



UNIVERSIDADE FEDERAL DO TOCANTINS
CÂMPUS CIMBA ARAGUAÍNA
MESTRADO PROFISSIONAL EM MATEMÁTICA



Hans Müller Silva Oliveira

Congruências Modulares para Olimpíadas de Matemática e
Algumas Aplicações

Araguaína-TO
2021

Hans Müller Silva Oliveira

Congruências Modulares para Olimpíadas de Matemática e Algumas
Aplicações

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação stricto sensu em Matemática, câmpus Araguaína, da UFT, como parte dos requisitos necessários para a obtenção do Título de Mestre em Matemática.

Orientador: Prof. Dr. Matheus Pereira Lobo

Araguaína-TO
2021

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da Universidade Federal do Tocantins

- O48c Oliveira, Hans Müller Silva.
Congruências Modulares para Olimpíadas de Matemática e Algumas Aplicações. / Hans Müller Silva Oliveira. – Araguaína, TO, 2021.
59 f.
- Dissertação (Mestrado Profissional) - Universidade Federal do Tocantins – Câmpus Universitário de Araguaína - Curso de Pós-Graduação (Mestrado) Profissional em Matemática, 2021.
Orientador: Dr. Matheus Pereira Lobo
1. Olimpíadas de Matemática. 2. Congruências Modulares. 3. Resolução de Problemas . 4. Aplicações. I. Título

CDD 510

TODOS OS DIREITOS RESERVADOS – A reprodução total ou parcial, de qualquer forma ou por qualquer meio deste documento é autorizado desde que citada a fonte. A violação dos direitos do autor (Lei nº 9.610/98) é crime estabelecido pelo artigo 184 do Código Penal.

Elaborado pelo sistema de geração automática de ficha catalográfica da UFT com os dados fornecidos pelo(a) autor(a).

Hans Müller Silva Oliveira

Congruências Modulares para Olimpíadas de Matemática e Algumas Aplicações

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação stricto sensu em Matemática, câmpus Araguaína, da UFT, como parte dos requisitos necessários para a obtenção do Título de Mestre em Matemática.

Trabalho aprovado em 29 de julho de 2021

BANCA EXAMINADORA:

Prof. Dr. Matheus Pereira Lobo
Orientador

**Prof. Dr. José Carlos de Oliveira Junior -
Universidade Federal do Tocantins(UFT)**
Examinador Interno

**Profa. Dra. Shirlei Nabarrete Dezidério -
Universidade Federal do Tocantins(UFT)**
Examinador Externo

Araguaína-TO
2021

Dedico este trabalho a Deus, que me deu toda capacidade para realizá-lo, também a meus pais Miltom Ramos e Enedina Diogo, que são meus maiores incentivadores, à minha esposa Camilla e aos meus filhos, Raphael e Paulo. Também quero dedicar de uma maneira especial a meu amigo Giordane que sempre foi solícito e nos apoiou durante todo curso e, também, a todos que contribuíram para a realização desse sonho.

Agradecimentos

Agradeço, em primeiro lugar, a Deus, que me deu a vida e a capacidade para estudar, aprender e colocar em prática a Matemática e que me proporcionou a possibilidade de chegar até este momento com muito aprendizado.

Agradeço aos meus pais, Milton Ramos de Oliveira *in memoriam* e Enedina Diogo da Silva, por sempre me incentivarem a estudar e me ensinarem que a educação pode mudar a história de uma pessoa, dando-lhe maiores oportunidades na vida, pois sabiam que o estudo transforma tanto a mente quanto a sociedade onde o indivíduo está inserido.

Agradeço ao meu orientador, Matheus Pereira Lobo, por todos os conselhos, pela paciência e ajuda neste período, por ter me mostrado que os estudos são primordiais para o crescimento e me mostrar o que é ter paixão pelo aprendizado, sempre primando pela qualidade do processo ensino-aprendizagem.

Aos meus companheiros de turma, pois juntos tivemos grandes batalhas, mas graças ao companheirismo de todos, conseguimos a vitória. E, de modo especial, quero citar meu amigo Giordane, que nos momentos mais complicados, foi solícito e dedicado a me ajudar e ensinar independente da situação ou do momento.

Aos professores que arduamente foram exemplares, para que todos nós, alunos, tivéssemos acesso ao melhor conteúdo e da melhor maneira possível, sem a ajuda de vocês jamais estaria aqui. Se hoje tenho uma bagagem de conhecimento muito maior, é devido a tanta dedicação em repassar e compartilhar o que sabiam e estudaram.

Aos senhores Bruno Vasconcelos Torres e Thiago Alves Miranda, que oportunizaram os meios pelos quais pude cursar as aulas durante o mestrado, mudando meus horários de trabalho, compreendendo quando precisava fazer alguma atividade ou trabalho, além do apoio e do incentivo que sempre houve por parte deles.

À minha esposa Camilla, que sempre me cobrou os estudos e, em todo tempo, esteve ao meu lado, inclusive durante os períodos das noites em claro, sempre com uma palavra de incentivo e motivação, me ajudando a seguir em frente e continuar firme na batalha.

Jesus respondeu: “Porque a fé que vocês têm é pequena. Eu asseguro que, se vocês tiverem fé do tamanho de um grão de mostarda, poderão dizer a este monte: Vá daqui para lá, e ele irá. Nada será impossível para vocês.”

(Mateus 17:20)

Resumo

Ao longo da história, a matemática sempre foi um desafio para muitos, sendo inclusive objeto de disputa intelectual entre os matemáticos de épocas passadas. Há uma certa carência no sistema educacional brasileiro com relação à qualidade do ensino de matemática, mas isso tem mudado gradativamente nos últimos anos, principalmente pela introdução das olimpíadas de matemática, que têm gerado um avanço neste processo, envolvendo tanto alunos, quanto professores, com esforços engendrados a melhorar e aprimorar as técnicas de ensino-aprendizagem para que bons resultados sejam alcançados pelos alunos e por suas instituições. Neste trabalho, apresentamos um breve histórico estrutural da Olimpíada Brasileira de Matemática (OBM) e, também, da Olimpíada Internacional de Matemática (IMO). Sabemos que esses certames valorizam muito o conhecimento matemático básico e a capacidade de resolver problemas de raciocínio lógico. Apresentamos as fundamentações teóricas de Congruências Modulares, um breve histórico de como surgiu esse objeto de estudo, descrevendo sua origem, definições, demonstrações de suas principais propriedades e, ainda, aplicações de congruências modulares nas olimpíadas de matemática e provas que geralmente cobram um nível de excelência em matemática. Esta dissertação foi produzida para facilitar o acesso a este tema, visando transmitir o conhecimento de uma maneira prática e de fácil entendimento.

Palavras-chaves: Olimpíada Brasileira de Matemática. Olimpíada Internacional de Matemática. Congruência Modular.

Abstract

Throughout history, mathematics has always been a challenge for many, and it has even been the object of intellectual dispute among mathematicians of past times. There is a certain lack in the Brazilian educational system regarding the quality of mathematics teaching, but this has gradually changed in recent years, mainly due to the introduction of the mathematics olympics, which have generated an advance in this process, involving both students and teachers, with efforts to improve and improve teaching and learning techniques so that great results are achieved by students and their institutions. In this work, we present a brief structural history of the Brazilian Mathematical Olympiad (OBM) and also of the International Mathematical Olympiad (IMO). We know that these place great value on basic mathematical knowledge and the ability to solve logical reasoning problems. We present the theoretical foundations of Modular Congruences, a brief history of how this object of study arose, describing its origin, definitions, demonstrations of its main properties, and also applications of modular congruences in mathematics and exams that generally require a level of excellence in mathematics. This dissertation was produced to facilitate the access to this topic, aiming to transmit knowledge in a practical and easy-to-understand manner.

Keywords: Brazilian Mathematical Olympiad. International Mathematical Olympiad. Modular Congruence.

Lista de ilustrações

Figura 1 – Relógio 1.	23
Figura 2 – Relógio 2.	24
Figura 3 – ISBN-10 do Livro Fundamentos da Matemática Elementar Volume 1. .	49
Figura 4 – Código de barras do Livro Fundamentos da Matemática Elementar Volume 1.	51

Lista de tabelas

Tabela 1 – Enumeração das letras do alfabeto.	52
Tabela 2 – Codificação da palavra matemática.	52
Tabela 3 – Alfabeto codificado com chave 3.	53
Tabela 4 – Palavra MATEMÁTICA codificada no alfabeto com chave 3.	53
Tabela 5 – Codificação da palavra MESTRE.	53
Tabela 6 – Enumeração das letras do alfabeto.	54

Lista de abreviaturas e siglas

ABNT	Associação Brasileira de Normas Técnicas
OMB	Olimpíadas de Matemática no Brasil
OBM	Olimpíada Brasileira de Matemática
IMO	Olimpíada Internacional de Matemática
AOBM	Associação Olimpíada Brasileira de Matemática
SBM	Sociedade Brasileira de Matemática
OBMEP	Olimpíada Brasileira de Matemática das Escolas Públicas
IMPA	Instituto de Matemática Pura e Aplicada
MCTIC	Ministério da Educação e do Ministério da Ciência, Tecnologia, Inovações e Comunicações
EFOMM	Escola de Formação de Oficiais da Marinha Mercante
BNCC	Base Nacional Curricular Comum

Lista de símbolos

\in	Pertence
\mathbb{N}	Conjunto dos Números Naturais
\mathbb{Z}	Conjunto dos Números Inteiros
\equiv	Congruente
\Rightarrow	Implica
Σ	Somatório
\forall	Para Todos
$>$	Maior
\geq	Maior ou Igual
$<$	Menor
\leq	Menor ou Igual
$a \mid b$	a divide b
\square	Aparece no final da demonstração

Sumário

1	INTRODUÇÃO	14
1.1	Motivação	14
1.2	Objetivos	15
1.3	Metodologia	15
2	REFERENCIAL TEÓRICO	17
2.1	OLIMPÍADA BRASILEIRA DE MATEMÁTICA	17
2.1.1	Nível de participação, fases e estrutura das provas	18
2.1.2	Premiação	19
2.1.3	Breve histórico da OBM	19
2.2	OLIMPÍADA INTERNACIONAL DE MATEMÁTICA	21
2.2.1	Nível de participação, fases e estrutura das provas	21
2.2.2	Premiação	21
2.2.3	Breve histórico da IMO	22
2.3	ARITMÉTICA MODULAR OU ARITMÉTICA DO RELÓGIO	23
2.4	PROPRIEDADES GERAIS DA ARITMÉTICA MODULAR	29
2.5	RESOLUÇÕES DE EXERCÍCIOS QUE ENVOLVEM CONGRUÊNCIA MODULAR	36
2.5.1	Questão 1	36
2.5.2	Questão 2	38
2.5.3	Questão 3	39
2.5.4	Questão 4	41
2.5.5	Questão 5	43
2.5.6	Questão 6	44
2.5.7	Questão 7	45
2.6	APLICAÇÕES DE ARITMÉTICA MODULAR	47
2.6.1	Cadastro de Pessoas Físicas (CPF)	47
2.6.2	ISBN-10	49
2.6.3	Código de Barras	50
2.6.4	Criptografia	52
3	CONSIDERAÇÕES FINAIS	55
	REFERÊNCIAS	57

1 Introdução

Um dos muitos obstáculos à evolução dos indicadores educacionais no Brasil, atualmente, são as elevadas taxas de repetência, que ocorrem por vários motivos, dentre eles pode-se destacar, segundo a Escola da Inteligência (2017), o fato de os estudantes receberem pouco ou nenhum incentivo à educação. Dentre as muitas dificuldades encontradas pelos alunos, o estudo e o domínio da matemática são os que mais se destacam. Muitas vezes, ouvem-se declarações de que os estudantes não gostam de matemática, de que a temem e de que a consideram uma disciplina complexa (REZENDE; MESQUITA, 2013).

A Olimpíada Brasileira de Matemática vem sendo, ao longo dos anos, um grande incentivo ao estudo e ao domínio da matemática, não só para os alunos, mas também para os professores e para todo o corpo docente das escolas da rede pública e privada, em todo território nacional, uma vez que a competição também serve como porta de entrada para a mais prestigiada olimpíada científica para estudantes do Ensino Médio, a Olimpíada Internacional de Matemática (IMO).

Dessa forma, o presente trabalho tem como intuito propor o entendimento da importância do evento, bem como a metodologia da competição em âmbito nacional e internacional. O estudo foi feito por meio de um levantamento bibliográfico do retrospecto das competições olímpicas, desde o surgimento da primeira até as diversas que existem, atualmente, em novo formato, assim como as premiações, aplicações, questões e resolução de provas passadas, a fim de exemplificar o nível da competição.

1.1 Motivação

A Olimpíada de Matemática tornou-se uma motivação para os alunos desde o início da sua realização no país, uma vez que, na grande maioria das competições olímpicas, há uma premiação para os competidores que se destacam. O fato de ser realizada em diversas escalas (mundial, nacional, regional), é um grande incentivo para os estudantes em nível escolar e universitário. Essa forma de competição ocorre há muito tempo e nasceu, primeiramente, com o objetivo de selecionar os melhores alunos em matemática para investir na sua carreira e, possivelmente, contribuir para o avanço científico-tecnológico do seu país (BAGATINI, 2010).

1.2 Objetivos

Este trabalho tem como objetivo geral mostrar de maneira sucinta como é a estrutura de cada olimpíada de matemática, analisando sua forma de aplicação, o formato de pontuação e o método de premiação, também trazer o conhecimento básico sobre aritmética modular com as propriedades mais utilizadas e também resoluções de problemas, de modo que o leitor possa compreender e aplicar todos os conhecimentos, e alcançar o sucesso em seus estudos posteriores.

Os objetivos específicos incluem:

- Mostrar a estrutura das olimpíadas de matemática;
- Trazer informações gerais sobre olimpíadas de matemática;
- Apresentar conhecimentos básicos de congruência modular;
- Apresentar as propriedades de congruência modular e suas demonstrações;
- Resolução de problemas de congruência modular com todas as etapas da resolução;
- Trazer aplicações práticas de congruência modular.

1.3 Metodologia

Segundo (MARCONI; LAKATOS, 2005), “não há ciência sem o emprego de métodos científicos”. Este trabalho foi elaborado por meio da pesquisa em dissertações, artigos, vídeos e sites oficiais, que possuem informações sobre as olimpíadas de matemática em geral. Vários vídeos foram assistidos, buscando uma ampla base de conteúdo, e também foram feitos estudos sistemáticos sobre congruência modular, para elaboração de um texto de fácil compreensão. Os problemas resolvidos foram explanados de modo a tornar cada passo acessível à compreensão, mostrando todas as propriedades utilizadas e também todas as etapas da resolução. O instrumento de pesquisa são a Olimpíada Internacional de Matemática e a Olimpíada Nacional de Matemática, como forma de incentivo ao estudo e domínio da matemática por estudantes dos níveis escolares e universitário e também um amplo estudo sobre congruências modulares, como mecanismo facilitador de obtenção de conhecimento.

O trabalho foi realizado em duas etapas. Inicialmente foi criado um acervo sobre as olimpíadas de matemática, procurando informações gerais sobre os certames, sua realização, premiação e curiosidades. Com esses conteúdos, foi criado um texto sucinto, porém com grande quantidade de informações, onde a estrutura de cada olimpíada é apresentada. Após concluir essa primeira etapa, iniciou-se um estudo sobre a congruência modular,

suas propriedades, demonstrações e problemas olímpicos que envolvem tais assuntos. Após essa coleta de informações, iniciou-se a elaboração de uma base teórica concisa e de fácil entendimento, apresentando primeiro a teoria completa, com todas as demonstrações e posteriormente os problemas olímpicos com toda explanação e detalhes. Para finalizar, foram apresentadas algumas aplicações das congruências modulares, onde podemos observar sua utilização de forma prática, e que envolve aplicações bastante recorrentes em sistemas de numeração, cadastro e organização.

2 Referencial Teórico

Quando ouvimos a palavra “Olimpíadas”, geralmente a relacionamos a competições esportivas, com as quais estamos familiarizados, em virtude da grande mídia criada em cima da paixão brasileira pelo esporte. A Olimpíada de Matemática é equivalente a tais competições na maneira como o concorrente compete com os outros candidatos a fim de conquistar a vitória, além de ser composta por regras e deveres como em qualquer modalidade. Nessa olimpíada, o “esporte” disputado não requer do concorrente força e/ou quaisquer habilidades físicas que lhe garantam capacidade de obter bons resultados, pois é uma disputa de caráter intelectual entre jovens em que as forças resumem-se em inteligência, criatividade, imaginação e disciplina mental.

Uma Olimpíada de Matemática é formada por uma sequência de provas, compostas por problemas instigantes, que englobam várias áreas da matemática, onde o candidato deve ter uma formação adequada para conseguir obter êxito. Na maioria das provas, das diversas competições existentes, os problemas que as compõem não requerem do aluno um alto padrão de conhecimentos matemáticos, mas sim principalmente a capacidade de interpretar, criar e improvisar o mais rápido possível.

2.1 OLIMPÍADA BRASILEIRA DE MATEMÁTICA

A Olimpíada Brasileira de Matemática (OBM) é uma competição para estudantes dos ensinos fundamental (a partir do 6º ano), médio e universitário das instituições públicas em âmbito nacional, realizada pela Associação da Olimpíada Brasileira de Matemática (AOBM) e conta com o apoio da Sociedade Brasileira de Matemática (SBM). É atribuída à comissão Nacional de Olimpíadas de Matemática a preparação e as soluções das provas da OBM, bem como a definição dos critérios de correção e de premiação (OBM, 2020), e tem como objetivos:

- a. Interferir decisivamente em prol da melhoria do ensino de Matemática no Brasil, estimulando alunos e professores a um aprimoramento maior propiciado pela participação em olimpíadas.
- b. Descobrir jovens com talento matemático excepcional e colocá-los em contato com matemáticos profissionais e instituições de pesquisa de alto nível, propiciando condições favoráveis para a formação e o desenvolvimento de uma carreira de pesquisa.
- c. Selecionar os estudantes que representarão o Brasil em competições internacionais de Matemática a partir do seu desempenho na OBM, realizando o seu devido treinamento.
- d. Apoiar as competições regionais de Matemática em todo o Brasil.
- e. Organizar as diversas competições internacionais de Matemática, quando sediadas no Brasil (OBM, 2020).

2.1.1 Nível de participação, fases e estrutura das provas

Em 2017, a OBM mudou de formato e, desde então, são quatro os níveis de participação, de acordo com a escolaridade do aluno.

- a. Nível 1 - alunos que estejam matriculados no 6º ou 7º ano do Ensino Fundamental no ano de 2020.
- b. Nível 2 - alunos matriculados no 8º ou 9º ano do Ensino Fundamental no ano de 2020.
- c. Nível 3 - alunos matriculados em qualquer série do Ensino Médio no ano de 2020.
- d. Nível Universitário - estudantes universitários, que ainda não tenham concluído o curso superior, normalmente estudantes universitários em nível de graduação, podendo ser estudantes de qualquer curso e qualquer período, ou aqueles que concluíram o Ensino Médio há menos de um ano e não tenham ingressado em curso de nível superior até a data de realização da prova da Competição Elon Lages Lima de Matemática, que substitui, a partir da 42ª edição, a prova da Primeira Fase do Nível Universitário. Alunos que concluíram o ensino superior no segundo semestre de 2020 também poderão participar do nível universitário.
- e. A Comissão Nacional de Olimpíadas de Matemática poderá, em casos excepcionais de comprovado mérito acadêmico, autorizar a participação de alunos na prova da OBM. Para os Níveis 1, 2 e 3, a OBM será realizada em Fase Única. Para o Nível Universitário, a OBM é realizada em duas fases, sendo a primeira fase, a Competição Elon Lages Lima de Matemática. As datas de todas as fases estão definidas no calendário oficial, publicado na página eletrônica da OBM. Casos omissos serão analisados e decididos pela Comissão Nacional de Olimpíadas de Matemática (REGULAMENTO-OBMEP, 2020).

Segundo o Regulamento da OBM, a estrutura das provas para o nível 1 conta com avaliação discursiva composta por 5 problemas, com duração de 4 horas e 30 minutos. Já os níveis 2 e 3 contam com prova discursiva, realizada em dois dias consecutivos, com 3 problemas em cada dia e duração de 4 horas e 30 minutos por dia.

Já para o Nível Universitário, a Competição Elon Lages Lima de Matemática é composta por uma prova objetiva com 25 perguntas de múltipla escolha, com duração de 3 horas. Na Segunda Fase, a prova discursiva é realizada em dois dias consecutivos, composta por 3 questões em cada dia e com duração de 4 horas e 30 minutos por dia.

Atualmente, no Brasil, temos duas competições semelhantes, sendo elas a Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP) e a Olimpíada Brasileira de Matemática (OBM). O que difere uma da outra, além da comissão organizadora, é que a OBMEP é para alunos do 6º ano do Ensino Fundamental até o último ano do Ensino Médio e composta por duas fases, enquanto a OBM abrange nível fundamental, médio e universitário e, no momento atual, mantém duas fases apenas para o nível universitário.

A Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP) é um projeto nacional que era dirigido apenas às escolas públicas, e que no ano de 2017 em sua 17ª edição foi aberta também para as escolas privadas brasileiras, realizada pelo Instituto de Matemática Pura e Aplicada (IMPA), com o apoio da Sociedade Brasileira de Matemática (SBM), e promovida com recursos do Ministério da Educação e do Ministério da Ciência, Tecnologia, Inovações e Comunicações – MCTIC (OBM, 2020).

2.1.2 Premiação

Ainda em conformidade com o regulamento da (OBM, 2020), aos alunos que obtiverem as melhores pontuações finais, em ordem decrescente de pontuação, são oferecidos prêmios, certificados e medalhas de ouro, prata e bronze. As quantidades de medalhas oferecidas atendem a proporção especificada em cada nível. São oferecidas, também, menções honrosas, que são definidas a critério da banca. Já na Competição Elon Lages Lima de Matemática não há entrega de medalhas ou troféus físicos. Todos os premiados nesta competição são aprovados para participar da prova da Segunda Fase do Nível Universitário.

A cerimônia de premiação é realizada anualmente durante a Semana Olímpica, podendo ocorrer presencialmente ou não. Aos alunos que não podem comparecer ao evento, é enviada a medalha através dos correios e disponibilizados os certificados em formato digital no sistema da página eletrônica da OBM.

Vale lembrar que o medalhista Fields brasileiro, Artur Avila, foi descoberto graças às iniciativas do IMPA de atrair, para seus programas de iniciação científica, mestrado e doutorado, jovens medalhistas das Olimpíadas de Matemática.

2.1.3 Breve histórico da OBM

Segundo (BAGATINI, 2010), a pioneira das Olimpíadas de Matemática no Brasil (OMB) foi organizada no estado de São Paulo, em 1977, criada pela Academia Paulista de Ciência. Na ocasião, foi destinada somente a alunos do estado e dividida em três níveis, Alfa (sexto e sétimo anos do ensino fundamental), Beta (oitavo e nono anos do ensino fundamental) e Gama (primeiro e segundo anos do ensino médio).

Desde 1894, as Olimpíadas de Matemática começaram a ser disputadas conforme os modelos utilizados até os dias de hoje. As primeiras edições foram realizadas na Hungria, e logo após, certames similares começaram a ser realizados no leste europeu, culminando na realização da 1ª Olimpíada Internacional de Matemática, na Romênia, em 1959. Essas competições foram ganhando cada vez mais prestígio e relevância entre os matemáticos do mundo. Com o tempo, vários países foram buscando participar e também fazer suas próprias olimpíadas.

Segundo informações disponibilizadas no site da (OBM, 2020), pode-se constatar que, em 1979, a Sociedade Brasileira de Matemática (SBM) organizou a 1ª Olimpíada Brasileira de Matemática (OBM) e, desde então, passou por diversas mudanças em seu formato. Em 1991, fizeram a inserção de dois níveis, Júnior (alunos que completassem 15 anos até 1991) e Sênior (para alunos que estivessem cursando o Ensino Médio). Em 1992, houve a inserção de duas fases. A prova da primeira fase era composta por vinte e cinco questões objetivas e a prova da segunda fase acontecia em dois dias, com três problemas por dia e o nível Júnior passa a ser para alunos que estivessem cursando até a oitava série. Em 1993, a segunda fase do nível Júnior voltou a ser realizada em um único dia e agora com cinco problemas. Em 1995, o nível Júnior volta a ser para alunos que tivessem a idade de quinze anos. Em 1998, são criados três níveis, I (5ª e 6ª séries), II (7ª e 8ª séries) e III (Ensino Médio) e três fases da prova, sendo a primeira objetiva com vinte ou vinte e cinco questões, a segunda era uma prova aberta com seis questões, já a terceira fase continha cinco questões para os níveis I e II e seis questões para o nível III que eram feitas em dois dias. As provas dos níveis I e II eram, então, aplicadas nas Escolas cadastradas. Em 1999, as provas do nível II na fase final também passam a ser aplicadas em dois dias. Em 2001, é criado o nível universitário, em duas fases.

Em 2005, surgiu a OBMEP, um projeto em âmbito nacional dirigido às escolas públicas e privadas brasileiras, realizada pelo Instituto de Matemática Pura e Aplicada (IMPA), com o apoio da Sociedade Brasileira de Matemática (SBM), e promovida com recursos do Ministério da Educação e do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), como uma realização do IMPA. A OBMEP foi criada com o intuito de incentivar alunos das escolas públicas de educação básica no estudo da matemática e revelar talentos na área; seus objetivos principais são

- Estimular e promover o estudo da Matemática;
- Contribuir para a melhoria da qualidade da educação básica, possibilitando que um maior número de alunos brasileiros possa ter acesso a material didático de qualidade;
- Identificar jovens talentos e incentivar seu ingresso em universidades, nas áreas científicas e tecnológicas;
- Incentivar o aperfeiçoamento dos professores das escolas públicas, contribuindo para a sua valorização profissional;
- Contribuir para a integração das escolas brasileiras com as universidades públicas, os institutos de pesquisa e com as sociedades científicas;
- Promover a inclusão social por meio da difusão do conhecimento (OBMEP, 2020).

Em 2017, a OBM se integra à OBMEP e institui prova em fase única para os níveis I, II e III, e em duas fases para o nível universitário. Mesmo que estivessem em constante mudança, a ideia central – que é estimular nos alunos o estudo e o gosto pela matemática, desenvolver e aperfeiçoar a capacitação dos professores, influenciar na melhoria do ensino

e descobrir jovens talentos – sempre foi mantida. Vale ressaltar, ainda, que os medalhistas da OBMEP recebem benefícios, como bolsas de estudo, ao ingressarem em cursos de graduação e pós-graduação de algumas universidades federais.

2.2 OLIMPÍADA INTERNACIONAL DE MATEMÁTICA

A Olimpíada Internacional de Matemática (IMO) é a maior, mais antiga e mais prestigiada olimpíada científica para estudantes do Ensino Médio do mundo. Segundo dados da IMO (2020), a primeira edição foi realizada na Romênia, em 1959, com a participação de sete países, Romênia, Hungria, Bulgária, Polônia, Tchecoslováquia, Alemanha Oriental e URSS. Desde então, o evento é realizado anualmente (com exceção de 1980, em que a prova foi cancelada devido a problemas políticos na Mongólia, local onde a prova seria realizada), sempre em um país diferente e, em 2017, a 58^o Olimpíada Internacional de Matemática foi realizada no Brasil, na cidade do Rio de Janeiro, onde a equipe brasileira conquistou três medalhas e três menções honrosas.

Os objetivos da IMO são:

- Descobrir, encorajar e desafiar jovens com talentos matemáticos em todos os países;
- Fomentar relações internacionais amigáveis entre matemáticos de todos os países;
- Criar oportunidade para a troca de informações sobre programas e práticas escolares em todo o mundo;
- Promover a matemática em geral (IMO, 2017).

2.2.1 Nível de participação, fases e estrutura das provas

Atualmente, mais de 100 países, dos 5 continentes, participam do evento. Cada país pode enviar uma equipe de até seis alunos do Ensino Médio ou indivíduos que não tenham ingressado na Universidade, ou equivalente, na data de realização da Olimpíada, mais um líder de equipe, um vice-líder e observadores, se desejar. Durante a competição, os participantes têm que resolver, individualmente, duas provas em dois dias consecutivos, com três problemas por dia. Cada problema vale sete pontos.

2.2.2 Premiação

As medalhas de ouro, prata e bronze são concedidas na proporção de 1 : 2 : 3 de acordo com o resultado geral, sendo que metade dos competidores recebe uma medalha. Ainda com o objetivo de incentivar o maior número possível de alunos a resolver problemas completos, são atribuídos certificados de menção honrosa aos alunos (sem medalha) que obtiveram 7 pontos em pelo menos um problema. Segundo (BAGATINI, 2010), as línguas

oficiais da Olimpíada Internacional são inglês, francês, alemão e russo. Caso seja necessário, os chefes de cada equipe se responsabilizam pelas traduções da prova.

2.2.3 Breve histórico da IMO

Durante toda a história das Olimpíadas, existem alguns fatos importantes que podem ser destacados na história da IMO; são eles:

Em 1965, a competição foi realizada em Berlim (Alemanha Oriental) com a participação de dez países, entre eles a Finlândia, que foi o primeiro país fora da “Cortina de Ferro” a participar do evento.

Em 1974, a competição ocorreu pela segunda vez em Berlim e, dentre os dezesseis países participantes, pela primeira vez, estava os Estados Unidos.

Em 1979, a competição realizou-se em Londres (Inglaterra) e, dentre os 23 países participantes, pela primeira vez, estava o Brasil.

Em 1980, não houve competição, pois a Mongólia passava por problemas internos políticos, e então foram realizados dois pequenos torneios de caráter não oficial.

Em 1981, pela primeira vez, a competição foi organizada fora da Europa, em Washington - Estados Unidos (MACIEL-CMPA; BASSO-UFRGS, 2009).

Quando a IMO iniciou, cada país participante era representado por, no máximo, oito alunos. Ao longo dos anos, foi alterado para quatro e seis participantes, sendo este último formato utilizado até hoje (BAGATINI, 2010). Como pré-requisitos para integrar-se na competição, segundo o regulamento, o país deve ser convidado a participar do certame, e o aluno não deve ultrapassar a idade máxima de 20 anos, deve estar normalmente matriculado no Ensino Fundamental ou Médio, e deve ser selecionado por meio da Olimpíada Brasileira de Matemática ou programa de seleção equivalente. A seleção é de livre escolha para cada país, sendo que o Brasil faz uso da Olimpíada Nacional.

Como premiação, os alunos que se destacarem nas provas, recebem medalhas de ouro, prata e bronze e menções honrosas. O número de medalhas é proporcional à metade dos competidores e tem distribuição seguindo a proporção 1:2:3. Os certificados de menção honrosa são distribuídos a alunos que não obtiveram medalhas, mas que conseguiram resolver corretamente alguma das questões. Estes certificados de menção honrosa objetivam, principalmente, incentivar o aluno a buscar a solução de alguns problemas (MACIEL-CMPA; BASSO-UFRGS, 2009).

2.3 ARITMÉTICA MODULAR OU ARITMÉTICA DO RELÓGIO

A aritmética modular, também conhecida como aritmética do relógio, é um sistema aritmético onde os ponteiros do relógio retornam à posição inicial após completarem um determinado ciclo. Essa abordagem teve como pioneiro o matemático Euler por volta do ano de 1750, onde começou a introduzir os conceitos de congruência modular de um número natural N . Já uma abordagem moderna sobre esses conceitos da aritmética modular foi introduzida por Carl Friedrich Gauss em 1801. A aritmética modular é utilizada em várias áreas da matemática, como por exemplo, na teoria dos números, álgebra abstrata, teoria dos grupos, criptografia, ciência da computação, música etc.



Figura 1 – Relógio 1. Fonte: Pixabay.com.

Podemos observar que um relógio possui 12 horas, quando o ponteiro chegar em 12 horas, automaticamente reinicia o ciclo e assim sucessivamente. Por exemplo, às 16 horas temos que 16 é maior que 12. Podemos observar que $12 + 4 = 16$, ou seja 16h é correspondente a 4 horas. Com base neste entendimento, podemos verificar que se o ponteiro estiver em 12 horas, então, se voltar 8 horas será 4 horas também, então cria-se um padrão para esses valores, que pode ser escrito como a seguinte progressão aritmética de razão 12, que recebe o nome de classe de equivalência (cujo representante é o número 4), $|4| = \{4 + 12k : k \in \mathbb{Z}\} = \{\dots, -20, -8, 4, 16, 28, \dots\}$, então todos os números que fazem parte deste conjunto são congruentes módulo 4.

Ao analisar esse conjunto, podemos verificar que todos os seus elementos possuem o mesmo resto na divisão por 12, afirmando assim, que todos eles estão na mesma classe de equivalência. Então, com esta análise, verifica-se que todo número n , ao ser dividido por um valor d , e que possui o mesmo resto r , faz parte de um mesmo conjunto, denominado

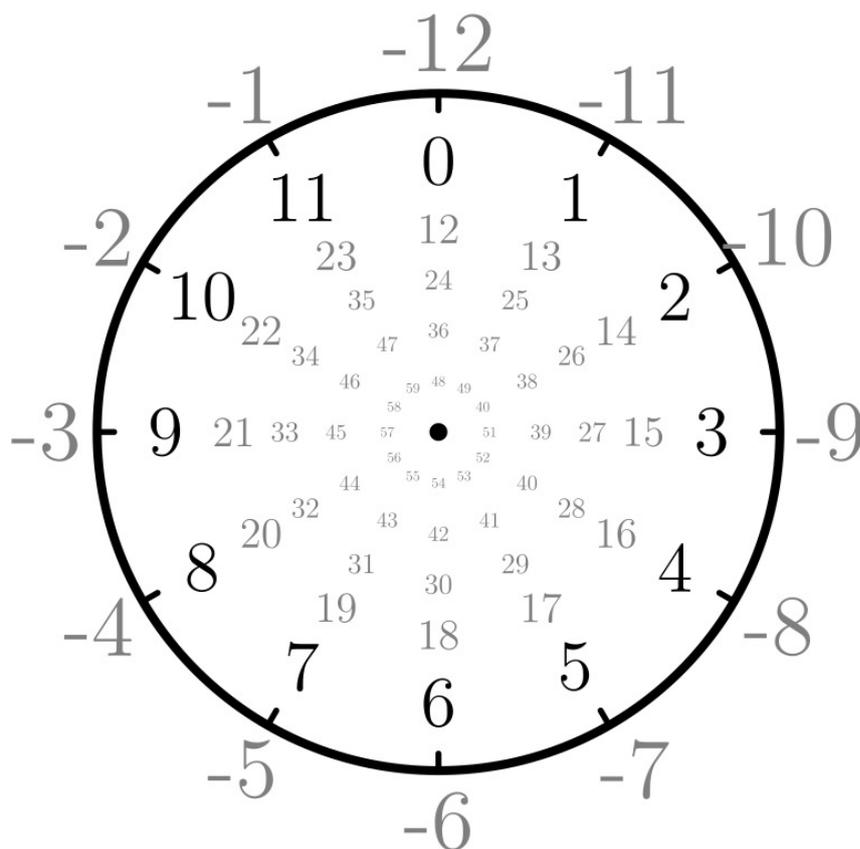


Figura 2 – Relógio 2. Fonte: <https://mathstats.uncg.edu/sites/pauli/112/HTML/images/image-11.svg>.

classe de equivalência módulo d . Com base nesta ideia, podemos escrever em forma de equação matemática, denotada por

$$n \equiv r \pmod{d},$$

onde n é o valor dado, r é o resto da divisão por d , ou seja, nesta equação não se leva em consideração o quociente da divisão, mas apenas o resto encontrado. Segundo o algoritmo de Euclides, na divisão, sabemos que a diferença entre o dividendo n e o resto r é divisível pelo divisor d , conforme podemos verificar na divisão do número 42 por 4,

$$42 = 10 \cdot 4 + 2,$$

então, $42 - 2$ é divisível por 4, e isto pode ser escrito conforme a definição matemática $4 \mid 42 - 2$.

Existem várias fontes de pesquisa em aritmética modular, ou aritmética do relógio. O livro *Aritmética da coleção Profmat* (HEFEZ, 2009) possui um vasto material sobre o objeto de estudo mencionado, o site *Polos Olímpicos de Treinamento Intensivo* (POTI, 2017) dispõe de vídeos produzidos por professores do Instituto de Matemática Pura e Aplicada (IMPA), onde a aritmética modular é analisada de maneira bem aprofundada. Vale ressaltar as seguintes dissertações que tratam do tema em questão (ESQUINCA, 2013), (WALTER et al., 2019), (RIBEIRO, 2019) e (SANT'ANNA, 2013). Diversas questões

que serão explanadas na sequência estão disponíveis nos sites Escola de Formação de Cadetes da Marinha Mercante (EFOMM, 2007), Olimpíada Cearense de Matemática (UFCE, 2014), Olimpíada Internacional de Matemática (IMO, 2017), site do Profmat (PROFMAT, 2007) e vídeos que contêm questões utilizadas como testes de seleção para olimpíadas internacionais (IMO, 2012). Podemos verificar que há uma grande quantidade de material disponível, e com base nestes, foi elaborado este texto para que de forma condensada e prática, o ensino da congruência modular possa ser repassado de forma sucinta e pragmática.

Definição 1

Seja $m > 1$ um número inteiro. Diz-se que x e y também inteiros são congruentes módulo m se x e y deixam o mesmo resto quando divididos por m (ESQUINCA, 2013).

Aplicando a definição, temos que $x \equiv y \pmod{m}$.

Observando esses exemplos anteriores, podemos verificar que há uma infinidade de modos de escrever as equações modulares, e com base nestes estudos iniciais verifica-se algumas propriedades que foram aplicadas nos exemplos analisados.

Tomando $x \pmod{y}$, e adicionando a x um múltiplo de y , o ponteiro sempre irá terminar no mesmo local do relógio dado, ou seja, na mesma classe de equivalência. Podemos verificar que

$$x \pmod{y} \equiv (x + k \cdot y) \pmod{y},$$

para qualquer k inteiro. Então, concluímos que

$$(4 + 0 \cdot 10) \pmod{10} \equiv 4 \pmod{10} \equiv 4,$$

$$(4 + 1 \cdot 10) \pmod{10} \equiv 14 \pmod{10} \equiv 4,$$

$$(4 + 2 \cdot 10) \equiv 24 \pmod{10} \equiv 4.$$

E, assim, sucessivamente para qualquer k inteiro.

Proposição 2

Sejam $x, y, m \in \mathbb{Z}$ e $m > 1$. $x \equiv y \pmod{m} \Leftrightarrow m \mid y - x$.

Demonstração

Com base no algoritmo de Euclides para a divisão, temos

$$x = mq_1 + r_1; \quad q_1, r_1 \in \mathbb{Z}; \quad 0 \leq r_1 < m,$$

$$y = mq_2 + r_2; \quad q_2, r_2 \in \mathbb{Z}; \quad 0 \leq r_2 < m.$$

(\Rightarrow)

x e y são congruentes, então deixam o mesmo resto na divisão por m . Portanto, sabemos que $r_1 = r_2 = r$. Então, podemos verificar que

$$y - x = mq_2 + r_2 - (mq_1 + r_1),$$

$$y - x = mq_2 + r - mq_1 - r,$$

$$y - x = m(q_2 - q_1).$$

Observamos que $y - x$ é múltiplo de m , então podemos concluir que $m \mid y - x$

(\Leftarrow)

Agora vamos tomar por hipótese que $m \mid y - x$ e, então, devemos verificar que $x \equiv y \pmod{m}$. Sejam

$$x = mq_1 + r_1; \quad q_1, r_1 \in \mathbb{Z}; \quad 0 \leq r_1 < m,$$

$$y = mq_2 + r_2; \quad q_2, r_2 \in \mathbb{Z}; \quad 0 \leq r_2 < m.$$

Pela hipótese, temos que

$$\begin{aligned} m \mid y - x &\Rightarrow m \mid mq_2 + r_2 - (mq_1 + r_1) \Rightarrow m \mid mq_2 + r_2 - mq_1 - r_1 \Rightarrow \\ &\Rightarrow m \mid m(q_2 - q_1) + r_2 - r_1. \end{aligned}$$

Podemos notar claramente que o termo $m(q_2 - q_1)$ é divisível por m , então o que devemos agora verificar é se $r_2 - r_1$ é também divisível por m . Assim, temos que verificar que $m \mid r_2 - r_1$. Para provarmos isso, devemos mostrar que $r_2 - r_1$ é múltiplo de m e que terá seu valor igual a zero.

Sabemos que $-m < r_2 - r_1 < m$. Com base nessa desigualdade e no algoritmo da divisão de Euclides, o único múltiplo de m que está entre $-m$ e m só pode ser zero. Então, com base nestas informações, podemos verificar que $0 \leq r_2 < m$. Subtraindo r_1 de todos os termos da desigualdade, temos que

$$0 - r_1 \leq r_2 - r_1 < m - r_1 \leq m,$$

pois $m > 1$. Assim, com base nos valores encontrados, temos que $r_2 - r_1 < m$.

Agora, tomando a desigualdade $0 \leq r_1 < m$, analisando somente $r_1 < m$, e multiplicando por -1 , temos que $-m < -r_1$. Aplicando a desigualdade $0 - r_1 \leq r_2 - r_1 < m - r_1 \leq m$, vamos obter $-m < -r_1 \leq r_2 - r_1 < m - r_1 \leq m$, então podemos verificar a proposição,

$$-m < r_2 - r_1 < m.$$

Portanto, podemos concluir que $m \mid r_2 - r_1$ e $-m < r_2 - r_1 < m$ e, com isso, $r_2 - r_1 = 0$, ou seja, $r_2 = r_1$. \square

Verificamos que $x \equiv y \pmod{m}$. Note que, se $m \mid y - x$, então $m \mid x - y$.

Exemplo 3

Dado o número natural 22 e aplicando o princípio do relógio, escreva a equação modular correspondente a este número.

O exemplo pede para encontrar um número congruente a 22 na divisão por 12.

Aplicando o algoritmo da divisão, podemos notar que $22 = 1 \cdot 12 + 10$. Então, temos que $22 \equiv 10 \pmod{12}$. Podemos notar que o foco deste processo é o resto, ou seja, o quociente não aparece explicitamente na equação modular.

Exemplo 4

Verifique se os números 38 e 57 são congruentes na divisão por 12.

Podemos verificar que

$$38 = 3 \cdot 12 + 2 \equiv 2 \pmod{12},$$

$$57 = 4 \cdot 12 + 9 \equiv 9 \pmod{12}.$$

Daí, concluímos que 38 e 57 não são congruentes, pois não possuem o mesmo resto na divisão por 12.

Exemplo 5

Verifique se os números 75 e 99 são congruentes na divisão por 12.

Podemos verificar que

$$75 = 6 \cdot 12 + 3 \equiv 3 \pmod{12},$$

$$99 = 8 \cdot 12 + 3 \equiv 3 \pmod{12}.$$

Daí, concluímos que 75 e 99 são congruentes, pois possuem o mesmo resto na divisão por 12, ou seja, eles pertencem à mesma classe de equivalência.

Agora que já fizemos uma breve introdução, mostrando o procedimento na divisão por 12, podemos avançar e verificar que o mesmo pode ser feito para qualquer divisor natural, e não somente com o número 12. Então, exemplificando, podemos verificar que 38 quando dividido por 5 pode ser escrito como

$$38 = 7 \cdot 5 + 3 \equiv 3 \pmod{5}.$$

Exemplo 6

Dado um relógio com os números 0, 1, 2, 3, 4, qual é o valor correspondente ao valor $13 \pmod{5}$?

Ao analisar o relógio no sentido horário podemos notar que temos os números sequencialmente 0, 1, 2, 3, 4, 0, 1, 2, 3, 4, ..., ou seja, temos 5 classes de equivalência. Então, com base

na sequência, podemos verificar que o 13 está na posição 3 do relógio. Assim, concluímos que

$$13 \pmod{5} \equiv 3.$$

As 5 classes de equivalência são: $|0| = \{0, 5, 10, 15, \dots\}$, $|1| = \{1, 6, 11, 16, \dots\}$, $|2| = \{2, 7, 12, 17, \dots\}$, $|3| = \{3, 8, 13, 18, \dots\}$, $|4| = \{4, 9, 14, 19, \dots\}$.

Exemplo 7

Dado um relógio com os números 0, 1, qual é o valor correspondente a $9 \pmod{2}$?

Ao analisar o relógio no sentido horário, podemos notar que temos os números sequencialmente 0, 1, 0, 1, 0, 1, ..., ou seja, temos 2 classes de equivalência. Então, com base na sequência, podemos verificar que o termo 9 está na posição 1 do relógio. Assim, concluímos que

$$9 \pmod{2} \equiv 1.$$

Exemplo 8

Dado um relógio com os números 0, 1, 2, qual é o valor correspondente a $-8 \pmod{3}$?

Ao analisar o relógio no sentido anti-horário, podemos notar que temos os números sequencialmente 0, 2, 1, 0, 2, 1, Então, com base na sequência, podemos verificar que o termo -8 está na posição 1 do relógio, concluindo que

$$-8 \pmod{3} \equiv 1.$$

Exemplo 9

Verifique se a seguinte congruência é verdadeira ou falsa:

$$8 \equiv -6 \pmod{7}.$$

Aplicando a propriedade demonstrada, temos que $7 \mid 8 - (-6) \Rightarrow 7 \mid 14$, o que mostra que a congruência é verdadeira, pois 14 é divisível por 7.

Exemplo 10

Verifique se a seguinte congruência é verdadeira ou falsa:

$$19 \equiv 10 \pmod{8}.$$

Aplicando a Proposição 8, temos que $8 \mid 19 - 10 \Rightarrow 8 \mid 9$, o que mostra que a congruência não é verdadeira, pois 9 não é divisível por 8.

2.4 PROPRIEDADES GERAIS DA ARITMÉTICA MODULAR

Sejam $a, b, c, d, m \in \mathbb{Z}$ e $m > 1$ (POTI, 2017).

Proposição 11

Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.

Demonstração

Tomando a definição da aritmética modular, $a \equiv b \pmod{m}$, temos que

$$a = k \cdot m + b \Rightarrow -b = k \cdot m - a \Rightarrow b = -k \cdot m + a.$$

Como $-k$ é um número inteiro qualquer, podemos afirmar que

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

Proposição 12

Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

Demonstração

Pelas definições $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, temos que $a = k \cdot m + b$ e $b = p \cdot m + c$.

Substituindo o valor de b da segunda equação na primeira, temos

$$a = k \cdot m + p \cdot m + c,$$

$$a = (k + p) \cdot m + c.$$

Como o valor de $k + p$ é um número inteiro, podemos afirmar que

$$a \equiv c \pmod{m}. \quad \square$$

Proposição 13

Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $ad \equiv b \pmod{m}$.

Demonstração

Pelas definições, temos que $a = k \cdot m + b$ e $c = p \cdot m + d$. Substituindo o valor de c da segunda equação na primeira, temos

$$a(p \cdot m + d) = k \cdot m + b \Rightarrow apm + ad = km + b \Rightarrow ad = (k - ap)m + b.$$

Como o valor de $k - ap$ é um número inteiro, podemos afirmar que

$$ad \equiv b \pmod{m}. \quad \square$$

Proposição 14

O resto da soma é a soma dos restos. Sabendo que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$.

Demonstração

Partindo do enunciado da proposição,

$$a \equiv b \pmod{m} \Rightarrow m \mid b - a,$$

$$c \equiv d \pmod{m} \Rightarrow m \mid c - d.$$

Como $b - a$ e $d - c$ são divisíveis por m , a soma desses dois números também é divisível por m . Então, podemos verificar que

$$m \mid b - a + d - c \Rightarrow m \mid b + d - (a + c).$$

Aplicando a definição $x \equiv y \pmod{m} \Rightarrow m \mid y - x$, temos que

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

Exemplo 15

Qual é o resto de $25 + 32$ na divisão por 7?

Aplicando o algoritmo da divisão, temos que

$$25 = 3 \cdot 7 + 4 \Rightarrow 4 \equiv 25 \pmod{7},$$

$$32 = 4 \cdot 7 + 4 \Rightarrow 4 \equiv 32 \pmod{7}.$$

Com base nos algoritmos apresentados, podemos verificar que sempre que subtraímos o dividendo do resto, encontramos um múltiplo do divisor. Aplicando isso nos algoritmos supracitados, é possível concluir que $25 - 4 = 21$ e $32 - 4 = 28$. Com isso, sabemos que tanto 21 quanto 28 são múltiplos de 7. Adicionando esses dois valores, obtemos $21 + 28 = 49$, que também é múltiplo de 7.

Aplicando a propriedade $a + c \equiv b + d \pmod{m}$,

$$4 + 4 \equiv 25 + 32 \pmod{7},$$

$$8 \equiv 1 \equiv 57 \pmod{7}, \text{ pois } 57 = 8 \cdot 7 + 1.$$

Então, concluímos que, o resto da soma é a soma dos restos.

Proposição 16

$a \equiv b \pmod{m}$ e $c \equiv d \pmod{m} \Rightarrow a - c \equiv b - d \pmod{m}$.

Demonstração

$$a \equiv b \pmod{m} \Rightarrow m \mid b - a,$$

$$c \equiv d \pmod{m} \Rightarrow m \mid d - c.$$

Dado que tanto $b - a$ e $d - c$ são divisíveis por m , sabemos que a subtração desses dois números é divisível por m . Então

$$\begin{aligned} m \mid b - a - (d - c) &\Rightarrow \\ \Rightarrow m \mid b - a - d + c &\Rightarrow \\ \Rightarrow m \mid (b - d) - (a - c). \end{aligned}$$

Aplicando a definição $x \equiv y \pmod{m} \Rightarrow m \mid y - x$, temos que

$$a - c \equiv b - d \pmod{m}. \quad \square$$

Exemplo 17

Qual é o resto de $42 - 27$ na divisão por 5?

Aplicando o algoritmo da divisão, temos que

$$27 = 5 \cdot 5 + 2 \Rightarrow 2 \equiv 27 \pmod{5},$$

$$32 = 6 \cdot 5 + 2 \Rightarrow 2 \equiv 32 \pmod{5}.$$

Ao subtrairmos o resto de cada um dos números, encontramos os resultados $27 - 2 = 25$ e $32 - 2 = 30$, que são múltiplos de 5. Agora verificamos que $32 - 27 = 5$, obtemos um valor que também é múltiplo de 5.

Aplicando a propriedade $a - c \equiv b - d \pmod{m}$ para os números 27 e 32, temos

$$2 - 2 \equiv 32 - 27 \pmod{5},$$

$$0 \equiv 5 \pmod{5}.$$

Então, com base nas informações obtidas após a aplicação da Proposição 16, $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m} \Rightarrow a - c \equiv b - d \pmod{m}$, podemos concluir que $0 \equiv 5 \pmod{5}$.

Proposição 18

$a \equiv b \pmod{m} \Rightarrow a + d \equiv b + d \pmod{m}$

Demonstração

Sabemos que $a \equiv b + k \cdot m$, então adicionando o mesmo número d em ambos os lados da equivalência, temos $a + d \equiv b + d + k \cdot m$. Agrupando a e d , e também b e d , temos que $(a + d) \equiv (b + d) + k \cdot m$, concluindo que

$$(a + d) \equiv (b + d) \pmod{m}. \quad \square$$

Proposição 19

$$a \equiv b \pmod{m} \Rightarrow a - d \equiv b - d \pmod{m}$$

Demonstração

Sabemos que $a \equiv b + k \cdot m$, então subtraindo o mesmo número d em ambos os lados da equivalência, temos que $a - d \equiv b - d + k \cdot m$. Agrupando a e d , e também b e d , temos que

$$(a - d) \equiv (b - d) + k \cdot m,$$

$$(a - d) \equiv (b - d) \pmod{m}. \quad \square$$

Proposição 20

O resto do produto é igual ao produto dos restos. Sabendo que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a \cdot c \equiv b \cdot d \pmod{m}$.

Demonstração

Pelas definições, temos que $a = k \cdot m + b$ e $c = p \cdot m + d$. Multiplicando cada um dos membros das igualdades, temos $ac \equiv (km + b)(pm + d)$. Aplicando a propriedade distributiva, temos $ac \equiv kmpm + kmd + bpm + bd$. Colocando m em evidência, $ac \equiv m(kpm + kd + bp) + bd$. Sabendo que o termo $kpm + kd + bp$ é uma constante inteira, pois é formado por produtos e adição de números inteiros, podemos afirmar que $(kpm + kd + bp) = y$, com $y \in \mathbb{Z}$. Então

$$ac \equiv my + bd \Rightarrow ac \equiv bd \pmod{m}. \quad \square$$

Proposição 21

$ac \equiv bc \pmod{m} \Rightarrow a \equiv b \pmod{\frac{m}{d}}$, $d = (c, m)$ é o mdc (Máximo Divisor Comum) de c e m .

Demonstração

Sabendo que d é o mdc de c e m , temos que

$$d = (c, m) \Rightarrow \left(\frac{c}{d}, \frac{m}{d} \right) = 1.$$

Com base nesse resultado, $ac \equiv bc \pmod{m} \Rightarrow ac \equiv bc + km \Rightarrow ac - bc = km \Rightarrow c(a - b) = km$. Dividindo os dois membros por d , temos

$$\frac{c}{d}(a - b) = k \frac{m}{d}.$$

Podemos verificar que as frações, tanto no primeiro quanto no segundo membro, são primos entre si, ou seja, não possuem divisor comum. Daí verificamos que $a - b$ é divisível por $\frac{m}{d}$ e k é divisível por $\frac{c}{d}$. Portanto,

$$\frac{m}{d} \mid a - b \Rightarrow (a - b) = \frac{m}{d} \cdot (\text{constante}) \Rightarrow a \equiv b + \frac{m}{d} \cdot (\text{constante}) \Rightarrow a \equiv b \pmod{m}. \quad \square$$

Proposição 22

$$a \equiv b \pmod{m} \Rightarrow a \cdot k \equiv b \cdot k \pmod{m}$$

Demonstração

Pela definição de congruência, temos que $a \equiv b \pmod{m} \Rightarrow m \mid b - a$. Sabendo que tanto $b - a$ é divisível por m , como o produto de qualquer valor k por $b - a$ também é divisível por m , logo $k \cdot (b - a)$ é divisível por m . \square

Exemplo 23

Qual é o resto de 101 na divisão por 5? E o resto de 404 na divisão por 5?

$$101 = 20 \cdot 5 + 1 \Rightarrow 1 \equiv 101 \pmod{5},$$

$$404 = 80 \cdot 5 + 4 \Rightarrow 4 \equiv 404 \pmod{5}.$$

Sabemos que $404 = 101 \cdot 4$. Aplicando a propriedade $a \cdot k \equiv b \cdot k \pmod{m}$,

$$1 \equiv 101 \pmod{5},$$

$$1 \cdot 4 \equiv 101 \cdot 4 \pmod{5},$$

$$4 \equiv 404 \pmod{5}.$$

Assim, verificamos que o resto de 101 na divisão por 5 é 1 e 404 na divisão por 5 é 4.

Proposição 24

$$a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}, \forall n \in \mathbb{N}$$

Demonstração por indução

i) Para $n = 1$ (caso base), temos que

$$a^1 \equiv b^1 \pmod{m} \Rightarrow a \equiv b \pmod{m}, \text{ constatando que é verdadeira a proposição.}$$

ii) Pela hipótese de indução, temos que $a^n \equiv b^n \pmod{m}$, para algum $n \in \mathbb{N}$. Então, precisamos mostrar que

$$a^{n+1} \equiv b^{n+1} \pmod{m}.$$

A partir de $a \equiv b \pmod{m}$ e $a^n \equiv b^n \pmod{m}$, e aplicando a propriedade onde podemos multiplicar membro a membro os termos das equivalências, Proposição 22, temos que

$$aa^n \equiv bb^n \pmod{m} \Rightarrow a^{n+1} \equiv b^{n+1} \pmod{m}. \quad \square$$

Assim, demonstramos que a Proposição 24 é verdadeira.

Pequeno Teorema de Fermat

Seja P um número primo e $a \in \mathbb{Z}$, então $a^p \equiv a \pmod{p}$ (HEFEZ, 2009).

Demonstração

Iremos demonstrar o pequeno teorema de Fermat em duas partes.

Caso 1. Se a é múltiplo de p .

Se a for múltiplo de p , então $a \equiv 0 \pmod{p}$. Aplicando a propriedade da potência, Proposição 24, vamos elevar a congruência ao expoente p . Então, temos

$$a^p \equiv 0^p \pmod{p} \Rightarrow a^p \equiv 0 \pmod{p}.$$

Mas sabemos que $a \equiv 0 \pmod{p}$, então concluímos que $a^p \equiv a \pmod{p}$.

Comprovando, assim, que o teorema é verdadeiro.

Caso 2. Se a não é múltiplo de p .

Para uma melhor compreensão teórica, utilizaremos algumas definições que são propostas conforme o livro (DOMINGUES, 2003), que define propriedades da multiplicação em um conjunto Z_m ($m > 1$) de classes de restos. Dadas duas classes $\bar{a}, \bar{b} \in \mathbb{Z}_m$, chama-se produto $\bar{a} \cdot \bar{b}$, a classe $\overline{a \cdot b}$. Então, para qualquer $\bar{a} \in \mathbb{Z}_m$, temos

$$\bar{a} \cdot \bar{1} = \overline{a \cdot 1} = \bar{a}.$$

Portanto, $\bar{1}$ é o neutro da multiplicação em \mathbb{Z}_m .

Provaremos que $\bar{a} \in \mathbb{Z}_m$ é simetrizável para a multiplicação se, e somente se, $\text{mdc}(a, m) = 1$.

(\rightarrow) Seja $\bar{a} \in \mathbb{Z}_m$ um elemento inversível. Existe, então, $\bar{a} \cdot \bar{a}' = \overline{a \cdot a'} = \bar{1}$. Daí, $aa' \equiv 1 \pmod{m}$ ou $aa' - 1 = mq$, para algum $q \in \mathbb{Z}$. A proposição 2, que também está no livro (DOMINGUES, 2003), na página 46, garante então que $\text{mdc}(a, m) = 1$.

(\leftarrow) Se $\text{mdc}(a, m) = 1$, então, devido à proposição 2 supracitada, existem $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + my_0 = 1$. Dessa igualdade segue que $ax_0 - 1 = m(-y_0)$ e, portanto, que $ax_0 \equiv 1 \pmod{m}$. De onde, $\overline{ax_0} = 1$ ou $\bar{a} \cdot \bar{x_0} = \bar{1}$, igualdade que mostra que \bar{a} é inversível e $\bar{x_0}$ é seu inverso.

Portanto, quando a não é múltiplo de p , eles são primos entre si e podemos concluir que $\text{mdc}(a, p) = 1$. Para garantir a propriedade do cancelamento em congruência modular, é necessário que esse número possua um inverso multiplicativo para garantir o elemento neutro da multiplicação, onde qualquer número multiplicado pelo seu inverso multiplicativo

é sempre 1. Então, a classe inversa são os números pelos quais multiplicados pelos números apresentados resultam no elemento neutro da multiplicação, garantindo assim a lei do cancelamento. Como a e p são primos entre si, a classe a tem classe inversa módulo p . Seja a' a classe inversa de a e sabendo que o produto de um número pela sua classe inversa é o elemento neutro da multiplicação, então é possível concluir que

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

Para provar essa segunda parte da demonstração, devemos provar que $a^{p-1} \equiv 1 \pmod{p}$ quando $\text{mdc}(a, p) = 1$. Iremos utilizar 4 etapas, descritas a seguir.

Considere a sequência $(a, 2a, 3a, \dots, (p-1)a)$.

i) Esta é uma sequência de $p-1$ múltiplos de a na qual não há múltiplos de p . Dado $k \in \{1, 2, 3, \dots, p-1\}$, vamos supor que exista k tal que ka seja múltiplo de p .

Então $p \mid ka$, sabendo que p é o maior de todos os valores de k possíveis. Assim, podemos concluir que $p \mid a$, o que contradiz a hipótese inicial, e isto é um absurdo, então não existe k tal que ka seja múltiplo de p .

ii) Na sequência não há dois números congruentes módulo p .

Para validarmos a afirmação que na sequência não existem dois números congruentes módulo p , iremos tomar dois valores da sequência inicialmente proposta $(a, 2a, 3a, \dots, (p-1)a)$ tais que $k_1, k_2 \in (1, 2, 3, \dots, p-1)$, sabendo que $k_1 \neq k_2$ e que $ak_1 \equiv ak_2 \pmod{p}$. Como a e p são primos entre si, a classe a tem classe inversa a' . Aplicando a' na congruência, temos que $aa'k_1 \equiv aa'k_2 \pmod{p}$, lembrando que o produto de a e sua classe inversa a' é o elemento neutro, então $k_1 \equiv k_2 \pmod{p}$.

Como $k_1, k_2 \in (1, 2, 3, \dots, p-1)$, isso garante que eles são congruentes, então eles são iguais, o que contradiz a hipótese inicial por absurdo.

iii) Cada um dos números da sequência é congruente \pmod{p} com apenas um elemento da sequência $(1, 2, 3, \dots, p-1)$, de forma biunívoca. Podemos verificar isso observando que, pelo item *ii)* acima, não há dois números da sequência $(a, 2a, 3a, \dots, (p-1)a)$ que sejam congruentes módulo p . Em outras palavras, não há dois números dessa sequência que possuam o mesmo resto na divisão por p . Assim, cada termo de $(a, 2a, 3a, \dots, (p-1)a)$ está associado a um único termo de $(1, 2, 3, \dots, p-1)$ (que são os possíveis restos da divisão por p), biunovocamente.

iv) Neste passo vamos multiplicar entre si todos os termos da sequência $(a, 2a, 3a, \dots, (p-1)a)$. Então, temos que

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

Lembrando que o $\text{mdc}(p, (p-1)!) = 1$, pois eles são primos entre si e isso garante a lei do corte, então $a^{p-1} \equiv 1 \pmod{p}$. Assim, o caso 2 é verdadeiro. Mostramos, então, as duas possibilidades que enunciamos no início da demonstração, provando assim a validade do pequeno teorema de Fermat. \square

2.5 RESOLUÇÕES DE EXERCÍCIOS QUE ENVOLVEM CONGRUÊNCIA MODULAR

2.5.1 Questão 1

(Colégio Naval - 2017) Os números x e y pertencem ao conjunto $C = \{17, 20, 23, 26, \dots, 2018\}$ e são tais que $x > y$. Sendo assim, pode-se concluir que $2017 \cdot 2^x + 8^y$, na divisão por 7, deixa qual valor de resto (EFOMM, 2007)?

- a) 0
- b) 1
- c) 3
- d) 4
- e) 5

Para resolver este problema, iremos utilizar as Proposições 14 e 20.

Proposição 14. O resto da soma é a soma dos restos. Sabendo que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$.

Iremos, agora, mostrar através de um exemplo, a aplicação da Proposição 14.

Dado o número 23, qual é o resto na divisão por 5? Verificamos que o resto é 3 quando dividimos 23 por 5. Fazendo uma decomposição de 23, podemos notar que

$$23 = 20 + 3,$$

$$20 = 4 \cdot 5 + 0 \Rightarrow 20 \equiv 0 \pmod{5},$$

$$3 = 0 \cdot 5 + 3 \Rightarrow 3 \equiv 3 \pmod{5}.$$

Então, aplicando a Proposição 14, temos que

$$23 = 4 \cdot 5 + 3 \Rightarrow 23 \equiv 3 \pmod{5}.$$

Proposição 20. O resto do produto é igual ao produto dos restos. Sabendo que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$ então, $a \cdot c \equiv b \cdot d \pmod{m}$

Iremos, agora, mostrar através de um exemplo, a aplicação da Proposição 20.

Dado o número 21, qual é o resto da divisão por 5? Verificamos que o resto é 1 quando dividimos 21 por 5. Fazendo a decomposição de 21, podemos notar que

$$21 = 3 \cdot 7,$$

$$3 \equiv 3 \pmod{5},$$

$$7 \equiv 2 \pmod{5}.$$

Aplicando a proposição 20, multiplicando os termos de uma equivalência pela outra, temos que

$$21 \equiv 6 \pmod{5} \equiv 1 \pmod{5}.$$

Resolução da Questão 1

Dado $2017 \cdot 2^x + 8^y$, podemos verificar que as Proposições 14 e 20 citadas podem ser utilizadas para efetuar o cálculo, então analisando cada um dos números de $2017 \cdot 2^x + 8^y$, sejam r_1 o resto da divisão de 2017 por 7, r_2 o resto da divisão de 2^x por 7, e r_3 o resto da divisão de 8^y por 7.

Vamos analisar separadamente cada uma das potências que fazem parte da expressão $2017 \cdot 2^x + 8^y$ e verificar seus últimos algarismos, para analisar se há algum padrão numérico, e logo após a verificação iremos aplicar as Proposições 14 e 20.

Podemos notar que $2017 = 2016 + 1 = 288 \cdot 7 + 1$, então concluímos que $r_1 = 1$.

Verificando a potência 2^x , podemos notar que

$$2^0 = 1 \equiv 1 \pmod{7},$$

$$2^1 = 2 \equiv 2 \pmod{7},$$

$$2^2 = 4 \equiv 4 \pmod{7},$$

$$2^3 = 8 \equiv 1 \pmod{7},$$

$$2^4 = 16 \equiv 2 \pmod{7},$$

$$2^5 = 32 \equiv 4 \pmod{7}.$$

Então, sabendo que $C = \{17, 20, 23, 26, \dots, 2018\}$, seguindo o raciocínio de modo análogo, concluímos que

$$2^{15} = 1 \pmod{7},$$

$$2^{16} = 2 \pmod{7},$$

$$2^{17} = 4 \pmod{7}.$$

Levando em conta o conjunto C e as sequências de restos, concluimos que $r_2 = 4$.

Verificando a potência 8^x , podemos notar que

$$8^1 = 1 \pmod{7},$$

$$8^2 = 1 \pmod{7},$$

$$8^3 = 1 \pmod{7}.$$

Então, independente do valor do expoente n , o resto sempre será o mesmo na divisão por 7, portanto concluimos que $r_3 = 1$.

Sabendo o valor dos restos e aplicando as propriedades da soma e produto dos restos (proposições 14 e 20), temos que

$$2017 \cdot 2^x + 8^y,$$

$$r_1 \cdot r_2 + r_3 = 1 \cdot 4 + 1 = 5.$$

Portanto, o resto de $2017 \cdot 2^x + 8^y$ por 7 é 5.

Verificamos que neste tipo de problema de cálculo de resto é necessário tomar cada termo e verificar os restos independentemente, para que venhamos descobrir o resto de cada um pelo valor determinado pelo enunciado do problema. E, após isso, aplicam-se as propriedades das congruências e, assim, chega-se ao resto geral de uma expressão.

2.5.2 Questão 2

(ENQ 2009 - b) Prove, usando congruências, que $11^{n+2} + 12^{2n+1}$ é divisível por 133, para qualquer número natural n (PROFMAT, 2007).

Para resolver este problema, iremos utilizar as Proposições 14, 22 e 24.

Proposição 14. O resto da soma é a soma dos restos. Sabendo que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$.

Proposição 22. $a \equiv b \pmod{m} \Rightarrow a \cdot k \equiv b \cdot k \pmod{m}$.

Proposição 24. $a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}, \forall n \in \mathbb{N}$.

Resolução da Questão 2

Sabendo que $11 \equiv 11 \pmod{133}$, então aplicando a propriedade das potências (Proposição 24), podemos elevar os dois membros da equivalência por $n + 2$, resultando em $11^{n+2} \equiv 11^{n+2} \pmod{133}$, chegando, assim, ao valor da primeira parcela da soma.

Analizando agora a potência 12^{2n+1} , podemos notar que

$$12^2 = 144 = 1 \cdot 133 + 11 \equiv 11 \pmod{133}.$$

Partindo da equivalência $12^2 \equiv 11 \pmod{133}$ e elevando os dois membros à potência n , temos que

$$(12^2)^n \equiv (11)^n \pmod{133}.$$

Obtemos, como resultado, $12^{2n} \equiv 11^n \pmod{133}$ e agora multiplicamos ambos os membros por 12,

$$12^{2n} \cdot 12 \equiv 11^n \cdot 12 \pmod{133}.$$

Então, obtemos exatamente o valor da segunda parcela conforme o enunciado da questão, $12^{2n+1} \equiv 11^n \cdot 12 \pmod{133}$. Com esses resultados, obtivemos duas congruências e podemos aplicar a propriedade da soma,

$$11^{n+2} \equiv 11^{n+2} \pmod{133},$$

$$12^{2n+1} \equiv 11^n \cdot 12 \pmod{133}.$$

Somando os dois termos,

$$11^{n+2} + 12^{2n+1} \equiv 11^{n+2} + 11^n \cdot 12 \pmod{133},$$

$$11^{n+2} + 12^{2n+1} \equiv 11^n \cdot 121 + 11^n \cdot 12 \pmod{133},$$

$$11^{n+2} + 12^{2n+1} \equiv 11^n \cdot 133 \pmod{133}.$$

Sabendo que $11^n \cdot 133$ é múltiplo de 133, então podemos concluir que $11^{n+2} + 12^{2n+1} \equiv 0 \pmod{133}$, o que confirma que $11^{n+2} + 12^{2n+1}$ é divisível por 133. \square

Verificamos nos tipos de problemas que aparecem uma soma de potências, devemos analisar separadamente as potências, iniciando das bases mais simples e ir elevando os membros aos expoentes convenientes para chegarmos ao valor da parcela em análise e depois disso aplicar a propriedade da adição para chegar ao resultado final esperado.

2.5.3 Questão 3

(Teste de Seleção Suíço para a IMO) Prove que a equação $14x^2 + 15y^2 = 7^{2000}$ não possui solução (x, y) inteira (IMO, 2012).

Para resolver este problema, iremos utilizar as Proposições 14, 22 e 24.

Proposição 14. O resto da soma é a soma dos restos. Sabendo que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$.

Proposição 22. $a \equiv b \pmod{m} \Rightarrow a \cdot k \equiv b \cdot k \pmod{m}$.

Proposição 24. $a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}, \forall n \in \mathbb{N}$.

Resolução da Questão 3

Uma estratégia interessante e eficaz para problemas que trazem potências com expoentes muito grandes é procurar valores para dividir a base de modo que o resto seja 0 ou 1, pois assim o processo de potenciação fica fácil de se resolver. Para esta questão, um valor interessante é a divisão por 3, pois sobrarão resto 1 na divisão por 7. Assim,

$$7 = 2 \cdot 3 + 1 \equiv 1 \pmod{3},$$

$$7 \equiv 1 \pmod{3}.$$

Podemos aplicar a propriedade das potências, elevando ambos os membros por 2000, então temos que

$$7^{2000} \equiv 1^{2000} \pmod{3} \Rightarrow 7^{2000} \equiv 1 \pmod{3}.$$

Determinamos que 7^{2000} possui resto 1, agora iremos verificar $14x^2 + 15y^2$, também baseado na divisão por 3.

Vamos verificar a parcela $14x^2$ termo a termo.

Verificamos que

$$14 = 4 \cdot 3 + 2 \equiv 2 \pmod{3},$$

$$14 \equiv 2 \pmod{3}.$$

Para o valor de x^2 , temos que um quadrado perfeito sempre deixa resto 0 ou 1 quando dividido por 3, como podemos verificar a seguir.

Todo número inteiro par pode ser escrito como $2k$; quando é elevado ao quadrado, temos $4k^2$, que é múltiplo de 4 cujos restos na divisão por 3 só podem ser 0 se for múltiplo de 3 e 4 ou 1 se for múltiplo de 4. Para um quadrado perfeito ímpar cuja forma geral é $2k + 1$, seu quadrado é $(2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$. Observamos que dois números consecutivos multiplicados, $k(k + 1)$, é par, e multiplicado por 4 continua sendo par e múltiplo de 4. Todo múltiplo de 4, multiplicado por um número par é múltiplo de 8, ao adicionarmos 1 a este produto, teremos um número ímpar, que ao ser dividido por 3, sempre deixa resto 1. Então, concluímos que

$$x^2 \equiv 0 \pmod{3} \text{ ou } x^2 \equiv 1 \pmod{3}.$$

Aplicando a propriedade da multiplicação, temos

$$14 \equiv 2 \pmod{3} \text{ e } x^2 \equiv 0 \pmod{3}, \text{ obtendo assim}$$

$$14x^2 \equiv 2 \cdot 0 \pmod{3} \Rightarrow 14x^2 \equiv 0 \pmod{3},$$

ou, também,

$14 \equiv 2 \pmod{3}$ e $x^2 \equiv 1 \pmod{3}$, obtendo assim

$$14x^2 \equiv 2 \cdot 1 \pmod{3} \Rightarrow 14x^2 \equiv 2 \pmod{3}.$$

Vamos analisar a parcela $15y^2$ termo a termo.

Verificamos que

$$15 = 5 \cdot 3 + 0 \equiv 0 \pmod{3},$$

$$15 \equiv 0 \pmod{3}.$$

Neste caso não precisamos mais analisar o valor y^2 , pois aplicando a propriedade da multiplicação, temos

$15 \equiv 0 \pmod{3}$ e $y^2 \equiv 0 \pmod{3}$, obtendo assim

$$15y^2 \equiv 0 \cdot 0 \pmod{3} \Rightarrow 15y^2 \equiv 0 \pmod{3},$$

ou, também,

$15 \equiv 0 \pmod{3}$ e $y^2 \equiv 1 \pmod{3}$, obtendo assim

$$15y^2 \equiv 0 \cdot 1 \pmod{3} \Rightarrow 15y^2 \equiv 0 \pmod{3}.$$

Com base nos resultados obtidos e aplicando a propriedade da soma, resulta em duas possibilidades. Primeiro, adicionando $14x^2 \equiv 0 \pmod{3}$ e $15y^2 \equiv 0 \pmod{3}$, resulta em $14x^2 + 15y^2 \equiv 0 \pmod{3}$. Já na segunda possibilidade, adicionando $14x^2 \equiv 2 \pmod{3}$ e $15y^2 \equiv 0 \pmod{3}$, resulta em $14x^2 + 15y^2 \equiv 2 \pmod{3}$.

Partindo da equação inicial $14x^2 + 15y^2 = 7^{2000}$ e sabendo que $7^{2000} \equiv 1 \pmod{3}$, chegamos a um absurdo. Assim, provamos que não há solução inteira (x, y) para a equação dada. \square

Neste tipo de questão em que é dada uma equação, devemos procurar um número conveniente para efetuarmos as divisões e analisar termo a termo cada uma das parcelas e membros da equação para chegarmos a um resultado verdadeiro ou a um absurdo, por isso os valores mais convenientes geralmente são 2 ou 3, mas isso não é uma regra, apenas uma sugestão.

2.5.4 Questão 4

(Olimpíada Cearense de Matemática 2014. Nível 3) Prove que não existem $x, y, z \in \mathbb{N}$ tais que $13x^4 + 3y^4 - z^4 = 2014$ (UFCE, 2014).

Para resolver este problema, iremos utilizar as Proposições 14, 16, 22 e 24.

Proposição 14. O resto da soma é a soma dos restos. Sabendo que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$.

Proposição 16. O resto da subtração é a subtração dos restos.

Proposição 22. $a \equiv b \pmod{m} \Rightarrow a \cdot k \equiv b \cdot k \pmod{m}$.

Proposição 24. $a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}, \forall n \in \mathbb{N}$.

Resolução da Questão 4

Devemos procurar valores para efetuar a divisão por números grandes sempre que sobra resto 1, mas também devemos observar as potências para que possamos encontrar um valor mais conveniente para usar como divisor.

O valor x^4 , ou seja, um número elevado à quarta potência deixa resto 0 ou 1 quando dividido por 8, como iremos verificar a seguir.

Todo número inteiro par pode ser escrito como $2k$; quando é elevado à quarta potência, temos $16k^4$, que é um múltiplo de 8 cujo resto na divisão por 8 só pode ser 0. Caso o número analisado seja ímpar, sua forma geral é $2k + 1$ e ao elevá-lo à quarta potência, temos

$$\begin{aligned} (2k + 1)^4 &= (4k^2 + 4k + 1)(4k^2 + 4k + 1) = \\ &= 16k^4 + 32k^3 + 24k^2 + 8k + 1 = 8(2k^4 + 4k^3 + 3k^2 + k) + 1, \end{aligned}$$

podemos observar que é um múltiplo de 8 adicionado a 1, ou seja, na divisão por 8, o resto é 1. Assim,

$$x^4 \equiv 0 \pmod{8} \text{ ou } x^4 \equiv 1 \pmod{8}.$$

Verificando os coeficientes de $13x^4 + 3y^4 - z^4$, temos que

$$13 = 1 \cdot 8 + 5 \equiv 5 \pmod{8},$$

$$3 = 0 \cdot 8 + 3 \equiv 3 \pmod{8},$$

$$1 = 0 \cdot 8 + 1 \equiv 1 \pmod{8}.$$

Aplicando as propriedades da multiplicação, temos

$$\begin{aligned} 13 &\equiv 5 \pmod{8} \text{ e } x^4 \equiv 0 \pmod{8} \text{ ou } x^4 \equiv 1 \pmod{8}, \text{ obtendo assim} \\ 13x^4 &\equiv 5 \cdot 0 \pmod{8} \Rightarrow 13x^4 \equiv 0 \pmod{8} \text{ ou } 13x^4 \equiv 5 \cdot 1 \pmod{8} \Rightarrow 13x^4 \equiv 5 \pmod{8}, \\ 3 &\equiv 3 \pmod{8} \text{ e } y^4 \equiv 0 \pmod{8} \text{ ou } y^4 \equiv 1 \pmod{8}, \text{ obtendo assim} \\ 3y^4 &\equiv 3 \cdot 0 \pmod{8} \Rightarrow 3y^4 \equiv 0 \pmod{8} \text{ ou } 3y^4 \equiv 3 \cdot 1 \pmod{8} \Rightarrow 3y^4 \equiv 3 \pmod{8}. \end{aligned}$$

Já para as potências de z , verificamos que $z^4 \equiv 0 \pmod{8}$ ou $z^4 \equiv 1 \pmod{8}$.

Agora que já temos os valores de cada parcela, podemos aplicar a propriedade da soma e subtração e concluir que os valores possíveis para o primeiro membro da equação podem ser $(0, 2, 3, 4, 5, 7) \pmod{8}$.

Analisando o segundo membro da equação, temos que

$$2014 = 151 \cdot 8 + 6 \equiv 6 \pmod{8}.$$

Então, ao compararmos os dois membros da equação, podemos notar um absurdo. Assim, concluímos que não existem $x, y, z \in \mathbb{N}$ tais que $13x^4 + 3y^4 - z^4 = 2014$. \square

Neste tipo de problema, foi fundamental a análise das potências, então devemos observar as potências que aparecem nas equações, e logo após isso, seus respectivos coeficientes. Em seguida, efetuamos as respectivas adições ou subtrações e, por fim, analisamos o outro membro da equação e comprovamos a igualdade ou o absurdo.

2.5.5 Questão 5

(ENQ 2019.2 Questão 8b) Determine os números primos tais que p divide $3^p + 382$ (PROFMAT, 2007).

Para resolver este problema, iremos utilizar a Proposição 14 e o Pequeno Teorema de Fermat.

Proposição 14. O resto da soma é a soma dos restos. Sabendo que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$.

Pequeno Teorema de Fermat. $a^p \equiv a \pmod{p}$

Resolução da Questão 5

Dado o pequeno teorema de Fermat, temos que

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

$$3^p \equiv 3 \pmod{p}.$$

Aplicando a propriedade da adição e somando 382 em ambos os membros da equivalência, temos

$$3^p + 382 \equiv 3 + 382 \pmod{p} \Rightarrow 3^p + 382 \equiv 385 \pmod{p}.$$

Para que p divida $3^p + 382$, ele também deve dividir 385 e vice-versa. Decompondo 385, temos que $385 = 5 \cdot 7 \cdot 11$, e como p é um número primo, podemos concluir que p pode ser tanto 5, 7 ou 11. \square

Quando o enunciado da questão citar números primos, devemos observar se há a possibilidade de aplicar o pequeno teorema de Fermat, para facilitar a resolução e aplicação

de outras propriedades de aritmética modular. Após a transformação da potência em um valor sem expoente, basta aplicar as propriedades adequadas. Nesta questão foi utilizada a soma de um número natural em ambos os membros da congruência, facilitando, assim, a resolução do problema.

2.5.6 Questão 6

(Colégio Naval - 2018) Qual é o último algarismo de $(2018^{2018})^{2018}$ (EFOMM, 2007)?

Para resolver este problema, iremos utilizar a Proposição 24.

Proposição 24. $a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}, \forall n \in \mathbb{N}$.

Resolução da Questão 6

Com base no enunciado $(2018^{2018})^{2018}$, tomamos o número 2018 e aplicamos o algoritmo da divisão, obtendo

$$2018 = 201 \cdot 10 + 8.$$

Para determinar o último algarismo no sistema de numeração decimal, basta fazer a divisão do número dado por 10. Com base neste conceito e tomando o valor de $x = 2018$, mostra-se que

$$x = 2018 = 201 \cdot 10 + 8 \equiv 8 \pmod{10}.$$

Aplicando a propriedade da potenciação, elevando os dois membros da equivalência por 2018, temos que

$$\begin{aligned} x^{2018} \equiv 8^{2018} \pmod{10} &\Rightarrow x^{2018} \equiv (2^3)^{2018} \pmod{10} \equiv 2^{6054} \pmod{10} \Rightarrow \\ &\Rightarrow x^{2018} \equiv 2^{6054} \pmod{10}. \end{aligned}$$

Com base nas análises dos expoentes da potência de 2, sabemos que seus últimos algarismos possuem um ciclo de repetição de 4 valores possíveis, que são 2, 4, 8 e 6, então devemos tomar o expoente 6054 e dividi-lo por 4, verificando, assim, que o resto é 2. Quando isso acontece, o último algarismo é 4. Então, temos

$$x^{2018} \equiv 2^{6054} \pmod{10} \equiv 4 \pmod{10}.$$

Agora, aplicando a potenciação novamente em ambos os membros da equivalência, temos

$$(x^{2018})^{2018} \equiv 4^{2018} \pmod{10}.$$

Sabemos que $x = 2018$, então já chegamos à expressão inicial do enunciado da questão, agora bastando observar novamente a regra dos finais da potência de 2. Assim,

$$(x^{2018})^{2018} \equiv (2018^{2018})^{2018} \equiv 4^{2018} \pmod{10},$$

$$(2018^{2018})^{2018} \equiv (2^2)^{2018} \pmod{10} \equiv 2^{4036} \pmod{10}.$$

Dividindo 4036 por 4 temos resto zero, então todas as potências de 2 quando seus expoentes são divididos por 4 e sobra resto zero, possuem 6 como último algarismo. Então, podemos concluir que

$$(2018^{2018})^{2018} \equiv 6 \pmod{10}. \quad \square$$

Portanto, o último algarismo é 6.

Neste tipo de exercício que pede o último algarismo, devemos utilizar a divisão por 10 como tentativa inicial, pois utilizamos o sistema de numeração decimal. Em seguida, devemos observar as potências que foram aplicadas e seus respectivos ciclos de últimos algarismos, para que venhamos a encontrar o último algarismo do problema.

Como podemos ver, a aritmética modular é bastante poderosa, por meio do método apresentado, podemos calcular, por exemplo, os últimos dois dígitos de 2 elevado a googol (10^{100})(LOBO, 2019).

2.5.7 Questão 7

(OBM - 2012) Qual é a maior potência de 2 que divide $2011^{2012} - 1$ (OBM, 2020)?

Para resolver este problema, iremos utilizar as Proposições 14 e 24.

Proposição 14. O resto da soma é a soma dos restos. Sabendo que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$.

Proposição 24. $a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}, \forall n \in \mathbb{N}$.

Resolução da Questão 7

Aplicando a fatoração do produto notável na diferença de dois quadrados, temos que

$$2011^{2012} - 1 = (2011^{1006} - 1)(2011^{1006} + 1) = (2011^{503} - 1)(2011^{503} + 1)(2011^{1006} + 1).$$

Sabendo que qualquer número ímpar elevado a um expoente natural continua sendo ímpar e adicionando -1 ou 1 a esta potência iremos obter um valor par, conseqüentemente um número divisível por 2. Tomando então $2011^{2012} - 1 = (2011^{503} - 1)(2011^{503} + 1)(2011^{1006} + 1)$, iremos verificar em cada parêntese resultante da decomposição do produto notável $2011^{2012} - 1$, a maior potência pela qual é divisível e, assim, encontraremos a maior potência de 2 pela qual $2011^{2012} - 1$ é divisível.

Agora iniciaremos a verificação de cada termo do produto individualmente.

Verificando a divisibilidade por 4 do primeiro termo, temos que $2011 = 502 \cdot 4 + 3 \equiv 3 \pmod{4} \equiv -1 \pmod{4}$. Elevando ambos os membros da congruência por 503 e adicio-

nando -1 em cada membro, temos

$$\begin{aligned} 2011^{503} &\equiv (-1)^{503} \pmod{4} \Rightarrow 2011^{503} \equiv -1 \pmod{4} \Rightarrow \\ &\Rightarrow 2011^{503} - 1 \equiv -1 - 1 \pmod{4} \equiv -2 \pmod{4} \equiv 2 \pmod{4}. \end{aligned}$$

Assim, podemos comprovar que $2011^{503} - 1$ não é divisível por 4, então a maior potência de 2 pelo qual $2011^{503} - 1$ é divisível é 2.

Vamos verificar a divisibilidade por 4 do segundo termo a partir de $2011 \equiv -1 \pmod{4}$. Elevando ambos os membros da congruência por 503 e adicionando $+1$ em cada membro, temos

$$\begin{aligned} 2011^{503} &\equiv (-1)^{503} \pmod{4} \Rightarrow 2011^{503} \equiv -1 \pmod{4} \Rightarrow \\ &\Rightarrow 2011^{503} + 1 \equiv -1 + 1 \pmod{4} \equiv 0 \pmod{4}. \end{aligned}$$

Concluimos que $2011^{503} + 1$ é divisível por 4. De modo análogo, iremos verificar a divisibilidade por 8, então podemos verificar que

$$2011 = 251 \cdot 8 + 3 \equiv 3 \pmod{8}.$$

Elevando ambos os membros da congruência por 503 e, após as operações matemáticas será adicionando $+1$ em cada membro, temos

$$\begin{aligned} 2011^{503} &\equiv 3^{503} \pmod{8} \Rightarrow 2011^{503} \equiv 3^{502} \cdot 3 \pmod{8} \Rightarrow 2011^{503} \equiv (3^2)^{251} \cdot 3 \pmod{8} \Rightarrow \\ &\Rightarrow 2011^{503} \equiv 9^{251} \cdot 3 \pmod{8}. \end{aligned}$$

Aplicando a definição da congruência modular no número 9, verificamos que ela possui resto 1 na divisão por 8. Então,

$$\begin{aligned} 2011^{503} &\equiv 1^{251} \cdot 3 \pmod{8} \Rightarrow 2011^{503} \equiv 3 \pmod{8} \Rightarrow \\ &\Rightarrow 2011^{503} + 1 \equiv 3 + 1 \pmod{8} \equiv 4 \pmod{8}. \end{aligned}$$

Verificamos, assim, que $2011^{503} + 1$ não é divisível por 8, então a maior potência de 2 pelo qual o segundo termo é divisível é 4.

Verificando a divisibilidade de $2011^{1006} + 1$ por 4, temos que $2011 \equiv -1 \pmod{4}$. Elevando ambos os membros da congruência por 1006 e adicionando $+1$ em cada membro, temos

$$\begin{aligned} 2011^{1006} &\equiv (-1)^{1006} \pmod{4} \Rightarrow 2011^{1006} \equiv 1 \pmod{4} \Rightarrow \\ &\Rightarrow 2011^{1006} + 1 \equiv 1 + 1 \pmod{4} \equiv 2 \pmod{4}. \end{aligned}$$

Verificamos que o terceiro termo não é divisível por 4, então a maior potência de 2 que é divisível é 2.

Com base nas informações obtidas nas análises dos três fatores do produto

$$(2011^{503} - 1) (2011^{503} + 1) (2011^{1006} + 1),$$

temos que, ao multiplicar essas três potências, encontramos a maior potência de 2 em que o número $2011^{2012} - 1$ é divisível.

A maior potência é 16, pois

$$2 \cdot 4 \cdot 2 = 16.$$

Neste tipo de problema devemos fazer as fatorações dos produtos notáveis que são possíveis na expressão inicial, e logo após verificar potência por potência em cada termo para constatar até qual delas o termo é divisível, e por fim multiplicar todas as potências encontradas, obtendo, assim, a maior potência pela qual a expressão é divisível.

2.6 APLICAÇÕES DE ARITMÉTICA MODULAR

2.6.1 Cadastro de Pessoas Físicas (CPF)

Com o aumento da população, é necessário criar formas de cadastro de identificação das pessoas, para um melhor acompanhamento das formas de negociação, organização ou até mesmo restrições que a pessoa possa sofrer devido seus atos. Então, foi necessário criar bases de dados para melhor controle da população em sua totalidade. No Brasil, temos vários cadastros como, por exemplo, o RG que possui um número de registro geral do cidadão, a CNH que define o número da carteira nacional de habilitação, temos o CNPJ que é um código que representa uma pessoa jurídica e, finalmente, o CPF que é um código numérico que representa uma pessoa física (CARVALHO; RODRIGUES; ARAÚJO, 2015).

Há sistemas de identificação que não usam um padrão definido como, por exemplo, o RG, mas já outros modelos são padronizados em todo território nacional como é o caso do CPF.

No Brasil, todo cidadão possui um código de pessoa física que é registrado na Receita Federal e este código recebe o nome de CPF e possui um padrão nacional. O CPF é composto de dois blocos de números. O primeiro é composto por 9 dígitos, que é chamado de número base. No número base, o nono dígito representa a região fiscal na qual o cadastro foi feito, já o segundo bloco é composto por 2 algarismos que recebe o nome de dígitos verificadores. O nono dígito representa o local onde o cadastro foi feito, se for 0 a região fiscal é Rio Grande do Sul, 1 (Distrito Federal, Goiás, Mato Grosso do Sul, Mato Grosso e Tocantins), 2 (Acre, Amazonas, Amapá, Pará, Rondônia e Roraima), 3 (Ceará, Maranhão e Piauí), 4 (Alagoas, Paraíba, Pernambuco e Rio Grande do Norte), 5 (Bahia e Sergipe), 6 (Minas Gerais), 7 (Espírito Santo e Rio de Janeiro), 8 (São Paulo) e 9 (Paraná e Santa Catarina).

Assim, todo CPF pode ser escrito obedecendo a seguinte ordenação

$$a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}, \text{ com } a_n \in \mathbb{Z} \text{ e } n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}.$$

Para determinar o décimo dígito que é o primeiro algarismo verificador, é necessário fazer o seguinte cálculo

$$\tilde{S} = \sum_{n=1}^9 n \cdot a_n, \text{ com } \tilde{S} \in \mathbb{Z}.$$

O número $\tilde{S} - a_{10}$ deve ser divisível por 11, que podemos escrever em forma da seguinte notação $11 \mid (\tilde{S} - a_{10})$, caso o resto for 0 ou 1 o décimo dígito será 0. Então, podemos concluir que

$$a_{10} \equiv \tilde{S} \pmod{11}.$$

Vamos calcular agora o décimo algarismo do CPF 331.125.248-XY, que por sinal foi registrado no estado de São Paulo, conforme podemos verificar pelo nono dígito do número base.

Para efetuar esse cálculo, devemos fazer as seguintes operações para determinar o valor de \tilde{S} .

$$\tilde{S} = a_1 \cdot 1 + a_2 \cdot 2 + a_3 \cdot 3 + a_4 \cdot 4 + a_5 \cdot 5 + a_6 \cdot 6 + a_7 \cdot 7 + a_8 \cdot 8 + a_9 \cdot 9,$$

$$\tilde{S} = 3 \cdot 1 + 3 \cdot 2 + 1 \cdot 3 + 1 \cdot 4 + 2 \cdot 5 + 5 \cdot 6 + 2 \cdot 7 + 4 \cdot 8 + 8 \cdot 9 = 174.$$

Sabendo que $174 = 15 \cdot 11 + 9$, aplicando a definição de congruências modulares, podemos concluir que $174 \equiv 9 \pmod{11}$. Da congruência conclui-se que o décimo dígito deste CPF é 9.

Para calcular o décimo primeiro dígito do CPF, ou seja, o segundo dígito verificador, o processo é similar, apenas acrescentando o algarismo zero como o primeiro termo da multiplicação pelos dígitos do CPF, conforme podemos verificar em

$$\tilde{S} = \sum_{n=1}^{10} (n - 1) \cdot a_n, \text{ com } \tilde{S} \in \mathbb{Z}.$$

O número $\tilde{S} - a_{11}$ deve ser também divisível por 11, que podemos escrever como $11 \mid (\tilde{S} - a_{11})$, caso o resto for 0 ou 1 o décimo dígito será 0. Assim, podemos concluir que

$$a_{11} \equiv \tilde{S} \pmod{11}.$$

Vamos calcular agora o décimo primeiro algarismo do CPF 331.125.248-9Y.

Para realizar esse cálculo devemos efetuar as seguintes operações para determinar o valor de \tilde{S} .

$$\tilde{S} = a_1 \cdot 0 + a_2 \cdot 1 + a_3 \cdot 2 + a_4 \cdot 3 + a_5 \cdot 4 + a_6 \cdot 5 + a_7 \cdot 6 + a_8 \cdot 7 + a_9 \cdot 8 + a_{10} \cdot 9,$$

$$\tilde{S} = 3 \cdot 0 + 3 \cdot 1 + 1 \cdot 2 + 1 \cdot 3 + 2 \cdot 4 + 5 \cdot 5 + 2 \cdot 6 + 4 \cdot 7 + 8 \cdot 8 + 9 \cdot 9 = 226.$$

Sabendo que $226 = 20 \cdot 11 + 6$, temos que $226 \equiv 6 \pmod{11}$, então podemos concluir que o décimo primeiro dígito deste CPF é 6.

Portanto, o CPF completo será 331.125.248-96.

2.6.2 ISBN-10

Em 1967, foi criado um sistema de catalogação de livros, sendo oficializado em 1972 como norma internacional, tal sistema é conhecido como ISBN ou *International Standard Book Number*. O ISBN-10 possui 10 algarismos, onde os nove primeiros são para a identificação do livro, que são distribuídos em três grupos de números de tamanho que pode variar e são separados por hífen. Sabe-se que os primeiros dígitos no sentido esquerda para direita representam um agrupamento nacional ou geográfico de editores da obra. Por exemplo, podemos verificar que o código do Brasil é 85, o segundo grupo é uma numeração que corresponde ao registro de uma editora e o último grupo de números é para identificar o título da obra que está sendo verificada. Mas como foi citado, esse sistema possui 10 algarismos e passou a ser identificado como ISBN-10. Já o décimo dígito é calculado através de congruência modular. Vamos descrever, a seguir, o procedimento do cálculo do ISBN-10 (BITTENCOURT et al., 2015).



Figura 3 – ISBN-10.

O ISBN-10 do livro Fundamentos da Matemática Elementar, Volume 1, é 85-357-0455-8. Para identificar o décimo dígito, que é de verificação, é realizado o seguinte cálculo. Vamos escrever o código no formato $a_1a_2a_3a_4\dots a_9N$, onde N é o dígito de controle. Tomemos, também, a sequência $(10, 9, 8, 7, \dots, 2, 1)$, onde multiplicaremos termo a termo os elementos

da primeira e da segunda sequência citadas anteriormente. Assim, temos

$$10a_1 + 9a_2 + 8a_3 + 7a_4 + \dots + 1a_{10} \equiv 0 \pmod{11}.$$

Aplicando o valor do ISBN-10 do livro citado anteriormente, temos

$$10 \cdot 8 + 9 \cdot 5 + 8 \cdot 3 + 7 \cdot 5 + 6 \cdot 7 + 5 \cdot 0 + 4 \cdot 4 + 3 \cdot 5 + 2 \cdot 5 + 1 \cdot N \equiv 0 \pmod{11},$$

$$80 + 45 + 24 + 35 + 42 + 0 + 16 + 15 + 10 + N \equiv 0 \pmod{11},$$

$$267 + N \equiv 0 \pmod{11}.$$

Aplicando o algoritmo da divisão no número 267, temos que $267 = 24 \cdot 11 + 3$. Podemos concluir que $267 \equiv 3 \pmod{11}$, então o valor de N , para que esse valor seja divisível por 11, deve ser 8, o que comprova o dígito de verificação do livro que estamos analisando. Quando o dígito da divisão por 11 for 10, foi convencionado que será utilizada a letra X em referência aos números romanos. Outra curiosidade sobre esse sistema é que até dezembro de 2006 ele foi amplamente utilizado, mas em janeiro de 2007 foi criado o ISBN-13 com 13 algarismos.

2.6.3 Código de Barras

Devido às grandes demandas de produtos, tanto na forma individual quanto em lotes, ou mesmo pessoas, foi necessário criar códigos de identificação para facilitar tanto o processo de estocagem de mercadorias quanto o transporte e rastreamento de produtos. O código de barras foi criado com essa finalidade, ou seja, para facilitar todos os processos citados. Esses códigos tiveram suas primeiras versões em estudos que se iniciaram por volta de 1850 e chegou ao formato que conhecemos pela primeira vez em 1973, quando teve sua apresentação por George J. Laurer (PONTES; SILVA, 2020). Inicialmente foi identificado como *Universal Product Code* com sigla (UPC) e possuía 12 algarismos, mas meses depois recebeu um décimo terceiro dígito para facilitar a identificação do país de origem. E com o acréscimo desse décimo terceiro dígito teve seu nome alterado para *European Article Numbering System* (EAN-13). A nomenclatura código de barras veio do advento que este é formado por um conjunto de barras que possuem larguras diferentes e isso faz com que esse conjunto venha a corresponder a um código numérico definido, onde houve a aplicação da congruência modular no processo. Então, um código pode representar um lote de mercadorias que possui as mesmas especificações ou apenas um único produto. Segundo fontes atuais, existem cerca de mais de 20 modelos diferentes de códigos de barra, mas iremos detalhar o modelo EAN-13, que é formado por treze algarismos. Vamos estudá-lo, pois é um dos mais utilizados no mundo atualmente. Este sistema utiliza a multiplicação por 1 e 3 nos algarismos do código da esquerda para a direita com os doze primeiros



Figura 4 – Código de barras.

algarismos e para determinar o último é necessário fazer a congruência módulo 10, obtendo, assim, o último algarismo que é chamado de dígito de controle.

Vamos agora mostrar como é o procedimento para obter esse dígito de controle. Seja a sequência dos doze primeiros dígitos de um código de barras $(a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10} a_{11} a_{12})$ e a sequência de multiplicação $(1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3)$. O produto deve ser feito e o resultado deve obedecer a seguinte congruência $S + a_{13} \equiv 0 \pmod{10}$. Para confirmação e verificação deste processo, vamos utilizar um código de barras real também retirado do livro Fundamentos da Matemática Elementar, Volume 1, de Gelson Iezzi e Carlos Murakami.

Com base no código de barras, os doze primeiros algarismos são $(9, 7, 8, 8, 5, 3, 5, 7, 0, 4, 5, 5)$. Aplicando a multiplicação, temos que

$$S = 9 \cdot 1 + 7 \cdot 3 + 8 \cdot 1 + 8 \cdot 3 + 5 \cdot 1 + 3 \cdot 3 + 5 \cdot 1 + 7 \cdot 3 + 0 \cdot 1 + 4 \cdot 3 + 5 \cdot 1 + 5 \cdot 3 = 134.$$

Aplicando a regra para a definição do dígito de controle, temos $S + a_{13} \equiv 0 \pmod{10}$, então

$$134 + a_{13} \equiv 0 \pmod{10}.$$

Assim, aplicando o algoritmo da divisão no número 134, temos que $134 = 13 \cdot 10 + 4$. Podemos concluir que $134 \equiv 4 \pmod{10}$, então o valor de a_{13} para que esse valor seja divisível por 10 deve ser 6, o que comprova o dígito de controle do código de barras do livro que estamos analisando.

2.6.4 Criptografia

A etimologia da palavra criptografia vem do grego e significa “escrita escondida”, ou seja, vem da ideia de se comunicar por meio de mensagens secretas, tanto para assuntos militares quanto para diplomacia. Podemos constatar que os egípcios, os gregos e no geral, os romanos, utilizavam esse recurso para que as mensagens não fossem decifradas, caso fossem interceptadas (PINHEIRO et al., 2018). Já na segunda guerra mundial em 1939, a utilização de mensagens criptografadas foi de maneira bastante difundida. Países como a Inglaterra possuíam pessoas especializadas para decodificar esses códigos e decifrar mensagens secretas, que poderiam ser de grande importância para a vitória de uma batalha. Hoje em dia, a criptografia é de suma importância devido ao grande volume de troca de mensagens, informações importantes, estudos científicos, entre várias outras aplicações. Um sistema criptográfico bem antigo, utilizado pelo imperador romano Júlio César é a criptografia de César ou Cifra de César, que consistia em trocar uma letra do alfabeto por outra letra que ficava três posições a frente dela para o envio, chamado de chave 3, e quando o receptor recebia o código cifrado, fazia o processo inverso, voltando três posições para cada letra. A Cifra de César é baseada na aritmética modular, pois temos um alfabeto com 26 letras, ao qual é atribuído um valor de zero até vinte e cinco, conforme a Tabela 1.

LETRA	A	B	C	D	E	F	G	H	I	J	K	L	M
NÚMERO CORRESPONDENTE	0	1	2	3	4	5	6	7	8	9	10	11	12
LETRA	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
NÚMERO CORRESPONDENTE	13	14	15	16	17	18	19	20	21	22	23	24	25

Tabela 1 – Enumeração das letras do alfabeto.

Conforme os valores da Tabela 1, para fazer a codificação, vamos aplicar a congruência modular. Para isso, definimos que P é equivalente ao valor numérico de uma letra da Tabela 1, que corresponde à enumeração das letras do alfabeto e C é equivalente ao valor numérico da letra no sistema cifrado. De acordo com a cifra de César, a fórmula de codificação é $C \equiv P + 3 \pmod{26}$, com $0 \leq C \leq 25$. Já o receptor da mensagem utilizaria a fórmula $P \equiv C - 3 \pmod{26}$, com $0 \leq C \leq 25$.

Vamos codificar MATEMÁTICA na Cifra de César com chave 3. Para isso, vamos transformar a palavra em código numérico.

M	A	T	E	M	A	T	I	C	A
12	0	19	4	12	0	19	8	2	0

Tabela 2 – Codificação da palavra matemática.

Sabendo que na cifra de César, cada letra do alfabeto avança 3 posições em relação a sua posição inicial, temos a Tabela 3 que indica a conversão.

LETRA	A	B	C	D	E	F	G	H	I	J	K	L	M
NÚMERO CORRESPONDENTE	3	4	5	6	7	8	9	10	11	12	13	14	15
LETRA	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
NÚMERO CORRESPONDENTE	16	17	18	19	20	21	22	23	24	25	0	1	2

Tabela 3 – Alfabeto codificado com chave 3.

Aplicando a Cifra de César com chave 3, temos que a palavra MATEMÁTICA é escrita conforme representado na Tabela 4.

J	X	Q	B	J	X	Q	F	Y	X
12	0	19	4	12	0	19	8	2	0

Tabela 4 – Palavra MATEMÁTICA codificada no alfabeto com chave 3.

Então, JXQBJXQFYX corresponde à palavra MATEMÁTICA na cifra de César com chave 3.

Podemos ver que a aplicação da cifra de César pode ser amplamente utilizada com as mais diversas chaves k . Portanto, podemos definir uma fórmula geral para essas cifras, sendo $C \equiv P + K \pmod{26}$ utilizada pela pessoa que irá enviar a mensagem e $P \equiv C - K \pmod{26}$, com $0 \leq C \leq 25$, para o receptor da mensagem fazer a decodificação.

Para exemplificar mais uma vez a cifra de César, vamos codificar a Palavra MESTRE com chave 15. Para iniciarmos o processo, vamos codificar a palavra conforme atribuímos valores para as letras do nosso alfabeto, mencionadas na Tabela 1 e agora aplicado na Tabela 5.

M	E	S	T	R	E
12	4	18	19	17	4

Tabela 5 – Codificação da palavra MESTRE.

Aplicando a chave 15 em cada uma das letras e utilizando a fórmula da cifra de César, temos

$$M = 12 + 15 = 27 \equiv 1 \pmod{26},$$

$$E = 4 + 15 \equiv 19 \pmod{26},$$

$$S = 18 + 15 = 33 \equiv 7 \pmod{26},$$

$$T = 19 + 15 = 34 \equiv 8 \pmod{26},$$

$$R = 17 + 15 = 32 \equiv 6 \pmod{26},$$

$$E = 4 + 15 \equiv 19 \pmod{26}.$$

Podemos notar que o código da palavra MESTRE com chave 15 está representado na Tabela 6.

M	E	S	T	R	E
1	19	7	8	6	19

Tabela 6 – Enumeração das letras do alfabeto.

Aplicando a numeração do nosso alfabeto, a palavra mestre com chave 15 é BTHIGT, lembrando que para fazer a decodificação basta utilizar a fórmula $P \equiv C - 15 \pmod{26}$, com $0 \leq C \leq 25$ e obtemos a palavra MESTRE novamente.

Podemos verificar que apesar de ser um modelo simples, a aritmética modular já fazia parte desse sistema de conversão de modo eficiente.

3 Considerações Finais

As Olimpíadas de Matemática têm difundido o ensino da matemática de modo que os profissionais da área procurem a cada dia criar mecanismos para facilitar o ensino desta área do conhecimento, que durante muito tempo foi colocada como uma barreira intransponível. Hoje em dia, professores têm procurado uma capacitação e mecanismos facilitadores para o ensino de matemática. Podemos ver amplamente como a OBMEP e também a IMO a cada dia ficam mais conhecidas no ambiente escolar, graças a estas alterações do sistema educacional desde a implantação da nova Base Nacional Curricular Comum (BNCC), proporcionando o avanço da matemática como objeto do conhecimento e também como ponte para níveis cada vez maiores do aprimoramento e desenvolvimento de novas tecnologias. Os resultados que o Brasil tem alcançado na IMO cada vez motivam mais os alunos, e também os professores, consolidando totalmente esse processo.

A aritmética modular era algo inacessível aos alunos do Ensino Fundamental II e Médio, mas hoje devido a este processo supracitado, podemos ver muitos artigos e dissertações sendo produzidas para esta barreira transposta. Neste material, foi utilizado uma linguagem acessível para que o leitor possa compreender a origem da aritmética modular, e compreender como esse tema foi iniciado. Após a introdução do objeto de estudo, foram oportunizados exemplos, que simplificam todo o aprendizado, deixando bem claro o que é a aritmética modular e como é utilizada.

A parte de propriedades foi demonstrada de modo simples para que o leitor possa compreender de onde surgiu cada uma delas e de um modo mais eficiente, conseguir abstrair onde pode aplicá-las na resolução de um problema matemático.

Atualmente, grandes concursos militares e as olimpíadas têm utilizado esse conhecimento e podemos demonstrar isso na resolução de alguns problemas retirados de provas e olimpíadas. Cada problema foi resolvido de modo a explicar todas as passagens da resolução de modo simples e de fácil entendimento. Foram informados quais propriedades foram utilizadas, tornando a resolução objetiva. No final de cada problema, foi feito um resumo de como proceder em cada tipo de problema, tentando fazer com que a resolução de questões similares seja um processo simples e eficiente.

As aplicações de congruências modulares foram explanadas tanto a teoria quanto a prática, por meio de resoluções de exemplos e problemas olímpicos, de modo que o processo ficasse bem simples e de fácil entendimento. Vários processos que foram citados são amplamente utilizados e por falta de conhecimento do assunto, não havia ciência do envolvimento de congruência na elaboração das aplicações. Todas as aplicações foram mostradas com exemplos para facilitar a compreensão dos mesmos.

Hoje em dia, com a internet, as informações cada vez mais têm se tornado comuns, e torná-las cada vez mais simples de serem compreendidas, é um processo importante. Portanto, foi primado na elaboração deste texto, tornar a congruência modular um objeto de estudo, que hoje pode e deve ser ministrado nas séries iniciais do Ensino Fundamental II, de modo que o professor possa fornecer todos os subsídios para um aluno compreender e aplicar de modo eficiente.

Referências

- BAGATINI, Alessandro. **Olimpíadas de Matemática, Altas Habilidades e Resolução de Problemas**. [s.n.], 2010. v. 1. 10-32 p. Disponível em: <<https://www.lume.ufrgs.br/bitstream/handle/10183/29144/000775916.pdf?sequence=1>>. Acesso em: 20 de jan. de 2020. Citado 4 vezes nas páginas 14, 19, 21 e 22.
- BITTENCOURT, Larisse Araújo et al. aplicações de congruência módulo m. **Caderno de Graduação-Ciências Exatas e Tecnológicas-UNIT-SERGIPE**, v. 2, n. 3, p. 109–116, 2015. Citado na página 49.
- CARVALHO, Alandesson Linhares; RODRIGUES, Daniel Vivorio; ARAÚJO, Leonardo Henrique R. Aplicações da aritmética modular na criptografia. **Caderno de Graduação-Ciências Exatas e Tecnológicas-UNIT-SERGIPE**, v. 3, n. 1, p. 11–24, 2015. Citado na página 47.
- DOMINGUES, Hygino H Iezzi. Gelson. **Álgebra Moderna. Quarta edição reform. São Paulo: Atual**, 2003. Citado na página 34.
- EFOMM, Escola de Formação da Marinha Mercante. **Admissão**. 2007. Disponível em: <<https://www.marinha.mil.br/ciaga/efommadmissao>>. Acesso em: 25 de fev. de 2021. Citado 3 vezes nas páginas 25, 36 e 44.
- ESQUINCA, Josiane Colombo Pedrini. Aritmética: códigos de barras e outras aplicações de congruências. 2013. Citado 2 vezes nas páginas 24 e 25.
- HEFEZ, Abramo. Iniciação à aritmética. **Sociedade Brasileira de Matemática**, 2009. Citado 2 vezes nas páginas 24 e 34.
- IMO, Olimpíada Internacional de Matemática. **Regulamento**. 2017. Disponível em: <<https://www.imo2017.org.br/sobre-a-imo.html>>. Acesso em: 28 de jan. de 2020. Citado 2 vezes nas páginas 21 e 25.
- IMO, Qualificação Para Olimpíada Internacional da Suíça. **Teste de Seleção para Olimpíadas Internacional de Matemática**. 2012. Disponível em: <<https://www.youtube.com/watch?v=ANFjJZkGOQc>>. Acesso em: 28 de fev. de 2021. Citado 2 vezes nas páginas 25 e 39.
- LOBO, Matheus Pereira. Last two digits of 2^{googol} . OSF Preprints, 2019. Citado na página 45.
- MACIEL-CMPA, Marcos Vinicius Milan; BASSO-UFRGS, Marcus Vinicius de Azevedo. Olimpíada brasileira de matemática das escolas públicas (obmep): as origens de um projeto de qualificação do ensino de matemática na educação básica. 2009. Citado na página 22.
- MARCONI, Marina de Andrade.; LAKATOS, Eva Maria. **Fundamentos da Metodologia Científica**. Atlas S.A, 2005. v. 1. Disponível em: <https://docente.ifrn.edu.br/olivianeta/disciplinas/copy_of_historia-i/historia-ii/china-e-india>. Acesso em: 20 de jan. de 2020. Citado na página 15.

- OBM, Olimpíada Brasileira de Matemática. **Histórico**. 2020. Disponível em: <<https://www.obm.org.br/quem-somos/historico/>>. Acesso em: 25 de jan. de 2020. Citado 4 vezes nas páginas 17, 19, 20 e 45.
- OBMEP, Olimpíada Brasileira de Matemática das Escolas Públicas. **Apresentação**. 2020. Disponível em: <<http://www.obmep.org.br/apresentacao.htm>>. Acesso em: 25 de jan. de 2020. Citado na página 20.
- PINHEIRO, Rodolfo Cavalcante et al. Aritmética modular: uma aplicação no ensino fundamental. Universidade Federal de Goiás, 2018. Citado na página 52.
- PONTES, Edel Alexandre Silva; SILVA, Luciano Martins da. Aritmética modular na interpretação de sistemas codificados no processo de ensino e aprendizagem de matemática. **Revista de Ciência e Inovação**, v. 5, n. 1, 2020. Citado na página 50.
- POTI, Polos Olímpicos de Treinamento Intensivo. **Aritmética Modular**. 2017. Disponível em: <<https://potiimpa.br/index.php/modulo/ver?modulo=4#>>. Acesso em: 20 de fev. de 2021. Citado 2 vezes nas páginas 24 e 29.
- PROFMAT, Mestrado Profissional em Rede Nacional. **ENQ**. 2007. Disponível em: <<https://www.profmtat-sbm.org.br/exame-nacional-de-qualificacao/>>. Acesso em: 25 de fev. de 2021. Citado 3 vezes nas páginas 25, 38 e 43.
- REGULAMENTO-OBMEP, Olimpíada Brasileira de Matemática. **Regulamento**. 2020. Disponível em: <<https://www.obm.org.br/informacoes-gerais/regulamento/>>. Acesso em: 25 de jan. de 2020. Citado na página 18.
- REZENDE, Giovane.; MESQUITA, Maria da Gloria Bastos de Freitas. Principais dificuldades percebidas no processo ensino-aprendizagem de matemática em escolas do município de divinópolis, mg. <https://revistas.pucsp.br/>, v. 1, p. 200–215, 2013. Disponível em: <<http://revistas.pucsp.br/index.php/emp/article/download/9841/pdf>>. Acesso em: 20 de jan. de 2020. Citado na página 14.
- RIBEIRO, Helen Alessandra. Mestrado profissional em matemática em rede nacional-profmtat. 2019. Citado na página 24.
- SANT'ANNA, Iury Kersnowsky de. A aritmética modular como ferramenta para as séries finais do ensino fundamental. 2013. Citado na página 24.
- UFCE, Olimpíada Cearense de Matemática. **Olimpíadas Cearense de Matemática**. 2014. Disponível em: <<http://www.mat.ufc.br/ocm/>>. Acesso em: 28 de fev. de 2021. Citado 2 vezes nas páginas 25 e 41.
- WALTER, André et al. Divisibilidade e congruência modular. 2019. Citado na página 24.