comum

O estudo do máximo divisor comum (mdc) desempenha um papel fundamental na resolução de diversos tipos de problemas, surgindo de forma natural em contextos que envolvem divisão em partes iguais, determinação de medidas máximas ou análise de relações de divisibilidade entre quantidades.

Sejam a e b dois números inteiros. Dizemos que um inteiro d é um divisor comum de a e b quando $d \mid a$ e $d \mid b$.

Definição 2.5. Um inteiro $d \geq 0$ é chamado de *máximo divisor comum* de a e b quando satisfaz as seguintes propriedades:

- (i) d é divisor comum de a e b ;
- (ii) todo divisor comum de a e b divide d .

A condição (ii) pode ser reescrita como: sempre que c é divisor comum de a e b , tem-se $c \mid d$. Nesse caso, escrevemos $(a, b) = d$.

A definição acima garante imediatamente a unicidade do máximo divisor comum, conforme apresentamos a seguir.

Proposição 2.6. *Sejam $a, b \in \mathbb{Z}$, não ambos nulos. Então o máximo divisor comum de a e b é único.*

Demonstração. Se d e d' satisfazem simultaneamente as condições da definição de máximo divisor comum de a e b , então

$$d \mid d' \quad \text{e} \quad d' \mid d.$$

Como $d \geq 0$ e $d' \geq 0$, segue que $d = d'$. □

Assim, a notação (a, b) está bem definida. Além disso, a ordem dos números não altera o valor do máximo divisor comum, ou seja, $(a, b) = (b, a)$.

Alguns casos simples ilustram propriedades imediatas do mdc:

$$(0, a) = |a|, \quad (1, a) = 1, \quad (a, a) = |a|.$$

Além disso, vale que $a \mid b$ se, e somente se, $(a, b) = |a|$. Com efeito, suponha primeiro que $a \mid b$. Então $|a|$ é divisor comum de a e b . Se c é outro divisor comum desses números, então $c \mid a$ e, portanto, $c \mid |a|$, o que mostra que $(a, b) = |a|$. Reciprocamente, se $(a, b) = |a|$, então $|a|$ divide b , logo $a \mid b$.

No caso particular em que $a = b = 0$, define-se $(0, 0) = 0$. De fato, como todo número inteiro divide 0, o número 0 é um divisor comum de 0 e 0, sendo essa escolha compatível com a definição de máximo divisor comum, conforme (11).

Observe que, se $(a, b) = d$, então qualquer divisor comum c de a e b satisfaz $|c| \leq d$. Com efeito, sendo $d \geq 0$ o mdc de a e b , temos que $c \mid d$, de modo que $|c| \leq |d| = d$. Logo, quando o mdc existe, ele é o maior dos divisores comuns.

Além disso, observe que $(a, b) = (a, -b) = (-a, b) = (-a, -b)$. Isso ocorre porque os conjuntos de divisores comuns de a e b coincidem com os de a e $-b$, de $-a$ e b , e de $-a$ e $-b$, uma vez que $d \mid a$ implica $d \mid -a$. Assim, ao calcular o mdc, podemos sempre supor $a \geq 0$ e $b \geq 0$ sem perda de generalidade.

A definição apresentada garante a unicidade do máximo divisor comum. Resta, portanto, assegurar a sua existência, o que é estabelecido no resultado a seguir.

Proposição 2.7. *Sejam $a, b \in \mathbb{Z}$, não ambos nulos. Então existe um inteiro $d \geq 0$ que é o máximo divisor comum de a e b .*

Demonstração. Considere o conjunto $I(a, b) = \{ax + by \mid x, y \in \mathbb{Z}\}$. Como a e b não são ambos nulos, tem-se $I(a, b) \cap \mathbb{N} \neq \emptyset$. Seja $d = \min(I(a, b) \cap \mathbb{N})$.

Mostremos que $d = (a, b)$.

Se c é um divisor comum de a e b , então $c \mid a$ e $c \mid b$, logo c divide toda combinação linear $ax + by$. Portanto, c divide todos os elementos de $I(a, b)$, e, consequentemente, $c \mid d$.

Por outro lado, seja $z \in I(a, b)$. Suponha, por absurdo, que $d \nmid z$. Pela divisão euclidiana, existem inteiros q e r tais que $z = dq + r$, $0 < r < d$. Como $z = xa + yb$ e $d = ma + nb$, para alguns $x, y, m, n \in \mathbb{Z}$, segue que $r = z - dq = (x - qm)a + (y - qn)b$, isto é, $r \in I(a, b) \cap \mathbb{N}$, com $r < d$, o que contradiz a minimalidade de d . Logo, $d \mid z$ para todo $z \in I(a, b)$.

Em particular, como $a, b \in I(a, b)$, segue que $d \mid a$ e $d \mid b$. Assim, d é divisor comum de a e b , e todo divisor comum divide d . Logo, $d = (a, b)$. $\square$

A existência do máximo divisor comum permite descrever uma propriedade fundamental em termos de combinações lineares, como mostra o resultado a seguir.

Lema 2.8. (*Lema de Bézout*) Sejam $a, b \in \mathbb{Z}$, não ambos nulos. Então existem inteiros $x, y \in \mathbb{Z}$ tais que $(a, b) = ax + by$.

Demonstração. Pela Proposição 2.7, existe $d = (a, b)$ e, além disso, $d \in I(a, b)$. Logo, existem $x, y \in \mathbb{Z}$ tais que

$$d = ax + by.$$

Portanto,

$$(a, b) = ax + by.$$

□

Apresentamos a seguir um resultado fundamental para o cálculo do máximo divisor comum.

Lema 2.9. (*Lema de Euclides*) Sejam $a, b, n \in \mathbb{Z}$. Então $(a, b) = (a, b - na)$.

Demonstração. Pela proposição 2.7, existe $d = (a, b - na)$. Por definição, $d \mid a$ e $d \mid (b - na)$. Como todo divisor de a divide qualquer múltiplo inteiro de a , em particular na , segue que $d \mid na$; portanto, d divide a combinação linear $(b - na) + na = b$. Assim, d é divisor comum de a e b .

Por outro lado, seja c um divisor comum de a e b . Então $c \mid a$ e $c \mid b$, e como um divisor comum divide qualquer combinação linear desses números, temos $c \mid (b - na)$. Logo, c é divisor comum de a e de $b - na$, o que implica, pela definição do mdc, que $c \mid d$.

Desse modo, d é divisor comum de a e b , e todo divisor comum desses números divide d . Pela definição de mdc, isso mostra que d é o mdc de a e b , e portanto

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

□

O *Lema de Euclides* mostra que é possível substituir um dos números do par por uma combinação linear sem alterar o mdc. Essa propriedade é a base do processo sucessivo descrito por Euclides, no qual o mdc é obtido por meio de divisões sucessivas que reduzem progressivamente os valores envolvidos.

Mostraremos a seguir que a aplicação sucessiva do *Lema de Euclides* conduz a um procedimento finito para o cálculo do máximo divisor comum, conhecido como Algoritmo de Euclides.

Dados $a, b \in \mathbb{N}$, podemos supor $b \leq a$. Se $b = 1$ ou $b = a$, ou ainda se $b \mid a$, então $(a, b) = b$, e nada há a demonstrar.

Suponhamos, portanto, que $1 < b < a$ e $b \nmid a$. Pela divisão euclidiana, existem inteiros q_1 e r_1 tais que

$$a = bq_1 + r_1, \quad 0 < r_1 < b.$$

Pelo *Lema de Euclides*, obtemos

$$(a, b) = (b, r_1).$$

Se $r_1 \mid b$, então $(b, r_1) = r_1$ e o processo termina. Caso contrário, realizamos nova divisão

$$b = r_1q_2 + r_2, \quad 0 < r_2 < r_1,$$

e, pelo *Lema de Euclides*,

$$(b, r_1) = (r_1, r_2).$$

Prosseguindo dessa forma, obtemos divisões sucessivas

$$r_{i-2} = r_{i-1}q_i + r_i, \quad 0 < r_i < r_{i-1},$$

até que algum resto se torne zero. Como a sequência

$$b > r_1 > r_2 > \cdots > r_k > 0$$

é estritamente decrescente de inteiros não negativos, ela termina após um número finito de passos. O último resto não nulo r_k é o máximo divisor comum de a e b :

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

Podemos sintetizar esse procedimento em um diagrama que organiza as divisões sucessivas. A primeira divisão $a = bq_1 + r_1$ é disposta como segue:

	q_1	
a	b	
r_1		

A segunda divisão, $b = r_1q_2 + r_2$, é acrescentada ao esquema:

	q_1	q_2	$\cdots$
a	b	r_1	$\cdots$
r_1	r_2	r_3	$\cdots$

Repetindo o processo para cada divisão, obtém-se ao final o resto r_k , que aparece como último número não nulo na linha inferior. Esse valor é o mdc de a e b .

Além disso, ao substituir cada resto pela igualdade correspondente, no sentido contrário das divisões, obtemos r_k como combinação linear de a e b . Assim, o algoritmo de Euclides também permite determinar inteiros m e n tais que $(a, b) = ma + nb$.

A seguir, calculamos o mdc de 314 e 146 utilizando o diagrama do algoritmo de Euclides e, em seguida, reconstruímos o valor obtido como combinação linear desses números.

As entradas da primeira linha correspondem aos quocientes sucessivos q_i , enquanto as linhas inferiores registram os divisores e os restos produzidos por cada divisão.

	2	6	1	1	1	3
314	146	22	14	8	6	2
22	14	8	6	2	0	

Das divisões do algoritmo seguem as igualdades:

$$22 = 314 - 2 \cdot 146,$$

$$14 = 146 - 6 \cdot 22,$$

$$8 = 22 - 14,$$

$$6 = 14 - 8,$$

$$2 = 8 - 6.$$

Iniciando pelo último resto não nulo e substituindo sucessivamente, obtemos:

$$\begin{aligned}
 2 &= 8 - 6 \\
 &= 8 - (14 - 8) \\
 &= 2 \cdot 8 - 14 \\
 &= 2(22 - 14) - 14 \\
 &= 2 \cdot 22 - 3 \cdot 14 \\
 &= 2 \cdot 22 - 3(146 - 6 \cdot 22) \\
 &= 20 \cdot 22 - 3 \cdot 146 \\
 &= 20(314 - 2 \cdot 146) - 3 \cdot 146 \\
 &= 20 \cdot 314 - 43 \cdot 146.
 \end{aligned}$$

Portanto, $(314, 146) = 2 = 20 \cdot 314 - 43 \cdot 146$, de modo que o mdc pode ser escrito como combinação linear de 314 e 146, com $m = 20$ e $n = -43$.

O cálculo do mdc por meio do algoritmo de Euclides, bem como sua escrita como combinação linear dos inteiros envolvidos, desempenha papel central em diversos resultados da aritmética elementar.

Antes de introduzirmos o mínimo múltiplo comum, apresentamos dois resultados que serão úteis nas demonstrações subsequentes. Ambos decorrem diretamente das propriedades básicas do mdc e da noção de divisibilidade, permitindo simplificar expressões e caracterizar situações em que certos inteiros são coprimos.

Definição 2.10. Dizemos que dois inteiros a e b são coprimos quando seu máximo divisor comum é igual a 1, ou seja, $(a, b) = 1$.

Corolário 2.11. Sejam $a, b \in \mathbb{Z}$, ambos não nulos, e seja $d = (a, b)$. Então

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Demonstração. Como $d = (a, b)$, temos $d \mid a$ e $d \mid b$, e portanto existem inteiros a' e b' tais que

$$a = d a' \quad \text{e} \quad b = d b'.$$

Para verificar o valor de (a', b') , seja k um divisor comum de a' e b' . Assim, existem inteiros u e v tais que

$$a' = ku, \quad b' = kv.$$

Substituindo nas igualdades acima, obtemos

$$a = d a' = d(ku) = (kd)u, \quad b = d b' = d(kv) = (kd)v.$$

Portanto, kd divide simultaneamente a e b , isto é, kd é um divisor comum desses números.

Pela definição de máximo divisor comum, todo divisor comum de a e b divide d . Como kd é divisor comum, segue que

$$kd \mid d.$$

Como $d > 0$, a divisibilidade acima implica $k \mid 1$, o que força $k = 1$.

Assim, o único divisor comum de a' e b' é 1, e concluímos que

$$(a', b') = 1,$$

ou seja,

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

□

Lema 2.12. (*Lema de Gauss*) Sejam $a, b, c \in \mathbb{Z}$. Se $(a, b) = 1$ e $a \mid bc$, então $a \mid c$.

Demonstração. Como $(a, b) = 1$, pelo Lema de Bézout 2.8, existem inteiros $m, n \in \mathbb{Z}$ tais que

$$1 = ma + nb.$$

Multiplicando ambos os lados por c , obtemos

$$c = mac + nbc.$$

Como $a \mid bc$, existe um inteiro k tal que $bc = ak$. Substituindo na expressão acima, temos

$$c = mac + nak = a(mc + nk),$$

o que mostra que $a \mid c$, como queríamos. $\square$

Encerramos assim as propriedades fundamentais do máximo divisor comum, bem como os fatos que utilizaremos nas demonstrações subsequentes. A seguir, passamos ao estudo do mínimo múltiplo comum e de sua relação com o mdc.

2.4 Mínimo múltiplo comum

O mínimo múltiplo comum (mmc) de alguns inteiros é o menor número que é múltiplo comum de todos eles. Em várias situações do dia a dia, como quando acontecimentos se repetem em tempos diferentes e queremos saber quando vão coincidir, precisamos determinar esse menor número.

Sejam a e b inteiros. Diremos que um número inteiro m é um múltiplo comum de a e b quando $a \mid m$ e $b \mid m$. Observe que ab , $|ab|$ e 0 são sempre múltiplos comuns de a e b .

Definição 2.13. Um inteiro $m \geq 0$ é chamado de mmc de a e b quando satisfaz:

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

Nesse caso, escrevemos $[a, b] = m$.

Da condição (ii) segue imediatamente a unicidade: se m e m' são dois mmc de a e b , então $m \mid m'$ e $m' \mid m$, e como ambos são inteiros não negativos, conclui-se que $m = m'$.

Por outro lado, se m é o mmc de a e b , então, para qualquer múltiplo comum c desses números, tem-se $m \mid c$. Assim, quando $c > 0$, obtemos $m \leq c$, o que mostra que m é o menor dos múltiplos comuns positivos de a e b .

Alterar o sinal de a ou b não modifica o valor de $[a, b]$:

$$[-a, b] = [a, -b] = [-a, -b] = [a, b].$$

Dessa forma, podemos trabalhar supondo $a \geq 0$ e $b \geq 0$.

Observa-se que $[a, b] = 0$ se, e somente se, pelo menos um dos números a ou b é zero. De fato, se $[a, b] = 0$, como ab é um múltiplo comum de a e b , tem-se $[a, b] \mid ab$, e portanto $0 \mid ab$, o que implica $ab = 0$, isto é, $a = 0$ ou $b = 0$. Reciprocamente, se $a = 0$ ou $b = 0$, então 0 é o único múltiplo comum de a e b , logo $[a, b] = 0$.

A seguir, estabelecemos a relação fundamental entre o mínimo múltiplo comum e o máximo divisor comum.

Proposição 2.14. *Sejam a e b inteiros. Então $[a, b]$ existe e satisfaz $a, b = |ab|$.*

Demonstração. Se $a = 0$ ou $b = 0$, a igualdade é imediata: de fato, o único múltiplo comum de a e b é 0, logo $[a, b] = 0$, e $a, b = 0 = |ab|$.

A identidade também permanece válida se substituirmos a ou b por $-a$ ou $-b$. Assim, sem perda de generalidade, podemos supor $a, b \in \mathbb{N}$.

Definamos

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

Como

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

e os quocientes $\frac{b}{(a, b)}$ e $\frac{a}{(a, b)}$ são inteiros, concluímos que $a \mid m$ e $b \mid m$. Portanto, m é um múltiplo comum de a e b .

Para mostrar que m é o menor múltiplo comum, seja c um múltiplo comum arbitrário de a e b . Então existem inteiros n e n' tais que

$$c = na = n'b.$$

Dividindo ambas as igualdades por (a, b) , obtemos

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

Os inteiros $\frac{a}{(a, b)}$ e $\frac{b}{(a, b)}$ são coprimos pelo corolário 2.11. Aplicando o *Lema de Gauss* 2.12 à igualdade acima, concluímos que

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

Assim, existe $k \in \mathbb{Z}$ tal que

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

Multiplicando por b , segue que

$$bn' = k \frac{ab}{(a, b)}.$$

Mas $bn' = c$ e $\frac{ab}{(a, b)} = m$. Logo,

$$c = km,$$

isto é, $m \mid c$.

Portanto, m divide todo múltiplo comum de a e b , o que mostra que m é o mínimo múltiplo comum. Assim,

$$[a, b] = m = \frac{|ab|}{(a, b)}.$$

Multiplicando ambos os lados por (a, b) , obtemos a identidade desejada:

$$[a, b] (a, b) = |ab|.$$

□

Com essas ferramentas, dispomos de uma caracterização completa do mmc e de sua relação com o mdc, o que nos permite resolver uma grande variedade de problemas. O domínio dessas propriedades torna o cálculo do mmc mais simples e eficiente quando aplicado a diferentes situações.

2.5 Equações Diofantinas Lineares

As equações diofantinas lineares têm papel fundamental na resolução de diversos problemas da aritmética em $\mathbb{Z}$, elas são expressas, em sua forma geral, por

$$aX + bY = c, \quad \text{com } a, b, c \in \mathbb{Z}.$$

As chamadas equações diofantinas são equações polinomiais com coeficientes inteiros, nas quais se buscam soluções inteiras ou racionais. No caso particular das equações lineares com duas incógnitas, estamos interessados em estudar as condições sob as quais há solução inteira e como essas soluções podem ser determinadas. Essas equações recebem esse nome em homenagem a Diofanto de Alexandria, matemático grego que, segundo Domingues (13), viveu provavelmente no século III d.C. e é considerado um dos precursores da Álgebra, pois, em sua obra *Aritmética*, apresentou uma coleção de problemas indeterminados resolvidos por meio de métodos essencialmente algébricos.

Nem toda equação diofantina admite solução em números inteiros. Em alguns casos, é possível determinar uma solução por simples inspeção; em outros, a existência de solução não é evidente. Surge, então, a necessidade de estabelecer condições que garantam a existência de soluções e, caso existam, um método para determiná-las.

Nesse sentido, apresentamos a seguinte proposição:

Proposição 2.15. *Sejam $a, b, c \in \mathbb{Z}$. A equação $ax + by = c$ admite solução inteira se, e somente se, $(a, b) \mid c$.*

Demonstração. Como visto anteriormente na discussão sobre o máximo divisor comum, sabe-se que o mdc de dois inteiros a e b pode ser escrito como combinação linear desses

números. Assim, existem inteiros m e n tais que

$$(a, b) = am + bn.$$

Primeiramente, suponhamos que a equação $ax + by = c$ admita uma solução inteira, a qual denotaremos por (x_0, y_0) . Nesse caso,

$$ax_0 + by_0 = c.$$

Como (a, b) divide simultaneamente a e b , ele divide qualquer combinação linear desses inteiros e, em particular, divide o lado esquerdo da igualdade acima. Conclui-se, portanto, que $(a, b) \mid c$.

Reciprocamente, suponhamos que $d = (a, b)$ divide c . Assim, existe $t \in \mathbb{Z}$ tal que $c = dt$. Por outro lado, como o mdc pode ser escrito como combinação linear de a e b , então

$$d = am + bn.$$

Multiplicando essa igualdade por t , obtemos

$$c = dt = a(tm) + b(tn).$$

Definindo

$$x_0 = tm \quad \text{e} \quad y_0 = tn,$$

verificamos que (x_0, y_0) é uma solução inteira particular da equação $ax + by = c$.

Dessa forma, a equação diofantina linear $ax + by = c$ admite solução em inteiros exatamente quando $(a, b) \mid c$. $\square$

Uma vez estabelecida a condição necessária e suficiente para que a equação $ax + by = c$ tenha solução inteira, podemos descrever a seguir todas as suas soluções a partir de uma solução particular.

Proposição 2.16. *Seja (x_0, y_0) uma solução inteira da equação diofantina $ax + by = c$, em que $(a, b) = 1$. Então todas as soluções inteiras são dadas por*

$$x = x_0 + tb \quad \text{e} \quad y = y_0 - ta, \quad t \in \mathbb{Z}.$$

Demonstração. Se (x, y) é outra solução da equação $ax + by = c$, então $ax + by = ax_0 + by_0$, e portanto $a(x - x_0) + b(y - y_0) = 0$, isto é, $a(x - x_0) = -b(y - y_0)$.

Como $(a, b) = 1$, segue do Lema de Gauss que $b \mid (x - x_0)$; assim, existe $t \in \mathbb{Z}$ tal que $x - x_0 = tb$, ou simplesmente $x = x_0 + tb$.

Substituindo essa expressão em $a(x - x_0) = -b(y - y_0)$, obtemos $a(tb) = -b(y - y_0)$ e, cancelando b , resulta $at = -(y - y_0)$; portanto, $y = y_0 - ta$.

Assim, todas as soluções inteiras são da forma $x = x_0 + tb$ e $y = y_0 - ta$, com $t \in \mathbb{Z}$. $\square$

Observa-se, portanto, que as equações diofantinas lineares possuem infinitas soluções sempre que o máximo divisor comum de a e b for igual a 1.

Além disso, uma solução particular pode ser obtida utilizando o algoritmo de Euclides. De fato, se $(a, b) = 1$, então existem $m, n \in \mathbb{Z}$ tais que

$$1 = am + bn.$$

Multiplicando ambos os lados por c , obtemos

$$c = (cm)a + (cn)b.$$

Assim, $(x_0, y_0) = (cm, cn)$ constitui uma solução particular da equação

$$aX + bY = c.$$

A partir dessa solução particular, todas as demais podem ser determinadas pelas expressões

$$X = x_0 + tb, \quad Y = y_0 - ta, \quad t \in \mathbb{Z}.$$

A seguir utilizaremos o seguinte resultado, cuja demonstração pode ser encontrada em Hefez (11).

Teorema 2.17. *A equação $ax + by = c$, onde $(a, b) = 1$, tem solução em números naturais se, e somente se, $c \notin L(a, b)$, onde o conjunto lacunar é definido por*

$$L(a, b) = \{ma - nb \in \mathbb{N} ; m, n \in \mathbb{N}, m < b\}.$$

Este teorema desempenha um papel particularmente importante quando analisamos equações diofantinas da forma $ax + by = c$ cujas soluções buscamos nos números naturais. Em alguns problemas, o valor de c não é previamente conhecido, ou depende de condições adicionais do enunciado. Nessas situações, é fundamental determinar para quais valores de c a equação admite solução e, sobretudo, para quais valores ela certamente não admite.

O conjunto lacunar $L(a, b)$, descrito no teorema, fornece exatamente essa informação: ele reúne todos os valores naturais que não podem ser escritos como combinação linear positiva de a e b . Dessa forma, torna-se possível identificar de maneira precisa os valores de c para os quais a equação não possui solução, bem como determinar a partir de qual ponto todas as quantidades naturais passam a ser representáveis na forma $ax + by$.

As equações diofantinas lineares surgem naturalmente como uma aplicação direta do máximo divisor comum. Uma vez conhecido o valor de (a, b) , é possível não apenas verificar a existência de soluções inteiras ou naturais, mas também descrevê-las de forma explícita. Esse fato reforça o papel central do cálculo do mdc na resolução de problemas aritméticos, especialmente no contexto dos desafios propostos nas olimpíadas de matemática.

2.6 Números primos

Definição 2.18. Um número natural maior que 1, que possui exatamente dois divisores positivos distintos, 1 e ele próprio, é chamado número primo.

Considere dois números primos p e q , e um número inteiro qualquer a . A partir da definição de número primo, decorrem os seguintes fatos:

I) Se $p \mid q$, então $p = q$.

De fato, como p divide q e q é primo, temos que $p = 1$ ou $p = q$. Mas, sendo p também primo, segue que $p > 1$, logo $p = q$.

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

Sabemos que $(p, a) = d$, de modo que $d \mid p$ e $d \mid a$. Como p é primo, o divisor d só pode ser 1 ou p . Mas, como $p \nmid a$, temos $d \neq p$, e portanto $d = 1$. Assim, concluímos que $(p, a) = 1$.

Um número natural maior que 1 que não é primo é chamado composto. Por exemplo, os números 2, 3, 5, 7, 11, 13 e 17 são primos, enquanto 4, 6, 8, 9, 10, 12 e 14 são compostos.

Do ponto de vista multiplicativo, os números primos podem ser vistos como os blocos fundamentais de construção dos números naturais, pois a partir deles é possível obter todos os demais números. Esse fato é conhecido como Teorema Fundamental da Aritmética, que será apresentado mais adiante.

A seguir, apresentamos o Lema de Euclides, que estabelece uma relação entre a divisibilidade e a primalidade.

Proposição 2.19. (*Lema de Euclides*) Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Demonstração. Suponhamos que $p \mid ab$ e que $p \nmid a$. Como p é primo e não divide a , temos que $\text{mdc}(p, a) = 1$.

Pelo Lema de Gauss 2.12, que afirma que se $a \mid bc$ e $\text{mdc}(a, b) = 1$, então $a \mid c$, segue que $p \mid b$.

Logo, se $p \mid ab$, então $p \mid a$ ou $p \mid b$. □

Esse lema expressa uma propriedade essencial dos números primos: um número primo que divide um produto precisa dividir ao menos um dos fatores.

Uma consequência imediata desse *Lema de Euclides* é o seguinte corolário:

Corolário 2.20. *Se $p, p_1, p_2, \dots, p_n$ são números primos e se $p \mid (p_1 p_2 \cdots p_n)$, então $p = p_i$ para algum $i = 1, 2, \dots, n$.*

Demonstração. A prova é feita por indução sobre n .

Para $n = 1$, temos $p \mid p_1$, o que implica $p = p_1$, pois ambos são primos.

Suponhamos o resultado verdadeiro para $n = k$ e consideremos o caso $n = k + 1$. Se $p \mid (p_1 p_2 \cdots p_k p_{k+1})$, então, pelo Lema de Euclides,

$$p \mid (p_1 p_2 \cdots p_k) \quad \text{ou} \quad p \mid p_{k+1}.$$

No primeiro caso, pela hipótese de indução, $p = p_i$ para algum $i \leq k$; no segundo, $p = p_{k+1}$. Em ambos os casos, o resultado é verdadeiro. $\square$

Esse corolário garante que, se um número primo aparece como divisor de um produto de primos, então ele já está presente entre os fatores. Essa propriedade será necessária para demonstrar a unicidade da decomposição em fatores primos.

Teorema 2.21. *(Teorema Fundamental da Aritmética) Todo número natural $n > 1$ é primo ou pode ser escrito, de modo único (a menos da ordem dos fatores), como um produto de números primos.*

Demonstração. A demonstração será dividida em duas partes: existência e unicidade.

I) **Existência.** Provaremos por indução sobre n .

Para $n = 2$, o resultado é verdadeiro, pois 2 é primo. Suponha que todo número natural maior que 1 e menor que n pode ser escrito como produto de primos. Se n é primo, não há o que demonstrar. Caso n seja composto, então existem n_1 e n_2 tais que

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

Pela hipótese de indução, n_1 e n_2 admitem fatoração em primos, dessa forma:

$$n_1 = p_1 p_2 \cdots p_r \quad \text{e} \quad n_2 = q_1 q_2 \cdots q_s.$$

Então,

$$n = n_1 n_2 = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s,$$

ou seja, n é produto de primos. Assim, a decomposição existe para todo $n > 1$.

II) **Unicidade.** Provaremos por indução sobre n .

Para $n = 2$, o resultado é imediato, pois 2 é primo e, portanto, possui apenas uma decomposição em fatores primos.

Suponhamos que todo número natural maior que 1 e menor que n admite uma única decomposição em fatores primos, a menos da ordem dos fatores.

Suponha que um mesmo número n possa ser escrito de duas formas distintas:

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

onde todos os p_i e q_j são números primos.

Como p_1 divide o produto $q_1 q_2 \cdots q_s$, pelo Corolário 2.20, p_1 divide algum q_j , mas, como q_j é primo, segue que $p_1 = q_j$.

Trocando, se necessário, a ordem dos fatores na segunda decomposição, podemos supor que $p_1 = q_1$.

Dividindo ambos os lados por p_1 , obtemos:

$$\frac{n}{p_1} = p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s.$$

Como $\frac{n}{p_1} < n$, podemos aplicar a hipótese de indução, segundo a qual a decomposição em primos é única para todos os números menores que n . Logo, as duas decomposições restantes coincidem, o que implica que $r = s$ e, a menos da ordem dos fatores, $p_i = q_i$ para todo i .

Portanto, a decomposição de n em fatores primos é única, a menos da ordem dos fatores.

□

O teorema anterior assegura que qualquer número natural maior que 1 pode ser decomposto de maneira única em fatores primos. Vejamos um exemplo simples que ilustra essa propriedade, $60 = 2^2 \cdot 3 \cdot 5$. Não há outra forma de escrever 60 como produto de primos, exceto pela ordem dos fatores: $60 = 3 \cdot 2 \cdot 5 \cdot 2 = 2^2 \cdot 3 \cdot 5$.

Assim, todo número inteiro n , diferente de 0, 1 e -1 , pode ser escrito, de maneira única, como o produto de números primos. Em outras palavras, existem primos distintos $p_1 < p_2 < \cdots < p_r$ e inteiros positivos $\alpha_1, \alpha_2, \dots, \alpha_r$ tais que $n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$.

A partir dessa fatoração, podemos identificar propriedades importantes dos números naturais, como a determinação de seus divisores e o reconhecimento dos quadrados perfeitos.

Proposição 2.22. *Seja $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ a decomposição em fatores primos de um número natural $n > 1$. Então, todo divisor positivo n' de n é da forma*

$$n' = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r},$$

onde $0 \leq \beta_i \leq \alpha_i$, para todo $i = 1, 2, \dots, r$.

Demonstração. Seja n' um divisor positivo de n . Como n e n' são naturais, ambos possuem decomposição única em fatores primos. Se p^β é uma potência de primo que aparece na decomposição de n' , então p^β divide n , o que implica que p^β divide algum dos fatores primos de n , digamos $p_i^{\alpha_i}$. Logo, $p = p_i$ e $0 \leq \beta \leq \alpha_i$. $\square$

Consequentemente, é possível determinarmos a quantidade de divisores positivos de um número natural n , denotada por $d(n)$, em que $d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$, pois para cada primo p_i , o expoente correspondente β_i pode assumir qualquer valor entre 0 e α_i , inclusive. Desta forma, há exatamente $\alpha_i + 1$ possibilidades para cada β_i . Como as escolhas são independentes, o número total de combinações possíveis é o produto de todas essas quantidades.

O número $n = 36$, por exemplo, tem a seguinte decomposição em fatores primos $36 = 2^2 \cdot 3^2$. Logo, $d(36) = (2 + 1)(2 + 1) = 9$. De fato, os divisores positivos de 36 são

$$1, 2, 3, 4, 6, 9, 12, 18 \text{ e } 36.$$

Note que 36 possui uma quantidade ímpar de divisores e isso ocorre porque ele é um quadrado perfeito, pois todos os seus expoentes são pares. Relacionado a essa propriedade, apresentamos um problema que costuma aparecer nas aulas sobre este tema.

Exemplo 2.23. (Problema dos armários) No vestiário de uma escola com n alunos, numerados de 1 até n , há n armários fechados enfileirados em um corredor, também numerados de 1 a n . Um dia, os alunos resolvem fazer a seguinte brincadeira: O primeiro aluno abre todos os armários. O segundo aluno fecha todos os armários cujos números são múltiplos de 2. O terceiro aluno inverte a posição (abre se estiver fechado, e fecha se estiver aberto) dos armários múltiplos de 3. O processo continua até que o aluno de número n realize a ação com os armários múltiplos de n .

Pergunta-se: ao final, quais armários permanecerão abertos?

Solução. Um armário k tem sua posição alterada uma vez para cada divisor de k . Portanto, ele será aberto ou fechado um número igual a $d(k)$ vezes. Se $d(k)$ for par, o armário voltará ao estado inicial (fechado); se $d(k)$ for ímpar, permanecerá aberto. Pelo resultado anterior, isso ocorre se, e somente se, k é um quadrado perfeito. Logo, os armários que permanecerão abertos são aqueles de número 1, 4, 9, 16, 25, $\dots$

A partir da fatoração em primos, também é possível calcular o mdc e o mmc de um conjunto qualquer de números. Essa relação é direta, uma vez que a decomposição em fatores primos organiza os números de maneira a permitir comparar os expoentes de cada primo envolvido.

Teorema 2.24. *Sejam $a = \pm p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ e $b = \pm p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_n^{\beta_n}$, as decomposições em fatores primos de dois inteiros a e b . Defina,*

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

tem-se que

$$(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n}, \quad e \quad [a, b] = p_1^{\delta_1} p_2^{\delta_2} \cdots p_n^{\delta_n}.$$

Demonstração. De acordo com a Proposição 2.22, o número $p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n}$ é divisor comum de a e b , pois para todo i temos $\gamma_i = \min\{\alpha_i, \beta_i\} \leq \alpha_i$ e $\gamma_i \leq \beta_i$.

Seja c um divisor comum de a e b . Escrevendo $c = \pm p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_n^{\varepsilon_n}$, como $c \mid a$ e $c \mid b$, segue que $\varepsilon_i \leq \alpha_i$ e $\varepsilon_i \leq \beta_i$ para todo i . Logo, $\varepsilon_i \leq \gamma_i$, e portanto $c \mid p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n}$.

Assim, $p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n}$ é o máximo divisor comum de a e b .

Para o mínimo múltiplo comum, note que $p_1^{\delta_1} p_2^{\delta_2} \cdots p_n^{\delta_n}$ é múltiplo comum de a e b , pois $\delta_i = \max\{\alpha_i, \beta_i\} \geq \alpha_i$ e $\delta_i \geq \beta_i$ para todo i . Portanto, $a \mid p_1^{\delta_1} p_2^{\delta_2} \cdots p_n^{\delta_n}$ e $b \mid p_1^{\delta_1} p_2^{\delta_2} \cdots p_n^{\delta_n}$.

Seja agora c um múltiplo comum de a e b , com fatoração $c = \pm p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_n^{\varepsilon_n} \cdot k$, com $k \in \mathbb{Z}$ em que $p_i \nmid k$, para $i = 1, \dots, n$. Como $a \mid c$ e $b \mid c$, temos $\varepsilon_i \geq \alpha_i$ e $\varepsilon_i \geq \beta_i$ para todo i . Assim, $\varepsilon_i \geq \max\{\alpha_i, \beta_i\} = \delta_i$, o que implica $p_1^{\delta_1} p_2^{\delta_2} \cdots p_n^{\delta_n} \mid c$.

Logo, $p_1^{\delta_1} p_2^{\delta_2} \cdots p_n^{\delta_n}$ é o mínimo múltiplo comum de a e b .

□

Dessa forma, a fatoração em primos fornece um caminho direto para compreender a estrutura dos divisores e múltiplos de números naturais.

Uma questão clássica que naturalmente surge é: quantos números primos existem? A resposta, dada por Euclides em *Os Elementos*, é elegante e fundamental: existem infinitos números primos. Essa demonstração elementar não só ilustra o poder do raciocínio dedutivo na matemática, como também serve como ponto de partida para discussões em sala de aula sobre a lógica e a criatividade envolvidas na resolução de problemas.

Teorema 2.25. *Existem infinitos números primos.*

Demonstração. Suponhamos que exista apenas uma quantidade finita de números primos. Denotemos esses primos por $p_1, p_2, \dots, p_r$. Consideremos o número

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_r + 1.$$

Pelo Teorema 2.21, todo número natural maior que 1 pode ser escrito como produto de números primos. Assim, o número n possui pelo menos um divisor primo, digamos p .

Como, por hipótese, todos os primos existentes são $p_1, p_2, \dots, p_r$, esse divisor primo p deve coincidir com um deles, isto é, existe um primo $p = p_i$ para algum $i = 1, 2, \dots, r$.

No entanto, observe que n deixa resto 1 quando dividido por cada um dos primos $p_1, p_2, \dots, p_r$.

De fato, para qualquer i , temos

$$n = (p_1 p_2 \cdots p_r) + 1 = p_i \cdot k + 1,$$

para algum número inteiro k , o que implica que o resto da divisão de n por p_i é 1. Logo, nenhum dos primos $p_1, p_2, \dots, p_r$ divide n .

Essa contradição mostra que a suposição inicial de que existia apenas um número finito de primos é falsa. Portanto, conclui-se que existem infinitos números primos. $\square$

Sabemos que existem infinitos números primos e, naturalmente, surge o questionamento: como identificá-los? Um dos métodos mais antigos para encontrar todos os primos até certo limite é o Crivo de Eratóstenes. O procedimento é simples: escrevemos os inteiros de 2 até o limite escolhido. Repetidamente, escolhemos o menor número ainda não riscado que é primo e riscamos todos os seus múltiplos exceto ele próprio. Surge então uma dúvida: até onde precisamos continuar esse processo?

Um fato crucial que permite parar o processo é dado pelo seguinte lema.

Lema 2.26. *Seja $n > 1$ um número natural. Se n não é divisível por nenhum primo p tal que $p^2 \leq n$, então n é primo.*

Demonstração. Suponha, por absurdo, que n seja composto e que não seja divisível por nenhum primo p tal que $p^2 \leq n$. Então existem inteiros a, b com $1 < a \leq b < n$ tais que $n = ab$. Escolha a como o menor divisor de n maior que 1. Essa escolha é importante porque garante que a não pode ser composto: se a fosse composto, teria uma fatoração $a = uv$ com $1 < u \leq v < a$, e u seria um divisor de n menor que a , contradizendo a minimalidade de a . Portanto, a é primo.

Como $a \leq b$, segue $a^2 \leq ab = n$, segue daí que $a^2 \leq n$. Assim, existe um primo a divisor de n com $a^2 \leq n$, o que contradiz a hipótese. Logo, n não pode ser composto e, portanto, é primo. $\square$

Em particular, para testar a primalidade de n basta verificar se ele não é divisível por nenhum primo $p \leq \sqrt{n}$.

Por exemplo, para listar todos os primos até 150 pelo crivo de Eratóstenes, basta riscar múltiplos dos primos $p \leq \sqrt{150}$. Como $\sqrt{150} \approx 12,25$, os primos necessários são 2, 3, 5, 7, 11. Após eliminar múltiplos de 2, 3, 5, 7 e 11, começando em p^2 para cada p , já

que múltiplos menores já terão sido riscados por primos menores, os números que restarem não riscados são exatamente os primos menores ou iguais a 150.

Assim, o lema fornece a base teórica que explica por que podemos interromper o crivo em $\sqrt{n}$.

Embora o Crivo de Eratóstenes e o teste de divisibilidade por números primos sejam métodos eficientes para valores pequenos, tornam-se pouco práticos quando se deseja verificar a primalidade de números muito grandes. Ainda assim, do ponto de vista pedagógico, são excelentes ferramentas para ajudar o estudante a compreender a estrutura dos números primos e a distinguir entre números primos e compostos.

Entretanto, à medida que a matemática avançou, surgiram resultados teóricos que permitem testar a primalidade de números de forma mais rápida, ainda que não completamente decisiva. O *Pequeno Teorema de Fermat*, enunciado abaixo e demonstrado como corolário do *Teorema de Euler* na seção 2.7, fornece uma condição necessária para que um número seja primo.

Teorema 2.27. (*Pequeno Teorema de Fermat*) Se p é um número primo, então para todo número inteiro a , o número $a^p - a$ é divisível por p .

Uma consequência direta desse resultado é que, se p é primo e a é um número natural não divisível por p , ou seja, $(a, p) = 1$ então $p \mid a^{p-1} - 1$. Em outras palavras, $a^{p-1} - 1$ é um múltiplo de p .

Esse resultado é muito útil na resolução de problemas e na verificação de primalidade, pois fornece um teste de não primalidade. De fato, se para algum número a tivermos que $a^p - a$ não é múltiplo de p , então p certamente não é primo. Por outro lado, se a igualdade vale, não podemos garantir que p seja primo, uma vez que existem números compostos que também verificam essa propriedade.

2.7 Congruência

O estudo das congruências permite analisar números a partir do comportamento de seus restos obtidos em divisões por um mesmo inteiro positivo. Em diversas situações, dois números distintos podem apresentar o mesmo resto quando divididos por um mesmo número, o que faz com que se comportem de maneira equivalente em determinados cálculos. A noção de congruência formaliza essa equivalência e organiza a manipulação dos restos, sendo uma ferramenta recorrente em problemas que envolvem divisibilidade e certos padrões numéricos.

A aritmética dos restos também oferece uma vantagem prática importante: muitas verificações que, de maneira tradicional, exigiriam a análise separada dos possíveis restos de

uma divisão podem ser conduzidas de forma mais direta por meio das congruências. Esse tratamento reduz o trabalho algébrico e torna algumas demonstrações e resoluções mais simples e eficientes, especialmente em situações que envolvem divisibilidade ou expressões cujo comportamento depende apenas do resto assumido módulo n .

Definição 2.28. Seja m um número natural. Dizemos que dois inteiros a e b são *congruentes módulo m* quando os restos da divisão euclidiana de a e de b por m coincidirem. Nesse caso, escrevemos

$$a \equiv b \pmod{m}.$$

Se os restos não coincidirem, afirmamos que a e b não são congruentes módulo m , o que é indicado por

$$a \not\equiv b \pmod{m}.$$

Como exemplo, note que 17 e 26 deixam resto 2 quando divididos por 3. Portanto,

$$17 \equiv 26 \pmod{3}.$$

Observe que, para $m = 1$, todo número inteiro deixa resto zero. Assim, quaisquer inteiros a e b satisfazem $a \equiv b \pmod{1}$, o que torna trivial a aritmética dos restos nesse caso. Portanto, assumiremos sempre $m > 1$.

Da definição de congruência, seguem imediatamente algumas propriedades básicas que serão características fundamentais de uma relação de equivalência.

Proposição 2.29. *Sejam $a, b, c \in \mathbb{Z}$ e $m > 1$ um inteiro fixado. Então valem as seguintes propriedades:*

- (i) *Reflexividade:* $a \equiv a \pmod{m}$;
- (ii) *Simetria:* se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$;
- (iii) *Transitividade:* se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

Demonstração. A reflexividade segue imediatamente da definição, ao dividir a por m , o resto obtido é o mesmo nas duas ocorrências, de modo que $a \equiv a \pmod{m}$.

No caso da simetria, suponha que $a \equiv b \pmod{m}$. Isso significa que a e b deixam o mesmo resto quando divididos por m , o que garante $b \equiv a \pmod{m}$.

Por fim, para a transitividade, suponha que $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$. Assim, a , b e c deixam o mesmo resto na divisão por m , o que implica $a \equiv c \pmod{m}$. $\square$

Para determinar se dois inteiros são congruentes módulo m , não é necessário efetuar a divisão euclidiana de cada um e comparar os respectivos restos. Em vez disso, a verificação

pode ser feita de forma mais direta, dispensando etapas que tradicionalmente seriam mais trabalhosas. O próximo resultado formaliza esse procedimento.

Proposição 2.30. *Sejam $a, b, m \in \mathbb{Z}$ com $m > 1$. Tem-se que*

$$a \equiv b \pmod{m} \quad \text{se, e somente se,} \quad m \mid (b - a).$$

Demonstração. Suponha que $a \equiv b \pmod{m}$. Pelo algoritmo da divisão, existem inteiros q_1, q_2 e um resto r , com $0 \leq r < m$, tais que

$$a = q_1m + r \tag{2.1}$$

e

$$b = q_2m + r. \tag{2.2}$$

Subtraindo (2.1) de (2.2), obtemos

$$b - a = (q_2 - q_1)m,$$

de modo que $m \mid (b - a)$.

Reciprocamente, suponha que $m \mid (b - a)$. Então existe um inteiro k tal que

$$b - a = km. \tag{2.3}$$

Logo,

$$b = a + km. \tag{2.4}$$

Aplicando o algoritmo da divisão a a , existem inteiros q e r , com $0 \leq r < m$, tais que

$$a = qm + r. \tag{2.5}$$

Substituindo (2.5) em (2.4), obtemos

$$b = (qm + r) + km = (q + k)m + r.$$

Assim, a e b deixam o mesmo resto r quando divididos por m , o que nos permite concluir que $a \equiv b \pmod{m}$. $\square$

Ao dividir um inteiro a por m , o resto obtido pertence ao conjunto $\{0, 1, \dots, m-1\}$. Esses m valores são, dois a dois, incongruentes módulo m e representam todas as classes de restos possíveis.

Definição 2.31. Um *sistema completo de resíduos módulo m* é qualquer conjunto formado por m inteiros, dois a dois, incongruentes módulo m ; isto é, um conjunto que contém exatamente um representante de cada classe de restos.

O conjunto usual $\{0, 1, \dots, m-1\}$ é um sistema completo de resíduos, assim como qualquer conjunto de m inteiros consecutivos. De forma mais geral, vale o resultado seguinte.

Proposição 2.32. *Se $a_1, \dots, a_m$ são inteiros dois a dois incongruentes módulo m , então o conjunto $\{a_1, \dots, a_m\}$ é um sistema completo de resíduos módulo m .*

Demonstração. Como $a_1, \dots, a_m$ são, dois a dois, incongruentes módulo m , os restos que produzem ao serem divididos por m são todos distintos. Existem exatamente m restos possíveis, de modo que cada classe é representada uma única vez, o que caracteriza um sistema completo de resíduos. $\square$

Embora o conjunto $\{0, 1, \dots, m-1\}$ seja a escolha mais comum, qualquer sistema completo de resíduos pode ser usado para representar classes módulo m . A divisão euclidiana corresponde ao caso em que o resto pertence ao intervalo $0 \leq r < m$.

A relação de congruência é compatível com as operações usuais de adição e multiplicação dos inteiros. Os resultados a seguir descrevem essas propriedades.

Proposição 2.33. *Sejam $a, b, c, d, m \in \mathbb{Z}$ com $m > 1$. Valem as seguintes propriedades:*

- (i) *Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$.*
- (ii) *Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $ac \equiv bd \pmod{m}$.*

Demonstração. (i) Das hipóteses $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, temos $m \mid (b - a)$ e $m \mid (d - c)$. Como m divide cada uma das diferenças, também divide a sua soma. Assim,

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

é múltiplo de m . Portanto, $a + c \equiv b + d \pmod{m}$.

- (ii) Das congruências dadas, existem inteiros k e ℓ tais que $b = a + mk$ e $d = c + m\ell$. Consideremos a diferença entre os produtos,

$$bd - ac = (a + mk)(c + m\ell) - ac.$$

Efetuando a multiplicação, obtemos

$$bd - ac = am\ell + cmk + m^2k\ell,$$

e essa expressão é múltipla de m , pois pode ser reescrita como

$$bd - ac = m(al + ck + mk\ell).$$

Assim, $m \mid (bd - ac)$, e portanto $ac \equiv bd \pmod{m}$. $\square$

Corolário 2.34. *Sejam a, b e $m \in \mathbb{Z}$ com $m > 1$. Para todo $n \in \mathbb{N}$, se $a \equiv b \pmod{m}$ então $a^n \equiv b^n \pmod{m}$.*

Demonstração. A demonstração será feita por indução sobre n .

Para $n = 1$, temos $a^1 = a \equiv b = b^1 \pmod{m}$, como desejado.

Suponha que, para algum $n \in \mathbb{N}$, $a^n \equiv b^n \pmod{m}$, seja verdadeira. Como também temos $a \equiv b \pmod{m}$, a compatibilidade com o produto implica $a^{n+1} = a^n \cdot a \equiv b^n \cdot b = b^{n+1} \pmod{m}$.

Portanto, pelo princípio da indução, o resultado vale para todo $n \in \mathbb{N}$. $\square$

A seguir, apresentamos um resultado simples sobre a operação de adição em congruências. Ele será útil para caracterizar situações em que é possível realizar cancelamentos de termos somados nos dois lados de uma congruência.

Proposição 2.35. *Sejam $a, b, c \in \mathbb{Z}$ e $m > 1$ um inteiro. Vale que*

$$a + c \equiv b + c \pmod{m} \iff a \equiv b \pmod{m}.$$

Demonstração. Suponha inicialmente que $a + c \equiv b + c \pmod{m}$. Então

$$m \mid ((b + c) - (a + c)) = b - a,$$

e, portanto, $a \equiv b \pmod{m}$.

Reciprocamente $a \equiv b \pmod{m}$. Como $c \equiv c \pmod{m}$, segue da Proposição 2.33(i) (compatibilidade da soma) que

$$a + c \equiv b + c \pmod{m}.$$

$\square$

O cancelamento de termos somados funciona sem restrições, como visto acima. No entanto, o mesmo não ocorre para o produto, pois em geral não é possível cancelar um fator comum em ambos os lados de uma congruência. Para caracterizar quando esse cancelamento é válido, utilizamos o resultado a seguir.

Proposição 2.36. *Sejam $a, b, c \in \mathbb{Z}$ e $m > 1$. Vale que*

$$ac \equiv bc \pmod{m} \iff a \equiv b \pmod{\frac{m}{(c, m)}}.$$

Demonstração. Observe primeiro que

$$\frac{m}{(c, m)} \text{ e } \frac{c}{(c, m)}$$

são coprimos. Se um primo p dividisse ambas as quantidades, $p(c, m)$ dividiria m e c , o que contradiz a definição de (c, m) , pois $p(c, m) > (c, m)$.

Além disso,

$$ac \equiv bc \pmod{m} \iff m \mid (b - a)c$$

$$\iff \frac{m}{(c, m)} \mid (b - a) \frac{c}{(c, m)}.$$

Como as quantidades acima são coprimas, $\frac{m}{(c, m)}$ só pode dividir $(b - a)$. Portanto,

$$\frac{m}{(c, m)} \mid (b - a) \frac{c}{(c, m)} \iff \frac{m}{(c, m)} \mid (b - a) \iff a \equiv b \pmod{\frac{m}{(c, m)}}.$$

Isso conclui a demonstração. $\square$

Corolário 2.37. *Sejam $a, b, c \in \mathbb{Z}$ e $m > 1$. Se $(c, m) = 1$ e $ac \equiv bc \pmod{m}$, então $a \equiv b \pmod{m}$.*

Demonstração. Pela Proposição 2.36, tem-se

$$ac \equiv bc \pmod{m} \iff a \equiv b \pmod{\frac{m}{(c, m)}}.$$

Se $(c, m) = 1$, então $\frac{m}{(c, m)} = m$, de onde $a \equiv b \pmod{m}$. $\square$

Para demonstrar uma das propriedades apresentadas a seguir, utilizaremos uma propriedade simples do mínimo múltiplo comum, que enunciamos no lema seguinte.

Lema 2.38. *Sejam $m_1, \dots, m_r$ inteiros positivos e $k \in \mathbb{Z}$. Se $m_i \mid k$ para todo $i = 1, \dots, r$, então $[m_1, \dots, m_r] \mid k$.*

Demonstração. Como $m_i \mid k$ para todo i , o número k é um múltiplo comum de $m_1, \dots, m_r$. Como $[m_1, \dots, m_r]$ é o mínimo múltiplo comum desses inteiros, segue que $[m_1, \dots, m_r] \mid k$. $\square$

A seguir, apresentamos algumas propriedades gerais da congruência.

Proposição 2.39. *Sejam $a, b \in \mathbb{Z}$ e $m, m_1, \dots, m_r$ inteiros maiores do que 1. Valem as seguintes propriedades:*

- (i) Se $a \equiv b \pmod{m}$ e $n \mid m$, então $a \equiv b \pmod{n}$;
- (ii) $a \equiv b \pmod{m_i}$ para todo $i = 1, \dots, r$ se, e somente se, $a \equiv b \pmod{[m_1, \dots, m_r]}$;
- (iii) Se $a \equiv b \pmod{m}$, então $(a, m) = (b, m)$.

Demonstração. (i) Suponha $a \equiv b \pmod{m}$. Então $m \mid (b - a)$. Como $n \mid m$, segue $n \mid (b - a)$, isto é, $a \equiv b \pmod{n}$.

(ii) Primeiro, suponha $a \equiv b \pmod{m_i}$ para cada $i = 1, \dots, r$. Então $m_i \mid (b - a)$ para todo i . Pelo Lema 2.38, segue que $[m_1, \dots, m_r] \mid (b - a)$. Logo,

$$a \equiv b \pmod{[m_1, \dots, m_r]}.$$

Reciprocamente, suponha $a \equiv b \pmod{[m_1, \dots, m_r]}$. Então $[m_1, \dots, m_r] \mid (b - a)$. Pelo item (i), como $m_i \mid [m_1, \dots, m_r]$ para todo i , concluímos que $m_i \mid (b - a)$ para cada i . Assim, $a \equiv b \pmod{m_i}$ para todo i .

(iii) Suponha $a \equiv b \pmod{m}$. Então $m \mid (b - a)$, isto é, $b - a = tm$ para algum $t \in \mathbb{Z}$. Assim, $b = a + tm$.

Pelo Lema de Euclides 2.9, obtemos $(a, m) = (a + tm, m)$. Como $a + tm = b$, segue $(a, m) = (b, m)$, o que conclui o resultado.

□

As definições e propriedades apresentadas fornecem as ferramentas necessárias para lidar com diferentes tipos de problemas envolvendo congruências, como determinar restos de divisões, verificar divisibilidade, identificar algarismos específicos ou caracterizar números que satisfazem certas condições aritméticas. Embora muitos desses problemas admitam abordagens diretas, a aritmética modular organiza os argumentos e reduz etapas desnecessárias.

Entretanto, quando lidamos com potências muito elevadas, os métodos elementares tornam-se pouco eficientes. Para tratar expressões da forma $a^k \pmod{m}$, precisamos de um resultado mais forte, capaz de descrever o comportamento das potências módulo m de forma geral. O principal resultado que permite esse avanço é o Teorema de Euler.

Para introduzir essa ideia, partimos do sistema completo de resíduos módulo m , que reúne m inteiros, dois a dois, incongruentes, representando todas as classes de restos. Dentre esses representantes, alguns podem compartilhar fatores com m , enquanto outros são coprimos com ele. Selecionando apenas os inteiros cujo máximo divisor comum com m é igual a 1, obtemos um subconjunto formado exatamente pelos elementos coprimos com m . Esse subconjunto, fundamental para a formulação do *Teorema de Euler*, recebe o nome de *sistema reduzido de resíduos* módulo m e sua quantidade de elementos é dada pela função $\varphi(m)$, a função *fi de Euler*.

Definição 2.40. Seja $m > 1$. Um sistema reduzido de resíduos módulo m é qualquer conjunto

$$\{a_1, a_2, \dots, a_{\varphi(m)}\}$$

de inteiros tais que:

- (i) $(a_i, m) = 1$, para todo i ;
- (ii) $a_i \not\equiv a_j \pmod{m}$, se $i \neq j$;
- (iii) para todo inteiro n com $(n, m) = 1$, existe i tal que $n \equiv a_i \pmod{m}$.

Da definição, segue que cada inteiro coprimo com m é congruente módulo m a um único elemento do sistema.

Observe que o sistema reduzido é obtido a partir de um sistema completo de resíduos módulo m pela remoção dos elementos que não são coprimos com m . Assim, $\varphi(m)$ representa exatamente o número de inteiros entre 1 e m que não compartilham fatores primos com m .

Exemplo 2.41. Se p é primo, então todos os inteiros $1, 2, \dots, p-1$ são coprimos com p . Assim, o sistema reduzido de resíduos módulo p coincide com o sistema completo de resíduos exceto pelo 0 e portanto

$$\varphi(p) = p - 1.$$

Proposição 2.42. *Sejam $m, n > 1$ inteiros coprimos. Então*

$$\varphi(mn) = \varphi(m) \varphi(n).$$

Demonstração. Organizamos os inteiros de 1 a mn em uma tabela com m linhas e n colunas. A i -ésima coluna contém exatamente os números da forma

$$i, i + n, i + 2n, \dots, i + (m-1)n, \quad \text{para } i = 1, \dots, n.$$

	Coluna 1	Coluna 2	...	Coluna n
Linha 1	1	2	...	n
Linha 2	$1 + n$	$2 + n$	...	$n + n$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
Linha m	$1 + (m-1)n$	$2 + (m-1)n$	...	$n + (m-1)n$

Observemos primeiro como identificar, nessa tabela, os inteiros coprimos com n . Para um número da coluna i , isto é, um inteiro da forma $i + kn$, vale

$$(i + kn, n) = (i, n),$$

pois qualquer divisor comum de i e n divide $i + kn$ e vice-versa. Assim, todos os números de uma mesma coluna são simultaneamente coprimos com n ou nenhum deles é. Como entre 1 e n existem exatamente $\varphi(n)$ inteiros coprimos com n , segue que exatamente $\varphi(n)$ colunas da tabela contêm inteiros coprimos com n .

Fixemos agora uma dessas colunas, digamos a coluna i . Seus elementos são

$$i, i + n, i + 2n, \dots, i + (m - 1)n.$$

Como $(m, n) = 1$, a sequência $i, i + n, i + 2n, \dots, i + (m - 1)n$ percorre todas as classes de restos módulo m exatamente uma vez. De fato, suponhamos que $i + k_1n \equiv i + k_2n \pmod{m}$, com $0 \leq k_1, k_2 < m$, então $m \mid (k_1 - k_2)n$. Como $(m, n) = 1$, segue que $m \mid (k_1 - k_2)$. Como $0 \leq k_1, k_2 < m$ e $m \mid (k_1 - k_2)$, concluímos que $k_1 - k_2 = 0$, isto é, números diferentes na mesma coluna possuem classes diferentes. Assim, entre esses m inteiros, exatamente $\varphi(m)$ são coprimos com m .

Um inteiro é coprimo com mn se, e somente se, é coprimo com m e com n . Portanto, cada coluna cujo índice é coprimo com n contém exatamente $\varphi(m)$ inteiros que são coprimos com m e, conseqüentemente, com mn .

Como há $\varphi(n)$ colunas “boas” e cada uma contém $\varphi(m)$ inteiros coprimos com mn , o total de inteiros entre 1 e mn que são coprimos com mn é

$$\varphi(n) \varphi(m).$$

□

Dando sequência ao estudo da função φ , analisamos agora seu comportamento quando o argumento é uma potência de primo.

Proposição 2.43. *Seja p primo e $r \geq 1$. Então*

$$\varphi(p^r) = p^r - p^{r-1} = p^r \left(1 - \frac{1}{p}\right).$$

Demonstração. No conjunto $\{1, 2, \dots, p^r\}$ há exatamente p^r números. Como p é primo, não são coprimos com p^r exatamente aqueles que são múltiplos de p . Os múltiplos de p no referido conjunto são $p, 2p, 3p, \dots, (p^{r-1})p$, portanto existem p^{r-1} desses múltiplos. Excluindo-os do total de p^r inteiros, obtém-se $\varphi(p^r) = p^r - p^{r-1}$, o que equivale à forma $p^r \left(1 - \frac{1}{p}\right)$. □

A seguir, vamos determinar $\varphi(m)$ para qualquer $m > 1$. Para isso, basta utilizar a decomposição de m em fatores primos.

Teorema 2.44. *Se $m > 1$ e*

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$

é a decomposição de m em fatores primos, então

$$\varphi(m) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_n}\right).$$

Demonstração. Como m é produto de primos distintos elevados a potências, temos

$$\varphi(m) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}).$$

Pela Proposição 2.42, aplicável a fatores coprimos entre si, segue que

$$\varphi(m) = \varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \cdots \varphi(p_n^{\alpha_n}).$$

Pela Proposição 2.43,

$$\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i-1} = p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) \quad \text{para cada } i.$$

Substituindo essas expressões, obtemos

$$\varphi(m) = \left(p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right)\right) \left(p_2^{\alpha_2} \left(1 - \frac{1}{p_2}\right)\right) \cdots \left(p_n^{\alpha_n} \left(1 - \frac{1}{p_n}\right)\right).$$

Reagrupando os fatores, podemos reescrever a expressão exatamente na forma apresentada no enunciado:

$$\varphi(m) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_n}\right).$$

□

Observa-se ainda que a fórmula do teorema 2.44 pode ser escrita como

$$\varphi(m) = p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_n^{\alpha_n-1} (p_1 - 1)(p_2 - 1) \cdots (p_n - 1),$$

obtida ao colocar em evidência $p_i^{\alpha_i-1}$ em cada fator.

A determinação de $\varphi(m)$ permite descrever o comportamento das potências módulo m quando a base é coprima com o módulo. Esse comportamento é formalizado no *Teorema de Euler*.

Teorema 2.45. (*Teorema de Euler*) Se $m > 1$ e a é um inteiro coprimo com m , então

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Demonstração. Considere um sistema reduzido de resíduos módulo m ,

$$\{r_1, r_2, \dots, r_{\varphi(m)}\},$$

cujos elementos são todos coprimos com m .

Como a é coprimo com m , cada produto ar_i permanece coprimo com m , e os elementos

$$ar_1, ar_2, \dots, ar_{\varphi(m)}$$

são dois a dois incongruentes módulo m . Assim,

$$\{ar_1, \dots, ar_{\varphi(m)}\}$$

é outro sistema reduzido de resíduos módulo m .

Tomando o produto dos elementos de cada sistema, obtemos a congruência

$$\begin{aligned} r_1 r_2 \cdots r_{\varphi(m)} &\equiv (ar_1)(ar_2) \cdots (ar_{\varphi(m)}) \pmod{m} \\ &\equiv a^{\varphi(m)} (r_1 r_2 \cdots r_{\varphi(m)}) \pmod{m}. \end{aligned}$$

Como o produto $r_1 r_2 \cdots r_{\varphi(m)}$ é coprimo com m , podemos cancelá-lo na congruência, concluindo que

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

□

No caso particular em que $m = p$ é primo, a identidade $\varphi(p) = p - 1$ conduz ao Pequeno Teorema de Fermat, enunciado na seção 2.6.

Corolário 2.46. *Seja $a \in \mathbb{Z}$ e p um número primo. Se $(a, p) = 1$, então*

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

Demonstração. Como p é primo e $(a, p) = 1$, vale $\varphi(p) = p - 1$. Substituindo esse valor no Teorema de Euler, obtém-se

$$a^{p-1} = a^{\varphi(p)} \equiv 1 \pmod{p},$$

.

□

A forma completa do Pequeno Teorema de Fermat decorre imediatamente desse corolário. De fato, se $(a, p) = 1$, multiplicando ambos os lados de $a^{p-1} \equiv 1 \pmod{p}$ por a , obtém-se

$$a^p \equiv a \pmod{p}.$$

Para completar o resultado, consideremos o caso em que $(a, p) \neq 1$. Nessa situação, como $p \mid a$, tem-se $a \equiv 0 \pmod{p}$ e portanto $a^p \equiv 0 \pmod{p}$. Assim, a congruência

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

permanece válida também nesse caso.

Dessa forma, reunindo os dois casos obtém-se a forma completa do *Pequeno Teorema de Fermat*.

Os resultados apresentados fornecem ferramentas gerais para lidar com congruências que envolvem potências elevadas, independentemente de que o módulo seja primo ou composto, permitindo resolver de forma direta problemas que, de outro modo, exigiriam cálculos longos ou verificações caso a caso. Essas ideias consolidam a estrutura da aritmética modular e revelam o papel central das congruências na compreensão de propriedades aritméticas.

2.8 Teorema Chinês dos Restos

Com o intuito de estudarmos o *Teorema Chinês dos Restos*, é necessário compreender como resolver congruências lineares da forma

$$aX \equiv b \pmod{m},$$

em que $a, b, m \in \mathbb{Z}$ e $m > 1$. O problema consiste em determinar se existem números inteiros x que satisfaçam essa congruência e, caso existam, encontrar todas as soluções.

Para isso, começamos investigando o critério que garante a existência de solução. Isto é, desejamos saber sob quais condições a congruência

$$aX \equiv b \pmod{m}$$

admite pelo menos uma solução inteira.

Proposição 2.47. *Dados $a, b, m \in \mathbb{Z}$ com $m > 1$, a congruência*

$$aX \equiv b \pmod{m}$$

possui solução se, e somente se, $(a, m) \mid b$.

Demonstração. A congruência $aX \equiv b \pmod{m}$ possui solução se, e somente se, existe $Y \in \mathbb{Z}$ tal que

$$aX - b = mY,$$

ou, equivalentemente,

$$aX - mY = b.$$

Trata-se, portanto, de uma equação diofantina linear. Sabemos, pela Proposição 2.15, que a equação $aX - mY = b$ admite solução inteira se, e somente se, $(a, m) \mid b$. Assim, a congruência $aX \equiv b \pmod{m}$ possui solução se, e somente se, $(a, m) \mid b$.

□

A proposição anterior garante quando a congruência $aX \equiv b \pmod{m}$ admite solução. Suponhamos, portanto, que essa condição esteja satisfeita. Nosso objetivo agora é

mostrar que toda congruência dessa forma é equivalente a uma congruência mais simples, $X \equiv c \pmod{n}$, que é precisamente a forma utilizada na aplicação do *Teorema Chinês dos Restos*.

Seja $d = (a, m)$. Por definição, $d \mid a$ e $d \mid m$. Supondo que a congruência $aX \equiv b \pmod{m}$ admite solução, temos necessariamente $d \mid b$. Assim, podemos escrever

$$a = da', \quad b = db', \quad m = dn,$$

com $a', b', n \in \mathbb{Z}$. Substituindo essas expressões na congruência original e dividindo por d , obtemos a congruência equivalente

$$a'X \equiv b' \pmod{n}.$$

Como, por construção, $(a', n) = 1$, pelo Lema de Bézout 2.8, existe $u \in \mathbb{Z}$ tal que $a'u \equiv 1 \pmod{n}$. Esse u é o inverso multiplicativo de a' módulo n . Multiplicando a congruência $a'X \equiv b' \pmod{n}$ por u , obtemos $X \equiv ub' \pmod{n}$.

Em particular, tomando $c = ub'$, concluímos que toda congruência $aX \equiv b \pmod{m}$ que admite solução é equivalente a uma congruência da forma

$$X \equiv c \pmod{n}.$$

Esta forma reduzida será a base para o estudo de sistemas de congruências simultâneas e permitirá a aplicação direta do *Teorema Chinês dos Restos* que fornece as condições sob as quais há existência e unicidade de solução.

Dado um sistema de congruências lineares da forma $a_i x \equiv b_i \pmod{n_i}, i = 1, \dots, r$. Sabemos que sistema possui solução se, e somente se, $(a_i, n_i) \mid b_i$ para todo i . Quando isso ocorre, cada congruência equivale a $x \equiv c_i \pmod{m_i}, i = 1, \dots, r$.

Portanto, basta trabalhar com sistemas nessa forma reduzida. É nesse contexto que se aplica o Teorema Chinês dos Restos, apresentado a seguir de acordo com o texto de referência.

Teorema 2.48. (*Teorema Chinês dos Restos*) Se $(m_i, m_j) = 1$ para todo par m_i, m_j com $i \neq j$, então o sistema

$$\begin{cases} x \equiv c_1 \pmod{m_1}, \\ x \equiv c_2 \pmod{m_2}, \\ \vdots \\ x \equiv c_r \pmod{m_r} \end{cases}$$

possui uma única solução módulo $M = m_1 m_2 \cdots m_r$, ou seja, todas as soluções inteiras são congruentes entre si módulo M .

As soluções são dadas por, $x = M_1 y_1 c_1 + \cdots + M_r y_r c_r + tM$, em que, $t \in \mathbb{Z}$, $M_i = \frac{M}{m_i}$, e y_i é solução de $M_i Y \equiv 1 \pmod{m_i}, i = 1, \dots, r$.

Demonstração. Vamos inicialmente verificar que

$$x = M_1 Y_1 c_1 + \cdots + M_r Y_r c_r$$

é uma solução simultânea do sistema $x \equiv c_i \pmod{m_i}, i = 1, \dots, r$.

Fixemos $i \in \{1, \dots, r\}$ e consideremos a expressão anterior módulo m_i . Para $j \neq i$, observamos que $m_i \mid M_j$. De fato, $M_j = \frac{M}{m_j} = \frac{m_1 m_2 \cdots m_r}{m_j}$, de modo que M_j contém todos os fatores m_k com $k \neq j$, e em particular contém o fator m_i . Assim, $M_j \equiv 0 \pmod{m_i}$ para todo $j \neq i$. Como $M_i y_i \equiv 1 \pmod{m_i}$, temos

$$x = M_1 y_1 c_1 + \cdots + M_r y_r c_r \equiv M_i y_i c_i \equiv c_i \pmod{m_i},$$

o que mostra que x satisfaz a congruência correspondente.

Para estabelecer a unicidade, suponhamos que x' seja outra solução do sistema. Então $x \equiv x' \pmod{m_i}$ para todo $i = 1, \dots, r$. O que equivale a $m_i \mid (x - x')$ para todo i .

Como os módulos $m_1, \dots, m_r$ são coprimos dois a dois, segue-se que o mmc desses módulos é $[m_1, \dots, m_r] = m_1 m_2 \cdots m_r = M$. Assim, pela Proposição 2.39(ii), concluímos que $M \mid (x - x')$, isto é,

$$x \equiv x' \pmod{M}.$$

□

Com o *Teorema Chinês dos Restos* completamos o panorama dos principais tópicos de aritmética necessários para este estudo. Os resultados aqui apresentados constituem a base teórica que permitirá compreender, analisar e resolver os problemas olímpicos discutidos no capítulo seguinte.

Além disso, tais conceitos serão fundamentais na construção da sequência didática proposta, uma vez que diversas estratégias de resolução utilizadas em competições matemáticas se apoiam diretamente nos métodos e propriedades estudados ao longo deste capítulo.

3 Resolução de problemas

A resolução de problemas é uma estratégia que pode ser utilizada para consolidar a aprendizagem de conceitos matemáticos. Ao enfrentar desafios que exigem raciocínio lógico, interpretação e aplicação de conteúdos estudados, o estudante pode desenvolver a capacidade de generalizar, interpretar e aprender significativamente. No contexto de olimpíadas de matemática, essa prática permite fixar conteúdos de forma efetiva e promove uma compreensão mais profunda dos temas estudados.

Autores como Polya (15) defendem o ensino da matemática por meio da resolução de problemas. Para o autor, o processo de resolução não se limita à obtenção de um resultado final, mas inclui etapas fundamentais que ajudam o estudante a compreender o problema, planejar uma estratégia, executá-la com clareza e, por fim, revisar e validar a solução encontrada. Essa perspectiva reforça que a compreensão do enunciado é o primeiro passo indispensável em que o estudante deve identificar os dados, as condições e as incógnitas do problema com o intuito de perceber o que se pede e reconhecer quais conteúdos e técnicas podem ser utilizados para resolução da situação proposta.

Nesse sentido, Polya (15) apresenta quatro etapas que podem orientar o estudante no momento da resolução de um problema:

- (i) Compreensão do problema: identificar o que é dado, o que é pedido e quais relações podem ser estabelecidas; quando necessário, realizar anotações, representações ou desenhos que facilitem a visualização da situação.
- (ii) Estabelecimento de um plano: buscar conexões entre os dados; relacionar o problema com outros já resolvidos; considerar problemas auxiliares; avaliar possíveis caminhos ou métodos que permitam avançar.
- (iii) Execução do plano: seguir cuidadosamente o roteiro traçado, justificando cada passo e verificando a coerência das operações realizadas.
- (iv) Retrospecto: revisar o resultado, analisar se ele atende às condições do problema e refletir sobre o processo realizado, podendo identificar formas alternativas de resolução ou generalizações.

Desta forma, é essencial que o estudante desenvolva a capacidade de analisar criticamente a solução obtida, verificando se ela é coerente com as condições apresentadas no problema e se faz sentido no contexto proposto, pois a resolução de problemas não se encerra no cálculo, ela envolve reflexão, validação e argumentação.

É importante que essas etapas ocorram de forma natural quando o estudante estiver diante de um problema. Por isso, cabe ao professor reforçar continuamente tais passos, ajudando-o a perceber qual postura adotar, quais informações são relevantes e como organizar o raciocínio. Essa mediação, como afirma Polya (15), deve ocorrer de forma equilibrada, o professor deve orientar com sugestões e questionamentos que estimulam a autonomia, sem antecipar a solução e sem impedir que o aluno experimente, teste ideias e aprenda com suas próprias tentativas.

Outro aspecto importante é que, ao propor novas situações-problema, o professor incentive que os alunos estabeleçam relações com problemas já estudados. Conforme sugere Polya (15), uma das perguntas fundamentais que o estudante pode fazer é: “conheço um problema semelhante?”. Essa associação é parte do desenvolvimento da maturidade matemática, pois permite reconhecer padrões, identificar estruturas conhecidas e reaproveitar estratégias previamente utilizadas. Dessa forma, resolver problemas anteriores não apenas amplia o repertório de métodos, como também fortalece a autonomia e a confiança ao enfrentar novos desafios.

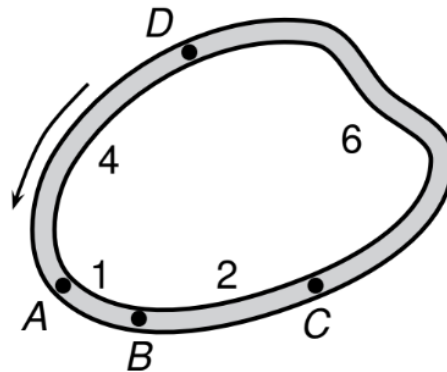
Essa dinâmica está diretamente relacionada ao trabalho realizado nas olimpíadas de matemática. Em cada edição, os estudantes são confrontados com situações e problemas que exigem deles a capacidade de compreender o enunciado, identificar os conteúdos envolvidos, estabelecer estratégias adequadas e elaborar raciocínios consistentes. Nesse processo, é comum que recorram a técnicas já experimentadas ou que construam novas abordagens a partir de sua experiência e da compreensão que têm dos conceitos já estudados, buscando construir uma solução coerente com o enunciado.

Por isso, em aulas ou encontros preparatórios para as olimpíadas de matemática, o trabalho com questões de edições anteriores mostra-se particularmente efetivo. Esse tipo de prática oferece ao estudante maior familiaridade com o estilo das provas, desenvolvendo maturidade para lidar com o formato das questões e com o nível de raciocínio exigido. Além disso, possibilita que o aluno acumule experiência com situações semelhantes às que encontrará nas avaliações, ampliando seu repertório estratégico e fortalecendo sua habilidade de reconhecer conteúdos, padrões e abordagens típicas das competições.

Em síntese, a resolução de problemas contribui de maneira significativa para o desenvolvimento do raciocínio matemático, da autonomia intelectual e da capacidade de análise crítica. No contexto das Olimpíadas, esse processo se intensifica, pois o estudante é convidado a explorar ideias, estabelecer conexões, revisar conceitos e construir soluções de forma criativa e consciente. Assim, trabalhar com problemas olímpicos não apenas prepara o aluno para a competição, mas também enriquece sua formação matemática e amplia sua competência na resolução de problemas em diferentes contextos, despertando o espírito da investigação científica.

3.1 Problemas

1. **OBMEP - 2ª fase:** A figura representa o traçado de uma pista de corrida. Os postos A, B, C e D são usados para partidas e chegadas de todas as corridas. As distâncias entre postos vizinhos, em quilômetros, estão indicadas na figura e as corridas são realizadas no sentido indicado pela flecha.



Por exemplo, uma corrida de 17 km pode ser realizada com partida em D e chegada em A.

- Quais são os postos de partida e chegada de uma corrida de 14 quilômetros?
- E para uma corrida de 100 quilômetros, quais são esses postos?
- Mostre que é possível realizar corridas com extensão igual a qualquer número inteiro de quilômetros.

Solução:

Item A:

No sentido indicado na figura, as distâncias são

$$A \rightarrow B = 1, \quad B \rightarrow C = 2, \quad C \rightarrow D = 6, \quad D \rightarrow A = 4,$$

de modo que uma volta completa na pista corresponde a

$$1 + 2 + 6 + 4 = 13 \text{ km.}$$

Como desejamos uma corrida de 14 km, temos

$$14 = 13 + 1.$$

Assim, o competidor deve dar uma volta completa (13 km) e percorrer mais 1 km. Portanto, a corrida de 14 km deve começar em A e terminar em B.

Item B:

Sabemos que uma volta completa na pista tem 13 km. Para uma corrida de 100 km, aplicamos a divisão euclidiana:

$$100 = 13 \cdot 7 + 9.$$

Assim, o competidor deve dar 7 voltas completas ($13 \times 7 = 91$ km) e percorrer mais 9 km.

Como a distância de A até D é de 9 km ($A \rightarrow D = 1 + 2 + 6 = 9$), a corrida de 100 km deve começar em A , dar 7 voltas completas e terminar em D .

Item C:

Queremos mostrar que é possível realizar corridas com extensão igual a qualquer número inteiro de quilômetros.

Sabemos que uma volta na pista tem 13 km. Assim, para qualquer número inteiro N , pela divisão euclidiana, existem inteiros q e r tais que

$$N = 13q + r, \quad 0 \leq r \leq 12,$$

em que q representa o número de voltas completas e r indica quantos quilômetros devem ser percorridos após essas voltas.

Como os possíveis restos estão entre 0 e 12, basta observar que cada um desses valores de r pode ser representado na pista. A tabela a seguir mostra, para cada resto r , um possível par de pontos de partida e chegada cuja distância é exatamente r km.

Resto r	0	1	2	3	4	5	6	7	8	9	10	11	12
Partida	qualquer ponto	A	B	A	D	D	C	D	B	A	C	C	B
Chegada	mesmo ponto	B	C	C	A	B	D	C	D	D	A	B	A

Assim, é possível realizar uma corrida com extensão igual a qualquer número inteiro de quilômetros.

2. **OBMEP - 1ª fase:** Quantos são os números naturais n tais que $\frac{5n-12}{n-8}$ é também um número natural?

- A) 4
- B) 5
- C) 6
- D) 7
- E) 8

Solução:

Inicialmente, observamos que $n \neq 8$, pois o denominador não pode ser nulo.

Queremos que a fração seja um número natural, isto é, que a divisão entre $5n - 12$ e $n - 8$ resulte em um número inteiro não negativo.

Para isso, reescrevemos o numerador de modo a evidenciar o fator $(n - 8)$:

$$5n - 12 = 5(n - 8) + 28.$$

Assim, temos:

$$\frac{5n - 12}{n - 8} = \frac{5(n - 8)}{n - 8} + \frac{28}{n - 8} = 5 + \frac{28}{n - 8}.$$

Para que essa expressão seja um número natural, é necessário que $\frac{28}{n - 8}$ seja um número inteiro e que a soma $5 + \frac{28}{n - 8}$ resulte em um número natural.

Logo, $n - 8$ deve ser um divisor inteiro de 28.

Os divisores inteiros de 28 são:

$$\pm 1, \pm 2, \pm 4, \pm 7, \pm 14, \pm 28.$$

Para cada divisor $d = n - 8$, temos $n = d + 8$. Verifiquemos os casos:

d	$n = d + 8$	$5 + \frac{28}{d}$
1	9	33
2	10	19
4	12	12
7	15	9
14	22	7
28	36	6
-1	7	-23
-2	6	-9
-4	4	-2
-7	1	1
-14	-6	3
-28	-20	4

Dentre esses, apenas os valores de n naturais e com quociente natural são:

$$n = 1, 9, 10, 12, 15, 22, 36.$$

Portanto, existem 7 números naturais n que satisfazem a condição dada.

Alternativa correta: D) 7.

3. **OBMEP - 1ª fase:** Um número de três algarismos possui as seguintes propriedades:

- Quando trocamos os algarismos das unidades e das dezenas, ele aumenta em 18 unidades;
- Quando trocamos os algarismos das dezenas e das centenas, ele aumenta em 180 unidades.

Quantas unidades aumentará o número se trocarmos o algarismo das unidades e das centenas?

- A) 36
- B) 396
- C) 468
- D) 486
- E) 3960

Solução: Seja o número de três algarismos $ABC = 100A + 10B + C$.

(1) *Troca das unidades com as dezenas:* o número aumenta em 18 unidades.

$$\begin{aligned}
 ACB &= ABC + 18. \\
 100A + 10C + B &= 100A + 10B + C + 18 \\
 10C + B - 10B - C &= 18 \\
 9(C - B) &= 18 \\
 C - B &= 2
 \end{aligned} \tag{3.1}$$

(2) *Troca das dezenas com as centenas:* o número aumenta em 180 unidades.

$$\begin{aligned}
 BAC &= ABC + 180. \\
 100B + 10A + C &= 100A + 10B + C + 180 \\
 100B + 10A - 100A - 10B &= 180 \\
 90(B - A) &= 180 \\
 B - A &= 2
 \end{aligned} \tag{3.2}$$

(3) *Relação entre os algarismos A, B e C:* Da equação (3.2), tem-se $B = A + 2$. Substituindo em (3.1):

$$\begin{aligned}
 C - (A + 2) &= 2 \\
 C - A &= 4
 \end{aligned} \tag{3.3}$$

(4) *Troca das unidades com as centenas:* Seja X o aumento obtido nessa troca. Então:

$$\begin{aligned} CAB &= ABC + X \\ 100C + 10B + A &= 100A + 10B + C + X \\ 99(C - A) &= X \end{aligned}$$

Substituindo o valor de $C - A$ obtido em (3.3):

$$X = 99 \cdot 4 = 396$$

A troca dos algarismos das unidades e das centenas aumenta o número em 396 unidades.

Alternativa correta: B) 396.

4. **OPEMAT - 2ª Fase:** Comumente, utilizamos o sistema de numeração decimal ou na base 10 que nos permite representar qualquer número utilizando os dígitos 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9. Por exemplo, quando escrevemos o número $1374 = (1374)_{10}$, significa que

$$1374 = 1 \cdot 10^3 + 3 \cdot 10^2 + 7 \cdot 10^1 + 4 \cdot 10^0 = (1374)_{10}.$$

No entanto, podemos representar números em outras bases. Por exemplo, a base 2, ou sistema binário é bastante utilizada na linguagem computacional. Nesta utilizamos apenas os algarismos 0 e 1 para representar qualquer número. Por exemplo, o número $11 = (11)_{10}$ pode ser representado na base 2 por $(1011)_2$, pois:

$$11 = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = (1011)_2.$$

Outro exemplo seria considerarmos a base 5. Nesta, o número $163 = (163)_{10}$ é representado na base 5 por $(1123)_5$, pois:

$$163 = 1 \cdot 5^3 + 1 \cdot 5^2 + 2 \cdot 5^1 + 3 \cdot 5^0 = (1123)_5.$$

Analise as afirmações a seguir e marque (V) se a afirmação for verdadeira e (F) se a afirmação for falsa.

- A) (V) (F) $(100)_2 + (100)_5 = (200)_{10}$
- B) (V) (F) $(1)_2 + (3)_5 + (5)_{10} = (9)_{10}$
- C) (V) (F) $26 = (26)_{10}$ é representado na base 3 por $(222)_3$
- D) (V) (F) O número $2 = (2)_{10}$ possui a mesma representação nas bases 2 e 5.

E) (V) (F) Não existe um número que seja representado pelo mesmo algarismo nas bases 2, 5 e 10.

Solução:

Item A: Verificar se $(100)_2 + (100)_5 = (200)_{10}$.

Conversão para a base decimal:

$$(100)_2 = 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 = 4,$$

$$(100)_5 = 1 \cdot 5^2 + 0 \cdot 5^1 + 0 \cdot 5^0 = 25.$$

Somando em decimal:

$$4 + 25 = 29 \neq 200.$$

Portanto, a afirmação é falsa.

Item B: Verificar se $(1)_2 + (3)_5 + (5)_{10} = (9)_{10}$.

Conversão para a base decimal:

$$(1)_2 = 1 \cdot 2^0 = 1,$$

$$(3)_5 = 3 \cdot 5^0 = 3,$$

$$(5)_{10} = 5.$$

Somando:

$$1 + 3 + 5 = 9.$$

Logo, a afirmação é verdadeira.

Item C: Verificar se $26 = (26)_{10}$ é representado na base 3 por $(222)_3$.

Divisões sucessivas para converter 26 para a base 3:

$$26 = 3 \cdot 8 + \boxed{2},$$

$$8 = 3 \cdot 2 + \boxed{2},$$

$$2 = 3 \cdot 0 + \boxed{2}.$$

Como a leitura dos restos é feita de baixo para cima, obtemos $(222)_3$. Assim, a representação está correta e a afirmação é verdadeira.

Item D: Verificar se o número $2 = (2)_{10}$ possui a mesma representação nas bases 2 e 5.

Conversão para a base 2:

$$2 = 2 \cdot 1 + \boxed{0},$$

$$1 = 2 \cdot 0 + \boxed{1}.$$

Lendo os restos de baixo para cima, obtemos $(10)_2 = 2$.

Conversão para a base 5:

$$2 = 5 \cdot 0 + \boxed{2}.$$

Logo, $(2)_5 = 2$.

As representações são diferentes, portanto a afirmação é falsa.

Item E: A afirmação diz que não existe número representado pelo mesmo algarismo nas bases 2, 5 e 10. Entretanto, o número 1 possui exatamente a mesma representação em todas essas bases:

$$1 = (1)_2 = (1)_5 = (1)_{10}.$$

Portanto, a afirmação é falsa.

5. **OBMEP - 1ª fase:** 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 escreveu o número 100 e Daniela escreveu o número 88, qual é o número que vai ficar escrito no quadro-negro ao final da brincadeira?

- A) 2
- B) 4
- C) 6
- D) 8
- E) 10

Solução:

Inicialmente, listamos todas as trocas feitas segundo a regra, sempre substituindo o maior número pela diferença entre o maior e o menor, em que os pares ilustram cada passo:

	Interação										
Ana	100	12	12	12	12	12	12	12	12	8	4
Daniela	88	88	76	64	52	40	28	16	4	4	4

Ao final observamos que ambas escrevem o número 4.

Note que a sequência de operações proposta na brincadeira preserva o máximo divisor comum dos dois números. Mais precisamente, se $a, b, n \in \mathbb{Z}$, então, pelo *Lema de Euclides*, $(a, b) = (b, a - nb)$.

Aplicando o lema ao par inicial $(a, b) = (100, 88)$, temos:

$$(100, 88) = (100 - 1 \cdot 88, 88) = (12, 88),$$

$$(12, 88) = (12, 88 - 7 \cdot 12) = (12, 4),$$

$$(12, 4) = (12 - 3 \cdot 4, 4) = (0, 4).$$

Logo, $(100, 88) = 4$, que representa o número que ficará no quadro.

Alternativa correta: B) 4.

6. **ENQ-PROFMAT:** O máximo divisor comum de dois inteiros positivos é 20. Para se chegar a esse resultado pelo processo das divisões sucessivas, os quocientes encontrados foram, pela ordem, 1, 5, 3, 3, 1 e 3. Encontre os dois números

Solução.

Pelo processo das divisões sucessivas do algoritmo de Euclides, sejam a e b os inteiros positivos procurados. Os quocientes fornecidos são, na ordem:

$$q_1 = 1, \quad q_2 = 5, \quad q_3 = 3, \quad q_4 = 3, \quad q_5 = 1, \quad q_6 = 3.$$

Assim, as divisões euclidianas correspondentes são:

$$a = 1b + r_1 \quad 0 < r_1 < b,$$

$$b = 5r_1 + r_2 \quad 0 < r_2 < r_1,$$

$$r_1 = 3r_2 + r_3 \quad 0 < r_3 < r_2,$$

$$r_2 = 3r_3 + r_4 \quad 0 < r_4 < r_3,$$

$$r_3 = 1r_4 + r_5 \quad 0 < r_5 < r_4,$$

$$r_4 = 3r_5 + r_6 \quad 0 = r_6 < r_5.$$

Como o mdc é 20, o último resto não nulo deve ser

$$r_5 = 20,$$

e como r_5 divide r_4 , o processo encerra com

$$r_6 = 0.$$

Procede-se então à substituição recursiva a partir do último resto não nulo:

$$r_4 = 3 \cdot 20 + 0 = 60,$$

$$r_3 = 60 + 20 = 80,$$

$$r_2 = 3 \cdot 80 + 60 = 300,$$

$$r_1 = 3 \cdot 300 + 80 = 980,$$

$$b = 5 \cdot 980 + 300 = 5200,$$

$$a = b + 980 = 6180.$$

Portanto, os inteiros positivos que possuem mdc igual a 20 e produzem os quocientes indicados são

$$a = 6180 \quad \text{e} \quad b = 5200.$$

7. **OPEMAT - 1º FASE** Um professor dispõe de R\$300,00 para comprar 30 presentes para seus alunos. Ele vai em uma loja que tem três opções de presentes: chaveiros, copos e camisas. Um chaveiro custa R\$1,00, um copo custa R\$5,00 e uma camisa custa R\$20,00. Sabendo que o professor comprou x chaveiros, y copos e z camisas, que o produto $xyz > 0$ e que não sobrou dinheiro, qual o número de fatores primos do produto xyz ?

- A) 2
- B) 4
- C) 5
- D) 8
- E) 10

Solução:

Do enunciado, obtemos o seguinte sistema:

$$\begin{cases} x + y + z = 30, \\ x + 5y + 20z = 300. \end{cases}$$

Subtraindo a primeira equação da segunda, obtemos a seguinte equação diofantina:

$$4y + 19z = 270. \tag{3.4}$$

Para resolvermos a equação diofantina, aplicamos o algoritmo de Euclides para determinar $(4, 19)$:

	4	1	3
19	4	3	1
3	1	0	

Como $(4, 19) = 1$, a equação possui soluções inteiras. Escrevendo o mdc como combinação linear:

$$1 = 4 - 1 \cdot 3$$

$$1 = 4 - 1 \cdot (19 - 4 \cdot 4)$$

$$1 = 4 - 1 \cdot 19 + 4 \cdot 4$$

$$1 = 4 \cdot (5) + 19 \cdot (-1)$$

$$270 = 4 \cdot (5 \cdot 270) + 9 \cdot (-1 \cdot 270)$$

$$270 = 4 \cdot (1350) + 9 \cdot (-270)$$

Logo, uma solução particular é $y_0 = 1350$ e $z_0 = -270$.

Assim, a solução geral é

$$y = 1350 - 19t, \quad z = -270 + 4t, \quad t \in \mathbb{Z}.$$

Como o problema exige que $xyz > 0$, então $x = 30 - (y + z) > 0$, $y > 0$ e $z > 0$, a partir dessas desigualdades, obtemos restrições para t :

$$y > 0 \implies 1350 - 19t > 0 \implies t \leq 71,$$

$$z > 0 \implies -270 + 4t > 0 \implies t \geq 68.$$

Escrevendo $y + z$ em função de t :

$$y + z = (1350 - 19t) + (-270 + 4t) = 1080 - 15t.$$

A condição $x > 0$ equivale a $y + z < 30$, portanto

$$1080 - 15t < 30 \implies t > 70.$$

Assim, combinando as restrições inteiras ($68 \leq t \leq 71$ e $t > 70$), obtemos $t = 71$.

Substituindo $t = 71$, temos:

$$y = 1350 - 19 \cdot 71 = 1, \quad z = -270 + 4 \cdot 71 = 14,$$

e então

$$x = 30 - (y + z) = 30 - (1 + 14) = 15.$$

Logo, a solução é $(x, y, z) = (15, 1, 14)$, e

$$xyz = 15 \cdot 1 \cdot 14 = 210 = 2 \cdot 3 \cdot 5 \cdot 7,$$

que possui quatro fatores primos distintos.

Alternativa correta: B) 4.

8. **OPEMAT - 2ª FASE:** Em um determinado país, as cédulas de dinheiro são de \$5 e de \$9 apenas.

- A) É possível comprar algo, que custa \$31, sem receber troco ou pagar a mais por isso? Justifique.
- B) A partir de que valor, sempre é possível pagar com notas de \$5 e \$9, sem que seja necessário receber troco?

Solução:

A) *É possível pagar \$31 sem troco?*

Para que seja possível pagar exatamente \$31, devemos verificar se esse valor pode ser escrito como uma combinação de notas de \$5 e \$9, isto é, se existem inteiros $x, y > 0$ tais que:

$$5x + 9y = 31.$$

Para resolvermos a equação diofantina, aplicamos o *Algoritmo de Euclides* para determinar $(5, 9)$:

	1	1	4
9	5	4	1
4	1	0	

Como $(5, 9) = 1$, a equação possui soluções inteiras. Vamos escrever o máximo divisor comum como combinação linear:

$$1 = 5 - 1 \cdot 4$$

$$1 = 5 - 1 \cdot (9 - 1 \cdot 5)$$

$$1 = 5 - 1 \cdot 9 + 1 \cdot 5$$

$$1 = 5 \cdot (2) + 9 \cdot (-1)$$

$$31 = 5 \cdot (2 \cdot 31) + 9 \cdot (-1 \cdot 31)$$

$$31 = 5 \cdot (62) + 9 \cdot (-31)$$

Logo, uma solução particular é $x_0 = 62$, $y_0 = -31$.

A solução geral inteira é:

$$x = 62 - 9t, \quad y = -31 + 5t, \quad \text{com } t \in \mathbb{Z}.$$

Para que a solução faça sentido no contexto do problema, precisamos que x e y sejam números inteiros não negativos, correspondendo à quantidade de notas. Assim:

$$62 - 9t \geq 0 \Rightarrow t \leq 6, \quad \text{e} \quad -31 + 5t \geq 0 \Rightarrow t \geq 7.$$

Como não existe valor inteiro de t que satisfaça ambas as desigualdades, não há solução natural. Logo, não é possível pagar exatamente \$31.

B) A partir de que valor sempre é possível pagar sem troco?

Para determinar a partir de qual valor é sempre possível pagar com notas de \$5 e \$9, utilizaremos o conceito de *conjunto de lacunas*. Esse conjunto reúne os números naturais que **não podem** ser escritos como combinação linear positiva dos números 5 e 9.

Definimos:

$$L(5, 9) = \{ m \cdot 5 - n \cdot 9 \in \mathbb{N} : m, n \in \mathbb{N}, m < 9 \}.$$

A seguir, construímos o conjunto $L(5, 9)$ calculando $m \cdot 5 - n \cdot 9$ para $m = 1, \dots, 8$, considerando valores de n que tornem o resultado positivo. Temos:

$m = 1 :$

$$1 \cdot 5 - 1 \cdot 9 = -4 \notin \mathbb{N}$$

$m = 2 :$

$$2 \cdot 5 - 1 \cdot 9 = 1 \in \mathbb{N}$$

$$2 \cdot 5 - 2 \cdot 9 = -8 \notin \mathbb{N}$$

$m = 3 :$

$$3 \cdot 5 - 1 \cdot 9 = 6 \in \mathbb{N}$$

$$3 \cdot 5 - 2 \cdot 9 = -3 \notin \mathbb{N}$$

$m = 4 :$

$$4 \cdot 5 - 1 \cdot 9 = 11 \in \mathbb{N}$$

$$4 \cdot 5 - 2 \cdot 9 = 2 \in \mathbb{N}$$

$$4 \cdot 5 - 3 \cdot 9 = -7 \notin \mathbb{N}$$

$m = 5 :$

$$5 \cdot 5 - 1 \cdot 9 = 16 \in \mathbb{N}$$

$$5 \cdot 5 - 2 \cdot 9 = 7 \in \mathbb{N}$$

$$5 \cdot 5 - 3 \cdot 9 = -2 \notin \mathbb{N}$$

$m = 6 :$

$$6 \cdot 5 - 1 \cdot 9 = 21 \in \mathbb{N}$$

$$6 \cdot 5 - 2 \cdot 9 = 12 \in \mathbb{N}$$

$$6 \cdot 5 - 3 \cdot 9 = 3 \in \mathbb{N}$$

$$6 \cdot 5 - 4 \cdot 9 = -6 \notin \mathbb{N}$$

$m = 7 :$

$$7 \cdot 5 - 1 \cdot 9 = 26 \in \mathbb{N}$$

$$7 \cdot 5 - 2 \cdot 9 = 17 \in \mathbb{N}$$

$$7 \cdot 5 - 3 \cdot 9 = 8 \in \mathbb{N}$$

$$7 \cdot 5 - 4 \cdot 9 = -1 \notin \mathbb{N}$$

$m = 8 :$

$$8 \cdot 5 - 1 \cdot 9 = 31 \in \mathbb{N}$$

$$8 \cdot 5 - 2 \cdot 9 = 22 \in \mathbb{N}$$

$$8 \cdot 5 - 3 \cdot 9 = 13 \in \mathbb{N}$$

$$8 \cdot 5 - 4 \cdot 9 = 4 \in \mathbb{N}$$

$$8 \cdot 5 - 5 \cdot 9 = -5 \notin \mathbb{N}$$

Reunindo todos os números naturais obtidos, encontramos:

$$L(5, 9) = \{1, 2, 3, 4, 6, 7, 8, 11, 12, 13, 16, 17, 21, 22, 26, 31\}.$$

Se o valor a ser pago pertence ao conjunto $L(5, 9)$, a equação $5x + 9y = n$ não admite solução em números naturais. Observa-se que o maior elemento desse conjunto é 31, o que significa que esse é o último valor que não pode ser obtido com notas de \$5 e \$9.

A partir de \$32, todos os valores podem ser formados, pois basta adicionar múltiplos de \$5 e \$9 a combinações já possíveis. Portanto, 31 é a última lacuna do conjunto $L(5, 9)$ e qualquer valor $n \geq 32$ pode ser pago exatamente, sem necessidade de troco.

9. **OPEMAT - 2ª FASE:** Na terra de π -raia, a moeda utilizada é o “ π -real” ($\pi\mathbb{R}$). Lá, as notas de “ π -reais” utilizadas são compostas por valores representados por números primos menores do que 100.



Julgue as afirmações a seguir atribuindo (V) se a afirmação for verdadeira e (F) se a afirmação for falsa.

- A- (V) (F) A nota de 91 π -reais não existe na terra do π -raia.
- B- (V) (F) Nesse mundo, existem notas de 97 π -reais.
- C- (V) (F) Há exatamente 19 notas diferentes.
- D- (V) (F) É possível passar um troco de 100 π -reais utilizando apenas notas de 11 e 13.
- E- (V) (F) Conseguimos passar o troco de 11 π -reais de seis maneiras diferentes.

Solução:

O Crivo de Eratóstenes é um método clássico e eficiente para listar os números primos até um dado limite. No contexto desta questão, aplicamos o crivo aos números $2, 3, \dots, 100$ e, iterativamente, para cada número primo ainda não riscado, riscamos todos os seus múltiplos, o que torna explícito quais valores correspondem às notas (números primos menores que 100).

	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

Item A. A nota de 91 π -reais não existe na terra do π -raia, pois $91 = 7 \times 13$, portanto, a afirmação é falsa.

Item B. O número 97 é primo, pois não possui divisores inteiros além de 1 e 97. Portanto, existe a nota de 97 π -reais, assim, a afirmação é verdadeira.

Item C. Contando os primos menores do que 100 obtemos 25 primos:

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.

Logo a afirmação é falsa.

Item D:

Queremos verificar se é possível passar um troco de 100 π -reais utilizando apenas cédulas de 11 e 13 π -reais.

Isso equivale a determinar se a equação diofantina linear

$$11x + 13y = 100$$

admite solução em inteiros não negativos.

Para resolver a equação diofantina, aplicamos o *Algoritmo de Euclides* para determinar $(11, 13)$:

	1	5	2
13	11	2	1
2	1	0	

Como $(11, 13) = 1$ e $1 \mid 100$, o teorema 2.15 garante que a equação admite solução inteira.

Vamos escrever o mdc como combinação linear:

$$1 = 11 - 5 \cdot 2$$

$$1 = 11 - 5 \cdot (13 - 11)$$

$$1 = 11 - 5 \cdot 13 + 5 \cdot 11$$

$$1 = 11 \cdot (6) + 13 \cdot (-5)$$

$$100 = 11 \cdot (6 \cdot 100) + 13 \cdot (-5 \cdot 100)$$

$$100 = 11 \cdot (600) + 13 \cdot (-500)$$

Logo, uma solução particular é $x_0 = 600$, $y_0 = -500$.

A solução geral é dada por

$$x = 600 - 13t$$

$$y = -500 + 11t,$$

com $t \in \mathbb{Z}$.

Como x e y representam quantidades de cédulas, devemos ter

$$x, y \in \mathbb{Z}_{\geq 0},$$

isto é, soluções inteiras não negativas.

Assim, impomos as condições

$$x \geq 0 \quad \text{e} \quad y \geq 0.$$

Logo,

$$600 - 13t \geq 0 \Rightarrow t \leq \frac{600}{13},$$

$$-500 + 11t \geq 0 \Rightarrow t \geq \frac{500}{11}.$$

Como

$$\frac{500}{11} \approx 45,45 \quad \text{e} \quad \frac{600}{13} \approx 46,15,$$

segue que

$$45,45 \leq t \leq 46,15.$$

Como $t \in \mathbb{Z}$, concluímos que

$$t = 46.$$

Substituindo,

$$x = 600 - 13 \cdot 46 = 2,$$

$$y = -500 + 11 \cdot 46 = 6.$$

Portanto,

$$100 = 2 \cdot 11 + 6 \cdot 13,$$

isto é, são necessárias duas cédulas de 11 π -reais e seis cédulas de 13 π -reais.

Solução alternativa

Como 100 não é múltiplo de 11, é necessário utilizar ao menos uma cédula de 13. Subtraindo sucessivamente 13 de 100:

$$100 - 13 = 87$$

$$87 - 13 = 74$$

$$74 - 13 = 61$$

$$61 - 13 = 48$$

$$48 - 13 = 35$$

$$35 - 13 = 22.$$

Observamos que 22 é múltiplo de 11, pois

$$22 = 2 \cdot 11.$$

Logo,

$$100 = 6 \cdot 13 + 2 \cdot 11.$$

Existe solução inteira não negativa. Portanto, a afirmação é verdadeira.

Item E: Devemos determinar de quantas maneiras é possível formar a quantia de 11 π -reais utilizando as notas disponíveis de valores primos 2, 3, 5, 7 e 11. Como a ordem das notas não altera o valor total e é permitida a repetição de notas, procuramos todas as combinações possíveis de primos cuja soma seja igual a 11.

Listando as possibilidades:

- 11;
- $7 + 2 + 2$;
- $5 + 3 + 3$;
- $5 + 2 + 2 + 2$;
- $3 + 3 + 3 + 2$;
- $3 + 2 + 2 + 2 + 2$.

Verificamos que não há outras combinações possíveis de primos que somem 11, concluindo que existem exatamente 6 maneiras distintas de formar o valor de 11 π -reais com as notas disponíveis. Portanto, a afirmação é verdadeira.

10. **OPEMAT - 1ª FASE:** Durante uma feira de ciências, os organizadores montaram um painel interativo com cartões contendo todos os divisores positivos de 2025^2 . Cada cartão contém um único divisor e cada divisor foi escrito em apenas um cartão. Três visitantes escolhem, sem reposição, um cartão cada um. Seja

$$P = \frac{m}{n},$$

com m e n primos entre si, a probabilidade de que entre os três números escolhidos, haja exatamente um número **primo** e dois **quadrados perfeitos**. Assinale a alternativa que corresponde à soma $m + n$.

- A) 48
- B) 480
- C) 2.028
- D) 2.943
- E) 14.400

Solução. Para determinar a probabilidade, iniciamos analisando os divisores de 2025^2 . Para isso, fatoramos:

$$2025 = 5^2 \cdot 3^4.$$

Elevando essa fatoração ao quadrado, obtemos

$$2025^2 = 5^4 \cdot 3^8.$$

Assim, o número total de divisores positivos de 2025^2 é

$$(4 + 1)(8 + 1) = 45.$$

Os únicos divisores de 2025^2 que são números *primos* são

$$3 \text{ e } 5,$$

então podemos concluir que existem exatamente 2 divisores primos.

Em seguida, determinamos os divisores que são quadrados perfeitos. Um divisor é quadrado perfeito quando apresenta expoentes pares na sua decomposição em fatores primos. Para a base 5, os expoentes possíveis são

$$5^0, 5^2, 5^4 \quad (3 \text{ opções}),$$

e, para a base 3, os expoentes possíveis são

$$3^0, 3^2, 3^4, 3^6, 3^8 \quad (5 \text{ opções}).$$

Pelo princípio multiplicativo, o número total de divisores que são quadrados perfeitos é

$$3 \times 5 = 15.$$

Passamos então ao cálculo da probabilidade. Três cartões são escolhidos sem reposição. Consideremos inicialmente uma ordem fixa em que o primeiro cartão selecionado é primo e os dois seguintes são quadrados perfeitos. A probabilidade dessa configuração é

$$\frac{2}{45} \cdot \frac{15}{44} \cdot \frac{14}{43}.$$

Como a ordem em que aparecem o número primo e os dois quadrados perfeitos não é relevante, multiplicamos essa probabilidade pelo número de permutações distintas da sequência (pr, qp, qp), que é

$$\frac{3!}{2!} = 3.$$

Portanto,

$$P = 3 \cdot \frac{2}{45} \cdot \frac{15}{44} \cdot \frac{14}{43}.$$

Efetuada as simplificações, obtemos

$$P = \frac{7}{473}.$$

Assim, com $m = 7$ e $n = 473$, concluímos que

$$m + n = 7 + 473 = 480.$$

Alternativa correta: B) 480.

11. **OPEMAT - 2ª FASE:** Decida se as afirmações abaixo são verdadeiras ou falsas:

A- (V) (F) $59^{20} - 1$ não é divisível por 11.

B- (V) (F) O dígito das unidades de 2467^{101} é 1.

C- (V) (F) O número 24567894534344446 é quadrado perfeito.

D- (V) (F) Os números naturais m , n e k são tais que $21m = 28n = 12k$. Então, $m \cdot n \cdot k$ é múltiplo de 84.

E- (V) (F) 999919 é primo.

Solução:

Item A: Queremos saber se $59^{20} - 1$ é divisível por 11. Sabemos que $(59, 11) = 1$, pelo Pequeno Teorema de Fermat $a^{p-1} \equiv 1 \pmod{p}$, temos $59^{10} \equiv 1 \pmod{11}$. Logo,

$$\begin{aligned}(59^{10})^2 &= 59^{20} \equiv 1^2 = 1 \pmod{11}. \\ 59^{20} - 1 &\equiv 0 \pmod{11}.\end{aligned}$$

Desta forma $59^{20} - 1$ é divisível por 11 e a afirmação é falsa.

Item B: Para determinar o dígito das unidades de 2467^{101} , devemos calcular tal potência módulo 10.

$$2467 \equiv 7 \pmod{10}.$$

Assim,

$$2467^{101} \equiv 7^{101} \pmod{10}.$$

Pelo Teorema de Euler, $\varphi(10) = 4$, e portanto $7^4 \equiv 1 \pmod{10}$.

Escrevendo $7^{101} = 7^{100} \cdot 7 = (7^4)^{25} \cdot 7$, obtemos

$$(7^4)^{25} \cdot 7 \equiv 1^{25} \cdot 7 \equiv 7 \pmod{10}.$$

Logo, o dígito das unidades de 2467^{101} é 7 e a afirmação é falsa.

Item C: Seja

$$N = 24567894534344446.$$

Queremos verificar se N é um quadrado perfeito. Para isso, analisaremos os possíveis restos que quadrados perfeitos deixam em diferentes módulos.

Análise módulo 10. Considerando os possíveis restos $x \equiv 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 \pmod{10}$, temos:

$$\begin{array}{cccccc} 0^2 \equiv 0, & 1^2 \equiv 1, & 2^2 \equiv 4, & 3^2 \equiv 9, & 4^2 \equiv 6, \\ 5^2 \equiv 5, & 6^2 \equiv 6, & 7^2 \equiv 9, & 8^2 \equiv 4, & 9^2 \equiv 1. \end{array}$$

Logo, os quadrados perfeitos são congruentes a 0, 1, 4, 5, 6 ou 9 (mod 10). Como N termina em 6, ele pode ser um quadrado perfeito — esse teste não elimina a possibilidade.

Análise módulo 2. Os possíveis restos são $x \equiv 0, 1 \pmod{2}$, e temos:

$$0^2 \equiv 0, \quad 1^2 \equiv 1.$$

Logo, quadrados perfeitos são sempre congruentes a 0 ou 1 (mod 2). Como N é par, temos $N \equiv 0 \pmod{2}$, o que também é compatível com ser um quadrado.

Análise módulo 3. Para $x \equiv 0, 1, 2 \pmod{3}$, temos:

$$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 4 \equiv 1 \pmod{3}.$$

Portanto, quadrados perfeitos são congruentes a 0 ou 1 (mod 3). Somando os algarismos de N :

$$2 + 4 + 5 + 6 + 7 + 8 + 9 + 4 + 5 + 3 + 4 + 3 + 4 + 4 + 4 + 4 + 6 = 72.$$

Como $72 \equiv 0 \pmod{3}$, temos $N \equiv 0 \pmod{3}$, o que ainda é compatível com um quadrado perfeito.

Análise módulo 4. Os possíveis restos são $x \equiv 0, 1, 2, 3 \pmod{4}$, e temos:

$$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 0, \quad 3^2 \equiv 1 \pmod{4}.$$

Assim, quadrados perfeitos são sempre congruentes a 0 ou 1 (mod 4). Para determinar $N \pmod{4}$, observamos seus dois últimos algarismos:

$$46 \equiv 2 \pmod{4}.$$

Como 2 não pertence a $\{0, 1\}$, concluímos que N não pode ser um quadrado perfeito.

Embora N passe nos testes módulo 10, 2 e 3, ele falha no módulo 4. Portanto, 24567894534344446 não é um quadrado perfeito e a afirmação é falsa.

Item D: Queremos verificar se $m \cdot n \cdot k$ é múltiplo de 84. Começamos observando que da igualdade $21m = 28n$ podemos simplificar ambos os lados por 7, obtendo

$$3m = 4n. \tag{3.5}$$

Sabemos que $(3, 4) = 1$. Portanto, dividindo toda a expressão (3.5) por 3, temos

$$m = \frac{4n}{3}.$$

Como 3 não divide 4, o fator 3 deve dividir n . Assim, podemos escrever

$$n = 3a, \quad (3.6)$$

para algum número natural a .

Substituindo (3.6) em (3.5), obtemos

$$3m = 4(3a) \Rightarrow 3m = 12a.$$

Dividindo ambos os lados por 3, resulta

$$m = 4a. \quad (3.7)$$

Agora consideremos a outra igualdade dada: $21m = 12k$. Simplificando por 3, obtemos

$$7m = 4k. \quad (3.8)$$

Sabendo que $(7, 4) = 1$, dividimos toda a expressão (3.8) por 7:

$$m = \frac{4k}{7}.$$

Como 7 não divide 4, o 7 deve dividir k . Assim, podemos escrever

$$k = 7c, \quad (3.9)$$

para algum número natural c .

Substituindo (3.9) em (3.8), temos

$$7m = 4(7c) \Rightarrow m = 4c.$$

Mas, de (3.7), já havíamos encontrado que $m = 4a$. Igualando as duas expressões de m , obtemos $4a = 4c$, portanto $a = c$.

Substituindo agora os valores encontrados em (3.6), (3.7) e (3.9), temos:

$$n = 3a, \quad m = 4a, \quad k = 7a.$$

Calculando o produto:

$$m \cdot n \cdot k = (4a) \cdot (3a) \cdot (7a) = 84a^3.$$

Logo, $m \cdot n \cdot k$ é múltiplo de 84 e a afirmação é verdadeira.

Item E: Podemos observar que o número dado pode ser escrito como

$$999\,919 = 1\,000\,000 - 81.$$

Reescrevendo-o como uma diferença de quadrados, obtemos

$$999\,919 = 1\,000^2 - 9^2.$$

Aplicando a identidade de fatoração da diferença de quadrados, temos:

$$1\,000^2 - 9^2 = (1\,000 - 9)(1\,000 + 9).$$

Logo,

$$999\,919 = 991 \times 1\,009.$$

Assim, o número 999 919 é expresso como o produto de dois inteiros maiores que 1, o que mostra que ele não é primo. Portanto, a afirmação é falsa.

12. **OPEMAT - 1ª FASE:** O π -raia escreve uma lista de números do seguinte modo: Ele começa escrevendo $a_1 = 2022$, depois escreve $a_2 = 20222022$ e assim sucessivamente, sendo o n -ésimo número:

$$a_n = \underbrace{202220222022202 \dots 2022}_{\text{"2022" escrito } n \text{ vezes}}.$$

Ele decide continuar escrevendo a lista até que o primeiro a_n múltiplo de 23 apareça. Quantos números ele escreveu na lista até parar?

- A) 3
- B) 5
- C) 7
- D) 11
- E) 13

Solução. Note que os primeiros termos da sequência são dados por:

$$a_1 = 2022.$$

$$a_2 = 20222022 = 2022 \cdot 10^4 + 2022.$$

$$a_3 = 202220222022 = 2022 \cdot 10^8 + 2022 \cdot 10^4 + 2022.$$

Observando o padrão, para $n \geq 1$ temos:

$$a_n = 2022 \cdot 10^{4(n-1)} + 2022 \cdot 10^{4(n-2)} + \dots + 2022 \cdot 10^4 + 2022.$$

Colocando 2022 em evidência:

$$a_n = 2022 \left(1 + 10^4 + 10^8 + \dots + 10^{4(n-1)} \right).$$

O que está entre parênteses é uma soma de n termos de uma progressão geométrica de razão 10^4 e primeiro termo 1. Aplicando a fórmula da soma da P.G., obtemos:

$$1 + 10^4 + 10^8 + \dots + 10^{4(n-1)} = \frac{10^{4n} - 1}{10^4 - 1} = \frac{10^{4n} - 1}{9999}.$$

Portanto,

$$a_n = 2022 \cdot \frac{(10^{4n} - 1)}{9999}.$$

Queremos o menor n tal que a_n seja múltiplo de 23. Assim,

$$a_n \equiv 0 \pmod{23}.$$

Substituindo a expressão de a_n :

$$2022 \cdot \frac{(10^{4n} - 1)}{9999} \equiv 0 \pmod{23}.$$

Sabemos que $2022 \equiv 21 \pmod{23}$ e $9999 \equiv 17 \pmod{23}$. Como o $\text{mdc}(2022, 23) = 1$ e o $\text{mdc}(9999, 23) = 1$, podemos multiplicar toda a congruência por 9999 e dividir por 2022 sem alterar o resultado. Assim, o problema se reduz a:

$$10^{4n} - 1 \equiv 0 \pmod{23},$$

ou seja,

$$10^{4n} \equiv 1 \pmod{23}.$$

Pelo Pequeno Teorema de Fermat, sabemos que

$$10^{22} \equiv 1 \pmod{23}.$$

Comparando com a congruência que obtivemos,

$$10^{4n} \equiv 1 \pmod{23},$$

concluimos que, para que isso aconteça, o expoente $4n$ deve ser múltiplo de 22.

Portanto,

$$4n \equiv 0 \pmod{22},$$

o que significa que 22 divide $4n$. Podemos escrever

$$4n = 22k,$$

para algum inteiro k . Assim,

$$n = \frac{22k}{4} = \frac{11k}{2}.$$

Como n precisa ser inteiro, isso só ocorre quando k é par. O menor valor par de k é $k = 2$, o que fornece

$$n = \frac{11 \cdot 2}{2} = 11.$$

Portanto, o primeiro termo da sequência que é múltiplo de 23 ocorre para $n = 11$. Concluímos que o π -raia escreveu 11 números até parar, sendo este o primeiro termo da sequência múltiplo de 23.

Alternativa correta: B) 11.

13. **ENQ-PROFMAT:** Determine um número inteiro entre 1200 e 1400 que deixa restos 2 e 6 quando dividido, respectivamente, por 11 e 13.

Solução: Teorema Chinês do Resto (TCR).

Seja x o número inteiro procurado. O enunciado fornece o seguinte sistema de congruências:

$$\begin{cases} x \equiv 2 \pmod{11}, \\ x \equiv 6 \pmod{13}. \end{cases}$$

Pelo Teorema Chinês do Resto, definimos:

$$M = 11 \cdot 13 = 143.$$

Considere:

$$M_1 = 13, \quad M_2 = 11.$$

Agora, determinamos os inversos y_1 e y_2 tais que:

$$M_1 y_1 \equiv 1 \pmod{11}, \quad M_2 y_2 \equiv 1 \pmod{13}.$$

Para calcular os inversos, fazemos::

$$13y_1 \equiv 1 \pmod{11} \Rightarrow 2y_1 \equiv 1 \pmod{11} \Rightarrow y_1 \equiv 6 \pmod{11}.$$

$$11y_2 \equiv 1 \pmod{13} \Rightarrow 66y_2 \equiv 6 \pmod{13} \Rightarrow y_2 \equiv 6 \pmod{13}$$

Aplicando o Teorema Chinês do Resto:

$$x \equiv r_1 M_1 y_1 + r_2 M_2 y_2 \pmod{M}.$$

Substituindo os valores:

$$x \equiv 2 \cdot 13 \cdot 6 + 6 \cdot 11 \cdot 6 \pmod{143}.$$

$$x \equiv 156 + 396 = 552 \pmod{143}.$$

Efetuada a redução módulo 143:

$$552 \equiv 123 \pmod{143}.$$

Logo, todas as soluções são da forma:

$$x = 143t + 123, \quad t \in \mathbb{Z}.$$

Como o problema exige que $1200 \leq x \leq 1400$, tomamos $t = 8$, o que fornece:

$$x = 143 \cdot 8 + 123 = 1267.$$

Portanto, o número inteiro procurado é:

$$\boxed{1267}.$$

Solução Alternativa:

Seja x o número a determinar. As condições fornecem:

$$x \equiv 2 \pmod{11} \tag{3.10}$$

$$x \equiv 6 \pmod{13} \tag{3.11}$$

Da congruência (3.11), escrevemos:

$$x = 13a + 6, \quad a \in \mathbb{Z}. \tag{3.12}$$

Substituindo a expressão da equação (3.12) na congruência (3.10), obtemos:

$$\begin{aligned} 13a + 6 &\equiv 2 \pmod{11} \\ 2a &\equiv -4 \pmod{11} \\ a &\equiv -2 \pmod{11} \\ a &\equiv 9 \pmod{11}. \end{aligned} \tag{3.13}$$

Assim:

$$a = 11b + 9, \quad b \in \mathbb{Z}. \tag{3.14}$$

Substituindo (3.14) em (3.12), encontramos:

$$x = 13(11b + 9) + 6 = 143b + 117 + 6 = 143b + 123.$$

Portanto, a solução geral do sistema é:

$$x = 143b + 123 \quad b \in \mathbb{Z}.$$

Para encontrar a solução no intervalo $1200 \leq x \leq 1400$, tomamos $b = 8$, então:

$$x = 143 \cdot 8 + 123 = 1267.$$

O número inteiro procurado é 1267.

14. **OPEMAT – 2ª fase:** Um general deseja verificar o número de soldados em um de seus pelotões. Então, mandou que os soldados formassem alinhados de 9 em 9 e verificou que sobraram 2 soldados. Em seguida, ordenou que formassem alinhados de 11 em 11 e verificou que sobraram 4. Finalmente, fez os soldados se alinharem de 13 em 13 e sobraram 8. Sabendo que o pelotão tem entre dois mil e três mil soldados, determine quantos soldados sobraram quando o general os mandou formar de 100 em 100.

Solução: Teorema Chinês do Resto (TCR).

Para modelar a situação, consideremos x o número total de soldados do pelotão. As informações do enunciado conduzem ao seguinte sistema de congruências:

$$\begin{cases} x \equiv 2 \pmod{9}, \\ x \equiv 4 \pmod{11}, \\ x \equiv 8 \pmod{13}. \end{cases}$$

Pelo Teorema Chinês do Resto, definimos:

$$M = 9 \cdot 11 \cdot 13 = 1287.$$

Para cada congruência, calculamos:

$$M_1 = \frac{M}{9} = 143, \quad M_2 = \frac{M}{11} = 117, \quad M_3 = \frac{M}{13} = 99.$$

Em seguida, determinamos os inversos y_i tais que:

$$M_1 y_1 \equiv 1 \pmod{9}, \quad M_2 y_2 \equiv 1 \pmod{11}, \quad M_3 y_3 \equiv 1 \pmod{13}.$$

Cálculo dos inversos:

$$143y_1 \equiv 1 \pmod{9} \quad \Rightarrow 8y_1 \equiv 1 \pmod{9} \quad \Rightarrow y_1 \equiv 8 \pmod{9},$$

$$117y_2 \equiv 1 \pmod{11} \quad \Rightarrow 7y_2 \equiv 1 \pmod{11} \quad \Rightarrow y_2 \equiv 8 \pmod{11},$$

$$99y_3 \equiv 1 \pmod{13} \quad \Rightarrow 8y_3 \equiv 1 \pmod{13} \quad \Rightarrow y_3 \equiv 5 \pmod{13}.$$

Aplicando o Teorema Chinês do Resto, obtemos:

$$x \equiv r_1 M_1 y_1 + r_2 M_2 y_2 + r_3 M_3 y_3 \pmod{M},$$

isto é,

$$x \equiv 2 \cdot 143 \cdot 8 + 4 \cdot 117 \cdot 8 + 8 \cdot 99 \cdot 5 \pmod{1287}.$$

Efetuando os cálculos:

$$x \equiv 2288 + 3744 + 3960 = 9992 \pmod{1287}.$$

Reduzindo o resultado módulo 1287:

$$x \equiv 983 \pmod{1287}.$$

Isso significa que todos os números da forma

$$x = 1287t + 983, \quad t \in \mathbb{Z},$$

satisfazem simultaneamente as três condições do problema.

Como o pelotão possui entre 2000 e 3000 soldados, tomamos $t = 1$, obtendo:

$$x = 1287 \cdot 1 + 983 = 2270.$$

Assim, o pelotão possui 2270 soldados. Ao formar grupos de 100 soldados, temos:

$$2270 \equiv 70 \pmod{100}.$$

Portanto, restam exatamente 70 soldados.

Solução Alternativa: Consideremos x o número total de soldados do pelotão. As informações do enunciado podem ser expressas pelo seguinte sistema de congruências:

$$x \equiv 2 \pmod{9}, \tag{3.15}$$

$$x \equiv 4 \pmod{11}, \tag{3.16}$$

$$x \equiv 8 \pmod{13}. \tag{3.17}$$

Da congruência (3.17), isolamos o x :

$$x = 13a + 8, \quad a \in \mathbb{Z}. \tag{3.18}$$

Substituímos (3.18) na segunda congruência (3.16):

$$\begin{aligned} 13a + 8 &\equiv 4 \pmod{11} \\ 2a &\equiv 7 \pmod{11} \\ a &\equiv 9 \pmod{11}. \end{aligned} \tag{3.19}$$

Logo,

$$a = 11b + 9, \quad b \in \mathbb{Z}. \quad (3.20)$$

Substituimos (3.20) em (3.18):

$$x = 13(11b + 9) + 8 = 143b + 125. \quad (3.21)$$

Agora, substituimos (3.21) em (3.15):

$$\begin{aligned} 143b + 125 &\equiv 2 \pmod{9} \\ 8b + 8 &\equiv 2 \pmod{9} \\ 8b &\equiv -6 \pmod{9} \\ b &\equiv 6 \pmod{9}. \end{aligned} \quad (3.22)$$

Portanto,

$$b = 9c + 6, \quad c \in \mathbb{Z}. \quad (3.23)$$

Substituimos (3.23) em (3.21):

$$x = 143(9c + 6) + 125 = 1287c + 983. \quad (3.24)$$

Assim, todas as soluções são da forma:

$$x = 1287c + 983, \quad c \in \mathbb{Z}.$$

Como o enunciado impõe $2000 \leq x \leq 3000$, tomamos $c = 1$ em (3.24), obtendo:

$$x = 1287 \cdot 1 + 983 = 2270.$$

Logo, o número total de soldados que satisfaz simultaneamente as três condições é $x = 2270$.

Ao formar grupos de 100 soldados, verifica-se:

$$2270 \equiv 70 \pmod{100}.$$

Portanto, restam exatamente 70 soldados.

4 Sequência Didática

Neste capítulo, apresenta-se a sequência didática, com foco no estudo da Aritmética a partir de problemas provenientes das Olimpíadas de Matemática. A estrutura foi organizada de modo a possibilitar um acompanhamento detalhado do processo de ensino e aprendizagem, oferecendo ao leitor uma visão clara das etapas que compõem sua execução.

O conceito de sequência didática corresponde a um conjunto de atividades articuladas e encadeadas em torno de determinados objetivos educacionais, concebidas para dar sentido e coerência ao trabalho pedagógico (16). De maneira complementar, destaca-se que a sequência didática constitui uma modalidade organizativa que, ao apresentar desafios progressivos, contribui para que os estudantes desenvolvam novas competências e alcancem níveis mais elevados de aprendizagem (17).

Estruturar este trabalho em forma de sequência didática decorre da necessidade de organizar os encontros de maneira planejada. Com isso, pretende-se criar condições para que os alunos se envolvam ativamente com os desafios, ampliem sua compreensão matemática e desenvolvam confiança diante de situações-problema.

A seguir, apresentam-se informações sobre a sequência didática e, posteriormente, o detalhamento de cada encontro, incluindo a descrição das atividades e das estratégias de exploração em sala de aula.

4.1 Orientação Docente

A sequência didática proposta tem como objetivo aproximar os estudantes do estilo de provas das olimpíadas de matemática, favorecendo a familiarização com os tipos de questões e estratégias de resolução. A ideia é introduzir e explorar temas recorrentes em avaliações olímpicas, de modo a despertar o interesse dos alunos e fortalecer sua confiança para participar desses eventos.

Não se trata de desenvolver de forma exaustiva todos os conteúdos, mas de abrir caminhos para que os estudantes conheçam e compreendam tópicos que muitas vezes não aparecem de forma contínua no currículo escolar. Essa proposta oferece a oportunidade de perceber que a matemática olímpica também pode ser acessível aos alunos do ensino médio da rede pública, ampliando suas perspectivas e experiências de aprendizagem.

Para alcançar esse propósito, recomenda-se que os encontros sejam conduzidos em um ambiente colaborativo e motivador, com atividades que envolvam desafios e problemas instigantes. A dinâmica deve valorizar a participação ativa e frequente dos estudantes, estimulando o trabalho em grupo, a troca de estratégias e o prazer em resolver problemas.

Dessa forma, a proposta deixa de ser “mais uma aula de matemática” e se torna uma experiência, capaz de envolver os estudantes em um processo de descoberta, cooperação e preparação para as olimpíadas de matemática.

4.2 Proposta Didática

Informações Gerais

- **Área de Conhecimento:** Matemática e suas Tecnologias.
- **Componente Curricular:** Matemática.

Conteúdos Abordados

1. Divisibilidade
2. Sistemas de numeração
3. Máximo divisor comum (mdc) e mínimo múltiplo comum (mmc)
4. Equações diofantinas
5. Números primos
6. Congruências
7. Teorema chinês dos restos

Tema

Aritmética nas olimpíadas de matemática: uma proposta para o ensino médio.

Justificativa

A Aritmética envolve conceitos e operações matemáticas estudados, desde o Ensino Fundamental, que podem ser utilizados na resolução de problemas encontrados em olimpíadas de matemática, como a OBMEP. Muitos desses conteúdos, como divisibilidade, mdc, mmc e números primos, servem como base para a compreensão de tópicos mais avançados e para a construção de estratégias de resolução.

Esta sequência didática cria um espaço para que os estudantes explorem esses conteúdos de forma investigativa e cooperativa, revisitando conceitos prévios e avançando para temas como equações diofantinas, congruências e teorema chinês dos restos, despertando a

curiosidade, estimulando o raciocínio lógico e incentivando a busca de soluções de forma autônoma.

Ao oferecer essa oportunidade na escola pública, busca-se reconhecer talentos, proporcionar experiências de aprendizado significativo e ampliar as perspectivas acadêmicas dos estudantes, valorizando seu potencial e promovendo equidade no acesso a conhecimentos específicos de preparação para olimpíadas de matemática.

Competências

- Compreender conceitos fundamentais de aritmética.
- Desenvolver pensamento lógico-matemático e estratégias de resolução de problemas.
- Aplicar conhecimentos matemáticos em contextos desafiadores (olímpicos).

Habilidades

A sequência didática retoma e consolida habilidades aritméticas do ensino fundamental (6º e 7º anos) que servem como base para a resolução de problemas mais complexos e para o estudo de conceitos avançados presentes em olimpíadas de matemática. Entre as habilidades trabalhadas, destacam-se:

- BNCC: EF06MA02/PE: EF06MA02PE - reconhecer o sistema de numeração decimal, destacando base, valor posicional e função do zero, e utilizar a composição e decomposição de números naturais e racionais em representação decimal.
- BNCC: EF06MA05/PE: EF06MA05PE - identificar e classificar números naturais em primos e compostos, estabelecer relações entre números (“é múltiplo de”, “é divisor de”, “é fator de”) e investigar critérios de divisibilidade.
- BNCC: EF06MA06, EF07MA01/PE: EF06MA06PE, EF07MA01PE - resolver e elaborar problemas envolvendo múltiplos e divisores, incluindo máximo divisor comum e mínimo múltiplo comum, utilizando estratégias diversas, sem aplicação de algoritmos.

Essas habilidades são o ponto de partida para o desenvolvimento da proposta didática, permitindo que os estudantes avancem para temas que não estão presentes no currículo escolar do ensino médio, conforme a Base Nacional Comum Curricular e o Currículo de Pernambuco(1, 9), tais como equações diofantinas, congruências e o Teorema Chinês dos Restos. A sequência é organizada de forma que cada tema seja construído a partir dos conhecimentos prévios, proporcionando coerência e facilitando a compreensão gradual dos conteúdos.

Objetivos

Objetivo Geral

Promover, no ambiente da escola pública, um espaço formativo que desperte nos estudantes o interesse pelas olimpíadas de matemática por meio de um curso de aritmética, fortalecendo sua confiança, desenvolvendo habilidades matemáticas e ampliando suas perspectivas acadêmicas. Além disso, oferecer um material de apoio aos professores, incentivando novas iniciativas semelhantes em diferentes contextos escolares.

Objetivos Específicos

- Estudar, de forma acessível e significativa, os principais conteúdos de aritmética recorrentes nas olimpíadas de matemática.
- Resolver e analisar questões olímpicas da 1ª e 2ª fases.
- Apresentar soluções alternativas para um mesmo problema, quando possível, incentivando diferentes formas de raciocínio.
- Estimular a leitura, a escrita e a argumentação matemática, preparando os estudantes para provas discursivas.
- Despertar o interesse e a confiança dos estudantes para a participação em olimpíadas de matemática.
- Promover o desenvolvimento matemático por meio de atividades desafiadoras.
- Estimular o raciocínio lógico-dedutivo na resolução de problemas.
- Produzir um material didático acessível e adaptável que possa ser utilizado por outros professores da educação básica.

Público alvo

Estudantes do ensino médio da rede estadual de Pernambuco, com faixa etária entre 14 e 19 anos, interessados em participar de olimpíadas de matemática.

Perfil das Turmas

Grupos de aproximadamente 15 a 25 estudantes, com diferentes níveis de desempenho em matemática, com interesse em aprimorar a resolução de problemas olímpicos.

Recursos

- Jogos matemáticos;

- Quadro, piloto, papel e lápis.
- Notebook e Datashow.
- Material impresso (listas de exercícios, definições e resumos).
- Acesso digital a materiais complementares por meio do grupo no WhatsApp (Portal da OBMEP, vídeos, etc).

Avaliação

A avaliação será contínua e formativa, considerando:

- **Participação e socialização:**

Observação das apresentações de soluções, individual ou em grupo, promovendo troca de ideias e estratégias entre os estudantes.

- **Escrita matemática:**

Observação da clareza, organização lógica e estrutura das resoluções, com possibilidade de devolutivas construtivas do professor.

- **Avaliação dos encontros:**

Reflexão sobre a produtividade do encontro, nível de dificuldade das atividades e sugestões de melhoria para os próximos encontros.

4.3 Encontros e questões propostas

A seguir, apresentam-se os encontros que compõem a sequência didática, detalhando o desenvolvimento das atividades propostas em cada etapa.

4.3.1 Encontro 01 – Divisibilidade

Plano de aula

Público-alvo: Ensino médio.

Tema: Divisão nos inteiros.

Quantidade de aulas/horas: 2 aulas / 1h40.

Conteúdos

- Divisão inteira e algoritmo da divisão;
- Conceitos de dividendo, divisor, quociente e resto;

- Propriedades de divisibilidade: múltiplos e divisores.

Objetivos

- Compreender os conceitos de divisor, dividendo, quociente e resto.
- Aplicar o algoritmo da divisão inteira;
- Identificar múltiplos, divisores e padrões em restos de divisões.

Momento 1: acolhimento e diagnose

O primeiro encontro inicia-se com a apresentação dos objetivos dos encontros, seguida da aplicação de um questionário diagnóstico.

Objetivos:

- Levantar o perfil dos estudantes: histórico em olimpíadas, familiaridade com provas discursivas e expectativas.
- Identificar como os estudantes organizam seu raciocínio, registram suas ideias por escrito e escolhem estratégias de resolução.

Questionário diagnóstico

1. Você já participou de alguma olimpíada de matemática? Qual foi sua experiência?
2. Quais tipos de problemas matemáticos você mais gosta ou sente dificuldade?
3. Como você organiza seu raciocínio ao resolver problemas matemáticos?
4. Descreva como costuma registrar suas soluções e justificativas ao resolver um problema matemático.
5. O que espera aprender neste curso preparatório para provas olímpicas?
6. **Questão Desafiadora (OBMEP - 1ª FASE):** Nove amigos comeram 5 pizzas, algumas cortadas em 6 fatias e outras cortadas em 8 fatias. Todos comeram o mesmo número de fatias e não sobrou nada. Quantas fatias cada um comeu?
 - A) 4
 - B) 5
 - C) 6
 - D) 7

E) 8

7. Descreva como você pensou para tentar resolver a questão acima. Quais passos você seguiu? Testou alguma possibilidade? Quais alternativas considerou?

Esta atividade diagnóstica tem como objetivo identificar o perfil de escrita matemática dos participantes e oferecer subsídios para o planejamento dos próximos encontros. Em seguida, os alunos participam de uma breve roda de conversa, compartilhando percepções, sentimentos e dificuldades observadas durante o diagnóstico. Esse momento inicial permite preparar o grupo para o trabalho efetivo com o tema proposto sobre divisibilidade.

Momento 2: divisibilidade

Para introduzir de forma lúdica o conceito de divisibilidade e o algoritmo da divisão inteira, propomos a atividade *Trilha dos Restos* (18).

Motivação - jogo trilha dos restos

O jogo permite que os estudantes experimentem a operação de divisão na prática e observem como o resto varia de 0 até o divisor menos uma unidade, reforçando a compreensão da expressão $a = bq + r$, $0 \leq r < b$, em que a é o dividendo, b o divisor, q o quociente e r o resto.



Figura 1 – Tabuleiro do jogo trilha dos restos

Objetivos

- Fixar os conceitos de dividendo, divisor, quociente e resto.

- Explorar a expressão da divisão $a = bq + r$, $0 \leq r < b$
- Desenvolver raciocínio estratégico e percepção de múltiplos e divisores.

Materiais

- Tabuleiro.
- Peça de marcação (1 por aluno ou grupo).
- Dado ou spinner com números de 1 a 6 (divisores).

Etapas

Introdução

Apresentar o jogo e explicar os conceitos de dividendo (a), divisor (b), quociente (q) e resto (r).

Regras do Jogo:

- Número de jogadores: 4.
- Primeira rodada: cada jogador lança o dado e posiciona seu peão na trilha de acordo com o número obtido. O participante que obtiver o maior número inicia a próxima rodada. Em caso de empate, os empatados realizam novo lançamento para definir a ordem. As jogadas seguem no sentido anti-horário.
- A partir da segunda rodada:
 - O jogador lança o dado e o número sorteado será o seu divisor na operação a ser realizada.
 - O dividendo é o número da casa em que o peão parou.
 - O resto é o número de casas que o jogador deve andar.
- O jogador que, na sua vez, efetuar um cálculo errado, perde a sua vez de jogar.
- Será vencedor o jogador que sair primeiro da trilha.

Jogo

O jogo trilha dos restos é uma ferramenta pedagógica eficaz para ensinar divisibilidade e a expressão algébrica da divisão. Ao jogar, os alunos aplicam a fórmula $a = bq + r$, em que:

- a é o número da casa onde o peão está;

- b é o número sorteado no dado (o divisor);
- q é o quociente da divisão;
- r é o resto da divisão, que determina o número de casas a serem avançadas.

A dinâmica do jogo reforça a compreensão de que o resto r deve ser menor que o divisor b , alinhando-se às propriedades fundamentais da divisão. É importante que o professor oriente o estudante a registrar suas jogadas na folha de cálculos [A](#).

Em busca de soluções

A atividade possibilita discussões sobre estratégias de cálculo, verificação de resultados e generalização do algoritmo da divisão para diferentes números, promovendo a compreensão conceitual e a aplicação prática da divisibilidade. Além disso, durante o jogo, os alunos podem refletir sobre questões como:

1. Quais divisores são mais vantajosos e por quê?
2. Em quais situações o avanço é máximo ou nulo?
3. Que padrões podem ser observados nos restos das divisões?
4. Existe alguma casa no tabuleiro em que o jogador não consiga mais avançar, independentemente do divisor sorteado? Qual seria e por quê?

Ao final da rodada, o professor deverá relacionar os registros feitos pelos estudantes com a expressão da divisão $a = bq + r$, $0 \leq r < b$, sendo possível reforçar a relação entre o jogo e conceitos de divisibilidade, bem como propor uma reflexão coletiva sobre as estratégias utilizadas, os padrões observados nos restos e em como esses conhecimentos podem ser aplicados em problemas matemáticos mais complexos.

Desse modo, tem-se que o jogo *trilha dos Restos* permite que os alunos consolidem a compreensão do algoritmo da divisão e a divisibilidade de forma mais lúdica.

Exposição do conceito e algoritmo

Na sequência do jogo e da formalização das observações, o professor apresenta os conceitos de divisibilidade entre dois números inteiros, suas propriedades e, nos casos em que a divisão não é exata, o algoritmo da divisão euclidiana, enfatizando a existência do resto e sua aplicação em problemas matemáticos.

Durante essa etapa, é importante que o professor conecte os registros feitos pelos estudantes no jogo com a expressão algébrica da divisão $a = bq + r$, $0 \leq r < b$, reforçando

a compreensão conceitual do algoritmo. Além disso, essa exposição permite preparar o grupo para a resolução de situações-problema, mostrando de forma estruturada como aplicar o algoritmo em diferentes contextos.

Generalização e aplicação

Após a explanação teórica, propõe-se a realização de situações-problema que envolvam conceitos de divisibilidade. Durante a resolução, o professor acompanha o processo, orientando os estudantes diante das dificuldades, estimulando a socialização das ideias e promovendo melhorias na escrita matemática. Espera-se que os alunos, ao resolver os problemas, reconheçam padrões, relacionem diferentes casos e apliquem o algoritmo da divisão em contextos variados, consolidando a compreensão e a generalização do conteúdo estudado.

Questões referentes ao encontro 01 - Divisibilidade

1. **OBMEP - 1ª FASE:** Lucas pensou em um número, dividiu-o por 285 e obteve resto 77. Se ele dividir o número em que pensou por 57, qual é o resto que ele vai encontrar?
 - A) 0
 - B) 20
 - C) 40
 - D) 54
 - E) 56
2. **OPEMAT - 2ª FASE:** Considere a lista periódica conforme a situação na figura abaixo: A lista é ordenada, ou seja, o primeiro termo é o número 1, o segundo o número 2, o terceiro o número 3, o quarto o número 1 e assim por diante. Julgue as afirmações a seguir atribuindo (V) se a afirmação for VERDADEIRA e (F) se a afirmação for FALSA.

1 2 3 1 2 4 1 2 3 1 2 4 1 2 3 1 2 4 1 2 3 1 2 4 1 2 3 1 2 4 1 2 3 1 2 4 ...

 - A) (V) (F) A sequência se repete a cada agrupamento de 7 números.
 - B) (V) (F) O número que ocupa a 2021ª posição é o número 3.
 - C) (V) (F) Observando a lista até o 2020º termo (incluindo este número), o número 3 aparece 336 vezes.
 - D) (V) (F) Olhando a lista até o 2019º termo (incluindo este número), o agrupamento 12 aparece 673 vezes.

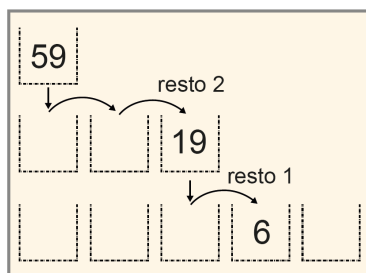
E) (V) (F) Somando os primeiros 2018 números dessa sequência obtemos o valor 4371.

3. **OBMEP - 2ª FASE:** Em uma brincadeira, Euclides escolhe um número natural, coloca esse número no topo do tabuleiro ao lado e realiza o seguinte procedimento:

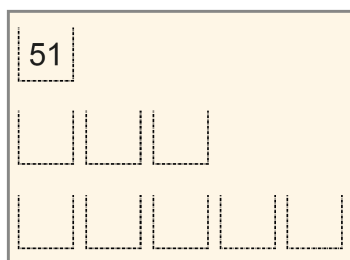
- divide o número escolhido por 3 e anota o quociente e o resto;
- se o resto for 0 coloca o quociente logo abaixo do número;
- se o resto for 1 coloca o quociente deslocando uma casa para a direita;
- se o resto for 2 coloca o quociente deslocando duas casas para a direita.

A seguir, ele repete o mesmo procedimento para o quociente obtido. Na figura vemos a brincadeira de Euclides que começa com 59 e termina com o 6 na quarta casa da base do tabuleiro.

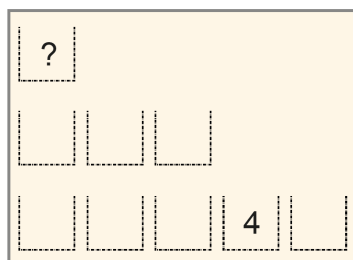
$$\begin{array}{r} 59 \overline{) 3} \\ 2 \quad 19 \\ \hline 59 = 19 \times 3 + 2 \\ 19 \overline{) 3} \\ 1 \quad 6 \\ \hline 19 = 6 \times 3 + 1 \end{array}$$



A) Faça a brincadeira de Euclides com o número 51.



B) Quais números Euclides pode ter escolhido se a brincadeira terminou com o 4 na quarta casa da base do tabuleiro?



C) Quantos números entre 10 e 99 começam uma brincadeira de Euclides que terminam na quarta casa da base do tabuleiro?

4. **OPEMAT - 1ª FASE:** Quantos pares (m, n) de números inteiros satisfazem a igualdade

$$3n + 5m = mn + 13.$$

- A) Quatro pares.
- B) Cinco pares.
- C) Seis pares.
- D) Sete pares.
- E) Oito pares.

Avaliação e reflexão

A socialização das soluções dos problemas propostos permite que os estudantes exponham suas estratégias, dificuldades e percepções em relação ao nível de desafio das atividades. Esse momento favorece a reflexão sobre diferentes caminhos de resolução e fortalece a compreensão dos conceitos trabalhados ao longo do encontro.

Além disso, possibilita ao professor acompanhar o desenvolvimento do grupo, identificar necessidades específicas e ajustar o planejamento. Assim, a avaliação não se restringe apenas ao encerramento das atividades, se trata de um processo contínuo que permite compreender não apenas o domínio dos conteúdos, mas também o desenvolvimento de competências como raciocínio lógico e comunicação matemática, alinhando-se aos objetivos gerais da sequência didática.

4.3.2 Encontro 02 - Sistema de Numeração

Plano de Aula

Público-alvo: ensino médio.

Tema: sistema de numeração posicional, representação de números inteiros em base 10 e base binária e mudança de base.

Quantidade de aulas/horas: 2 aulas / 1h40.

Conteúdos

- Sistemas de numeração decimal e posicional;
- Expansão de um número em uma base;
- Mudança de base.

Objetivos

- Compreender o sistema de numeração posicional e sua expansão polinomial;
- Representar números naturais em diferentes bases numéricas;
- Realizar mudanças de base.

Motivação - Cartas Mágicas

Para introduzir o conceito de sistema de numeração posicional e a mudança de base, propomos a seguinte atividade lúdica, baseada no programa de iniciação científica do PIC/OBMEP ([14](#)).

As cartelas apresentadas a seguir permitem realizar a atividade de descoberta do número secreto:

1	3	5	7
9	11	13	15
17	19	21	23
25	27	29	31
33	35	37	39
41	43	45	47
49	51	53	55
57	59	61	63

2	3	6	7
10	11	14	15
18	19	22	23
26	27	30	31
34	35	38	39
42	43	46	47
50	51	54	55
58	59	62	63

4	5	6	7
12	13	14	15
20	21	22	23
28	29	30	31
36	37	38	39
44	45	46	47
52	53	54	55
60	61	62	63

8	9	10	11
12	13	14	15
24	25	26	27
28	29	30	31
40	41	42	43
44	45	46	47
56	57	58	59
60	61	62	63

16	17	18	19
20	21	22	23
24	25	26	27
28	29	30	31
48	49	50	51
52	53	54	55
56	57	58	59
60	61	62	63

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

Imagine que o estudante escolha secretamente um número inteiro entre 1 e 63. Para descobrir o número pensado, o professor mostra cada uma das cartas e pede que o estudante informe se o número escolhido está na cartela. O processo se repete até que

todas as cartelas sejam apresentadas. Ao final do processo, somando as potências de 2 correspondentes às cartelas selecionadas, o professor consegue “adivinhar” o número escolhido como em um passe de mágica.

Em busca de soluções

Após a atividade, podemos refletir sobre como a mágica funciona e quais princípios matemáticos estão por trás dela. Alguns questionamentos que podem surgir são:

- Como a mágica funciona?
- Como as cartas são construídas?
- Como podemos modificar as cartelas para trabalhar com números maiores, como de 1 a 100?

O segredo da atividade é a decomposição única de números naturais como soma de potências de 2. Cada número aparece apenas nas cartelas correspondentes às potências de 2 que o compõem. Por exemplo, o número 22 pode ser escrito como $22 = 2 + 4 + 16$, aparecendo somente nas cartelas correspondentes às potências 2^1 , 2^2 e 2^4 .

Exposição do conceito e algoritmo

A atividade das cartas mágicas permite explorar, de forma concreta, conceitos relacionados ao sistema de numeração. Os estudantes observam a representação de números em sistemas posicionais, reconhecendo que cada dígito (ou carta) corresponde a uma potência de uma base. Além disso, a atividade introduz de maneira intuitiva a mudança de base, mostrando que um mesmo número pode ser representado em diferentes sistemas, aqui exemplificada pela base binária. Dessa forma, a atividade funciona como um ponto de partida, permitindo que os estudantes compreendam intuitivamente os princípios antes de aprofundar a teoria.

Após essa exploração inicial, os conceitos de sistema posicional e mudança de base são apresentados formalmente. Para reforçar o conteúdo, sugere-se que os estudantes produzam suas próprias cartas mágicas na base binária para números de 1 a 15. No Apêndice B, disponibilizamos versões em branco das cartelas, destinadas à impressão e preenchimento durante a prática em sala de aula.

Essa abordagem favorece o desenvolvimento da autonomia do estudante e estimula a generalização do procedimento, seja para intervalos numéricos maiores ou para representações em diferentes bases.

Generalização e aplicação

Ao final da atividade, espera-se que os estudantes percebam que o funcionamento das cartelas está fundamentado na decomposição de números em potências de uma base, e não em um truque. A partir dessa compreensão inicial, devem ser capazes de generalizar o método, reconhecendo que qualquer número pode ser representado em qualquer sistema posicional.

Essa generalização possibilita compreender o papel de cada dígito em função da potência correspondente da base escolhida. Com isso, o domínio do sistema posicional passa a servir de base para resolver problemas mais complexos, envolvendo conversão entre bases, análise de padrões numéricos e situações-problema típicas de contextos desafiadores, como as olimpíadas de matemática.

Questões referentes ao encontro 02 - sistemas de numeração

1. **OBMEP - 1ª FASE:** O contrário de um número de dois algarismos, ambos diferentes de zero, é o 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 seu contrário?
 - A) 44
 - B) 99
 - C) 121
 - D) 165
 - E) 181
2. **OPEMAT - 1ª FASE:** Os números naturais m, n, p, q, r e s são formados por 3 algarismos não nulos. Assumindo que estes números são distintos e formados pelos mesmos algarismos, então $m + n + p + q + r + s$ é um múltiplo de:
 - A) 10
 - B) 100
 - C) 110
 - D) 200
 - E) 222

Avaliação e reflexão

A avaliação deste encontro busca favorecer a socialização das soluções das questões propostas, bem como estimular a reflexão crítica sobre os conceitos estudados.

Em um primeiro momento, os alunos socializam suas resoluções, discutindo os diferentes caminhos adotados e levantando possíveis dificuldades encontradas. Essa troca de estratégias contribui para o fortalecimento da aprendizagem colaborativa e para a identificação de pontos que necessitam de maior aprofundamento.

A seguir, propõe-se a construção coletiva de um mapa mental ou esquema síntese, de modo que os estudantes expressem os principais temas abordados no encontro, tais como o sistema posicional, a escrita decimal, a mudança de base e exemplos práticos discutidos em sala. Esse registro visual possibilita organizar os conhecimentos adquiridos, além de favorecer a memória e a conexão entre conceitos.

A avaliação tem caráter formativo, valorizando o processo de aprendizagem e permitindo que o professor acompanhe o progresso dos alunos e planeje ações futuras.

4.3.3 Encontro 03 - Máximo divisor comum

Plano de Aula

Tema: máximo divisor comum (mdc)

Ano/série: ensino médio

Tempo estimado: 1 aula (50 minutos)

Conteúdos

- Divisores de um número natural e identificação de divisores comuns;
- Máximo divisor comum (mdc);
- Métodos de cálculo do MDC: listagem, decomposição em fatores primos e algoritmo de Euclides.

Objetivos

- Compreender o conceito de máximo divisor comum (mdc) e sua importância na resolução de problemas;
- Conhecer, aplicar e comparar diferentes métodos para o cálculo do MDC;
- Desenvolver a habilidade de interpretar e resolver problemas envolvendo o MDC em diferentes contextos;
- Identificar contextos matemáticos e problemas em que o MDC é a ferramenta adequada de resolução.

Motivação

Nesta etapa da sequência didática, propomos uma atividade prática para introduzir o conceito de Máximo Divisor Comum (MDC) a partir de uma situação concreta, inspirada no problema motivador (14).

O professor apresenta os dois cordões e explica:

“Temos dois rolos de arame: um com 210 cm e outro com 330 cm. Precisamos cortá-los em pedaços de mesmo comprimento, mas queremos que esses pedaços sejam os maiores possíveis. Qual deve ser o comprimento de cada pedaço?”

Materiais

- Dois cordões para cada dupla (um de 210 cm e outro de 330 cm);
- Tesoura;
- Fita métrica ou régua;
- Quadro branco para registro coletivo.

A turma é dividida em duplas. Cada dupla analisa os cordões e testa cortes possíveis (10 cm, 15 cm, 20 cm, 30 cm, etc.), registrando as tentativas e verificando em quais comprimentos ambos os cordões podem ser divididos sem sobra.

Em busca de soluções

O professor organiza a socialização dos resultados no quadro. Pergunta-se:

- Qual o maior comprimento que serve para os dois cordões?
- Como garantir que este é o maior comprimento que atende as condições dadas?
- Que estratégias foram utilizadas para chegar à resposta?

Conclui-se que o cordão de 210 cm rende 7 pedaços de 30 cm e o cordão de 330 cm rende 11 pedaços de 30 cm. Assim, como $(210, 330) = 30$ e esse é o maior comprimento possível dos pedaços.

Exposição do conceito e algoritmo

Após a socialização do problema motivador, o professor deve realizar a formalização do conteúdo que está por trás da situação apresentada. Nesse momento, é fundamental retomar os conhecimentos prévios dos estudantes acerca do conceito do mdc, discutindo a

noção de divisores comuns e a importância de identificar o maior entre eles. Introduz-se a definição do mdc e em seguida, o professor deverá apresentar e exemplificar diferentes métodos para o cálculo do mdc, a fim de oferecer aos alunos um repertório diversificado de estratégias de resolução. Entre esses métodos, destacam-se: a listagem de divisores de cada número e a identificação do maior divisor comum, a decomposição dos números em fatores primos e a utilização dos fatores comuns para determinar o mdc e o algoritmo de Euclides, cuja relevância vai além do cálculo imediato do mdc, uma vez que será útil no desenvolvimento posterior do estudo de equações diofantinas.

Generalização e aplicação

Após a sistematização do conteúdo, o professor deve propor problemas mais complexos de caráter olímpico, que explorem a aplicação do mdc em diferentes contextos. Espera-se que os estudantes consigam reconhecer situações em que o mdc é a ferramenta adequada de resolução, selecionando e aplicando a estratégia de cálculo mais eficiente. Essa experiência possibilita que generalizem o uso do mdc para problemas variados, promovendo o desenvolvimento do raciocínio lógico, da abstração matemática e da capacidade de aplicar os conceitos em situações novas e desafiadoras.

Questões referentes ao encontro 03 - máximo divisor comum

1. **OPEMAT - 1ª FASE:** O responsável pela organização das prateleiras de um supermercado estava muito pensativo. Ele precisava organizar 168 biscoitos de chocolate e 120 biscoitos de morango e gostaria de organizá-los de acordo com as regras 1 e 2 abaixo. Sabendo que o organizador utilizou a menor quantidade de prateleiras possível respeitando os critérios de organização abaixo, assinale a alternativa que indica a quantidade total de prateleiras utilizadas.
 1. Cada prateleira deve possuir quantidades iguais de biscoitos;
 2. Cada prateleira deve conter apenas um sabor de biscoito.

A) 5
B) 7
C) 10
D) 11
E) 12
2. **OBMEP - 1ª FASE:** Qual é o maior valor possível para o máximo divisor comum de dois números naturais cujo produto é 6000?

- A) 10
- B) 20
- C) 30
- D) 40
- E) 60

Encontro 03 - Mínimo múltiplo comum

Plano de Aula

Tema: Mínimo múltiplo comum (mmc)

Ano/Série: Ensino Médio

Tempo estimado: 1 aula (50 minutos)

Conteúdos

- Múltiplos de um número natural e identificação de múltiplos comuns;
- Mínimo múltiplo comum;
- Métodos de cálculo do mmc: listagem de múltiplos, decomposição em fatores primos, cálculo do mmc a partir do mdc.

Objetivos

- Compreender o conceito de mmc e suas aplicações em diferentes situações-problema;
- Conhecer e comparar diferentes métodos para o cálculo do mmc, avaliando suas vantagens e limitações;
- Desenvolver a habilidade de distinguir se um problema envolve mdc ou mmc;

Motivação

Utilizaremos problemas que podem remeter a situações do cotidiano e podem despertar a curiosidade dos estudantes. O objetivo é levá-los a refletir sobre a necessidade de encontrar um valor que satisfaça condições específicas em cada situação.

1. “Uma lâmpada pisca de 14 em 14 segundos e uma outra lâmpada pisca de 20 em 20 segundos. Um cronômetro zerado foi ligado exatamente quando essas lâmpadas piscam juntas. Se o cronômetro foi desligado na primeira vez em que as lâmpadas piscaram juntas novamente, que tempo ele marcou?” (14).

2. “Dois ciclistas correm numa pista circular e gastam respectivamente 30 segundos e 35 segundos para completar uma volta na pista. Eles partem no mesmo local e no mesmo instante. Após algum tempo, os dois atletas se encontram pela primeira vez no local de largada. Neste momento, o atleta mais veloz estará completando quantas voltas? E o menos veloz? Depois de quanto tempo da largada ocorrerá o encontro?” (14).

Em busca de soluções

Após a apresentação dos problemas motivadores, o professor organiza a socialização das ideias iniciais dos estudantes. Cada grupo ou dupla pode compartilhar as estratégias utilizadas, mesmo que não tenham chegado à resposta final. O objetivo é valorizar os diferentes caminhos de resolução e relembrar conceitos já vistos no ensino fundamental.

A seguir, apresentamos alguns questionamentos que podem orientar a discussão:

- Como vocês pensaram em resolver o problema?
- Que estratégia usaram para encontrar o tempo ou a quantidade de voltas em que os eventos coincidem?
- Listar os múltiplos é sempre eficiente? Em quais situações pode ser pouco prático?
- Existe uma forma de garantir que o valor encontrado é realmente o menor múltiplo comum?
- O que diferencia um problema de mmc de um de mdc?

Durante a discussão, é possível perceber que alguns estudantes tenham recorrido à listagem de múltiplos para resolver os problemas. Nesse caso, o professor pode estimular a reflexão sobre as limitações desse método, mostrando que, embora válido em situações simples, ele se torna pouco prático quando os números envolvidos são maiores ou quando o mínimo múltiplo comum está mais distante na sequência.

Exposição do conceito e algoritmo

O professor deve conduzir a formalização do conteúdo, iniciando com a listagem de múltiplos como estratégia para encontrar o mmc, evidenciando que, embora funcione para números pequenos, esse método se torna pouco eficiente para números maiores ou quando o menor múltiplo comum está distante das listas.

Em seguida, introduz-se a fatoração em primos como método mais eficiente para determinar o mmc. O professor deve destacar a relação com o mdc, permitindo que os estudantes percebam as diferenças entre os conceitos: no cálculo do mdc, consideram-se

apenas os fatores comuns aos números com os menores expoentes; já no cálculo do mmc, consideram-se todos os fatores que aparecem na fatoração de qualquer número, tomando os maiores expoentes. Essa distinção possibilita que os estudantes compreendam de maneira estruturada como os mesmos fatores podem ser combinados de formas diferentes para obter resultados distintos.

Por fim, o professor deve apresentar que, conhecendo previamente o mdc, é possível calcular o mmc de maneira mais eficiente, evidenciando a conexão entre os conceitos. Essa abordagem oferece uma visão integrada, preparando os alunos para aplicar o método em diversos problemas. Além disso, é importante que o professor demonstre a consistência entre os métodos, mostrando que os resultados obtidos são equivalentes.

Generalização e aplicação

Na sequência, o professor apresenta problemas que envolvem o cálculo do mmc em diferentes contextos, incluindo situações em que o estudante precisa determinar valores ou intervalos que satisfaçam condições de múltiplos comuns. Espera-se que os alunos reconheçam quando o mmc é a ferramenta adequada, relacionando-o ao mdc previamente calculado, e que apliquem estratégias eficientes, como a fatoração em primos e a análise de expoentes. Essa generalização permite que compreendam a estrutura do mmc para valores genéricos, consolidando a conexão entre mdc e mmc e promovendo o desenvolvimento do raciocínio lógico, da abstração matemática e da capacidade de resolver problemas.

Questões referentes ao encontro 03 - Mínimo Múltiplo Comum

1. **OPEMAT - 1ª FASE:** Para quantos valores de k , o número 12^{12} é o mínimo múltiplo comum de 6^6 , 8^8 e k ?
 - A) 6
 - B) 8
 - C) 12
 - D) 24
 - E) 25
2. **OPEMAT - 2ª FASE:** Na terra de π -raia, um observador registrou que um cometa X e um cometa Y poderiam ser vistos a cada período de 76 e y anos, respectivamente. Sabendo que este ano os dois cometas foram vistos juntos e que a próxima vez que eles serão vistos juntos novamente ocorre daqui a 684 anos, responda os seguintes itens.
 - a) Quantas vezes os cometas serão vistos juntos durante os próximos 13.000 anos?

- b) Determine todos os possíveis valores para y .

Avaliação do encontro

A avaliação deste encontro busca compreender o aprendizado dos estudantes, valorizando o processo de construção do conhecimento em torno dos conceitos do mdc e do mmc. Para isso, os alunos devem registrar e descrever suas soluções para os problemas propostos, destacando os métodos utilizados, os raciocínios adotados e as dificuldades encontradas.

Essa prática possibilita ao professor analisar não apenas a correção das respostas, mas também a clareza, a organização e o rigor da escrita matemática. Ao mesmo tempo, os estudantes são incentivados a refletir sobre os conceitos trabalhados, relacionando situações concretas e contextualizadas com as definições formais. Assim, a avaliação vai além da verificação de respostas, pois permite que o estudante reconheça avanços e dificuldades, e oferece ao professor elementos para planejar intervenções e aprofundamentos nas aulas seguintes.

4.3.4 Encontro 04 - Equações Diofantinas

Plano de aula

Público-alvo: ensino médio.

Tema: equações diofantinas.

Quantidade de aulas/horas: 2 aulas / 1h40.

Conteúdos

- Equações diofantinas lineares do tipo $ax + by = c$.
- Critério de existência de soluções inteiras a partir do mdc.
- Solução particular e solução geral.

Objetivos

- Compreender a forma geral das equações diofantinas lineares do tipo $ax + by = c$.
- Identificar a condição de existência de soluções inteiras a partir do mdc.
- Determinar soluções particulares e expressar a solução geral.

Motivação 01: jogo da escova adaptado para equações diofantinas

Para introduzir o estudo das equações diofantinas lineares do tipo $ax + by = c$, faremos o uso de uma adaptação do tradicional jogo de cartas “Escova”, conhecida como *Escova Diofantina* (18). O objetivo deste jogo é permitir que os estudantes, de forma lúdica, explorem a existência de soluções de uma equação diofantina.

Regras:

Número de jogadores: 4 participantes.

1. O jogo possui 36 cartas numeradas de 2 a 10, sendo 4 cartas de cada. Embaralhe as cartas e distribua 3 cartas para cada jogador.
2. Pegue 4 cartas e coloque-as no centro da mesa com as faces visíveis para todos. O monte restante deve ser deixado de lado com as faces voltadas para baixo.
3. O primeiro jogador deve procurar cartas em sua mão que, somadas com as cartas da mesa, totalizem 15, o que é chamado de *escova diofantina*. Podem ser utilizadas no máximo dois números diferentes da mão do jogador. Isso significa que o jogador pode usar duas ou três cartas da sua mão, desde que sejam iguais. **Exemplo:** duas cartas de número 6 e uma carta de número 3.
4. O jogador coloca à sua frente as cartas que pegou da mesa, assim como a carta da sua mão que permitiu a soma 15, com a face voltada para baixo. Caso não consiga pegar nenhuma carta da mesa, deve simplesmente descartar na mesa uma das cartas de sua mão.
5. Quando os jogadores tiverem utilizado suas 3 cartas, uma nova mão de 3 cartas é distribuída, utilizando o monte que havia sido posto de lado inicialmente.
A partida prossegue da mesma maneira até que as cartas terminem.
6. Cada *escova diofantina* vale 1 ponto.
7. Vence a partida a dupla que alcançar o maior número de pontos.

Objetivos

O jogo trabalha com equações diofantinas elementares do tipo $ax + by = 15$, em que a e b representam os valores das cartas escolhidas e note que x e y são as quantidades utilizadas de cada uma. Assim cada jogada bem sucedida representa a resolução da equação. O jogo naturalmente conduz à investigação de:

1. Condições para que haja solução em números inteiros não negativos, discutindo a relação com $\text{mdc}(a, b)$.

2. Multiplicidade de soluções para um mesmo alvo.
3. Estratégias para maximizar a pontuação com base nas possibilidades de solução.

Em busca de soluções

A dinâmica do jogo promove a participação ativa dos estudantes e estimula a busca por combinações numéricas viáveis, criando um ambiente propício para a transição entre a resolução empírica de problemas e a formalização algébrica. Além disso, a restrição de ao máximo dois valores distintos simplifica a situação de jogo, evitando que rodadas se prolonguem excessivamente sem ação. Esta limitação também favorece a análise matemática, permitindo conexões diretas com o conteúdo de equações diofantinas.

Antes de apresentarmos o quadro com as soluções, é importante destacar o papel do jogo em sala de aula. A proposta é que todos os estudantes participem ativamente, buscando a maior quantidade possível de soluções da equação diofantina $ax + by = 15$, a partir das combinações possíveis com as cartas. Durante esse processo, também é relevante analisar os casos em que não há solução viável, seja por limitação no número de cartas disponíveis ou pela impossibilidade de se alcançar a soma desejada com determinados valores de a e b . Essa etapa permite levantar discussões importantes, como: até que ponto é possível prever, apenas observando as cartas em jogo, se uma determinada escolha poderá ou não resultar em solução?

Além disso, considerando que cada jogador tem inicialmente apenas três cartas na mão e quatro cartas dispostas na mesa, algumas escolhas de a e b se tornam inviáveis, tanto pela quantidade insuficiente de cartas quanto pelos valores necessários para atingir o resultado 15.

A seguir, destacamos alguns pares representativos de valores de a e b , correspondentes às cartas escolhidas pelos jogadores, de modo a evidenciar diferentes resultados possíveis ao definir tais valores.

Tabela 1 – Exemplos representativos de soluções da equação $ax + by = 15$

(a, b)	Soluções inteiras não negativas (x, y)
(1, 1)	(15, 0), (14, 1), ..., (1, 14), (0, 15)
(2, 3)	(6, 1), (3, 3), (0, 5)
(4, 7)	(2, 1)
(2, 4)	nenhuma

Alguns pares, como (2, 4), não apresentam solução. Essa observação será retomada em outro momento, quando discutiremos o papel do máximo divisor comum no que diz respeito a soluções de equações diofantinas.

Após a exploração prática do jogo *Escova Diofantina*, podemos propor aos estudantes uma discussão sobre a percepção de facilidade ou dificuldade em encontrar combinações. Alguns questionamentos podem ser levantados, como:

- Das soluções encontradas quais foram mais fáceis de perceber e quais exigiram mais atenção?
- Quais pares (a, b) que possuem maior número de soluções?
- Como a presença ou ausência da carta 1 influencia a jogada?

Essa atividade também permite discutir conceitos algébricos, como a existência de soluções inteiras não negativas, relacionando-se com o $\text{mdc}(a, b)$. Quando $\text{mdc}(a, b) = 1$, sempre existe pelo menos uma solução inteira para a equação diofantina. O número 1 é justamente o caso que garante que o mdc com qualquer outro valor seja 1, ampliando as possibilidades de soluções em comparação com pares de valores maiores.

Após serem feitas as discussões, o estudante poderá perceber que o número 1 tem um papel especial, pois permite complementar qualquer outro valor para atingir o alvo 15. Porém, sua presença não garante sucesso, pois depende da quantidade de cartas disponíveis na mão e na mesa. Essa reflexão permite que os estudantes percebam como a estrutura do conjunto de cartas influencia as soluções possíveis e a estratégia do jogo.

Dessa forma, o jogo não apenas favorece a prática experimental com números, mas também conduz os estudantes a compreender propriedades fundamentais das equações diofantinas, como a importância do mdc e a existência ou não de soluções inteiras.

Motivação 02: equação diofantina em um caixa eletrônico

Para ilustrar a aplicação de equações diofantinas lineares com coeficientes fixos, Imaginemos a seguinte situação prática: uma pessoa vai a um caixa eletrônico que só dispõe de cédulas de 20 e 50 reais. De quantas formas ela pode sacar exatamente R\$ 500,00?

Em busca de soluções

O problema é modelado pela equação diofantina linear $20x + 50y = 500$, em que x = número de cédulas de R\$ 20,00 e y = número de cédulas de R\$ 50,00.

Espera-se que os estudantes encontrem algumas soluções inteiras não negativas, como ilustrado na tabela a seguir:

Tabela 2 – Soluções inteiras não negativas para $2x + 5y = 50$

Cédulas de R\$ 20,00 (x)	Cédulas de R\$ 50,00 (y)	Valor Total
25	0	R\$ 500,00
20	2	R\$ 500,00
15	4	R\$ 500,00
10	6	R\$ 500,00
5	8	R\$ 500,00
0	10	R\$ 500,00

Com a participação dos estudantes, espera-se que o máximo de soluções seja apresentado e que eles socializem suas estratégias. A intenção é que percebam o padrão aritmético presente: a cada aumento de 2 cédulas de R\$50,00, o número de cédulas de R\$20,00 diminui em 5 unidades, mantendo o total de R\$500,00. Esse reconhecimento permite que, mesmo com poucas soluções iniciais, os estudantes consigam generalizar e determinar todas as demais soluções.

Para ampliar a compreensão dos estudantes acerca das soluções da equação diofantina $20x + 50y = 500$, propõe-se o uso do software GeoGebra (19). A representação gráfica dessa equação permite visualizar a reta correspondente no plano cartesiano e destacar os pontos de coordenadas inteiras que a satisfazem.

Para tal, é possível que o usuário altere apenas o valor total a ser sacado, isto é, o termo constante c na equação $50x + 20y = c$. Embora as cédulas disponíveis permaneçam fixas, a variação de c torna possível investigar diferentes cenários e analisar para quais valores existem soluções inteiras não negativas. A exploração visual apresenta a presença ou ausência de pontos inteiros sobre a reta indicando a existência ou não de soluções.

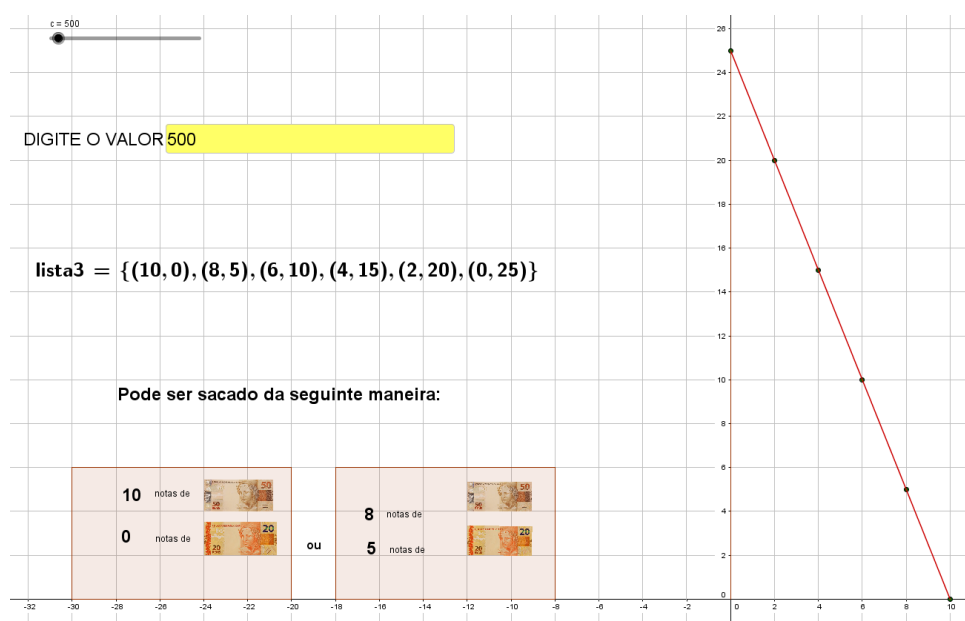


Figura 2 – Simulação da equação diofantina do caixa eletrônico no GeoGebra.

O recurso está disponível no GeoGebra Materiais (20), permitindo que professores e estudantes explorem livremente as representações propostas.

A escolha de uma situação próxima ao cotidiano busca facilitar a compreensão da utilidade das equações diofantinas na resolução de problemas reais. A partir dessa exploração inicial, o professor pode avançar para a formalização do método de resolução das equações diofantinas lineares, destacando a condição de existência das soluções e a obtenção da solução geral.

Exposição do conceito e algoritmo

Após a exploração das atividades práticas, é recomendável que o professor registre no quadro as soluções apresentadas pelos alunos, correspondentes a cada equação diofantina encontrada. Esses registros evidenciam as diferentes combinações possíveis e também os casos em que não há solução, servindo como base para introduzir a condição de existência de soluções inteiras, por meio do cálculo do mdc.

Em seguida, deve-se apresentar o conceito de solução particular, ou seja, uma solução específica que satisfaz a equação, e mostrar como construir a solução geral. A partir desse ponto, torna-se possível determinar as soluções que atendam às condições propostas, tanto nos inteiros quanto nos números naturais.

Dessa maneira, a formalização consolida o aprendizado, conectando as atividades práticas à compreensão teórica das equações diofantinas, permitindo que os estudantes percebam de forma clara a relação entre o mdc, a existência de soluções e a construção das soluções particulares ou gerais.

Generalização e aplicação

Os estudantes devem perceber que o método aprendido para resolver equações diofantinas lineares é geral e pode ser aplicado em diferentes situações; compreender a relação entre o mdc, a solução particular e a construção da solução geral permitem identificar rapidamente a existência de soluções e determinar todas as combinações possíveis. Além disso, a análise de padrões nas soluções auxilia na resolução de problemas. Um aspecto importante dessa generalização é a autonomia do estudante em construir a equação diofantina, pois nem sempre ela é apresentada pronta no problema, sendo necessário ler, interpretar e modelar a situação antes de aplicar a estratégia de resolução para determinar soluções.

Questões referentes ao encontro 04 - equações diofantinas

1. **OBMEP - 1ª FASE:** Os números a e b são inteiros positivos tais que $\frac{a}{11} + \frac{b}{3} = \frac{31}{33}$. Qual é o valor de $a + b$?

A) 5
B) 7
C) 14
D) 20
E) 31
2. **OBMEP - 1ª FASE:** De quantas maneiras podemos trocar uma nota de R\$ 20,00 por moedas de R\$ 0,10 e R\$ 0,25?

A) 21
B) 36
C) 38
D) 41
E) 56
3. **TM² - 1ª FASE:** Beatriz tem em seu bolso 33 moedas, algumas de 25 centavos e outras de 10 centavos. Sabendo que Luíze tem ao todo uma quantidade inteira de reais, quantas moedas de 25 centavos ela possui?

A) 16
B) 17
C) 18
D) 19
E) Não é possível determinar.

Avaliação do Encontro

Para consolidar o aprendizado e fixar o método de resolução de equações diofantinas lineares, propõe-se que cada estudante construa um esquema indicando o passo a passo do procedimento para a resolução de uma equação diofantina proposta por ele e que possua solução. O esquema deve incluir, de forma objetiva: identificação dos coeficientes, cálculo do mdc, verificação da existência de soluções e determinação de uma solução particular e construção da solução geral.

Essa atividade permite que o professor observe se os estudantes compreenderam o método, analisando se aprenderam a sequência de passos necessária para resolver qualquer equação diofantina linear. Ao final, cada aluno terá um material próprio que sintetiza o procedimento, servindo como referência para futuras aplicações.

4.3.5 Encontro 05 - Números Primos

Plano de aula

Público-alvo: ensino médio.

Tema: números primos.

Quantidade de aulas/horas: 2 aulas / 1h40.

Conteúdos

- Conceito de números primos e compostos;
- Crivo de Eratóstenes e teste de primalidade;
- Teorema fundamental da aritmética;
- Divisores de um número.

Objetivos

- Compreender o conceito de números primos e compostos;
- Investigar se determinado número é primo por meio do Crivo de Eratóstenes e de testes de primalidade;
- Realizar a fatoração única de números inteiros;
- Determinar os divisores de um número a partir da fatoração, incluindo a quantidade de divisores.

Motivação 01

Inicia-se o encontro com questionamentos investigativos:

- Quais números primos são facilmente lembrados?
- Como verificar se números como 91 ou 97 são primos?

Essas questões têm como finalidade despertar a curiosidade e evidenciar a necessidade de métodos sistemáticos para o reconhecimento dos números primos.

Motivação 02: construção do Crivo de Eratóstenes

Quantos primos existem entre 2 e 100? Como podemos listá-los de maneira prática e confiável?

Para investigar todos os primos de 2 a 100, distribui-se uma tabela contendo os números de 2 a 100, disponível no apêndice E. A atividade consiste em:

1. Comece com o menor número primo: 2. Risque todos os múltiplos de 2, exceto o próprio 2.
2. Passe para o próximo número que ainda não foi riscado. Risque todos os múltiplos deste número, exceto o próprio número.
3. Repita o processo com o próximo número não riscado e assim por diante, até que todos os números na tabela tenham sido analisados.

Os números que permanecerem sem riscar são os números primos.

Em busca de soluções

Após a realização da atividade, propõem-se reflexões para proporcionar a compreensão do conceito de número primo e do funcionamento do crivo de Eratóstenes:

- Quais números sobraram?
- Por que o número 1 não é considerado primo?
- Por que não precisamos continuar com múltiplos de números maiores, como 11, para determinar todos os primos até 100?

A discussão permite que os estudantes percebam a eficiência do método e reforcem a definição formal de número primo, observando o motivo pelo qual 1 não é considerado primo.

Em seguida, propõe-se analisar o número 211. Para verificar se é primo, discute-se se seria necessário testar todos os divisores menores que 211 e espera-se que os estudantes percebam que basta verificar a divisibilidade pelos números primos menores ou iguais a $\sqrt{211} \approx 14,5$, ou seja, 2, 3, 5, 7, 11, 13. Como nenhum deles divide 211, conclui-se que 211 é um número primo.

O vídeo *Crivo de Eratóstenes* (21) pode ser compartilhado com os estudantes para reforçar a atividade ou utilizado como material de apoio para o planejamento da aula pelo professor.

Exposição do conceito e algoritmo

Na exposição do conteúdo deve ser consolidada a compreensão de números primos e compostos, destacando que todo número composto pode ser decomposto como produto de números menores. Em seguida, apresenta-se o Teorema Fundamental da Aritmética, que garante que cada número natural maior que 1 possui uma fatoração única em primos, independentemente da ordem dos fatores. Para evidenciar essa unicidade, pode-se solicitar que os estudantes realizem a fatoração de um número no quadro, registrando as diferentes decomposições possíveis e observando que todas coincidem.

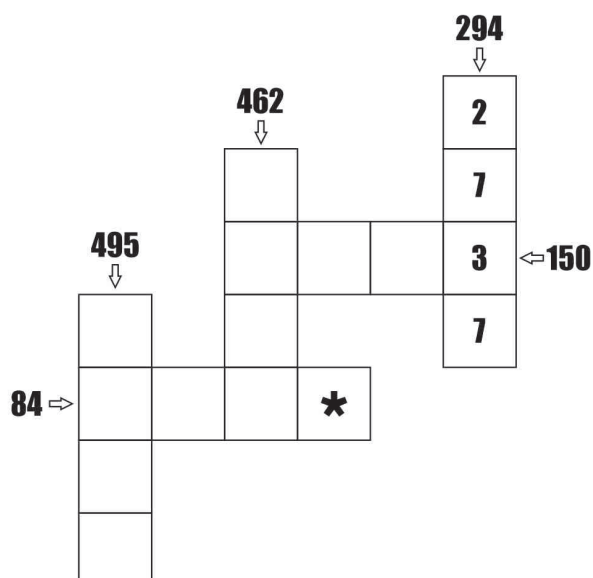
A partir da fatoração, introduzem-se os conceitos de divisores de um número e a contagem de todos os divisores positivos. Cada divisor pode ser expresso como um produto de primos, cujos expoentes variam de zero até o valor correspondente na fatoração, permitindo determinar todas as combinações possíveis. Ressalta-se que o conhecimento desses conceitos é fundamental para o desenvolvimento do raciocínio lógico e da capacidade de generalização.

Generalização e aplicação

Propõem-se problemas envolvendo números primos, fatoração e divisores, nos quais os estudantes aplicam os conceitos aprendidos para verificar se um número é primo, realizam sua fatoração ou calculam seus divisores. Essas atividades consolidam o conteúdo e mostram a utilidade prática dos conceitos.

Questões referentes ao encontro 05 - Números Primos

1. **OBMEP - 1ª FASE:** As casas da figura abaixo devem ser preenchidas com números primos. Em cada linha ou coluna, o produto dos números deve ser igual ao número indicado pela seta. A coluna indicada por 294 já está preenchida. Qual é o número que deve ser escrito na casa marcada com *?



- A) 2
B) 3
C) 5
D) 7
E) 11

2. **OBMEP - 1ª FASE:** Mariana escreveu as decomposições em fatores primos dos números naturais de 2 a 100:

$$2, 3, 2 \times 2, 5, 2 \times 3, \dots, 3 \times 3 \times 11, 2 \times 2 \times 5 \times 5.$$

Quantas vezes ela escreveu o algarismo 2?

- A) 99
B) 104
C) 152
D) 188
E) 191

3. **OPEMAT - 1ª FASE:** Seja n um número inteiro positivo. Defina o número n^* por

$$n^* = (n-1) \cdot (n-2) \cdot (n-3) \cdots 3 \cdot 2 \cdot 1.$$

Por exemplo,

$$6^* = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120.$$

Dentre as alternativas abaixo, podemos concluir que o número de divisores primos distintos do número 21^* é:

- A) 2
- B) 8
- C) 10
- D) 11
- E) 21

4. **TM² - 1ª FASE:** Seja n o menor natural que possui exatamente 35 divisores positivos. Determine a quantidade de divisores positivos de $n - 1$.

- A) 2
- B) 4
- C) 7
- D) 12
- E) 14

Avaliação do encontro

Ao final do encontro, propõe-se uma reflexão sobre a importância dos números primos na sociedade, especialmente em áreas como criptografia e segurança digital. Os estudantes podem discutir a necessidade de compreender os números primos, a dificuldade de identificar primos muito grandes e a aplicabilidade prática desse conhecimento em contextos cotidianos. Sugere-se, ainda, a exibição do vídeo **Como números primos te protegem na internet** (22), que apresenta uma aplicação, reforçando o valor do conteúdo estudado.

4.3.6 Encontro 06 - Congruências

Plano de aula

Público-alvo: ensino médio.

Tema: congruência

Quantidade de aulas/horas: 2 aulas / 1h40.

Conteúdos

- Conceito de congruência e notação;
- Propriedades da congruência;
- Operações com congruências;
- Sistema completo de resíduos e inverso multiplicativo.

Objetivos

- Compreender o conceito de congruência modular e a notação associada;
- Reconhecer e aplicar as propriedades da congruência em operações aritméticas;
- Resolver problemas de congruência, como determinação de restos, algarismos e condições de divisibilidade.

Motivação - dinâmica de formação de grupos

Os estudantes serão recebidos com um bombom, ao qual estará associado um número, que será utilizado na dinâmica inicial da aula. Em uma turma de 20 alunos, os números variam de 1 a 20, caso o número de estudantes seja diferente, o intervalo deve ser ajustado de acordo com a quantidade de participantes. Essa ação busca acolher os estudantes e preparar a turma para explorar o conteúdo da aula.

O professor deverá determinar, na sala, regiões que representarão os restos de 0 até 5. Inicialmente, os estudantes deverão realizar mentalmente a divisão de seu número por 6, identificar o resto e se posicionar na região correspondente, observando os colegas e os números que ficaram próximos. Em seguida, deverão realizar uma nova divisão por 5 e, seguindo as mesmas orientações, se reorganizem nas regiões de 0 até 4, novamente observando os integrantes e os números que deram origem ao grupo. Por fim, os estudantes realizarão a divisão por 4, organizando os grupos para o trabalho em sala.

A dinâmica permite perceber como pequenas alterações no divisor influenciam a composição dos grupos, evidenciando classes de números com propriedades comuns. Além disso, favorece a discussão acerca do tema das congruências modulares, promovendo uma aprendizagem significativa.

Em busca de soluções

Após a realização da dinâmica para a formação de grupos, o professor deve realizar questionamentos pontuais com o objetivo de introduzir a ideia de congruência modular, dentre os quais destacam-se:

- Quais números estavam no mesmo grupo após a divisão? Por que esses números caíram juntos no mesmo grupo?
- Quais mudanças ocorreram na composição dos grupos à medida que o divisor foi alterado?
- Se realizássemos a divisão por 5 e 10, haveria pessoas que se encontrariam no mesmo grupo?

Após a discussão inicial sobre os aspectos que envolvem congruência na formação dos grupos, podem ser propostos questionamentos motivadores que associem a aritmética modular à realidade cotidiana dos estudantes, estimulando-os a reconhecer a aplicabilidade do conceito em situações práticas. Alguns exemplos incluem:

- Determinar o horário no relógio analógico a partir de um horário observado em um celular. Se são 22h no celular, que horas serão no relógio analógico?
- Calcular os horários de doses subsequentes de um medicamento tomado a cada seis horas. Se a primeira dose foi administrada às 19h, qual será o horário da próxima dose?
- Identificar o dia da semana após um determinado número de dias. Se hoje é quinta-feira e um encontro ocorrerá daqui a 40 dias, em qual dia da semana ele acontecerá?

Esses questionamentos contribuem para que os estudantes compreendam que a aritmética modular é aplicável em diversos contextos do dia a dia, reforçando a relevância do tema para a resolução de problemas matemáticos.

Exposição do conceito e algoritmo

Nesta etapa, o professor deve apresentar o conceito de congruência, explicando o que significa dizer que dois números são congruentes módulo m . Relacionando com a dinâmica inicial, isso equivale a dizer que dois números são congruentes se o resto da divisão desses números por m for o mesmo. Além disso, deve-se apresentar a notação que representa dois números congruentes e enfatizar a relação entre congruência e divisibilidade, destacando que, se $a \equiv b \pmod{m}$, então $m \mid (b - a)$. É importante evidenciar que a congruência modular constitui uma relação de equivalência, apresentando suas propriedades reflexiva, simétrica e transitiva, bem como as propriedades operatórias de adição, multiplicação e potenciação. Em seguida, podem ser discutidos o sistema completo de resíduos e o conceito de inverso multiplicativo, elementos fundamentais para a resolução de problemas.

Durante toda a apresentação do conteúdo, é essencial que o professor utilize exemplos numéricos para facilitar a compreensão do estudante, proporcionando uma aprendizagem significativa. Merecem destaque exemplos clássicos, como a determinação do resto da divisão de alguns números, a identificação do algarismo das unidades em determinados casos e a análise de condições que garantem a divisibilidade de certas expressões numéricas.

Generalização e aplicação

A partir das atividades realizadas, dos exemplos analisados e da formalização do conteúdo, os estudantes são convidados a aplicar os conceitos de congruência modular em novas situações, resolvendo problemas e identificando padrões. Essa prática permite consolidar a compreensão dos conceitos estudados e desenvolver autonomia na resolução de questões.

Questões referentes ao encontro 06 - congruência

Os estudantes realizarão a atividade conforme os grupos previamente formados de acordo com o resto da divisão de seus números. Cada grupo se reúne em uma mesa identificada com o número do seu resto e, dentro de cada grupo, os alunos sorteiam papéis correspondentes a funções específicas, que visam garantir a participação colaborativa e a organização da atividade:

1. **Facilitador:** conduz a leitura e a discussão da tarefa no grupo.
2. **Harmonizador:** assegura a participação equilibrada de todos os integrantes.
3. **Monitor de recursos:** organiza os materiais e solicita apoio ao professor quando necessário.
4. **Repórter:** registra e apresenta as conclusões do grupo.
5. **Controlador do tempo:** informa os colegas sobre o tempo disponível.

Essa distribuição de funções busca promover a colaboração e assegurar que todos os alunos participem ativamente da resolução do problema.

Cada grupo recebe uma questão diferente relacionada ao tema da congruência modular. Com aproximadamente 10 minutos para a resolução, os estudantes elaboram estratégias em conjunto e registram suas conclusões em cartolina. Durante a atividade, cada integrante desempenha a função sorteada, assegurando a participação colaborativa. Ao final, o repórter apresenta a solução do grupo, promovendo a socialização das diferentes abordagens. Essa dinâmica fortalece a compreensão da congruência modular e amplia a capacidade de aplicação do conceito em novos problemas.

1. **OBMEP - 1ª FASE:** Qual é o resto da divisão de $1 \times 2 \times 3 \times 4 \times \dots \times 2011 + 21$ por 8?
 - A) 2
 - B) 3

- C) 5
D) 6
E) 7

2. **OBMEP - 1ª FASE:** Qual é o algarismo das dezenas da soma

$$\underbrace{7}_{\text{um sete}} + \underbrace{77}_{\text{dois setes}} + \underbrace{777}_{\text{três setes}} + \underbrace{7777}_{\text{quatro setes}} + \cdots + \underbrace{777 \cdots 77}_{\text{setenta e seis setes}} + \underbrace{777 \cdots 777}_{\text{setenta e sete setes}} ?$$

- A) 5
B) 6
C) 7
D) 8
E) 9

3. **OPEMAT - 1ª FASE:** O cadastro de pessoa física (CPF) é um documento de identificação usado pela receita federal que consiste de onze dígitos sendo os nove primeiros fornecidos pela receita federal e os dois últimos, chamados dígitos verificadores, calculados da seguinte forma: se $d_1 d_2 d_3 d_4 d_5 d_6 d_7 d_8 d_9$ são os nove primeiros dígitos do CPF fornecido, então calculamos

$$A = 10d_1 + 9d_2 + 8d_3 + 7d_4 + 6d_5 + 5d_6 + 4d_7 + 3d_8 + 2d_9,$$

e calculamos r , onde r é o resto da divisão de A por 11. Se o resto for 0 ou 1 então o décimo dígito d_{10} será 0. Caso contrário d_{10} será $11 - r$. Para calcular o décimo primeiro dígito, calculamos

$$B = 10d_2 + 9d_3 + 8d_4 + 7d_5 + 6d_6 + 5d_7 + 4d_8 + 3d_9 + 2d_{10},$$

e calculamos R , onde R é o resto da divisão de B por 11. Se $R = 0$ ou $R = 1$ então $d_{11} = 0$. Caso contrário, $d_{11} = 11 - R$. Se uma pessoa tem os nove primeiros dígitos de seu CPF dados por 299792458, os dígitos d_{10} e d_{11} são respectivamente:

- A) 1 e 8
B) 0 e 7
C) 2 e 6
D) 0 e 8
E) 3 e 5

4. **OPEMAT - 1ª FASE:** Uma determinada loja de livros de matemática resolveu fazer uma promoção que proporcionava 35% de desconto nos livros. Para obter o desconto, os clientes precisavam usar um cupom com um número de seis dígitos dado por $80AB35$ que é múltiplo de 99, e assim precisavam descobrir os valores de A e B . Assinale a alternativa abaixo que contém um possível valor de A .

- A) 2
- B) 5
- C) 7
- D) 8
- E) 9

Avaliação e reflexão

O encontro se encerra com uma atividade avaliativa coletiva, na qual os estudantes compartilham suas experiências e refletem sobre o trabalho em grupo, destacando pontos fortes e dificuldades enfrentadas.

Esse momento de socialização favorece a consolidação da aprendizagem, promove a construção coletiva do conhecimento e fortalece o engajamento e a cooperação entre os colegas.

4.3.7 Encontro 07 - Teorema chinês dos restos

Plano de aula

Público-alvo: ensino médio.

Tema: sistema de congruências - teorema chinês dos restos.

Quantidade de aulas/horas: 2 aulas / 1h40.

Conteúdos

- Sistemas de congruências;
- Teorema chinês dos restos (TCR);
- Padrões numéricos e solução geral.

Objetivos

- Compreender e representar sistemas de congruências a partir de problemas contextuais.

- Resolver sistemas de congruências por substituição ou pelo Teorema Chinês dos Restos.
- Identificar padrões numéricos e compreender a solução geral de um sistema.

Motivação 01 - desafio do número secreto

O professor convida um estudante para pensar em um número natural menor que 30. Em seguida, pede que divida esse número por 3 e por 5, anotando os restos. O estudante informa apenas os restos ao professor e à turma. O desafio consiste em adivinhar o número escolhido pelo estudante.

Em busca de soluções

Lançado o desafio para a turma, o professor deverá instigar os estudantes a desenvolverem estratégias para a resolução do problema.

- Como podemos descobrir o número a partir dos restos?
- Existe sempre um número que satisfaça essas condições?
- Pode haver mais de uma solução? Ou nenhuma solução?

Seria interessante que os estudantes registrassem o problema por meio de duas congruências modulares. Assim, o professor poderia mostrar que esse simples problema representa um sistema de equações.

Para aumentar o desafio, sugere-se a apresentação de um problema clássico:

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

Os estudantes são incentivados a investigar por meio de tentativa e erro. Ao obter a solução, o professor propõe novos questionamentos para estimular a reflexão:

- E se quisermos descobrir um número maior que 1000 e menor que 1200 que satisfaça as mesmas condições?
- Seria fácil continuar listando todos os números?
- Conseguem perceber algum padrão e prever qual seria o número?

Esses questionamentos evidenciam a necessidade de um método geral e eficiente para a resolução de sistemas de congruências.

Exposição do conceito e algoritmo

Após a resolução dos problemas motivadores, o professor deve conduzir a formalização do conteúdo, retomando os problemas apresentados e mostrando que eles representam sistemas de congruências. É importante esclarecer o que significa solucionar um sistema, ou seja, identificar o número que satisfaz todas as condições simultaneamente.

O professor deve apresentar duas estratégias principais de resolução: a substituição e a aplicação do teorema chinês dos restos, enfatizando o raciocínio por trás das soluções e preparando os estudantes para aplicar os conceitos em novas situações.

Generalização e Aplicação

O professor pode propor problemas contextualizados que possam ser modelados por sistemas de congruências. Ao conduzir os estudantes na identificação das congruências correspondentes e na resolução do sistema, promove-se a aplicação prática dos conceitos aprendidos.

Dessa forma, os estudantes têm a oportunidade de consolidar a compreensão do conteúdo, observando como os princípios do Teorema Chinês dos Restos e da resolução por substituição se aplicam a situações concretas. Em seguida, cada estudante deve resolver individualmente ou em grupo os problemas propostos para o encontro, reforçando a autonomia na aplicação dos conceitos.

Questões referentes ao encontro 07 - Teorema Chinês dos Restos

1. **OPEMAT – 2ª FASE:** Um general deseja verificar o número de soldados em um de seus pelotões. Então, mandou que os soldados formassem alinhados de 9 em 9 e verificou que sobraram 2 soldados. Em seguida, ordenou que formassem alinhados de 11 em 11 e verificou que sobraram 4. Finalmente, fez os soldados se alinharem de 13 em 13 e sobraram 8. Sabendo que o pelotão tem entre dois mil e três mil soldados, determine quantos soldados sobraram quando o general os mandou formar de 100 em 100.
2. **ENQ:** A Secretaria de Educação de um município recebeu uma certa quantidade de livros para distribuir entre as escolas do município. Sabe-se que a quantidade é superior a 1000, inferior a 2000, que se dividí-los entre 7 escolas, sobram 4, entre 9 sobram 2 e entre 13 sobram 6. Encontre a quantidade de livros.
3. **ENQ:** Em uma cesta contendo ovos, na contagem de dois em dois, de três em três, de quatro em quatro e de cinco em cinco, sobram 1, 2, 3 e 4 ovos, respectivamente. Qual é a menor quantidade de ovos que a cesta pode ter?

Avaliação e reflexão

Ao final da resolução das atividades, os estudantes são convidados a socializar suas soluções, apresentando no quadro e discutindo coletivamente os caminhos percorridos. Esse momento de partilha valoriza a diversidade de estratégias e permite que a turma reconheça as conexões entre os conceitos estudados.

Como encerramento do minicurso, realiza-se uma roda de conversa avaliativa, na qual os estudantes são convidados a refletir sobre sua trajetória de aprendizagem. O professor pode orientar a discussão a partir das seguintes questões:

- Qual conteúdo ou atividade você considerou mais interessante ou marcante durante o minicurso?
- Quais estratégias de resolução foram mais fáceis de compreender e aplicar?
- Quais conteúdos ou atividades apresentaram maior dificuldade?
- De que forma essa experiência pode contribuir para sua preparação para as olimpíadas de matemática?
- Como você se sentiria diante de problemas semelhantes em provas olímpicas?
- Quais habilidades você acredita ter desenvolvido ao longo dos encontros: lógica, criatividade, percepção de padrões, argumentação matemática, comunicação matemática ou outras?

Esse momento final de avaliação e reflexão busca consolidar a aprendizagem, valorizar o esforço coletivo e estimular os estudantes a perceberem sua evolução, fortalecendo a confiança e interesse para enfrentar novos desafios.

Conclusão

Esta dissertação teve como objetivo identificar fundamentos teóricos e atividades que pudessem compor uma sequência didática de aritmética voltada à preparação de estudantes para olimpíadas de matemática. Observa-se que, em muitas escolas públicas, a preparação específica para essas competições não costuma integrar o planejamento curricular regular, o que reforça a necessidade do uso de materiais que apoiem esse tipo de iniciativa.

Foram revisados e organizados conceitos aritméticos essenciais presentes em provas olímpicas, tais como divisibilidade, sistemas de numeração, máximo divisor comum, mínimo múltiplo comum, equações diofantinas, números primos, congruências e o teorema chinês dos restos. A análise de questões de edições anteriores permite identificar padrões estruturais, estratégias recorrentes de resolução e elementos característicos da linguagem dessas competições.

Com base nesse estudo, elaborou-se uma sequência didática destinada a apoiar o trabalho docente no ensino médio. Embora não tenha sido aplicada no contexto desta pesquisa, sua construção foi orientada por práticas comuns ao cotidiano da sala de aula e por observações recorrentes da atuação docente, favorecendo a organização progressiva das atividades e a coerência interna da proposta.

O material desenvolvido pode contribuir para ampliar o espaço da Aritmética no cotidiano escolar e apoiar iniciativas que promovam a resolução de problemas e o desenvolvimento do pensamento matemático. Trata-se de uma proposta flexível, que pode ser adaptada a diferentes contextos e integrada tanto a projetos específicos quanto às práticas regulares de sala de aula.

Como continuação desta investigação, recomenda-se a aplicação da sequência em turmas do ensino médio, a fim de analisar sua efetividade e identificar ajustes que aprimorem seu uso pedagógico. Essa etapa pode favorecer o aperfeiçoamento de práticas voltadas ao estudo de problemas desafiadores e à preparação para competições.

O trabalho realizado oferece um recurso que pode apoiar professores interessados em intensificar o estudo da aritmética e aproximar seus estudantes do universo das olimpíadas de matemática. Espera-se que essa proposta estimule oportunidades de aprendizagem que favoreçam o interesse dos estudantes e fortaleçam sua participação em atividades matemáticas desafiadoras.

Referências

- 1 BRASIL. *Base Nacional Comum Curricular: Educação Básica*. Brasília, DF: Ministério da Educação, 2017. Acesso em: 30 jun. 2025. Disponível em: <http://basenacionalcomum.mec.gov.br/>.
- 2 CNPq. *Olimpíadas Científicas*. 2020. <https://www.gov.br/cnpq/pt-br/assuntos/popularizacao-da-ciencia/olimpiadas-cientificas>. Acesso em: 06 novembro de 2025.
- 3 CNPq. *Olimpíadas Científicas e suas contribuições para o ensino e a alfabetização científica*. 2022. <https://www.gov.br/cnpq/pt-br/assuntos/noticias/cnpq-em-acao/olimpiadas-cientificas-e-suas-contribicoes-para-o-ensino-e-a-alfabetizacao-cientifica>. Acesso em: 06 novembro de 2025.
- 4 IMO. *International Mathematical Olympiad (IMO)*. 2025. <https://www.imo-official.org/>. Acesso em: 06 novembro de 2025.
- 5 OBM. *Olimpíada Internacional de Matemática (IMO) – OBM*. 2025. <https://www.obm.org.br/olimpiada-internacional-de-matematica/>. Acesso em: 06 novembro de 2025.
- 6 IMPA. *Olimpíadas de Matemática no IMPA*. 2025. <https://impa.br/acervo/imo2017/>. Acesso em: 06 novembro de 2025.
- 7 OBM. *A OBM — Quem Somos*. 2025. <https://www.obm.org.br/quem-somos/pagina-exemplo/>. Acesso em: 06 novembro de 2025.
- 8 OBMEP. *Em Números – 20ª OBMEP (2025)*. 2025. <http://www.obmep.org.br/em-numeros.htm>. Acesso em: 06 julho de 2025.
- 9 PERNAMBUCO, S. de Educação e Esportes de. *Currículo de Pernambuco: Ensino Fundamental – Anos Finais*. 2025. Acesso em: 30 jun. 2025. Disponível em: <https://portal.educacao.pe.gov.br/ensino-fundamental-anos-finais/>.
- 10 PERNAMBUCO, S. de Educação e Esportes de. *Currículo de Pernambuco: Ensino Médio*. 2025. Acesso em: 30 jun. 2025. Disponível em: <https://portal.educacao.pe.gov.br/ensino-medio-2/>.
- 11 HEFEZ, A. *Aritmética*. 3. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2022. (Coleção PROFMAT, COP 08). ISBN 978-85-8337-181-6.
- 12 HEFEZ, A. *Curso de Álgebra, Vol. 1*. 5. ed. Rio de Janeiro: Instituto Nacional de Matemática Pura e Aplicada (IMPA), 2013. 203 p. (Coleção Matemática Universitária). Inclui bibliografia. ISBN 978-85-244-0079-7.
- 13 DOMINGUES, H. H. *Fundamentos de Aritmética*. 1. ed. São Paulo: Atual Editora Ltda., 1991. Coleção Fundamentos da Matemática. ISBN 85-7056-342-6.
- 14 DUTENHEFNER, F.; CADAR, L. *Encontros de Aritmética*. Rio de Janeiro: IMPA, 2015. 121 p. Distribuição: IMPA/OBMEP. ISBN 978-85-244-0392-7.

- 15 POLYA, G. *A arte de resolver problemas: um novo aspecto do método matemático*. 2. ed. Rio de Janeiro: Interciência, 1995. Tradução de Heitor Lisboa de Araújo. 2^a reimpressão. 196 p.
- 16 ZABALA, A. *A prática educativa: como ensinar*. Porto Alegre: Artmed, 1998. Reimpressão 2010. ISBN 978-85-7307-426-0.
- 17 PANNUTI, M. R. V. Caminhos da prática pedagógica. *TVE Brasil*. Rio de Janeiro, p. 01–05, 2004.
- 18 MELLO, C. d.; PEREIRA, L. C. M.; RAINHA, M. L. d. S. Práticas de ensino na formação do futuro professor de matemática. *Revista Educação Pública*, v. 21, n. 3, 2021. ISSN 1984-6290. Disponível em: <<https://educacaopublica.cecierj.edu.br/artigos/21/3/praticas-de-ensino-na-formacao-do-futuro-professor-de-matematica>>.
- 19 GeoGebra. *GeoGebra: Mathematics Software*. 2025. <<https://www.geogebra.org/about>>. Acesso em: 13 out. 2025.
- 20 BRANCA, C. *Equação Diofantina: Caixa Eletrônico*. 2025. <<https://www.geogebra.org/material/copy/id/mpznahsk>>. Recurso interativo no GeoGebra. Acesso em: 13 out. 2025.
- 21 Reducatica. *Crivo de Eratóstenes / Como encontrar números primos*. 2020. Acesso em: 17 set. 2025. Disponível em: <<https://www.youtube.com/watch?v=uJaPQGtYg6g>>.
- 22 Reducatica. *Como números primos te protegem na internet / Criptografia e Números Primos*. 2025. Acessado em: 17 set. 2025. Disponível em: <https://www.youtube.com/watch?v=7sPjyualo_4>.

Apêndices

APÊNDICE A – Divisibilidade

Questionário Diagnóstico

Etapa Inicial

1. Você já participou de alguma Olimpíada de Matemática? Qual foi sua experiência?
2. Quais tipos de problemas você mais gosta ou sente dificuldade?
3. Como você organiza seu raciocínio ao resolver problemas matemáticos?
4. Descreva como costuma registrar suas soluções e justificativas ao resolver um problema matemático.
5. O que espera aprender neste curso preparatório para provas olímpicas?
6. **Questão Desafiadora (OBMEP - 1ª FASE):** Nove amigos comeram 5 pizzas, algumas cortadas em 6 fatias e outras cortadas em 8 fatias. Todos comeram o mesmo número de fatias e não sobrou nada. Quantas fatias cada um comeu?
 - A) 4
 - B) 5
 - C) 6
 - D) 7
 - E) 8
7. Descreva como você pensou para tentar resolver a questão acima. Quais passos você seguiu? Testou alguma possibilidade? Quais alternativas considerou?

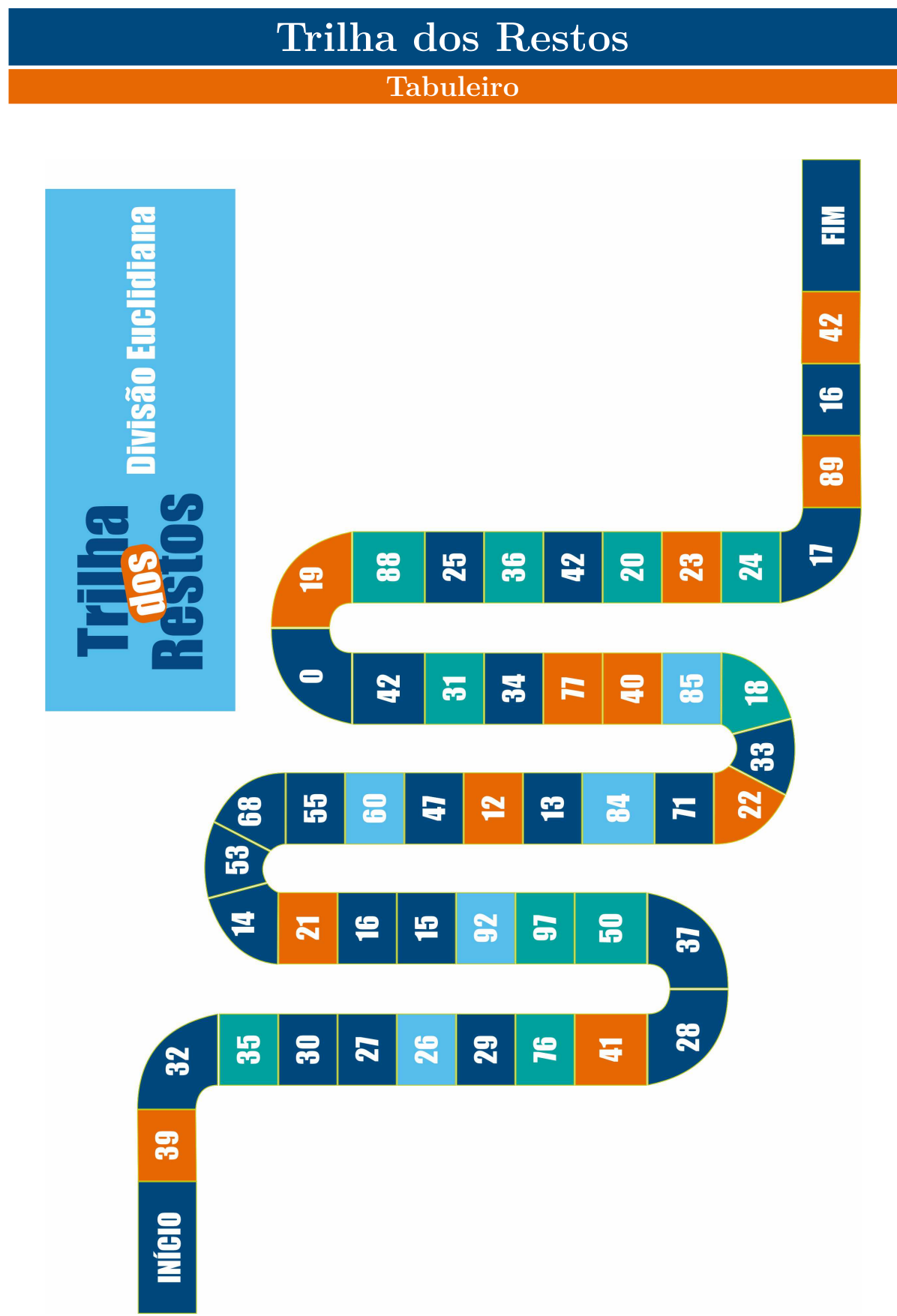


Figura 3 – Tabuleiro Trilha dos Restos

Questões Olímpicas - Encontro 01

Divisibilidade

1. **OBMEP - 1ª FASE:** Lucas pensou em um número, dividiu-o por 285 e obteve resto 77. Se ele dividir o número em que pensou por 57, qual é o resto que ele vai encontrar?

A) 0
B) 20
C) 40
D) 54
E) 56

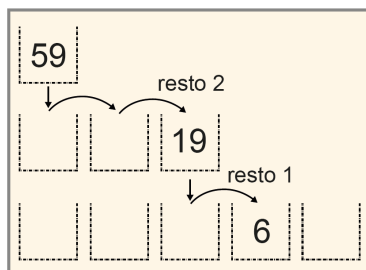
2. **OPEMAT - 2ª FASE:** Considere a lista periódica conforme a situação na figura abaixo: A lista é ordenada, ou seja, o primeiro termo é o número 1, o segundo o número 2, o terceiro o número 3, o quarto o número 1 e assim por diante. Julgue as afirmações a seguir atribuindo (V) se a afirmação for VERDADEIRA e (F) se a afirmação for FALSA.

1 2 3 1 2 4 1 2 3 1 2 4 1 2 3 1 2 4 1 2 3 1 2 4 1 2 3 1 2 4 1 2 3 1 2 4 ...

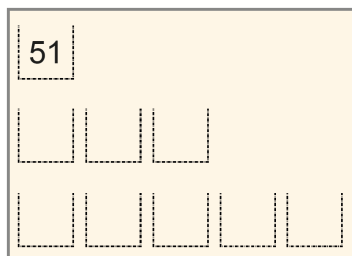
- A) (V) (F) A sequência se repete a cada agrupamento de 7 números.
B) (V) (F) O número que ocupa a 2021ª posição é o número 3.
C) (V) (F) Observando a lista até o 2020º termo (incluindo este número), o número 3 aparece 336 vezes.
D) (V) (F) Olhando a lista até o 2019º termo (incluindo este número), o agrupamento 12 aparece 673 vezes.
E) (V) (F) Somando os primeiros 2018 números dessa sequência obtemos o valor 4371.
3. **OBMEP - 2ª FASE:** Em uma brincadeira, Euclides escolhe um número natural, coloca esse número no topo do tabuleiro ao lado e realiza o seguinte procedimento:
- divide o número escolhido por 3 e anota o quociente e o resto;
 - se o resto for 0 coloca o quociente logo abaixo do número;
 - se o resto for 1 coloca o quociente deslocando uma casa para a direita;
 - se o resto for 2 coloca o quociente deslocando duas casas para a direita.

A seguir, ele repete o mesmo procedimento para o quociente obtido. Na figura vemos a brincadeira de Euclides que começa com 59 e termina com o 6 na quarta casa da base do tabuleiro.

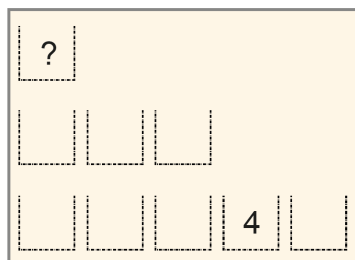
$$\begin{array}{r} 59 \overline{) 3} \\ 2 \quad 19 \\ \hline 59 = 19 \times 3 + 2 \\ 19 \overline{) 3} \\ 1 \quad 6 \\ \hline 19 = 6 \times 3 + 1 \end{array}$$



A) Faça a brincadeira de Euclides com o número 51.



B) Quais números Euclides pode ter escolhido se a brincadeira terminou com o 4 na quarta casa da base do tabuleiro?



C) Quantos números entre 10 e 99 começam uma brincadeira de Euclides que termina na quarta casa da base do tabuleiro?

4. **OPEMAT - 1ª FASE:** Quantos pares (m, n) de números inteiros satisfazem a igualdade

$$3n + 5m = mn + 13.$$

- A) Quatro pares.
- B) Cinco pares.
- C) Seis pares.
- D) Sete pares.
- E) Oito pares.

APÊNDICE B – Sistemas de Numeração

Atividade Motivacional - Cartas Mágicas

Sistema de Numeração

1	3	5	7
9	11	13	15
17	19	21	23
25	27	29	31
33	35	37	39
41	43	45	47
49	51	53	55
57	59	61	63

Carta do jogo com os números que possuem o fator 2^0 em sua decomposição em potências de 2.

2	3	6	7
10	11	14	15
18	19	22	23
26	27	30	31
34	35	38	39
42	43	46	47
50	51	54	55
58	59	62	63

Carta do jogo com os números que possuem o fator 2^1 em sua decomposição em potências de 2.

4	5	6	7
12	13	14	15
20	21	22	23
28	29	30	31
36	37	38	39
44	45	46	47
52	53	54	55
60	61	62	63

Carta do jogo com os números que possuem o fator 2^2 em sua decomposição em potências de 2.

8	9	10	11
12	13	14	15
24	25	26	27
28	29	30	31
40	41	42	43
44	45	46	47
56	57	58	59
60	61	62	63

Carta do jogo com os números que possuem o fator 2^3 em sua decomposição em potências de 2.

16	17	18	19
20	21	22	23
24	25	26	27
28	29	30	31
48	49	50	51
52	53	54	55
56	57	58	59
60	61	62	63

Carta do jogo com os números que possuem o fator 2^4 em sua decomposição em potências de 2.

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

Carta do jogo com os números que possuem o fator 2^5 em sua decomposição em potências de 2.

Cartas Mágicas

Sistema de Numeração

Descobrir um número pensado utilizando cartas numeradas e compreender a lógica do sistema binário de forma prática.

Objetivo: Construir suas próprias cartas mágicas para os números de 1 a 15, aplicando conceito de sistema binário e representação posicional.

Instruções para preenchimento:

- Cada cartela representa uma potência de 2 (1, 2, 4, 8).
- Para cada número de 1 a 15, determine em quais potências ele aparece na decomposição binária.
- Coloque o número na cartela correspondente à(s) potência(s) de 2 em que ele aparece.
- Exemplo: o número 5 tem representação binária 0101 — aparece nas potências 1 e 4, então entra nas cartelas 1 e 4.
- Preencha todas as cartelas de 1 a 15 seguindo essa lógica.

- Teste a mágica com colegas: alguém pensa em um número de 1 a 15 e você tenta adivinhar usando suas cartelas.
- Experimente generalizar o método para números maiores ou para outras bases numéricas.

Questões Olímpicas - Encontro 02

Sistema de Numeração

1. **OBMEP - 1ª FASE:** O contrário de um número de dois algarismos, ambos diferentes de zero, é o 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 seu contrário?
 - A) 44
 - B) 99
 - C) 121
 - D) 165
 - E) 181

2. **OPEMAT - 1ª FASE:** Os números naturais m, n, p, q, r e s são formados por 3 algarismos não nulos. Assumindo que estes números são distintos e formados pelos mesmos algarismos, então $m + n + p + q + r + s$ é um múltiplo de:
 - A) 10
 - B) 100
 - C) 110
 - D) 200
 - E) 222

APÊNDICE C – Máximo Divisor Comum e Mínimo Divisor Comum

Atividade Motivacional 01

MDC

Temos dois rolos de arame: um com 210 cm e outro com 330 cm. Precisamos cortá-los em pedaços de mesmo comprimento, mas queremos que esses pedaços sejam os maiores possíveis. Qual deve ser o comprimento de cada pedaço?

Questões Olímpicas - Encontro 03

MDC

1. **OPEMAT - 1ª FASE:** O responsável pela organização das prateleiras de um supermercado estava muito pensativo. Ele precisava organizar 168 biscoitos de chocolate e 120 biscoitos de morango e gostaria de organizá-los de acordo com as regras 1 e 2 abaixo. Sabendo que o organizador utilizou a menor quantidade de prateleiras possível respeitando os critérios de organização abaixo, assinale a alternativa que indica a quantidade total de prateleiras utilizadas.
 1. Cada prateleira deve possuir quantidades iguais de biscoitos;
 2. Cada prateleira deve conter apenas um sabor de biscoito.

A) 5
B) 7
C) 10
D) 11
E) 12
2. **OBMEP - 1ª FASE:** Qual é o maior valor possível para o máximo divisor comum de dois números naturais cujo produto é 6000?

A) 10
B) 20
C) 30
D) 40
E) 60

Atividade Motivacional 01

MMC

1. “Uma lâmpada pisca de 14 em 14 segundos e uma outra lâmpada pisca de 20 em 20 segundos. Um cronômetro zerado foi ligado exatamente quando essas lâmpadas piscam juntas. Se o cronômetro foi desligado na primeira vez em que as lâmpadas piscaram juntas novamente, que tempo ele marcou?” (14).
2. “Dois ciclistas correm numa pista circular e gastam respectivamente 30 segundos e 35 segundos para completar uma volta na pista. Eles partem no mesmo local e no mesmo instante. Após algum tempo, os dois atletas se encontram pela primeira vez no local de largada. Neste momento, o atleta mais veloz estará completando quantas voltas? E o menos veloz? Depois de quanto tempo da largada ocorrerá o encontro?”

Questões Olímpicas - Encontro 03

MMC

1. **OPEMAT - 1ª FASE:** Para quantos valores de k , o número 12^{12} é o mínimo múltiplo comum de 6^6 , 8^8 e k ?
 - A) 6
 - B) 8
 - C) 12
 - D) 24
 - E) 25

2. **OPEMAT - 2ª FASE:** Na terra de π -raia, um observador registrou que um cometa X e um cometa Y poderiam ser vistos a cada período de 76 e y anos, respectivamente. Sabendo que este ano os dois cometas foram vistos juntos, e que a próxima vez que eles serão vistos juntos novamente ocorre daqui a 684 anos, responda os seguintes itens.
 - a) Quantas vezes os cometas serão vistos juntos durante os próximos 13.000 anos?
 - b) Determine todos os possíveis valores para y .

APÊNDICE D – Equações Diofantinas

Atividade Motivacional 01

Escova Diofantina



Figura 4 – Cartas Escova Diofantina - Frente

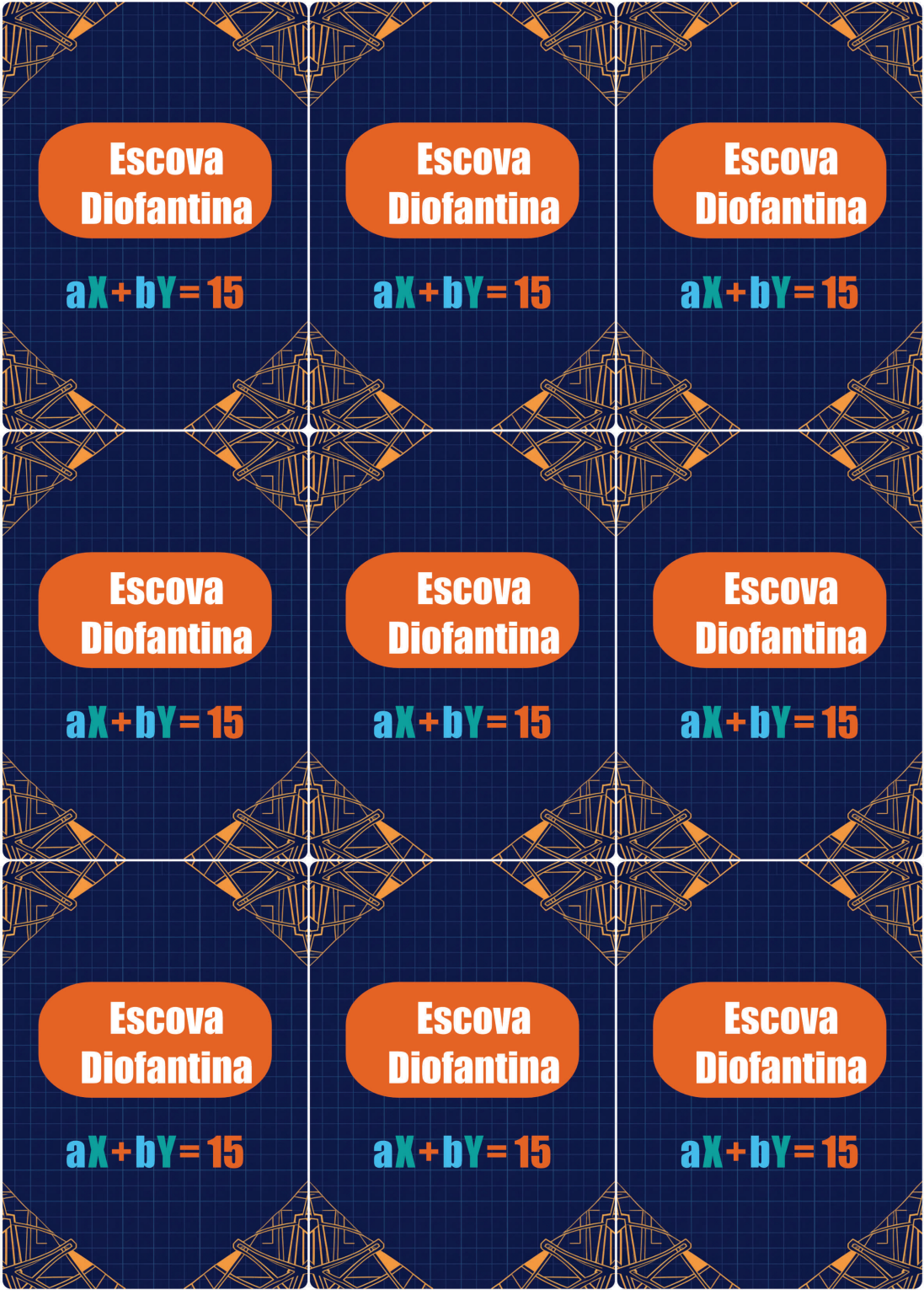


Figura 5 – Cartas Escova Diofantina - Verso

Atividade Motivacional 02

Equações Diofantinas

Um caixa eletrônico só dispõe de cédulas de 20 e 50 reais. De quantas formas é possível sacar exatamente R\$ 500,00? Modele a situação com uma equação diofantina e determine todas as soluções inteiras não negativas.

Questões Olímpicas - Encontro 04

Equações Diofantinas

1. **OBMEP - 1ª FASE:** Os números a e b são inteiros positivos tais que $\frac{a}{11} + \frac{b}{3} = \frac{31}{33}$. Qual é o valor de $a + b$?
 - A) 5
 - B) 7
 - C) 14
 - D) 20
 - E) 31
2. **OBMEP - 1ª FASE:** De quantas maneiras podemos trocar uma nota de R\$ 20,00 por moedas de R\$ 0,10 e R\$ 0,25?
 - A) 21
 - B) 36
 - C) 38
 - D) 41
 - E) 56
3. **TM² - 1ª FASE:** Beatriz tem em seu bolso 33 moedas, algumas de 25 centavos e outras de 10 centavos. Sabendo que Luíze tem ao todo uma quantidade inteira de reais, quantas moedas de 25 centavos ela possui?
 - A) 16
 - B) 17
 - C) 18
 - D) 19
 - E) Não é possível determinar.

APÊNDICE E – Números Primos

Atividade Motivacional 01

Números Primos

Questões Investigativas:

- Quais números primos você lembra facilmente?
- Como verificar se números como 91 ou 97 são primos?

Números Primos

Crivo de Eratóstenes

Siga os passos abaixo para descobrir os números primos de 2 a 100:

- Comece com o menor número primo: 2. Risque todos os múltiplos de 2, exceto o próprio 2.
- Passe para o próximo número que ainda não foi riscado. Risque todos os múltiplos deste número, exceto o próprio número.
- Repita o processo com o próximo número não riscado e assim por diante, até completar todos os números na tabela.
- Os números que permanecerem sem riscar são os números primos entre 1 e 100.

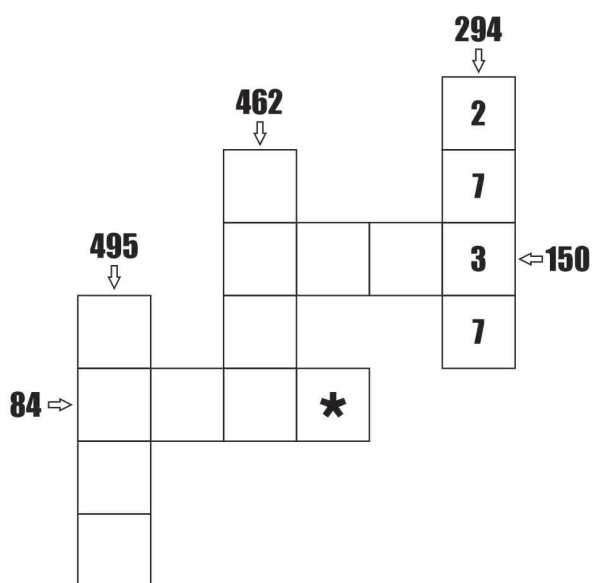
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Números primos obtidos: _____

Questões Olímpicas - Encontro 05

Números Primos

1. **OBMEP - 1ª FASE:** As casas da figura abaixo devem ser preenchidas com números primos. Em cada linha ou coluna, o produto dos números deve ser igual ao número indicado pela seta. A coluna indicada por 294 já está preenchida. Qual é o número que deve ser escrito na casa marcada com *?



- A) 2
B) 3
C) 5
D) 7
E) 11
2. **OBMEP - 1ª FASE:** Mariana escreveu as decomposições em fatores primos dos números naturais de 2 a 100:

$$2, 3, 2 \times 2, 5, 2 \times 3, \dots, 3 \times 3 \times 11, 2 \times 2 \times 5 \times 5.$$

Quantas vezes ela escreveu o algarismo 2?

- A) 99
B) 104
C) 152
D) 188

E) 191

3. **OPEMAT - 1^a FASE:** Seja n um número inteiro positivo. Defina o número n^* por

$$n^* = (n - 1) \cdot (n - 2) \cdot (n - 3) \cdots 3 \cdot 2 \cdot 1.$$

Por exemplo,

$$6^* = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120.$$

Dentre as alternativas abaixo, podemos concluir que o número de divisores primos distintos do número 21^* é:

- A) 2
- B) 8
- C) 10
- D) 11
- E) 21

4. **TM² - 1^a FASE:** Seja n o menor natural que possui exatamente 35 divisores positivos. Determine a quantidade de divisores positivos de $n - 1$.

- A) 2
- B) 4
- C) 7
- D) 12
- E) 14

APÊNDICE F – Congruência

Atividade Motivacional 01 - Formação de Grupos

Congruência

Os estudantes serão recebidos com um bombom, ao qual estará associado um número. Esse número será utilizado na dinâmica inicial da aula, visando acolher os alunos e introduzir o conceito de congruência modular de forma lúdica.

1. O professor determina, na sala, regiões que representarão os restos de 0 até 5.
2. Cada estudante realiza mentalmente a divisão de seu número por 6, identifica o resto e se posiciona na região correspondente, observando os colegas próximos.
3. Repita o procedimento com divisores 5 e 4, reorganizando os grupos de acordo com os restos.
4. Após a última divisão, cada grupo ficará formado e será a base para o trabalho colaborativo.
5. Cada grupo receberá uma questão diferente relacionada ao tema de congruência modular.
6. Os integrantes do grupo sortearão funções: facilitador, harmonizador, monitor de recursos, repórter e controlador do tempo.

Essa dinâmica permite perceber como pequenas alterações no divisor influenciam a composição dos grupos, evidenciando padrões nos números e introduzindo a ideia de congruência modular de forma significativa.

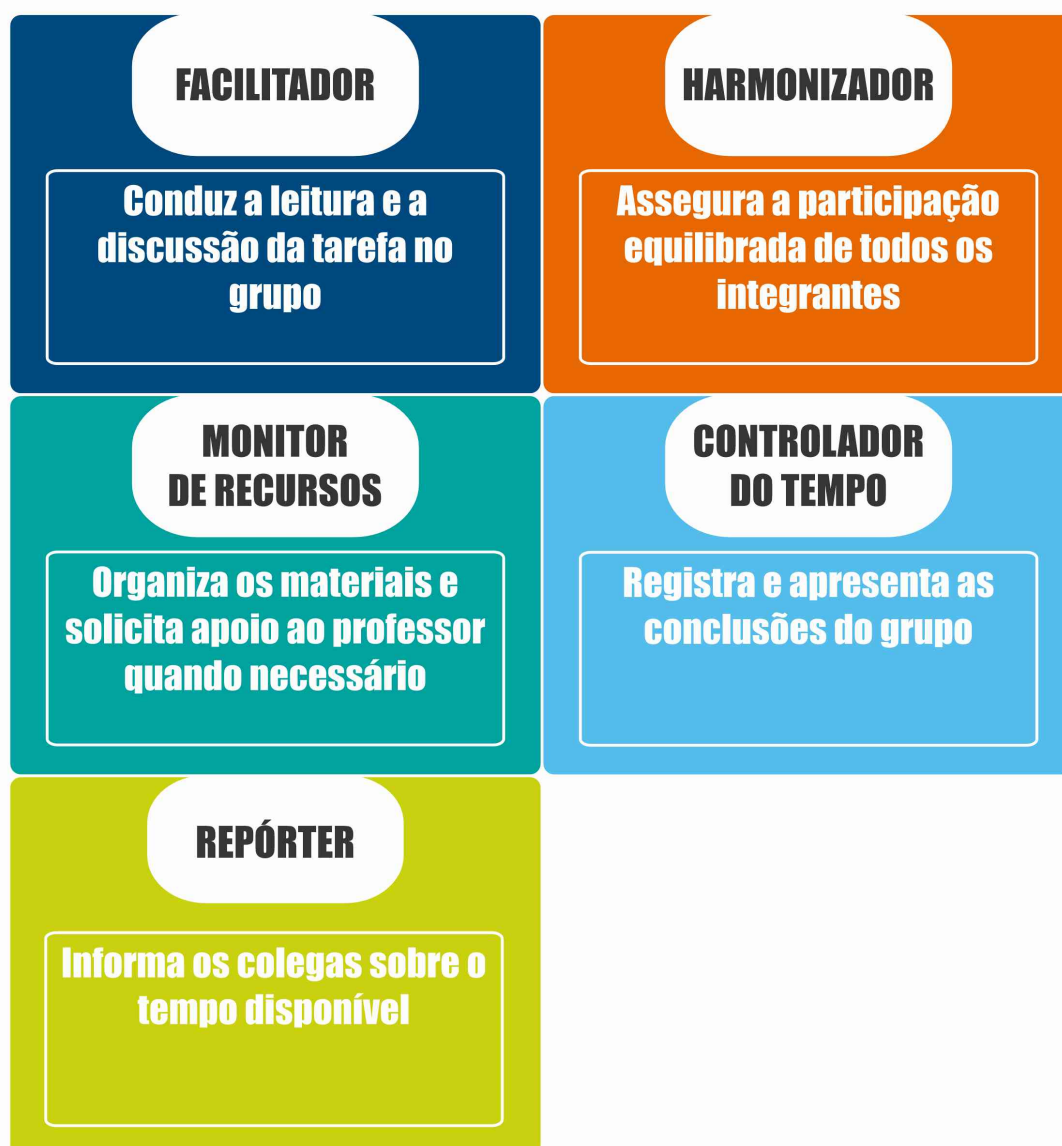
Papel dos Estudantes na Formação dos Grupos**Congruência**

Figura 6 – Distribuição dos papéis.

Questões Olímpicas - Encontro 06

Congruência

1. **OBMEP - 1ª FASE:** Qual é o resto da divisão de $1 \times 2 \times 3 \times 4 \times \dots \times 2011 + 21$ por 8?

A) 2
B) 3
C) 5
D) 6
E) 7

2. **OBMEP - 1ª FASE:** Qual é o algarismo das dezenas da soma

$$\underbrace{7}_{\text{um sete}} + \underbrace{77}_{\text{dois setes}} + \underbrace{777}_{\text{três setes}} + \underbrace{7777}_{\text{quatro setes}} + \dots + \underbrace{777 \dots 77}_{\text{setenta e seis setes}} + \underbrace{777 \dots 777}_{\text{setenta e sete setes}} ?$$

A) 5
B) 6
C) 7
D) 8
E) 9

3. **OPEMAT - 1ª FASE:** O cadastro de pessoa física (CPF) é um documento de identificação usado pela receita federal que consiste de onze dígitos sendo os nove primeiros fornecidos pela receita federal e os dois últimos, chamados dígitos verificadores, calculados da seguinte forma: se $d_1 d_2 d_3 d_4 d_5 d_6 d_7 d_8 d_9$ são os nove primeiros dígitos do CPF fornecido, então calculamos

$$A = 10d_1 + 9d_2 + 8d_3 + 7d_4 + 6d_5 + 5d_6 + 4d_7 + 3d_8 + 2d_9,$$

e calculamos r , onde r é o resto da divisão de A por 11. Se o resto for 0 ou 1 então o décimo dígito d_{10} será 0. Caso contrário d_{10} será $11 - r$. Para calcular o décimo primeiro dígito, calculamos

$$B = 10d_2 + 9d_3 + 8d_4 + 7d_5 + 6d_6 + 5d_7 + 4d_8 + 3d_9 + 2d_{10},$$

e calculamos R , onde R é o resto da divisão de B por 11. Se $R = 0$ ou $R = 1$ então $d_{11} = 0$. Caso contrário, $d_{11} = 11 - R$. Se uma pessoa tem os nove primeiros dígitos de seu CPF dados por 299792458, os dígitos d_{10} e d_{11} são respectivamente:

A) 1 e 8

B) 0 e 7

C) 2 e 6

D) 0 e 8

E) 3 e 5

4. **OPEMAT - 1ª FASE:** Uma determinada loja de livros de matemática resolveu fazer uma promoção que proporcionava 35% de desconto nos livros. Para obter o desconto, os clientes precisavam usar um cupom com um número de seis dígitos dado por $80AB35$ que é múltiplo de 99, e assim precisavam descobrir os valores de A e B . Assinale a alternativa abaixo que contém um possível valor de A .

A) 2

B) 5

C) 7

D) 8

E) 9

APÊNDICE G – Teorema Chinês dos Restos

Atividade Motivacional 01 - Desafio do número secreto

Teorema Chinês dos Restos

Pense em um número natural menor que 30.

Divida esse número por 3 e por 5, anotando apenas os restos.

Informe os restos ao professor e à turma.

O desafio consiste em adivinhar o número escolhido a partir dessas informações.

Questões Olímpicas - Encontro 07

Teorema Chinês dos Restos

1. **OPEMAT – 2ª FASE:** Um general deseja verificar o número de soldados em um de seus pelotões. Então, mandou que os soldados formassem alinhados de 9 em 9 e verificou que sobraram 2 soldados. Em seguida, ordenou que formassem alinhados de 11 em 11 e verificou que sobraram 4. Finalmente, fez os soldados se alinharem de 13 em 13 e sobraram 8. Sabendo que o pelotão tem entre dois mil e três mil soldados, determine quantos soldados sobraram quando o general os mandou formar de 100 em 100.
2. **ENQ:** A Secretaria de Educação de um município recebeu uma certa quantidade de livros para distribuir entre as escolas do município. Sabe-se que a quantidade é superior a 1000, inferior a 2000, que se dividí-los entre 7 escolas, sobram 4, entre 9 sobram 2 e entre 13 sobram 6. Encontre a quantidade de livros.
3. **ENQ:** Em uma cesta contendo ovos, na contagem de dois em dois, de três em três, de quatro em quatro e de cinco em cinco, sobram 1, 2, 3 e 4 ovos, respectivamente. Qual é a menor quantidade de ovos que a cesta pode ter?

Avaliação Final dos Encontros

Roda de Conversa

- Qual conteúdo ou atividade você considerou mais interessante ou marcante durante o minicurso?
- Quais estratégias de resolução foram mais fáceis de compreender e aplicar?
- Quais conteúdos ou atividades apresentaram maior dificuldade?
- De que forma essa experiência pode contribuir para sua preparação para as Olimpíadas de Matemática?
- Como você se sentiria diante de problemas semelhantes em provas olímpicas?
- Quais habilidades você acredita ter desenvolvido ao longo dos encontros: lógica, criatividade, percepção de padrões, argumentação matemática, comunicação matemática ou outras?