UNIVERSIDADE FEDERAL DE JATAÍ (UFJ)
UNIDADE ACADÊMICA DE CIÊNCIAS EXATAS E TECNOLÓGICAS (CIEXA)
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL (PROFMAT)

Marcieli Adamski Carvalho

Resolução de Sistema de Congruências Lineares

Jataí, GO
2022

UFJ

UNIVERSIDADE FEDERAL DE JATAÍ
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO (TECA) PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TESES

E DISSERTAÇÕES NA BIBLIOTECA DIGITAL DA UFJ

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Jataí (UFj) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFJ), regulamentada pela Resolução CEPEC nº 832/2007, sem ressarcimento dos direitos autorais, de acordo com a Lei 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo das Teses e Dissertações disponibilizado na BDTD/UFJ é de responsabilidade exclusiva do autor. Ao encaminhar o produto final, o autor(a) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do material bibliográfico

[x] Dissertação [ ] Tese

2. Nome completo do autor

MARCIELI ADAMSKI CARVALHO

3. Título do trabalho

RESOLUÇÃO DE SISTEMA DE CONGRUÊNCIAS LINEARES

4. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador)

Concorda com a liberação total do documento [x] SIM [ ] NÃO[1]

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante:

a) consulta ao(à) autor(a) e ao(à) orientador(a);

b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo da tese ou dissertação.

O documento não será disponibilizado durante o período de embargo.

Casos de embargo:

- Solicitação de registro de patente;

- Submissão de artigo em revista científica;

- Publicação como capítulo de livro;

- Publicação da dissertação/tese em livro.

Obs. Este termo deverá ser assinado no SEI pelo orientador e pelo autor.

Documento assinado eletronicamente por **WENDER JOSE DE SOUZA**, **Orientador**, em 21/07/2022, às 12:56, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **MARCIELI ADAMSKI CARVALHO**, **Usuário Externo**, em 21/07/2022, às 14:05, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufj.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0043766** e o código CRC **ED286481**.

Referência: Processo nº 23854.004269/2022-33 SEI nº 0043766

Marcieli Adamski Carvalho

Resolução de Sistema de Congruências Lineares

Dissertação apresentada ao Programa de Pós-Graduação em Matemática (PROFMAT), da Unidade Acadêmica de Ciências Exatas e Tecnológicas (CIEXA), da Universidade Federal de Jataí (UFJ), como requisito para obtenção do título de Mestre em Matemática.
Área de concentração: Matemática do Ensino Básico.
Linha de pesquisa: Aritmética.

Orientador: Prof. Dr.Wender José de Souza

Jataí, GO

2022

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFJ.

Carvalho, Marcieli Adamski
Resolução de Sistema de Congruências Lineares / Marcieli Adamski Carvalho. - 2022.
CII, 102 f.

Orientador: Prof. Dr. Wender José de Souza.
Dissertação (Mestrado) - Universidade Federal de Jataí, Unidade Acadêmica Especial de Ciências Exatas e Tecnológicas, Jataí, PROFMAT- Programa de Pós-graduação em Matemática em Rede Nacional - Sociedade Brasileira de Matemática (RJ), Jataí, 2022.

Inclui siglas, símbolos.

1. Números inteiros.. 2. Sistema de Congruência.. 3. Material de apoio. I. Souza, Wender José de , orient. II. Título.

CDU 51:37

UFJ

UNIVERSIDADE FEDERAL DE JATAI

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

ATA DE DEFESA DE DISSERTAÇÃO

Ata nº **33** da sessão de Defesa de Dissertação de MARCIELI ADAMSKI CARVALHO, que confere o título de Mestra em **Matemática**, na área de concentração em **Matemática do Ensino Básico**.

No dia quatro de julho de dois mil e vinte e dois, a partir das 09:30 horas, no Auditório do Prédio de Pós-graduação da Universidade Federal de Jataí, realizou-se a sessão pública de Defesa de Dissertação intitulada **"**RESOLUÇÃO DE SISTEMA DE CONGRUÊNCIAS LINEARES**"**. Os trabalhos foram instalados pelo Orientador, Professor Doutor Wender José de Souza (PROFMAT / UFJ), com a participação dos demais membros da Banca Examinadora: Professora Doutora Adriana Araujo Cintra (PROFMAT / UFJ) membro titular interno, Professor Doutor Julio César Conegundes da Silva, membro titular externo. Durante a arguição os membros da banca **não fizeram** sugestão de alteração do título do trabalho. A Banca Examinadora reuniu-se em sessão secreta a fim de concluir o julgamento da Dissertação, tendo sido a candidata **aprovada** pelos seus membros. Proclamados os resultados pelo Professor Doutor Wender José de Souza, Presidente da Banca Examinadora, foram encerrados os trabalhos e, para constar, lavrou-se a presente ata que é assinada pelos Membros da Banca Examinadora, no dia quatro de julho de dois mil e vinte e dois.

TÍTULO SUGERIDO PELA BANCA

Não houve sugestão

Documento assinado eletronicamente por **WENDER JOSE DE SOUZA**, **Orientador**, em 04/07/2022, às 18:38, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **ADRIANA ARAUJO CINTRA**, **Professora do Magistério Superior**, em 04/07/2022, às 18:41, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Julio César Conegundes da Silva**, **Usuário Externo**, em 04/07/2022, às 18:49, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufj.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0035800** e o código CRC **FB8D65C5**.

Referência: Processo nº 23854.004269/2022-33 SEI nº 0035800

Os Programas de Pós-Graduação stricto sensu, ora em funcionamento na Universidade Federal de Jataí (UFJ), em virtude de procedimentos técnicos relacionados à CAPES, continuam provisoriamente vinculados à Universidade Federal de Goiás (UFG), no entanto, todos os elementos pré-textuais do trabalho apresentado estão identificados como Universidade Federal de Jataí, em função da migração da BDTD ter ocorrido a partir de 16 de agosto de 2021, e pelo fato das pesquisas e produções estarem sendo realizadas na UFJ.

CARVALHO, Marcieli A. **Resolução de Sistema de Congruências Lineares.** 2022. 102 p. Dissertação (Programa de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional – PROFMAT), Unidade Acadêmica de Ciências Exatas, Universidade Federal de Jataí, Jataí- GO, 2022.

Resumo

A Teoria dos Números é um ramo da Matemática que se dedica a estudar as propriedades e as relações entre os números inteiros, em particular, estudamos a aritmética dos restos. Diante disso, este trabalho propõe a resolução de Sistema de Congruências Lineares com uma variável e Sistema de Congruências Lineares com duas variáveis, através de diferentes técnicas de resolução. Dessa forma, iniciamos com uma abordagem histórica acerca do tema Números Inteiros para, posteriormente, verificamos se esse conteúdo é apresentado na BNCC (Base Nacional Comum Curricular) e, caso seja, como é abordado. Em seguida, fazemos uma fundamentação teórica da Teoria dos Números, especialmente, sobre congruência módulo m, congruência linear, Sistema de Congruências Lineares e o Teorema Chinês dos Restos. Observa-se que, o conteúdo trazido na maioria dos materiais que trata sobre Sistema de Congruências Lineares é tratado de forma bem direta, com poucos exemplos práticos e um número inexpressivo de detalhes. Com base nas observações levantadas, este trabalho traz um material de apoio com exemplos mais detalhados e, sempre que possível, relacionados com o cotidiano. Espera-se que este material possa servir de apoio e motivação para os professores, que atuam em diferentes níveis de ensino, em especial, na Educação Básica e na graduação, que acreditam que devam ensinar além dos conteúdos propostos pelo currículo a fim de valorizar a formação integral de seus alunos.

Palavras chave: Números inteiros. Sistema de Congruências. Material de apoio.

CARVALHO, Marcieli A. **Resolution of a Linear Congruence System.** 2022. 102 p. Dissertation (Professional Master's Graduate Program in Mathematics in National Network - PROFMAT), Academic Unit of Exact Sciences, Federal University of Jataí, Jataí-GO, 2022.

Abstract

Number Theory is a branch of Mathematics that is dedicated to study the properties and relations between integers, in particular, it studies the arithmetic of remainders. In view of this, this dissertation proposes the resolution Systems of Linear Congruences, by different solving techniques in which we will apply the Chinese Remainder Theorem. Thus, we will begin with a historical approach to the subject of integer Numbers to subsequently verify whether this content is presented in the BNCC (Base Nacional Comum Curricular) and, if so, how it is approached. Then, we will stablish a theoretical foundation of Number Theory, especially on congruences modulo m, linear congruences, System of Linear Congruences and the Chinese Remainder Theorem. It is observed that, the content brought in most of the materials that deal with Systems of Linear Congruences is treated in a very direct way, with few practical examples and an inexpressive number of details. Based on the observations raised, this work brings a support material with more detailed examples and, whenever possible, related to everyday life. It is expected that this material can serve as support and motivation for teachers, who work at different levels of education, especially in Basic Education and undergraduate students, who believe that they should teach beyond the content proposed by the curriculum in order to enhance the integral formation of their students.

Keywords: Integer Numbers. Congruence system. Supporting material.

Lista de abreviaturas e siglas

BNCC	Base Nacional Comum Curricular
ENQ	Exame Nacional de Qualificação
SBM	Sociedade Brasileira de Matemática

Lista de símbolos

$\equiv$	Congruente
$\not\equiv$	Incongruente
$\mid$	Divide
$\nmid$	Não divide
(a, b)	Máximo divisor comum entre a e b
$[a, b]$	Mínimo múltiplo comum entre a e b
$\square$	Indica o fim de uma demonstração.
Passo n_{T_k}**:**	Indica passo da resolução de uma técnica, onde n identifica o número do passo, T a técnica e k número da técnica.
$\begin{pmatrix} x \\ y \end{pmatrix}$	Par ordenado que representa a solução do sistema com duas variáveis.

Sumário

INTRODUÇÃO

Desde o início da civilização, a Matemática já estava presente na vida do homem primitivo devido à necessidade de contar, registrar e operar com números. Ao longo da História, a Matemática foi sendo construída e aperfeiçoada, prosseguindo em constante evolução, investigando novas situações e estabelecendo relações com os acontecimentos cotidianos.

A importância dessa Ciência faz-se presente nos dias atuais em diferentes contextos como: interpretar tabelas de futebol, analisar gráficos de eleições, investir no mercado financeiro, decidir entre uma oferta ou outra, investir na poupança ou não. Tudo isso é possível se o homem conhecer e se apropriar de ferramentas Matemáticas.

Nesse sentido, a Teoria dos Números é o ramo da Matemática que tem por objetivo principal estudar as propriedades e relações entre os números inteiros. Essa teoria aparece como ferramenta em diversas áreas da Matemática, tais como: probabilidade, álgebra, Sistemas dinâmicos, etc., servindo de alicerce para resultados significativos. Neste sentido, restringimos à Aritmética: a parte que lida com os números e com as operações possíveis entre eles.

O presente trabalho tem como objetivo utilizar de diferentes técnicas para resolver Sistema de Congruências Lineares que admite solução, sendo uma delas o Teorema Chinês dos Restos. Dessa forma, para atingirmos este objetivo propomos elaborar um material de apoio, que comtemple essas técnicas de resolução com o intuito de auxiliar os professores da Formação Geral Básica que queiram se aprofundar nos conceitos de Teoria dos Números, para alunos da graduação que cursam da disciplina de Introdução a Teoria dos Números, para alunos da pós-graduação na disciplina de Aritmética e pode ainda ser direcionado a aqueles que têm um pouco de familiaridade com a Teoria dos Números.

Embora Sistema de Congruência Lineares não seja trabalhado em sala de aula no Ensino Básico, a teoria necessária para sua compreensão é amplamente discutida nos anos finais do Ensino Fundamental. Além disso, podemos citar algumas possibilidades de suas aplicações no dia-a-dia, tais como: na computação; os diferentes códigos numéricos de identificação, como os códigos de barras; os números dos documentos de identidade, CPF, CNPJ, ISBN; QR Code; as criptografías, os calendários, entre outros exemplos.

A fim de verificarmos se existe algum trabalho cujos temas envolvem Resolução de Sistemas de Congruências Lineares e o Teorema Chinês dos Restos realizamos uma revisão bibliográfica. Nesse sentido, encontramos alguns trabalhos relacionados com o tema, sendo que cinco deles desenvolvidos por alunos do Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT). Como muitos destes trabalhos são

semelhantes entre si, destacamos aqui os cinco que chamaram mais atenção.

A dissertação de PRAZERES (2014) inicia apresentando alguns tópicos da Teoria dos Números, como Algoritmo de Euclides, Divisibilidade, Máximo Divisor Comum, Equações Diofantinas Lineares, Congruências e o Teorema Chinês dos Restos. Em cada tópico é apresentado a teoria, sua importância, e sua aplicabilidade no dia a dia por meio da resolução de alguns exemplos. A principal aplicação do Teorema no seu trabalho é a Partilha de Senhas. A partilha de senhas é um mecanismo de segurança, onde uma certa quantidade de pessoas tomam posse de uma chave de acesso sem a possibilidade de obter a senha principal com a sua própria chave. Além disso, apresenta como proposta uma sequência didática dos conteúdos congruências, Equações Diofantinas e o Teorema Chinês dos Restos.

Já o trabalho de FILHO (2015), traz um breve histórico do Teorema Chinês dos Restos, em seguida, aborda os conceitos de congruências, Sistema de Congruências, Pequeno Teorema de Fermat e o Teorema Chinês dos Restos. Tem como objetivo mostrar a aplicação do Teorema Chinês dos Restos com números de alta cardinalidade e finaliza seu trabalho apresentando um problema que relaciona a teoria de informação da codificação com a Teoria dos Números Inteiros.

Na dissertação de SANTOS (2017), inicia com uma abordagem histórica do Teorema Chinês dos Restos, em seguida, discorre sobre os conceitos de: Conjunto dos Números Inteiros e suas Propriedades Básicas, a Divisão nos Inteiros, Máximo Divisor Comum, Mínimo Múltiplo Comum, Equações Diofantinas Lineares (apresenta a solução da equação diofantina por meio de congruências) e Congruências. Intercalando alguns exemplos resolvidos. Apresenta um capítulo para a demonstração do Teorema Chinês dos Restos e para isso utiliza o conceito de classe inversa e por fim, apresenta nove exemplos de suas aplicações.

A dissertação de GLÓRIA (2019), inicia com uma abordagem histórica do Teorema Chinês dos Restos, em seguida, traz uma revisão bibliográfica com os seguintes tópicos: Os Números Inteiros e suas Propriedades Básicas, Divisibilidade, Máximo Divisor Comum, Mínimo Múltiplo Comum, Números Primos, Equações Diofantinas Lineares e Congruências. Posteriormente, dedica um capítulo para a demonstração do Teorema Chinês dos Restos e para isso utiliza o conceito de classe inversa e por fim, apresenta vinte e dois exemplos de suas aplicações com a finalidade de melhor aprendizado baseado nas resoluções.

E o mais recente JÚNIOR (2020), neste trabalho, inicia com os conceitos de Congruências, Equações Diofantinas Lineares, Divisão nos Inteiros, Sistemas de Congruências, Inverso Módulo n, Potências, em seguida, demonstra os Teoremas de Fermat, Euler e Wilson. Dedica um capítulo para a demonstração do Teorema Chinês dos Restos e alguns exemplos de suas aplicações. No seu quarto capítulo aborda o conceito de Criptografia RSA relacionando com o Teorema chinês dos Restos e para finalizar apresenta como proposta

pedagógica uma sequência didática.

Este trabalho se difere dos demais por apresentar diferentes alternativas de resolução de Sistema de Congruências Lineares além de, resolver Sistema com duas variáveis. Outro ponto importante a destacar é o fato de que os trabalhos acima citados abordam a resolução por meio do conceito de Classes Residuais mas se analisarmos o sumário de diferentes autores sobre a Teoria dos Números e seguindo a lógica dos cursos que ministram a disciplina de Introdução a Teoria dos Números o conceito de Classes Residuais é contemplado depois da Resolução de Sistema de Congruências o que dificulta a resolução de um sistema por meio dessa ferramenta.

Quando me refiro a resoluções detalhadas é porque na maioria dos materias que encontramos a resolução, seja em livros ou em sites da internet, algumas senão todas as etapas de resolução são omitidas e as vezes dizendo que é fácil ver ou concluir, mas isso ao invés de motivar e facilitar a compreensão para se chegar a resposta final do problema causa uma desmotivação por parte do leitor.

Se fizermos uma pesquisa rápida em sites da internet procurando a resolução de sistemas que são propostos em livros da Teoria dos Números, verificamos que há, porém o método de resolução nem sempre é fácil de compreender e as vezes é resolvido através de conceitos que o aluno ainda não se apropriou, ou não os conhece dificultando assim a compreensão. Estes materiais são diretos e omitem boa parte da resolução, já os vídeos do canal do Youtube, na grande maioria não são gratuitos e sempre estão inseridos em pacotes que eleva o preço dificultando o acesso. Nesse sentido, buscamos elaborar um material que comtemple essas demandas e que é apresentado no decorrer deste trabalho.

Em relação à estrutura da dissertação, o texto está organizado em cinco capítulos, além da introdução e das considerações finais. São eles:

No capítulo 1, iniciamos com o contexto histórico dos Números Inteiros, mostrando como surgiram, sua importância e suas principais contribuições e para isto nos baseamos nas principais fontes como Eves, Boyer, Mol que abordam a história da Matemática entre outros autores.

No capítulo 2, buscamos mostrar a relevância de se estudar o conceito de Números Inteiros na Educação Básica e analisamos também se este conceito é abordado e como é abordado. Para isto, utilizamos como base um dos principais documentos que norteiam a construção do currículo da Educação Básica que é a Base Nacional Comum Curricular-BNCC.

Na sequência, apresentamos o capítulo 3, que contém os principais conceitos que embasam nossa proposta de trabalho, ou seja, definimos o conceito de congruência, suas propriedades básicas e as operatórias. Ao final de cada conceito ou propriedade apresentamos de forma detalhada a resolução de problemas extraídos de concursos a nível

fundamental e médio, de Livros didáticos e Olimpíadas.

No capítulo 4, mostramos como resolver Congruências e Sistema de Congruências Lineares. Damos ênfase para a aplicação do Teorema Chinês dos Restos mostrando algumas aplicações e por fim, como resolver Sistema de Congruências Lineares com duas variáveis.

O capítulo 5 traz o objeto de nosso estudo, isto é, a resolução de Sistemas de Congruências lineares. Quando temos um grupo de equações de congruências, no qual queremos obter uma solução que satisfaça estas equações, teremos um sistema de congruências. Para isto, exibimos diferentes métodos de resolver estes sistemas e o método de destaque é o Sistema com duas variáveis.

Nesse sentido, buscamos no capítulo 5 elaborar um material de apoio que apresente soluções detalhadas (com todos os passos da resolução), explicativas (uma linguagem culta, porém acessível) e relacionadas com os conceitos já estudados além daqueles que foram abordados no capítulo anterior.

1 Números Inteiros: contexto histórico

Este texto tem por finalidade apresentar o cenário histórico da Matemática, com foco nos números inteiros desde suas mais remotas origens até o século XIX, além de destacar sua importância e suas contribuições para a Matemática atual. Portanto, utilizamos obras importantes como base, como (BOYER; MERZBACH, 2012),(BURTON, 2016),(EVES, 1995) entre outras.

Os números inteiros positivos surgiram, inicialmente, da necessidade do homem de contar e de, posteriormente, fazer registros e, por consequência, de operar. "Acredita-se que o processo de contar começou a ser desenvolvido pelo ser humano muito antes de haver escrita ou civilização e, por isso, possuímos poucos elementos concretos para sua análise", (MOL, 2013, p.13).

A evolução da humanidade de uma vida primitiva para uma vida em sociedade incorporou novos desafios sociais e econômicos. "Novas demandas surgiram na organização do espaço, nas técnicas de produção e nas relações de natureza comercial. O homem se viu, assim, diante da necessidade de pensar numericamente", (MOL, 2013, p.13).

Embora os números inteiros positivos componham o sistema matemático mais simples, o estudo de suas propriedades exerce grande fascínio na mente humana desde a Antiguidade, desafiando vários estudiosos através de seus conceitos e propriedades que vão além de qualquer simplicidade.

A civilização egipíca, em 4241 a.C., devido sua localização ser próxima ao Rio Nilo, desenvolveu fortemente a agricultura e construiu um calendário para se orientar: era composto de 12 meses de 30 dias cada e mais 5 dias festivos, de acordo com o ciclo de cheias do rio Nilo. As habilidades aritméticas demandadas na organização do calendário egípcio dão uma medida das possibilidades do uso de conhecimentos matemáticos para solucionar problemas de natureza prática.

Um registro famoso da existência da Aritmética no antigo Egito é o Papiro de Rhind, adquirido pelo egiptólogo escocês Alexander Rhind, em 1858, datado de cerca de 1650 a.C.. Foi copiado por um escriba de nome Ahmes que detalha a solução de 84 problemas de geometria e de aritmética. Entre os problemas aritméticos, há estudos de frações unitárias e de equações lineares e é um documento de importante contribuição para a Matemática.

A Teoria dos Números é um ramo da Matemática que se preocupa com as propriedades dos números inteiros e com os problemas que surgiram naturalmente do estudo dos números inteiros. Na Grécia, originou-se o estudo sistemático da Matemática introduzido

por Tales (c. $624-546$ a.C.). Nesse período, Tales fundou a Escola Ioniana unindo o estudo da astronomia ao da geometria e da Teoria dos Números. Em decorrência disso, BURTON (2016, p.13) Pitagóras – que nasceu entre 580 e 562 a.C. na Ilha do Egeu de Samos – estudou no Egito e, após várias viagens ao Oriente como à Babilônia, retornou à cidade de Crotona e fundou a Escola Pitagórica cuja concepção do universo era de que "todas as coisas são números". Por número, ele considerava um inteiro positivo e destacava quatro campos do saber: Aritmética, Música, Geometria e Astronomia. Dessa Escola surgiu a primeira classificação dos números em pares, ímpares e primos por volta de 450 a.C.

A abordagem pelos gregos antigos origina-se da Teoria dos Números e traz o cálculo do máximo divisor comum de dois números, o conceito de número primo e a demonstração de que há uma infinidade de números primos.

Após todo esse conhecimento sobre números deixado por Tales e Pitagóras surge por volta de 300 a.C.em Alexandria, Euclides de Alexandria ($330-275$ a.C.) que organizou uma coleção de 13 livros chamados *Os Elementos*. Acredita-se que Euclides não demonstrou todos eles, mas que o trabalho reunia demostrações de seus alunos. Os livros VII, VIII e IX versam sobre a Teoria dos Números que, para os gregos, eram inteiros e positivos, relacionando os números à construção geométrica.

De acordo com BOYER & MERZBACH (2012, p.95), no livro VII são definidos os conceitos de divisibilidade, de número primo e de números perfeitos. Além, do famoso "algoritmo de Euclides" que consite em determinar o máximo divisor comum de dois números. Já o livro VIII começa com proposições sobre números em proporção continuada (progressão geométrica) e, depois, volta-se para propriedades simples de quadrados e cubos. E o livro IX apresenta vários teoremas interessantes, por exemplo, a Proposição 20 com a demonstração de que há infinitos números primos; a Proposição 14 enuncia o Teorema Fundamental da Aritmética; a Proposição 35 que traz a fórmula para a soma de números em progressão geométrica, e a última proposição com a fórmula para números perfeitos. Os gregos antigos conheciam os quatro primeiros números perfeitos: $6, 28, 496$ e 8128. Euclides não respondeu se essa fórmula fornece ou não todos os números perfeitos, mas hoje sabe-se que todos os números perfeitos pares são desse tipo.

Já a maior contribuição da Matemática Chinesa para a Teoria dos Números é o livro *K'ui-ch'ang Suanshu*, ou *Nove Capítulos sobre a Arte da Matemática*, que data do período Han (206 a.C.,-221d.C.), mas que muito provavelmente contém material bem mais antigo. De acordo com Eves (1995), uma síntese do conhecimento matemático chinês antigo e contém 246 problemas sobre mensuração de terras, agricultura, sociedades, engenharia, impostos, cálculos, solução de equações e propriedade dos triângulos retângulos.

Dividido em 9 capítulos, dos quais o oitavo trata sobre as soluções de equações Lineares simultâneas obtendo soluções positivas e negativas. A origem dos números inteiros negativos é incerta, mas acredita-se que os chineses foram os primeiros a descobri-las, no

entanto, não é claro se eles as consideravam como solução.

Outro matemático de destaque é Diofanto de Alexandria, nascido entre (201 e 214) e falecido entre (284 e 298). De acordo com BOYER & MERZBACH (2012), pouco se sabe sobre a vida de Diofanto e os únicos dados pessoais que se tem de sua carreira são descritos na redação de um problema-epigrama:

> Deus lhe concedeu ser um menino pela sexta parte de sua vida, e somando uma duodécima parte a isto cobriu-lhe as faces de penugem. Ele lhe acendeu a lâmpada nupcial após uma sétima parte, e cinco anos após seu casamento concedeu-lhe um filho. Ai! Infeliz, criança tardia; depois de chegar à metade da vida de seu pai, o destino frio o levou. Depois de consolar sua dor com a ciência dos números por quatro anos, ele terminou sua vida, (BOYER; MERZBACH, 2012, p.133).

Se x foi a idade com que Diofanto morreu, estes dados no levam à seguinte equação:

$$\frac{1}{6}x + \frac{1}{12}x + \frac{1}{7}x + 5 + \frac{1}{2}x + 4 = x$$

com solução $x = 84$. Logo, Diofanto viveu por 84 anos.

Suas contribuições para a Teoria dos Números se dividem em três obras, sendo: a primeira sobre Aritmética, a segunda sobre números poligonais da qual restou uma pequena parte do original e a última sobre prismas que foi totalmente perdido.

Dentre estes o de maior destaque é sua grandiosa obra *Arithmetica*, escrita por volta de 250 d.C., contendo cerca de 150 problemas que trata principalmente da solução de equações indeterminadas com coeficientes inteiros. Esse foi o primeiro tratado sobre álgebra que era, originalmente, em treze livros, dos quais só os seis primeiros se preservaram, BOYER & MERZBACH (2012, p.134).

Conforme BURTON (2016), é comum aplicar o termo equação Diofantina a toda equação em uma ou mais incógnitas que devem ser resolvidas nos números inteiros. Exemplo disso é a equação Diofantina linear em duas incógnitas:

$$ax + by = c$$

em que a, b e c são inteiros dados e a, b diferentes de zero. Uma solução dessa equação é um par de inteiros x_0, y_0 que quando substituído na equação, satisfaça-a, ou seja, $ax_0 + by_0 = c$. O mais interessante é que esse tipo de equação não aparece em sua obra *Arithmetica* e, sim, em *Elementos de Euclides*. Acredita-se que por ser trivial, pois a maioria de seus problemas era para encontrar quadrados e cubos com certas propriedades.

Apesar de não ficar claro que Diofante foi responsável pela introdução dos números inteiros negativos, no inicio do Livro I da sua *Arithmetica*, ele escreve: "O que está em falta multiplicado pelo que está em falta dá o que é positivo; enquanto que o que está em falta multiplicado pelo que é positivo, dá o que está em falta". Embora ele não oferecesse

demonstração, fica claro a regra de sinais que conhecemos hoje e ainda menciona o termo o que está em falta, ou seja, a presença dos números inteiros negativos, Glaeser (2010, p.10).

Já o Matemático indiano Brahmagupta reafirmou a existência dos números inteiros negativos e principalmente descatacou a utilização do zero. De acordo com Eves (1995, p.251),viveu e trabalhou no centro astronômico de Ujjain, na Índia Central. Em 628 escreveu Brahmasphuta-sidd'bãnta ("o sistema de Brahma revisado"), um trabalho de astronomia em 21 capítulos, dos quais o 12° e o 18° se ocupam de matemática.

Neste livro ele define o zero como resultado de uma subtração de um número por ele mesmo. A aritmética sistematizada dos números negativos e do zero encontram-se pela primeira vez em sua obra. Esta trouxe algumas regras de multiplicação e divisão sendo que atribuiu a metáfora afirmativo para positivo e cifra para zero, além da divisão por zero, a qual não se comprometeu em explicar a divisão de um número diferente de zero por zero.

> Positivo dividido por positivo, ou negativo por negativo, é afirmativo. Cifra dividida por cifra é nada. Positivo dividido por negativo é negativo. Negativo dividido por afirmativo é negativo. Positivo ou negativo dividido por cifra é uma fração com esse denominador, (BOYER; MERZBACH, 2012, p.159)

Na sequência, outro importante matemático indiano foi Bhaskara que buscou solucionar dentre outros, o problema de Brahmagupta à respeito da divisão de um número diferente de zero por zero. De acordo com BOYER & MERZBACH (2012, p.160), Bhaskara trás a seguinte afirmação em um de seus trabalhos: Dividendo 3. Divisor 0. Quociente a fração $\frac{3}{0}$. Essa fração cujo o denominador é cifra, chama-se uma quantidade infinita. Nessa quantidade, que consiste no que tem cifra como divisor, não há alteração mesmo que muito seja acrescentado ou retirado; como nenhuma alteração se dá no Deus infinito e imutável. Porém, essa afirmação não tornou claro o resultado da divisão por zero.

Bhaskara também viveu em Ujjain. Contribuiu com importantes obras, sendo duas em destaque a Lilavati que trata sobre aritmética e a segunda Vija-Ganita (extração de raízes) que trata sobre álgebra. Nestas obras encontramos vários problemas sobre os assuntos mais discutidos e pesquisados pelos hindus como equações lineares e quadráticas.

Diofanto, conforme mencionado anteriormente também buscava por soluções de equações determinadas e indeterminadas, porém "Bhaskara resolve a equação do segundo grau $x^2 - 45x = 250$ encontrando as soluções $x = 50$ e $x = -5$ como soluções, mas mostrou-se cético quanto à validade da raiz negativa" STRUIK, GUERREIRO & VIEIRA (1992, p.117). E agora? É possível um número negativo ser raiz de uma equação? Para Bhaskara as raízes negativas não podiam existir porque um número negativo não é um quadrado. Essa afirmação ele fez sem dar definições, axiomas ou teoremas. Contudo, apesar de descobrirem os números negativos, eles não os utilizavam ignoragem essas raízes o que

contribuiu para a demora na aceitação, BOYER & MERZBACH (2012, p.161) e Eves (1995, p.251).

Diofanto tinha como foco encontrar a solução de equações indeterminadas com coeficientes inteiros, e um dos problemas tratados por ele era a resolução em números racionais, ou inteiros, "da equação pitagórica $x^2 + y^2 = z^2$, chegando a descrever todas as suas soluções", este problema despertou o interesse de Pierre de Fermat HEFEZ (2013, p.63).

Além de Bkaskara, outros matemáticos dos séculos XVI e XVII, como Girolamo Cardano (1501-1576), François Viète (1540-1603), Descartes (1596-1650), G. Leibniz (1646-1716) e Pierre de Fermat (1601-1665) não reconheciam as soluções negativas como raízes de uma equações, alguns consideravam os inteiros negativos como falsos, fictícios ou impossíveis.

Mas já no final do século XVII, um Matemático mudou essa concepção. Colin MacLaurin que nasceu em Kilmodan, Escócia, no ano de 1698. Faleceu aos 48 anos e após dois anos de sua morte foi publicado seu livro *"A treatise on Algebra"* (Um Tratado sobre Álgebra).

Neste tratado, MacLaurin expõe a idéia de que uma quantidade negativa é tão real quanto uma positiva, porém tomada em sentido oposto. Para isto ele enunciou: "se uma quantidade negativa não possui outra que lhe seja oposta não se pode desta subtrair outra menor", SALAZAR (2019, p.115). Ou seja, Maclaurin somente admitia quantidades negativas em relação ao zero origem. Algo que outrora causava grandes conflitos, pois não se faziam a distinção do zero absoluto ao zero relativo à origem. Em um trecho de sua obra ele define a regra de sinais, esta dedução deu início a uma era de formalismo até então inexistente. Ele foi o primeiro matemático moderno que chegou muito perto de compreender os números negativos tornando-se, portanto, uma importante referência para as futuras gerações de matemáticos (MEDEIROS; MEDEIROS, 1992, p.) e (BOYER; MERZBACH, 2012, p.).

Outro matemático de destaque foi Leonarno de Pisa, filho de Bonacci, e por isso ficou conhecido por Fibonacci. Em 1202, publicou uma de suas maiores obras *Liber Abacci* onde complilou todo o conhecimento da época sobre números e álgebra presentes naquele período. "Essa obra foi responsavél pela introdução na Europa do sistema de númeração indo-arábico e pelo posterior desenvolvimento da álgebra e da aritmética no ocidente", HEFEZ (2013, p.41).

Embora a Matemática tenha sido continuadamente estudada por autores gregos e, posteriormente, por árabes, indianos e europeus, a parte da Teoria dos Números ficou esquecida até o início do século XVII. A Teoria dos Números ressurgiu com o francês Pierre de Fermat $(1601 - 1665)$ que, embora fosse advogado e político, tinha como *hobby*

a Matemática. O estudioso, ao ter contato com as publicações de Diofanto, fez diversas anotações na lateral do livro contribuindo significativamente para os números primos e nas propriedades de divisibilidade, além de restringir o universo de soluções possíveis aos números inteiros.

Para (BOYER; MERZBACH, 2012), alguns dos teoremas de Fermat foram demostrados por um método que denominou sua "descida infinita".

> Usando seu método, o francês demonstrou a afirmação de Girard de que todo número primo da forma $4n + 1$ pode ser escrito de uma única maneira como soma de dois quadrados. Posteriormente, Fermat usou seu método para demonstrar que nenhum cubo é soma de dois cubos – isto é, que não existem inteiros positivos x, y e z, tais que $x^3 + y^3 = z^3$. Porém, devido a margem lateral do livro ser pequena, o teórico não escreveu ali a demostração, por isso, não se sabe se realmente tinha essa demostração intitulada como o Último Teorema de Fermat.(BOYER; MERZBACH, 2012, p.249).

Além disso, Fermat escreveu que "se p é primo e a é primo com p, então $a^{p-1} - 1$ é divisível por p" e essa contribuição ficou conhecida como o Pequeno Teorema de Fermat. Depois da morte do teórico francês, em 1665, coube a Samuel Fermat, seu filho, coletar e publicar a obra de seu pai. Dessas anotações, a parte de maior destaque foi o Último Teorema de Fermat.

Este teorema despertou o interesse de vários matemáticos por mais de 350 anos, e só em 1995 o matemático Andrew Wiles conseguiu dar uma prova a ele encerrando assim mais um capítulo das contribuições para a Matemática HEFEZ (2013, p.162).

Ficou a cargo de seu sucessor, Leonhard Euler, a demostração do teorema que também verificou uma falha na conjectura de que todo número da forma $F_n = 2^{2^n} + 1$ é primo.

> Tendo demonstrado o Pequeno Teorema de Fermat por indução, Euler demostrou uma afirmação um pouco mais geral, a "função ϕ de Euler". Se m é um inteiro positivo maior que um, a função $\phi(m)$ é definida como o número de inteiros menores que m que são primos com m. Se p é primo, então claramente $\phi(p) = p - 1$. Pode-se demonstrar que $\phi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_r})$, onde $p_1, p_2, \cdots, p_r$ são os fatores primos distintos de m. Usando esse resultado, Euler mostrou que $a^{\phi(m)} - 1$ é divisível por m se a é primo com m, (BOYER; MERZBACH, 2012, p.310).

Em 1770, Lagrange publicou uma demostração do Teorema para o qual Fermat dissera ter uma demostração, a de que todo inteiro positivo é a soma de no máximo quatro quadrados perfeitos, o qual ficou conhecido como " o Teorema de Lagrange dos quatro quadrados". Ao mesmo tempo, ele demostrou pela primeira vez um resultado conhecido como Teorema de Wilson, para qualquer primo p, o inteiro $(p - 1)! + 1$ é divisível por p.

> Já o matemático Legendre publicou um *Essai sur la théoriedes nombres* $(1797 - 1798)$ em dois volumes, o primeiro dedicou-se à demonstração do

> Último Teorema de Fermat e o segundo, igualmente famoso, é um teorema sobre congruências. Se, dados inteiros p e q, existe um inteiro x tal que $x^2 - q$ é divisível por p, então q é chamado um resto quadrático de p, porém Legendre utilizou a notação de divisibilidade para sua demosntração ao invés da notação de congruências, (BOYER; MERZBACH, 2012, p.249).

Euler foi responsável pela divulgação da Teoria dos Números, mas o estudo de forma sistematizada, de forma metodológica, visando a elaboração do conhecimento, iniciou-se somente com o alemão Carl Friedrich Gauss (1777-1855), em sua obra *Disquisitiones Arithmeticae*, publicada em 1801, quando tinha apenas 24 anos.

Carl Friedrich Gauss $(1777-1855)$, conhecido como o "príncipe da matemática", foi um matemático, astrônomo e físico alemão que contribuiu muito em diversas áreas da ciência e desde cedo mostrava sua facilidade com números. Uma de suas obras que contribuiu para a Teoria dos Números foi *Disquisitiones Arithmeticae* (Investigações Aritméticas) em 1801, ainda no início de sua carreira Matemática, que se transformou em um clássico da literatura Matemática. Nessa obra, Gauss introduz a noção de congruência, desenvolve a teoria dos resíduos quadráticos, demostra a Lei da Reciprocidade quadrática entre outras contribuições. Já no primeiro capítulo do seu livro traz o conceito de congruência: e a notação que a torna uma técnica tão poderosa. Ou seja:

"Sejam a e b inteiros quaisquer e seja $m > 1$ um inteiro positivo fixo. Diz-se que a é congruente a b módulo m, se, e somente se, m divide a diferença $a - b$". Gauss foi o primeiro a usar a notação $a \equiv b \bmod m$, para dizer que a é congruente a b módulo m.

Após as contribuições de Gauss a Teoria dos Números, podemos reescrever o Teorema sobre Congruências de Legendre, conhecido como "Teorema de Ouro", da seguinte forma $x^2 \equiv q \bmod p$. Embora Gauss tenha contribuído para várias áreas do conhecimento, afirmou que "a matemática é a rainha das ciências e a teoria dos números é a rainha das matemáticas".

Diante das grandes contribuições deixadas pelos matemáticos em cada época da história para a Teoria dos Números destacamos a teoria de congruências que se relaciona com o objeto de estudo deste trabalho.

2 A importância dos números inteiros no currículo

Neste capítulo é feito uma análise da Base Nacional Comum Curricular- BNCC BRASIL (2017), o documento que norteia a elaboração das diretrizes da Educação Básica, com o objetivo de verificar se é apresentado e como é abordado o tema Números Inteiros.

Segundo REZENDE (2007),

> [...] A Teoria dos Números, ao ter como foco o estudo dos números inteiros, que é um campo propício para o desenvolvimento de atividades investigativas, pois a exploração de padrões e de relações numéricas, o uso da recursão e da indução Matemática, envolvendo os inteiros, a divisibilidade e números primos estiveram e estão presentes na Matemática e podem ser exploradas nas atividades escolares, em qualquer nível, (REZENDE, 2007, p.209)

Nesse sentido, é importante verificarmos se a Teoria dos Números tem relevância no currículo da Educação Básica e o que as normativas orientam. Em 2017, com o objetivo de uniformizar a Educação Básica no Brasil, após um longo período de discussões entre pesquisadores, professores e sociedade através de audiências públicas, foi criada a BNCC BRASIL (2017). O documento determina as competências (gerais e específicas), as habilidades e as aprendizagens essenciais que todos os alunos devem desenvolver durante cada etapa da Educação Básica. Além disso, determina que essas competências, habilidades e conteúdos devem ser os mesmos, independentemente de onde as crianças, os adolescentes e os jovens moram ou estudam.

Dentre as oito competências específicas de Matemática para o Ensino Fundamental destacamos a que evidência o campo da Aritmética:

> Compreender as relações entre conceitos e procedimentos dos diferentes campos da Matemática (Aritmética, Álgebra, Geometria, Estatística e Probabilidade) e de outras áreas do conhecimento, sentindo segurança quanto à própria capacidade de construir e aplicar conhecimentos matemáticos, desenvolvendo a autoestima e a perseverança na busca de soluções. (BRASIL, 2017, p.267).

A BNCC BRASIL (2017) propõe cinco unidades temáticas que se correlacionam entre si, a que se refere a números, por estar ligada diretamente à Teoria Elementar dos Números tem como finalidade:

> desenvolver o pensamento numérico, que implica o conhecimento de maneiras de quantificar atributos de objetos e de julgar e interpretar argumentos baseados em quantidades. [...] Para essa construção, é importante propor, por meio de situações significativas, sucessivas ampliações dos

> campos numéricos. No estudo desses campos numéricos, devem ser enfatizados registros, usos, significados e operações, (BRASIL, 2017, p.268).

A BNCC BRASIL (2017) enfatiza a importância da inserção gradativa da argumentação Matemática, por meio da leitura de textos para que se desenvolva o senso crítico em relação à argumentação utilizada. Porém, ao fazer um comparativo do 6º ao 9º ano, na unidade temática números, apenas no 7ª ano fica explícito o conceito de números inteiros, em objetos do conhecimento que abordam o uso, a história, a ordenação, a associação com pontos da reta numérica e as operações. Vale salientar, entretanto, que problemas relativos à teoria elementar dos números poderiam trazer o desenvolvimento de tal argumentação, com as discussões provenientes de suas resoluções.

Analisando se há continuidade do conceito de números inteiros no que se refere a Matemática para o Ensino Médio na BNCC BRASIL (2017), verificamos que, dentre as cinco competências específicas, a de número quatro menciona o termo Aritmética, dizendo que deve-se:

> Compreender e utilizar, com flexibilidade e precisão, diferentes registros de representação matemáticos (algébrico, aritmético, geométrico, estatístico, computacional etc.), na busca de solução e comunicação de resultados de problemas, (BRASIL, 2017, p.531).

Diante disso, podemos dizer que não há explicitamente uma preocupação em abordar os conceitos mais profundos da Teoria dos Números, ou seja, não é explorada de forma adequada no currículo da Educação Básica. Questionamos, a partir de então: é possível ensinar Aritmética dos Restos no Ensino Médio?

Uma proposta de currículo de Matemática para o Ensino Médio que aborde a temática Aritmética foi elaborada em 2014 pela Sociedade Brasileira de Matemática SBM (2015) em conjunto com professores universitários e professores atuantes na Educação Básica. A proposta considera quatro áreas do conhecimento: números e funções, geometria, Matemática discreta e tratamento da informação que permeiam as três séries do Ensino Médio, através de conteúdos chaves que conduzirão à aquisição das habilidades esperadas. Em seguida, é apresentada por série cada área do conhecimento dividindo-se em: estrutura de tópicos, habilidades e recomendações. Além disso, dentro de cada área, acrescentamos ainda um bloco chamado “temas suplementares”, a fim de provocar uma discussão ao optar por uma proposta relativamente ousada sobre o tipo de ensino que se pretende oferecer (Científico, Humanístico ou Geral).

A área do conhecimento Matemática Discreta para a 1º série do Ensino Médio traz o tema aritmética com os seguintes conteúdos: 2.1. Divisão Euclidiana, discussão sobre diferentes algoritmos e procedimentos e suas relações com a estrutura do sistema posicional de numeração. 2.2. Divisibilidade e Resto: aritmética dos restos, múltiplos e divisores, números primos, fatoração e critérios de divisibilidade; 2.3. Máximo Divisor Comum;

2.4. Mínimo Múltiplo Comum. e nos temas suplementares: 2.1. Aritmética Modular, 2.2. Sistema de numeração posicional e mudança de base. Na proposta, fica evidente que é possível introduzir os conceitos de Aritmética dos Restos no Ensino Médio o que vem de encontro com o nosso entendimento a cerca do tema.

Segundo GROENWALD & SAUER (2005) o estudo de tópicos da Teoria dos Números pode ser desenvolvido, na Educação Básica, de modo a

> estimular nos alunos o interesse pela Matemática, aprimorando o raciocínio lógico e ampliando a compreensão dos conceitos básicos para o refinamento do pensamento aritmético e algébrico, fazendo com que os mesmos desenvolvam a capacidade de manipular conceitos e propriedades de forma clara e objetiva, (GROENWALD; SAUER, 2005, p.02).

De fato, acreditamos que introduzir aritmética dos restos no currículo da Educação Básica possibilitará desenvolver a capacidade dos alunos de pensar aritmética e algebricamente, de modo que sejam capazes de perceber que a matemática, não é apenas decorar fórmulas prontas e reproduzi-las para obtenção de resultados em exames e avaliações, mas sim, como um conjunto de ferramentas que podem ser adaptadas e utilizadas às mais diversas situações do seu cotidiano.

3 Congruências

Nesta seção, damos ênfase aos conceitos que, certamente, compõem o ponto principal do nosso trabalho.

3.1 Congruência módulo m

Em Matemática, o termo Congruência é muito conhecido e usado quando comparamos duas figuras geométricas. De acordo com BARBOSA (2006, p.26) dizemos que dois triângulos são congruentes se for possível estabelecer uma correspondência biunívoca entre seus vértices de modo que lados e ângulos correspondentes sejam congruentes. Mas, em 1801, Carl F. Gauss aplicou a ideia de congruência aos números inteiros em seu livro Disquisitiones Arithmeticæ (Estudos de Aritmética), um trabalho de importância fundamental na moderna teoria dos números, Eves (1995, p.520).

É comum encontrarmos em livros de matemática questões do tipo: O número 5328695 é divisível por 5? Para respondermos essa questão vamos recorrer a definição a seguir.

Definição 3.1. Dados dois números inteiros a e b, dizemos que a divide b, escrevendo $a \mid b$, quando existir $c \in \mathbb{Z}$ tal que $b = ca$. Neste caso, dizemos também que: a é um divisor de b, b é um múltiplo de a, ou ainda que b é divisível por a. A negação dessa sentença é representada por $a \nmid b$, que significa que não existe nenhum número inteiro c tal que $b = ac$.

Notação: $a \mid b$. Lê-se: a divide b.

$a \nmid b$. Lê-se: a não divide b.

Respondendo a questão anterior, e de acordo com a Definição 3.1, sim! Pois, $5328695 = 1065739 \cdot 5$.

Outra maneira de verificarmos se um número é divisível por outro é através dos critérios de divisilividade. Um critério de divisibilidade é uma regra que permite avaliarmos se um dado número natural é ou não divisível por outro número natural, sem que seja necessário efetuarmos a divisão.

Vamos enunciar alguns, por exemplo:

- **Critério de divisibilidade por 2:** Um número é divisível por 2 quando ele for par, ou seja, todos os números cujo último algarismo é 0, 2, 4, 6 ou 8;

- **Critério de divisibilidade por** 3**:** Um número é divisível por 3 se a soma de seus algarismos for um número divisível por 3;
- **Critério de divisibilidade por** 4**:** Um número é divisível por 4 se termina em 00 ou quando os dois últimos algarismos formam um número divisível por 4;
- **Critério de divisibilidade por** 5**:** Um número é divisível por 5 quando termina em 0 ou 5.
- **Critério de divisibilidade por** 10**:** Um número natural n é divisível por 10 se, e somente se, o seu algarismo das unidades é 0.

Dessa forma podemos afirmar que o número 258435 é divisível por 5, pois o último algarismo é 5. É possível verificar também se um número é divisível por outro através da Divisão Euclidiana, pois se o resto for igual a zero, dizemos que o número é divisível.

Teorema 3.1. *(Divisão Euclidiana) Se a e b são dois inteiros, com $b > 0$, então existem e são únicos os inteiros q e r que satisfazem às condições: $a = bq + r$ e $0 \leqslant r < |b|$.*

Demonstração. Veja HEFEZ (2013, p.53). □

Nas condições do Teorema acima, os números a e b são o divisor e o dividendo, enquanto q e r são chamados, respectivamente de quociente e de resto da divisão de b por a.

Observação: O resto da divisão de a por b é zero se, e somente se, b divide a.

Exemplo 1. Na divisão de 247 por 16, encontramos $q = 15$ e $r = 7$.

Mas se desejarmos saber se o número 2^{2015} é divisível por 5? Neste caso, para números extremamente grandes não é tão facíl verificarmos e tão pouco de efetuarmos a divisão entre eles. Precisamos então, conhecer outras técnicas de resolução, e assim contamos com as contribuições deixadas por Gauss para responder essa questão no decorrer do capítulo.

Iniciamos com a definição de congruência. De acordo com HEFEZ (2013, p.192):

Definição 3.2. Seja m um número natural, diremos que dois inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros são congruentes módulo m, escreve-se

$$a \equiv b \bmod m.$$

Lê-se: a é congruente a b módulo m.

E se a relação for falsa, representa-se por:

$$a \not\equiv b \bmod m.$$

Lê-se: a é incongruente a b módulo m.

Exemplo 2. Verifique que $31 \equiv 6 \bmod 5$.

Solução: Sabemos que,

$$31 = 5 \cdot 6 + 1 \quad \text{e} \quad 6 = 5 \cdot 1 + 1.$$

Como, 31 e 6 deixam o mesmo resto quando divididos por 5, segue que

$$31 \equiv 6 \bmod 5.$$

Exemplo 3. Temos que $31 \not\equiv 6 \bmod 3$.

Solução: Sabemos que,

$$31 = 3 \cdot 10 + 1 \quad \text{e} \quad 6 = 3 \cdot 2 + 0.$$

Como, 31 e 6 não deixam o mesmo resto quando divididos por 3, segue que

$$31 \not\equiv 6 \bmod 3.$$

3.1.1 Propriedades das Congruências

Decorre da definição que a congruência, módulo um inteiro fixado m, é uma relação de equivalência, ou seja, é reflexiva, simétrica e transitiva. Conforme é apresentado na Proposição 3.1.

Proposição 3.1. *Seja $m > 1$ um inteiro fixo e a, b, c inteiros arbitrários. Então as seguintes propriedades são válidas:*

a) $a \equiv a \bmod m$ *(Reflexiva).*

b) Se $a \equiv b \bmod m$*, então* $b \equiv a \bmod m$ *(Simétrica).*

c) Se $a \equiv b \bmod m$ *e* $b \equiv c \bmod m$*, então* $a \equiv c \bmod m$ *(Transitiva).*

Demonstração. a) Esta é imediata, pois na divisão por m um número a deixa o mesmo resto que ele mesmo.

b) Sejam $a = mq_1 + r_1$ com $0 \leqslant r_1 < m$ e $b = mq_2 + r_2$, com $0 \leqslant r_2 < m$ as divisões euclidianas de a e b por m, respectivamente. Por hipótese, temos que $a \equiv b \bmod m$. Segue, da Definição 3.2 que $r_1 = r_2$. Mas se $r_1 = r_2$, por simetria, temos que $b \equiv a \bmod m$.

c) Sejam $a = mq_1 + r_1$ com $0 \leqslant r_1 < m$, $b = mq_2 + r_2$, com $0 \leqslant r_2 < m$ e $c = mq_3 + r_3$, com $0 \leqslant r_3 < m$ as divisões euclidianas de a,b e c por m, respectivamente. Por hipótese, temos que $a \equiv b \bmod m$ e pela Definição 3.2 temos que $r_1 = r_2$ e $b \equiv c \bmod m$ pela mesma definição temos que $r_2 = r_3$. Logo, por transitividade, $r_1 = r_3$, ou seja, $a \equiv c \bmod m$.

□

Segue da Proposição 3.2, item **(a)**, que $3 \equiv 3 \bmod 5$ e $4 \equiv 4 \bmod 6$. E do item **(b)** que $8 \equiv 3 \bmod 5$, assim como $3 \equiv 8 \bmod 5$.

3.1.2 Caracterização de inteiros congruentes

Esta seção traz alguns resultados úteis para verificar se dois inteiros são ou não congruentes.

Proposição 3.2. *Para verificar se dois números inteiros a e b são congruentes módulo m, basta verificar se m divide a diferença entre eles, ou seja,*

$$a \equiv b \bmod m \text{ se, e somente se, } m \mid b - a.$$

Demonstração. Sejam $a = mq_1 + r_1$ e $b = mq_2 + r_2$, com $0 \leqslant r_1, r_2 < m$, as divisões euclidianas de a e b por m, respectivamente. Suponha que $a \equiv b \bmod m$. Segue, da definição, que $r_1 = r_2$ e daí $b - a = m(q_2 - q_1) + r_2 - r_1 = m(q_2 - q_1)$, portanto $m \mid b - a$.

Reciprocamente, suponha que $m \mid b - a$. Como $r_2 - r_1 = b - a - m(q_2 - q_1)$ e $m \mid b - a$, concluimos que $m \mid r_2 - r_1$. Neste caso, $r_2 - r_1$ é zero, ou um múltiplo não nulo de m . Sendo $0 \leqslant r_1, r_2 < m$ temos que $0 \leqslant |r_2 - r_1| < m$, mas como m não pode ser um múltiplo negativo, logo $r_2 - r_1 = 0$, ou seja $r_2 = r_1$.

Portanto, $a \equiv b \bmod m$. □

Exemplo 4. Verifique que $7 \equiv 4 \bmod 3$.

Solução: Pela Proposição 3.2, $7 \equiv 4 \bmod 3$ se 3 divide $7 - 4 = 3$.

Como 3 divide 3, segue que, $7 \equiv 4 \bmod 3$.

Exemplo 5. Verifique que $8 \equiv 3 \bmod 2$.

Solução: Pela Proposição 3.2, $8 \equiv 3 \bmod 2$ se 2 divide $8 - 3 = 5$.

Como 2 não divide 5, segue que $8 \not\equiv 3 \bmod 2$.

O que torna útil e poderosa a noção de congruência é o fato de ser uma relação de equivalência compatível com as operações de adição e multiplicação nos inteiros, conforme a seguir.

Proposição 3.3. *Seja $m > 1$ um inteiro fixo e a, b, c, d inteiros arbitrários. Então as seguintes propriedades são válidas:*

a) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a + c \equiv b + d \bmod m$.

b) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $ac \equiv bd \bmod m$.

Demonstração. a) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, temos $a - b = km$ e $c - d = k_1 m$. Somando-se membro a membro obtemos $(a + c) - (b + d) = (k + k_1)m$ e isto implica que $a + c \equiv b + d \bmod m$.

b) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, temos $a - b = km$ e $c - d = k_1 m$. Multiplicando $a - b = km$ por c e $c - d = k_1 m$ por b obtemos $ac - bc = ckm$ e $bc - bd = bk_1 m$ somando membro a membro obtemos $ac - bc + bc - bd = ckm + bk_1 m$, ou seja, $ac - bd = m(ck + bk_1)$ o que implica $ac \equiv bd \bmod m$.

□

Exemplo 6. Verifique que $32 \equiv 7 \bmod 5$ e $21 \equiv 6 \bmod 5$ e conclua que $53 \equiv 13 \bmod 5$.

Solução: Note que, pela Proposição 3.2, $5 \mid 32 - 7$, ou seja, 5 divide $32 - 7 = 25$. Assim, $32 \equiv 7 \bmod 5$. Da mesma forma que 5 divide $21 - 6 = 15$. Assim, $21 \equiv 6 \bmod 5$.

Segue da Proposição 3.3 item **(a)** que $32 + 21 \equiv 7 + 6 \bmod 5$, logo temos que $53 \equiv 13 \bmod 5$. Podemos conferir que de fato, $5 \mid 53 - 13$, ou seja, $5 \mid 40$.

Exemplo 7. Verifique que $15 \equiv 8 \bmod 7$ e $9 \equiv 2 \bmod 7$ e conclua que $135 \equiv 16 \bmod 7$.

Solução: Observe que, pela Proposição 3.2, 7 divide $15 - 8 = 7$, e 7 divide $9 - 2 = 7$. Assim, $15 \equiv 8 \bmod 7$ e $9 \equiv 2 \bmod 7$ respectivamente.

Pela da Proposição 3.3, item **(b)** que $15 \cdot 9 \equiv 8 \cdot 2 \bmod 7$. Logo temos que $135 \equiv 16 \bmod 7$, $7 \mid 135 - 16$, ou seja, $7 \mid 119$.

Corolário 3.1. *Se $a \equiv b \bmod m$ então $a^k \equiv b^k \bmod m$ para todo inteiro positivo k.*

Demonstração. A prova deste resultado é dada por indução matemática sobre o número inteiro positivo k. De fato,

i) Para $n = 1$, temos $a^1 \equiv b^1 \bmod m$ implica que $a \equiv b \bmod m$.

ii) Suponha que a proposição seja verdadeira para $k = n$. Queremos mostrar que é verdadeira para um $k = n + 1, n \in \mathbb{Z}$. De fato, temos que a hipótese geral é $a \equiv b \bmod m$, a hipótese de indução: $a^n \equiv b^n \bmod m$ e a tese: $a^{n+1} \equiv b^{n+1} \bmod m$.

Pela Proposição 3.3 item(b), temos que $a \cdot a^n \equiv b \cdot b^n \bmod m$ o que implica $a^{n+1} \equiv b^{n+1} \bmod m$. □

Exemplo 8. Vamos utilizar a Proposição 3.3 para verificarmos quais elementos do conjunto $\{0, 1, 2, 3, \cdots, 12, 13\}$ são congruentes a elementos da sequência $6^1, 6^2, 6^3, 6^4, 6^5, \cdots$, módulo 14.

Temos que

$$\begin{aligned}
&6^1 \equiv 6 \bmod 14\\
&6^2 = 6^1 \cdot 6^1 \equiv 6 \cdot 6 \bmod 14 \Rightarrow \quad 6^2 \equiv 36 \bmod 14 \Rightarrow \quad 6^2 \equiv 8 \bmod 14\\
&6^3 = 6^2 \cdot 6^1 \equiv 8 \cdot 6 \bmod 14 \Rightarrow \quad 6^3 \equiv 48 \bmod 14 \Rightarrow \quad 6^3 \equiv 6 \bmod 14\\
&6^4 = 6^3 \cdot 6^1 \equiv 6 \cdot 6 \bmod 14 \Rightarrow \quad 6^4 \equiv 36 \bmod 14 \Rightarrow \quad 6^4 \equiv 8 \bmod 14\\
&6^5 = 6^4 \cdot 6^1 \equiv 8 \cdot 6 \bmod 14 \Rightarrow \quad 6^5 \equiv 48 \bmod 14 \Rightarrow \quad 6^5 \equiv 6 \bmod 14\\
&6^6 = 6^5 \cdot 6^1 \equiv 6 \cdot 6 \bmod 14 \Rightarrow \quad 6^6 \equiv 36 \bmod 14 \Rightarrow \quad 6^6 \equiv 8 \bmod 14.
\end{aligned}$$

Em geral, podemos provar por indução em $k \geqslant 0$ que

$$\begin{aligned}
6^1 \equiv 6^3 \equiv 6^5 \equiv \cdots \equiv 6^{2k+1} \equiv 6 \bmod 14\\
6^2 \equiv 6^4 \equiv 6^6 \equiv \cdots \equiv 6^{2k+2} \equiv 8 \bmod 14.
\end{aligned}$$

De fato, o resultado já foi verificado para o caso base $k = 0$. Supondo que

$$6^{2p+1} \equiv 6 \bmod 14 \qquad \text{e} \qquad 6^{2p+2} \equiv 8 \bmod 14.$$

Para $k = p + 1$, que

$$\begin{aligned}
&6^{2k+1} = 6^{2p+1} \cdot 6^2 \equiv 6 \cdot 8 \bmod 14 \Rightarrow \quad 6^{2k+1} \equiv 48 \bmod 14 \Rightarrow \quad 6^{2k+1} \equiv 6 \bmod 14\\
&6^{2k+2} = 6^{2p+2} \cdot 6^2 \equiv 8 \cdot 8 \bmod 14 \Rightarrow \quad 6^{2k+2} \equiv 64 \bmod 14 \Rightarrow \quad 6^{2k+2} \equiv 8 \bmod 14.
\end{aligned}$$

Logo, o Princípio de Indução Finita se aplica.

Exemplo 9. (Colégio Naval-2018- Adaptada) Considere a expressão $(2018^{2018})^{2018}$, que é potência de uma potência. É correto afirmar que o algarismo da unidade do resultado dessa expressão é 6?

Solução: Determinar o algarismo das unidades de um número qualquer é o mesmo que determinar o resto na divisão por 10. Dessa forma, pelo Teorema 3.1, Divisão Euclidiana qualquer número inteiro N pode ser escrito sob a forma $N = 10 \cdot k + r$, com k e r inteiros e $0 \leqslant r < 10$.

Assim,

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

Escrevendo na linguagem de congruência módulo 10, temos

$$2018 \equiv 8 \bmod 10.$$

Logo, pelo Corolário 3.1,

$$2018^{2018} \equiv 8^{2018} \bmod 10.$$

Para calcularmos, diretamente o resto da divisão de 8^{2018} por 10 precisaríamos saber o resultado dessa potência primeiro. E fazer esses cálculos na mão dá muito trabalho.

Então vamos escrever as potências de 8 módulo 10 para analisarmos os possíveis restos e verificarmos se é possível estabelecer um padrão.

$$\begin{aligned} 8^1 &= 8 \equiv 8 \bmod 10 \\ 8^2 &= 64 \equiv 4 \bmod 10 \\ 8^3 &= 512 \equiv 2 \bmod 10 \\ 8^4 &= 4096 \equiv 6 \bmod 10. \end{aligned}$$

Note que: $8^5 = 8^1 \cdot 8^4$, pelas propriedades de potência. Logo,

$$8^1 \equiv 8 \bmod 10 \qquad \text{e} \qquad 8^4 \equiv 6 \bmod 10.$$

Pela Proposição 3.3 item **(b)**, temos:

$$8^1 \cdot 8^4 \equiv 8 \cdot 6 \bmod 10 \Rightarrow \quad 8^5 \equiv 48 \bmod 10 \Rightarrow \quad 8^5 \equiv 8 \bmod 10.$$

De maneira análoga podemos obter:

$$\begin{aligned} 8^2 \cdot 8^4 \equiv 4 \cdot 6 \bmod 10 \Rightarrow \quad 8^6 \equiv 24 \bmod 10 \Rightarrow \quad 8^6 \equiv 4 \bmod 10. \\ 8^3 \cdot 8^4 \equiv 2 \cdot 6 \bmod 10 \Rightarrow \quad 8^7 \equiv 12 \bmod 10 \Rightarrow \quad 8^7 \equiv 2 \bmod 10. \\ 8^4 \cdot 8^4 \equiv 6 \cdot 6 \bmod 10 \Rightarrow \quad 8^8 \equiv 36 \bmod 10 \Rightarrow \quad 8^8 \equiv 6 \bmod 10. \end{aligned}$$

Em geral, mostra-se pelo Princípio de Indução Finita que, para todo $k \geqslant 0$

$$8^{4k+1} \equiv 8 \bmod 10, \quad 8^{4k+2} \equiv 4 \bmod 10, \quad 8^{4k+3} \equiv 2 \bmod 10 \quad \text{e} \quad 8^{4k+4} \equiv 6 \bmod 10.$$

Note que, $2018 = 4 \cdot 504 + 2$. Assim, $8^{(4 \cdot 504+2)} \equiv 4 \bmod 10$, ou seja, $8^{2018} \equiv 4 \bmod 10$.

Podemos reescrever

$$2018^{2018} \equiv 8^{2018} \bmod 10$$

como

$$2018^{2018} \equiv 4 \bmod 10.$$

Elevando ambos os lados a 2018, temos

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

Agora de maneira análoga vamos escrever as potências de 4 módulo 10 para analisarmos os possíveis restos.

$$
\begin{aligned}
&4^1 = 4 \equiv 4 \bmod 10\\
&4^2 = 16 \equiv 6 \bmod 10\\
&4^3 = 4^1 \cdot 4^2 \equiv 4 \cdot 6 \bmod 10 \Rightarrow \quad 4^3 \equiv 24 \bmod 10 \Rightarrow \quad 4^3 \equiv 4 \bmod 10.\\
&4^4 = 4^2 \cdot 4^2 \equiv 6 \cdot 6 \bmod 10 \Rightarrow \quad 4^4 \equiv 36 \bmod 10 \Rightarrow \quad 4^4 \equiv 6 \bmod 10.\\
&4^5 = 4^3 \cdot 4^2 \equiv 4 \cdot 6 \bmod 10 \Rightarrow \quad 4^5 \equiv 24 \bmod 10 \Rightarrow \quad 4^5 \equiv 4 \bmod 10.\\
&4^6 = 4^4 \cdot 4^2 \equiv 6 \cdot 6 \bmod 10 \Rightarrow \quad 4^6 \equiv 36 \bmod 10 \Rightarrow \quad 4^6 \equiv 6 \bmod 10.\\
&4^7 = 4^5 \cdot 4^2 \equiv 4 \cdot 6 \bmod 10 \Rightarrow \quad 4^7 \equiv 24 \bmod 10 \Rightarrow \quad 4^7 \equiv 4 \bmod 10.\\
&4^8 = 4^6 \cdot 4^2 \equiv 6 \cdot 6 \bmod 10 \Rightarrow \quad 4^8 \equiv 36 \bmod 10 \Rightarrow \quad 4^8 \equiv 6 \bmod 10.
\end{aligned}
$$

Dessa forma, como mostrado no exemplo anterior, para todo $k \geqslant 0$

$$4^{2k+1} \equiv 4 \bmod 10 \quad \text{e} \quad 4^{2k+2} \equiv 6 \bmod 10.$$

Note que, $2018 = 2 \cdot 1008 + 2$. Assim, $4^{(2\cdot 1008+2)} \equiv 6 \bmod 10$, ou seja, $4^{2018} \equiv 6 \bmod 10$.

Portanto, $(2018^{2018})^{2018} \equiv 4^{2018} \equiv 6 \bmod 10$. Ou seja, concluimos que o algarismo da unidade da expressão inicial é 6.

Proposição 3.4. *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$. Tem-se que*

$$a + c \equiv b + c \bmod m \Leftrightarrow a \equiv b \bmod m.$$

Demonstração. Se $a \equiv b \bmod m$, pela Proposição 3.3 item **(a)** temos que $a + c \equiv b + c \bmod m$, pois $c \equiv c \bmod m$.

Reciprocamente, se $a + c \equiv b + c \bmod m$ então $m \mid b + c - (a + c)$, o que implica que $m \mid b - a$ e, consequentemente, $a \equiv b \bmod m$. □

Exemplo 10. (Colégio Naval-2011) É correto afirmar que o número $5^{2011} + 2 \cdot 11^{2011}$ é múltiplo de 3?

Solução: Queremos mostrar que o resto da divisão de $5^{2011} + 2 \cdot 11^{2011}$ por 3 é 0.

Na linguagem de congruências, queremos verificar isso:

$$5^{2011} + 2 \cdot 11^{2011} \equiv 0 \bmod 3.$$

Vamos verificar se as bases $5, 2$ e 11 são múltiplas de 3.

Base 5:

$$5 \equiv 2 \bmod 3.$$

Base 2:

$$2 \equiv 2 \bmod 3.$$

Base 11:

$$11 \equiv 2 \bmod 3.$$

Pela Proposição 3.3,

$$5^{2011} + 2 \cdot 11^{2011} \equiv 2^{2011} + 2 \cdot 2^{2011} \bmod 3.$$

Colocando o termo 2^{2011} em evidência, no lado direito da congruência temos que

$$5^{2011} + 2 \cdot 11^{2011} \equiv 2^{2011}(1 + 2) \bmod 3$$

$$5^{2011} + 2 \cdot 11^{2011} \equiv 3 \cdot 2^{2011} \bmod 3.$$

Como $3 \cdot 2^{2011} \equiv 0 \bmod 3$, segue por transitividade que $5^{2011} + 2 \cdot 11^{2011} \equiv 0 \bmod 3$.

Portanto, o resto da divisão é 0, o que implica que $5^{2011} + 2 \cdot 11^{2011}$ é múltiplo de 3.

A Proposição 3.4 deixa claro que vale a lei do cancelamento em relação a adição. E em relação a multiplicação, é sempre possível?

Vamos analisar alguns exemplos.

Exemplo 11. Note que $245 \equiv 21 \bmod 8$, pois $8 \mid 245 - 21 = 224$.

Desta forma, temos $245 \equiv 21 \bmod 8$ se, e somente se, $7 \cdot 35 \equiv 7 \cdot 3 \bmod 8$. Observe que nesta situação podemos cancelar o número 7 e ainda obtermos a congruência verdadeira, $35 \equiv 3 \bmod 8$, pois 8 divide $35 - 3 = 32$.

Exemplo 12. Observe que $14 \equiv 6 \bmod 8$, pois 8 divide $14 - 6 = 8$.

Em particular, $2 \cdot 7 \equiv 2 \cdot 3 \bmod 8$.

Suponhamos que o número 2 possa ser cancelado, daí teríamos $7 \equiv 3 \bmod 8$. O que é um absurdo, pois pela Proposição 3.2, 8 não divide $7 - 3 = 4$.

Apresentamos a proposição a seguir que nos permite verificar quando é possível realizar o cancelamento na operação de multiplicação de maneira geral. Mas antes disso, se faz necessário definir alguns conceitos, como por exemplo o Máximo Divisor Comum entre dois números.

Definição 3.3. (Divisor Comum) Sejam dados dois inteiros a e b, distintos ou não. Um número inteiro d será dito um divisor comum de a e b se $d \mid a$ e $d \mid b$.

Definição 3.4. (Máximo Divisor Comum) Um número inteiro $d \geqslant 0$ é o máximo divisor comum (mdc) de a e b, se possuir as seguintes propriedades:

- d é um divisor comum de a e b;
- d é divisível por todo divisor comum de a e b.

Notação: Denotamos o Máximo Divisor Comum entre os números inteiros a e b por $mdc(a, b)$, ou apenas (a, b).

Exemplo 13. Os divisores de 12 e 30 são dados respectivamente pelos conjuntos $D(12) = \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm12\}$ e $D(30) = \{\pm1, \pm2, \pm3, \pm5, \pm6, \pm10, \pm15, \pm30\}$. Dessa forma, o máximo divisor comum entre 12 e 30 é 6.

Definição 3.5. Um número natural d será dito MDC de dados números inteiros $a_1, \cdots, a_n$, não todos nulos, se possuir as seguintes propriedades:

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

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

Proposição 3.5. *Dados números inteiros $a_1, \cdots, a_n$, não todos nulos, existe o seu MDC e*

$$(a_1, \cdots, a_n) = (a_1, \cdots, (a_{n-1}, a_n)).$$

Proposição 3.6. *Sejam $a, b, c, m \in \mathbb{Z}$, com $c \neq 0$ e $m > 1$. Temos que*

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

Demonstração. Veja HEFEZ (2013, p.196). □

Observe que na Proposição 3.6 podemos pensar em uma lei do cancelamento (generalizada), pois ao cancelar o c alteramos o valor do módulo. Contudo apresentamos a seguir o Corolário 3.2 o qual afirma que o cancelamento vale quando c e m são primos entre si, ou seja, quando o máximo divisor comum entre c e m for igual a 1.

Corolário 3.2. *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$ e $(c, m) = 1$. Temos que*

$$ac \equiv bc \bmod m \Leftrightarrow a \equiv b \bmod m.$$

Demonstração. Veja HEFEZ (2013, p.197). □

Antes de enunciar a Proposição 3.7 é necessário definir o conceito de Mínimo Múltiplo Comum.

Definição 3.6. (Múltiplo Comum) Um número inteiro m é um múltiplo comum de a e b se $a \mid m$ e $b \mid m$.

Definição 3.7. (Mínimo Múltiplo Comum) Um número inteiro $m \geqslant 0$ é um mínimo múltiplo comum (mmc) dos números inteiros a e b, se possuir as seguintes propriedades:

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

Notação: Denotamos o Mínimo Múltiplo Comum entre os números inteiros a e b por $mmc[a, b]$, ou apenas $[a, b]$.

Exemplo 14. Calcule o mmc $[12, 30]$.

Solução: Tomando M(12)= $\{\cdots, -72, -60, -48, -36, -24, -12, 0, 12, 24, 36, 48, 60, 72, \cdots\}$ e M(30)= $\{\cdots, -120, -90, -60, -30, 0, 30, 60, 90, 120, \cdots\}$, temos que $[12, 30] = 60$.

Proposição 3.7. *Dados dois números inteiros a e b, temos que $[a, b]$ existe e*

$$[a, b] \cdot (a, b) = |a \cdot b|$$

Demonstração. Veja HEFEZ (2013, p.106). □

Exemplo 15. Calcule o mmc $[5, 48]$.

Solução: Temos que, $(5, 48) = 1$. Logo, pela Proposição 3.7,

$$[5, 48] \cdot (5, 48) = |5 \cdot 48| \quad \Rightarrow \quad [5, 48] \cdot 1 = |5 \cdot 48| \quad \Rightarrow \quad [5, 48] = 240.$$

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

Proposição 3.8. *Sejam $a_1, \cdots, a_n$ números inteiros não nulos. Então existe o número $[a_1, \cdots, a_n]$ e $[a_1, \cdots, a_{n-1}, a_n] = [a_1, \cdots, [a_{n-1}, a_n]]$.*

Exemplo 16. Queremos determinar o MMM dos números 12, 85 e 32. Pela Proposição 3.8, temos que

$$[5, 84, 32] = [5, [84, 32] = [5, 672] = 3360.$$

Proposição 3.9. *Sejam $a, b \in \mathbb{Z}$, e $m, n, m_1, \cdots, m_r$ inteiros maiores do que 1. Temos que:*

a) Se $a \equiv b \bmod m$ e $n \mid m$, então $a \equiv b \bmod n$;

b) $a \equiv b \bmod m_i, \forall i = 1, \cdots, r \Leftrightarrow a \equiv b \bmod [m_1, \cdots, m_r]$;

c) Se $a \equiv b \bmod m$*, então* $(a, m) = (b, m)$*.*

Demonstração. Veja HEFEZ (2013, p.198). □

Diante da teoria que vimos até agora e conhecendo as diversas ferramentas podemos resolver a questão proposta no início do capítulo.

Exemplo 17. Qual o resto da divisão de 2^{2015} por 5?

Solução: Primeiro vamos tentar encontrar uma potência de 2^n que deixa resto 1 na divisão por 5, pois sabemos que qualquer expoente na base 1 o resultado é 1 o que falicita a resolução da congruência. Dessa forma, vamos escrever as potências de 2^n módulo 5 para analisarmos os possíveis restos.

$$2^1 = 2 \equiv 2 \bmod 5$$
$$2^2 = 4 \equiv 4 \bmod 5$$
$$2^3 = 8 \equiv 3 \bmod 5$$
$$2^4 = 16 \equiv 1 \bmod 5.$$

Sabemos que, $2015 = 503 \cdot 4 + 3$.

Como $2^4 \equiv 1 \bmod 5$, segue do Corolário 3.1 que,

$$(2^4)^{503} \equiv 1^{503} \bmod 5$$
$$2^{2012} \equiv 1 \bmod 5.$$

Além disso, pela Proposição 3.3,

$$2^{2012} \cdot 2^3 \equiv 1 \cdot 2^3 \bmod 5$$
$$2^{2012+3} \equiv 2^3 \bmod 5$$
$$2^{2015} \equiv 2^3 \bmod 5.$$

Como $2^3 \equiv 3 \bmod 5$, temos que

$$2^{2015} \equiv 3 \bmod 5.$$

A seguir, apresentamos vários exemplos da aplicação de congruências.

Exemplo 18. O resto da divisão de $2^{1000000}$ por 17 é 1.

Para verificar isso vamos tentar encontrar uma potência de 2^n que deixa resto 1 na divisão por 17.

Observe que

$$\begin{aligned} 2^1 &= 2 \equiv 2 \bmod 17 & 2^5 &= 32 \equiv 15 \bmod 17 \\ 2^2 &= 4 \equiv 4 \bmod 17 & 2^6 &= 64 \equiv 13 \bmod 17 \\ 2^3 &= 8 \equiv 8 \bmod 17 & 2^7 &= 128 \equiv 9 \bmod 17 \\ 2^4 &= 16 \equiv 16 \bmod 17 & 2^8 &= 256 \equiv 1 \bmod 17. \end{aligned}$$

Sabemos que, $1000000 = 125000 \cdot 8 + 0$.

Como $2^8 \equiv 1 \bmod 17$, segue do Corolário 3.1 que,

$$\begin{aligned} (2^8)^{125000} &\equiv (1)^{125000} \bmod 17 \\ 2^{1000000} &\equiv 1 \bmod 17. \end{aligned}$$

Portanto, o resto da divisão de $2^{1000000}$ por 17 é 1.

Exemplo 19. (Sistema de Ensino Poliedro) Qual a 1993ª letra da sequência ABCDEDCBABCDEDCBABCDEDCBABC $\cdots$?

Solução: Observe que a sequência ABCDEDCB se repete a cada 8 letras. Dessa forma, o problema proposto é equivalente a: Qual o resto da divisão de 1993 por 8?

Note que: $1993 = 8 \cdot 249 + 1$, ou seja, $1993 \equiv 1 \bmod 8$.

Logo, a letra de posição 1993 é a primeira letra da sequência ABCDEDCB, ou seja, a letra A.

Exemplo 20. (Colégio Naval-2019) O número E é obtido pela expressão formada pela soma de todas as potências naturais do número 2, desde 0 até 2019, ou seja,

$$\mathbf{E} = 2^0 + 2^1 + 2^2 + 2^3 + \cdots + 2^{2018} + 2^{2019}.$$

O resto da divisão de **E** por 7 é ?

Solução: Inicicialmente vamos analisar quais são os possíveis restos da divisão de 2^n por 7, sendo $n = 0, 1, 2, \cdots, 2019$.

$$\begin{aligned} &2^0 = 1 \equiv 1 \bmod 7 \quad 2^3 = 8 \equiv 1 \bmod 7 \quad 2^6 = 64 \equiv 1 \bmod 7 \quad \cdots \quad 2^{2019} \equiv 1 \bmod 7. \\ &2^1 = 2 \equiv 2 \bmod 7 \quad 2^4 = 16 \equiv 2 \bmod 7 \quad 2^7 = 128 \equiv 2 \bmod 7 \\ &2^2 = 4 \equiv 4 \bmod 7 \quad 2^5 = 32 \equiv 4 \bmod 7 \quad 2^8 = 256 \equiv 4 \bmod 7 \end{aligned}$$

Em geral, mostra-se pelo Príncipio de Indução Finita que, para $k \geqslant 0$

$$2^{3k} \equiv 1 \bmod 7, \qquad 2^{3k+1} \equiv 2 \bmod 7 \quad \text{e} \quad 2^{3k+2} \equiv 4 \bmod 7.$$

Segue da Proposição 3.3 item **a)** que,

$$2^{3k} + 2^{3k+1} + 2^{3k+2} \equiv 1 + 2 + 4 \equiv 7 \equiv 0 \mod 7.$$

Ou seja, a cada 3 elementos consecutivos da soma do número **E**, temos uma soma congruente a zero. Desta forma, como **E** é uma soma de 2020 parcelas e $2020 = 673 \cdot 3 + 1$, temos que $\mathbf{E} = (2^0 + 2^2 + 2^3) + (2^3 + 2^4 + 2^5) + \cdots + (2^{2016} + 2^{2017} + 2^{2018}) + 2^{2019}$. Logo, $\mathbf{E} \equiv 2^{2019} \mod 7$. Como $2019 = 673 \cdot 3 + 0$, concluímos que $\mathbf{E} \equiv 1 \mod 7$.

3.2 Algoritmo de Euclides

> O máximo divisor comum de dois inteiros pode ser encontrado ao listarmos todos os seus divisores positivos e escolhermos o maior comum aos dois, mas isto é embaraçoso para números maiores. Um processo mais eficiente, envolvendo aplicações repetidas do Algoritmo da Divisão, é dado no sétimo livro *Os elementos*. Embora haja evidências históricas de que este método é anterior a Euclides, hoje ele é apresentado como o Algoritmo de Euclides ,(BURTON, 2016, p.25).

Mas antes de descrevermos o algoritmo vamos enunciar o Lema a seguir que será útil na sua construção.

Lema 3.1. *(Lema de Euclides) Sejam a e b e n números inteiros tais que $0 < b - na$. Neste caso, vale a igualdade*

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

Demonstração. Seja $d = (a, b-na)$. Como $d \mid a$ e $d \mid b-na$, tem-se que $d \mid (b-na+na) = b$. Logo, d é um divisor comum de a e b. Suponha agora que c seja outro divisor comum de a e b. Desta forma, c é um divisor comum de a e $b - na$ e consequentemente, por definição de máximo divisor comum tem-se, $c \mid d$. Portanto, $d = (a, b)$. □

O Algoritmo de Euclides pode ser escrito da seguinte maneira: Sejam a e b dois inteiros dos quais se deseja obter o máximo divisor comum . Como $(|a|, |b|) = (a, b)$, pode-se supor, sem perda de generalidade, que $0 < b < a$.

Desta forma, fazendo a divisão euclidiana de a por b, tem-se que existem q_1 e r_1 tais que

$$a = b \cdot q_1 + r_1, \qquad 0 \leqslant r_1 < b.$$

Daí surgem duas possibilidades:

- Se $r_1 = 0$, então $b \mid a$ e consequentemente $(a, b) = b$.

- Se $r_1 \neq 0$, então $b \nmid a$. Nesse caso, efetuarmos a divisão euclidiana de b por r_1. Logo, existem inteiros q_2 e r_2 que satisfazem

$$b = r_1 \cdot q_2 + r_2, \qquad 0 \leqslant r_2 < r_1 < b.$$

Novamente, temos duas possibilidades:

- Se $r_2 = 0$, então $r_1 \mid b$ e $(b, r_1) = r_1$. Logo, segue do Lema 3.1 que o máximo divisor comum de a e b é dado por

$$(a, b) = (a - bq_1) = (r_1, b) = r_1.$$

- Se $r_2 \neq 0$, então $r_1 \nmid b$. Da mesma forma efetuamos a divisão euclidiana de r_1 por r_2, donde obtemos inteiros q_3 e r_3 tais que

$$r_1 = r_2 \cdot q_3 + r_3, \qquad 0 \leqslant r_3 < r_2 < r_1 < b.$$

Efetuamos este procedimento até que para algum n se tenha $r_n \mid r_{n-1}$. De fato, isso sempre ocorre, pois, caso contrário, teríamos uma sequência de números naturais $b > r_1 > r_2 > r_3 > \cdots$ limitada inferiormente e que não possui menor elemento. Isto contraria o Princípio da Boa Ordem.

Desta forma, temos

$$\begin{aligned}
a &= b \cdot q_1 + r_1, & 0 < r_1 < b \\
b &= r_1 \cdot q_2 + r_2, & 0 < r_2 < r_1 \\
r_1 &= r_2 \cdot q_3 + r_3, & 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1} \cdot q_n + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n \cdot q_{n+1} + 0.
\end{aligned}$$

Pelo Lema 3.1 (Lema de Euclides),temos

$$\begin{aligned}
(a, b) &= (b, a - b \cdot q_1) = (b, r_1) \\
&= (r_1, b - r_1 \cdot q_2) = (r_1, r_2) \\
&= (r_2, r_1 - r_2 \cdot q_3) = (r_2, r_3) \\
&\vdots \\
&= (r_{n-1}, r_{n-2} - r_{n-1} \cdot q_n) = (r_{n-1}, r_n) \\
&= (r_n \cdot q_{n+1}, r_n) \\
&= r_n
\end{aligned}$$

O algoritmo acima pode ser sintetizado e realizado na prática como mostramos a seguir.

Inicialmente, efetuamos a divisão $a = b \cdot q_1 + r_1$ e colocamos os números envolvidos no seguinte diagrama:

	q_1	
a	b	
r_1		

A seguir, continuamos efetuando a divisão $b = r_1 \cdot q_2 + r_2$ e colocamos os números envolvidos no diagrama

	q_1	q_2
a	b	r_1
r_1	r_2	

Prosseguindo com as divisões até que se obtenha um resto igual a zero, teremos

	q_1	q_2	q_3	$\ldots$	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	$\ldots$	r_{n-2}	r_{n-1}	$r_n = (a, b)$
r_1	r_2	r_3	r_4	$\ldots$	r_n	0	

O algorítimo acima, nos permite calcular o máximo divisor comum de números inteiros a e b. Contudo, uma propriedade muito útil do máximo divisor comum (a, b) é que existem os inteiros x_1 e x_2 tais que

$$(a, b) = ax_1 + bx_2.$$

Tão importante quanto conhecer o resultado, é saber como determinar os inteiros x_1 e x_2. Apresentamos a seguir, uma maneira de obtê-los.

Utilizando das finitas divisões euclidianas do algorítimo de euclides, verifica-se por meio de uma substituição recorrente dos restos que existem x_k e $y_k \in \mathbb{Z}$ tais que

$$(a, b) = r_n = x_k \cdot r_{n-k} + y_k \cdot r_{n-k-1}.$$

Em particular,

$$\begin{aligned}
(a, b) = r_n &= x_{n-2} \cdot r_2 + y_{n-2} \cdot r_1 \\
&= x_{n-2}(b - r_1 \cdot q_2) + y_{n-2} \cdot r_1 \\
&= r_1(y_{n-2} - x_{n-2} \cdot q_2) + x_{n-2} \cdot b \\
&= x_{n-1} \cdot r_1 + y_{n-1} \cdot b \\
&= x_{n-1}(a - b \cdot q_1) + y_{n-1} \cdot b \\
&= x_{n-1} \cdot a + (y_{n-1} - x_{n-1} \cdot q_1)b \\
&= x_1 a + x_2 b
\end{aligned}$$

onde $x_{n-1} = y_{n-2} - x_{n-2} \cdot q_2$, $\quad y_{n-1} = x_{n-2}$, $\quad x_1 = x_{n-1}$ $\quad$ e $\quad x_2 = y_{n-1} - x_{n-1} \cdot q_1$.

Exemplo 21. Encontre as soluções de $8x + 13y = 1$.

Temos que $(8, 13) = 1$. Então existem x e $y \in \mathbb{Z}$ tais que são as soluções da equação dada.

Para determinar os valores de x e y vamos inicialmente efetuar as divisões euclidianas do Algoritmo de Euclides de 13 por 8 até obtermos o resto nulo.

Note que,

$$\begin{aligned} 13 &= 8 \cdot 1 + 5, \quad 0 < 5 < 8 \\ 8 &= 5 \cdot 1 + 3, \quad 0 < 3 < 5 \\ 5 &= 3 \cdot 1 + 2, \quad 0 < 2 < 3 \\ 3 &= 2 \cdot 1 + 1, \quad 0 < 1 < 2 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Agora, isolamos o resto de cada equação obtida.

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ 2 &= 5 - 3 \cdot 1 \\ 3 &= 8 - 5 \cdot 1 \\ 5 &= 13 - 8 \cdot 1. \end{aligned}$$

Em seguida, fazemos sucessivas substituições partindo da equação cujo resto é o máximo divisor comum até que se obtenha a e b. Quando isso ocorrer, tem-se os valores procurados para x, $y \in \mathbb{Z}$.

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ &= 3 - (5 - 3 \cdot 1) \cdot 1 \\ &= 3 \cdot 2 - 5 \cdot 1 \\ &= (8 - 5 \cdot 1) \cdot 2 - 5 \cdot 1 \\ &= 8 \cdot 2 - 5 \cdot 3 \\ &= 8 \cdot 2 - (13 - 8 \cdot 1) \cdot 3 \\ &= 8 \cdot 5 + 13 \cdot (-3). \end{aligned}$$

Logo,

$$\begin{aligned} r_n &= (a, b) &&= ax + by \\ 1 &= (13, 8) &&= 8 \cdot x + 13 \cdot y \\ 1 &= (13, 8) &&= 8 \cdot 5 + 13 \cdot (-3). \end{aligned}$$

Portanto, $x = 5$ e $y = -3$ é solução da equação $8x + 13y = 1$.

4 Congruências Lineares

Neste capítulo, temos como objetivo encontrar as soluções de congruências do tipo $ax \equiv b \bmod m$ e de Sistemas de Congruências Lineares de uma ou duas variáveis. Além de apresentar um Teorema que possui muitas aplicações, o Teorema Chinês dos Restos.

Nesse sentido, uma congruência linear poderá ter uma solução, várias soluções ou até mesmo não ter nenhuma solução.

4.1 Resolução de Congruências Lineares com uma variável

Definição 4.1. Seja $m > 1$ um inteiro. Chamamos de congruência Linear a toda equação da forma:

$$ax \equiv b \bmod m$$

onde a, b e x são inteiros, onde x são as soluções procuradas. E dizemos que $k \in \mathbb{Z}$ é solução da equação acima caso $ak \equiv b \bmod m$.

A Proposição 4.1 traz uma caracterização da existência ou não de soluções das congruências lineares.

Proposição 4.1. *A congruência linear $ax \equiv b \bmod m$ possui solução se, e somente se, o máximo divisor comum de a e m divide b, ou seja,*

$$ax \equiv b \bmod m \Leftrightarrow (a, m) \mid b.$$

Demonstração. Veja HEFEZ (2013, p.246). □

Exemplo 22. A congruência linear $6x \equiv 4 \bmod 8$ tem solução, pois $(a, m) = (6, 8) = 2$ e $2 \mid 4$. Em particular, $k = 2$ é uma solução.

Exemplo 23. A congruência linear $4x \equiv 13 \bmod 20$ não tem solução, pois $(a, m) = (4, 20) = 4$ e $4 \nmid 13$.

Observação: Se x_0 é solução da congruência $ax \equiv b \bmod m$, então todo x tal que $x \equiv x_0 \bmod m$ é também solução da congruência pois, pela Proposição 3.1,

$$ax \equiv ax_0 \equiv c \bmod m.$$

Assim, podemos concluir que uma solução particular determina uma infinidade de soluções da congruência.

Definição 4.2. Um sistema completo de soluções da congruência

$$ax \equiv b \bmod m$$

é um conjunto S satizfazendo,

(i) Toda solução da equação é congruente a um elemento de S. E todo elemento de S é uma solução.

(ii) Os elementos de S são incongruentes entre si módulo m.

Teorema 4.1. *Sejam $a, b \in \mathbb{Z}$, com $m > 1$ e $(a, m) \mid b$. Se x_0 é uma solução da congruência $ax \equiv b \bmod m$, então*

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \cdots, x_0 + (d-1)\frac{m}{d},$$

onde $d = (a, m)$, formam um sistema completo de soluções da mesma congruência.

Demonstração. Veja HEFEZ (2013, p.247). □

Observação: Note que se o $(a, m) = d$ então nas condições do Teorema 4.1 a congruência $ax \equiv b \bmod m$ tem exatamente d soluções módulo m.

Exemplo 24. Verifique que a congruência linear $12x \equiv 36 \bmod 28$ tem solução e diga quantas são.

Solução: Temos que, $a = 12$, $b = 36$ e $m = 28$.

Como $d = (a, m) = (12, 28) = 4$ divide 36, temos que a congruência linear possui exatamente $d = 4$ soluções módulo 28.

Exemplo 25. Resolvamos a congruência linear $4x \equiv 12 \bmod 64$.

Note que, $a = 4$, $b = 12$ e $m = 64$.

Como $d = (a, m) = (4, 64) = 4$ divide 12, temos que a congruência linear possui exatamente $d = 4$ soluções módulo 64.

Por verificação, obtemos a solução $x_0 = 19$. Para exibir as demais soluções módulo 64, podemos utilizar o Teorema 4.1, obtendo

$$x_0 = 19, x_1 = 19 + 1\frac{64}{4}, x_2 = 19 + 2\frac{64}{4} \quad e \quad x_3 = 19 + 3\frac{64}{4}.$$

Portanto, as 4 soluções da congruência linear $4x \equiv 12 \bmod 64$ são: $x_0 = 19, x_1 = 35, x_2 = 51$ e $x_3 = 67$.

Corolário 4.1. *Se* $(a, m) = 1$*, então a congruência* $ax \equiv b \bmod m$ *possui uma única solução módulo* m*.*

A congruência $ax \equiv 1 \bmod m$, com $(a, m) = 1$, admite uma única solução módulo m. Esta solução é chamada de inverso multiplicativo de a módulo m.

Exemplo 26. Resolvamos a congruência linear $3x \equiv 7 \bmod 5$.

Solução: Note que, $a = 3$, $b = 7$ e $m = 5$.

Como $d = (a, m) = (3, 5) = 1$ divide 7, temos que a congruência linear possui exatamente $d = 1$ solução módulo $m = 5$.

Variando x entre 0 e 4 temos,

$$3 \cdot 0 \equiv 0 \bmod 5$$
$$3 \cdot 1 \equiv 3 \bmod 5$$
$$3 \cdot 2 \equiv 1 \bmod 5$$
$$3 \cdot 3 \equiv 4 \bmod 5$$
$$3 \cdot 4 \equiv 7 \bmod 5.$$

Logo, a única solução da congruência linear $3x \equiv 7 \bmod 5$ é $x_0 = 4$.

Observe que, o método de inspeção é viável quando o valor do módulo m é pequeno.

Corolário 4.2. *Toda congruência do tipo* $ax \equiv b \bmod m$ *que tem solução é equivalente a uma congruência do tipo*

$$x \equiv c \bmod n.$$

Demonstração. Perceba que se a congruência

$$ax \equiv b \bmod m,$$

admite solução, então o $d = (a, m) \mid b$. E, por definição, $d \mid a$ e $d \mid m$.

Tomando

$$a' = \frac{a}{d}, \quad b' = \frac{b}{d}, \quad n = \frac{m}{d},$$

temos pela Proposição 3.6 que a congruência acima é equivalente à

$$a'x \equiv b' \bmod n, \text{ com } (a', n) = 1.$$

Como $(a', n) = 1$, existe inverso multiplicativo a'' de a módulo n. Multiplicando a última congruência por a'' obtemos:

$$x \equiv c \bmod n,$$

onde $c = a''b'$. □

Exemplo 27. Na congruência $6x \equiv 10 \bmod 14$ temos que $d = (a, m) = (6, 14) = 2$ e divide 10. Assim, pela Definição 3.3, $2 \mid 6$ e $2 \mid 14$.

Dividindo a congruência $6x \equiv 10 \bmod 14$ por $d = 2$, temos pela Proposição 3.6 que a congruência acima é equivalente à

$$3x \equiv 5 \bmod 7, \text{ com } (3, 7) = 1.$$

Como $(3, 7) = 1$, existe inverso multiplicativo. Para encontrar esse número devemos resolver a congruência $3x \equiv 1 \bmod 7$. Perceba que, $3 \cdot 5 \equiv 1 \bmod 7 \Leftrightarrow x \equiv 25 \bmod 7$. Dessa forma, a congruência $6x \equiv 10 \bmod 14$ é equivalente à

$$x \equiv 4 \bmod 7,$$

onde $c = 5 \cdot 5$.

Diante da teoria apresentada até aqui podemos dar início ao estudo sobre Sistema de Congruências Lineares.

4.2 Sistema de Congruências Lineares com uma variável

De acordo com Eves (1995),

> o mais importante dos textos de Matemática chineses antigos é o K'ui-ch'ang Suanshu, ou Nove Capítulos sobre a Arte da Matemática, que data o período Han (206 a.C.,-221d.C.) mas que muito provavelmente contém material bem mais antigo. É uma síntese do conhecimento matemático chinês antigo. Em seus 9 capítulos, o de relevância para o presente trabalho encontra-se no capítulo 8 que fala sobre Sistema de equações Lineares, (EVES, 1995, p.242).

Definição 4.3. Chamamos de Sistema de Congruências Lineares a todo sistema da forma:

$$\begin{cases} a_1 x & \equiv & b_1 \bmod n_1 \\ a_2 x & \equiv & b_2 \bmod n_2 \\ \vdots & & \vdots \\ a_k x & \equiv & b_k \bmod n_k \end{cases} \tag{4.1}$$

onde $a_1, a_2, \cdots, a_k, b_1, b_2, \cdots, b_k, n_1, n_2, \cdots, n_k$ são inteiros fixados, com $n_i > 0$ para todo $i = 1, 2, 3, \cdots, k$.

Cada uma de suas congruências deve admitir solução. Logo, pelo Teorema 4.1, para que tal sistema admita solução, é necessário que $(a_i, n_i) \mid b_i$, para todo $i = 1, 2, 3, \cdots, k$.

De acordo, com a Proposição 4.2, o sistema acima é equivalente a um da forma

$$\begin{cases} x & \equiv & c_1 \bmod m_1 \\ x & \equiv & c_2 \bmod m_2 \\ \vdots & & \vdots \\ x & \equiv & c_k \bmod m_k \end{cases} \tag{4.2}$$

onde $c_1, c_2, \cdots, c_k, m_1, m_2, \cdots, m_k$ são inteiros fixados, com $m_i > 0$ para todo $i = 1, 2, \cdots, k$.

Desta forma, podemos concentrar nossos esforços em estudar sistemas do tipo (4.2). Uma das técnicas para encontrar a solução de um sistema, é uma ferramenta muito importante descoberta pelos chineses, ou seja, o Teorema Chinês do Resto. É possível aplicá-lo desde que as congruências lineares atendam suas condições específicas.

Segundo Eves (1995, p.244), após o período Han viveu o matemático Sun-Tzi (ou Sun Tsu Suan Ching), que escreveu um livro "Manual Aritmético do Mestre Sol" escrito provavelmente entre 280 d.C. e 483 d. C. O material assemelha-se muito aos "Nove Capítulos sobre a Arte da Matemática" dividido em 3 capítulos. Dentre eles, o capítulo 3 aborda problemas aritméticos, perfazendo um total de 36.

No Problema 26 (também conhecido como "problema do Mestre Sun"), encontra-se o primeiro problema chinês de análise indeterminada: "Um certo número desconhecido de coisas quando dividido por 3 deixa resto 2, por 5 resto 3 e por 7 resto 2. Qual é o (menor) número?" Aí encontramos a semente do famoso Teorema Chinês dos Restos da Teoria dos Números.

De acordo com BURTON (2016, p.78), definimos o Teorema Chinês dos Restos da seguinte forma:

Teorema 4.2. *(Teorema Chinês dos Restos) Sejam $m_1, m_2, \cdots, m_r$ inteiros positivos tais que $(m_i, m_j) = 1$ para $i \neq j$. Então o Sistema de Congruências Lineares*

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

possui uma solução simultânea, que é única módulo o inteiro $m = m_1 \cdot m_2 \cdot \cdots \cdot m_r$.

Demonstração. Começamos pela formação do produto $m = m_1 \cdot m_2 \cdot \cdots \cdot m_r$. Para $k = 1, 2, \cdots, r$ seja

$$M_k = \frac{m}{m_k} = m_1 \cdots m_{k-1} m_{k+1} \cdots m_r.$$

Em outras palavras, M_k é o produto de todos os inteiros m_i com o fator m_k omitido. Por hipótese, os m_i são em pares primos relativos, de modo que $(M_K, m_k) = 1$. De acordo

com a teoria de uma única congruência linear, por isso, é possível resolver a congruência $M_k y \equiv 1 \mod m_k$. Chame de y_k a solução única entre 0 e m_{k-1}. Nosso objetivo é provar que o inteiro

$$x = M_1 \cdot y_1 \cdot c_1 + M_2 \cdot y_2 \cdot c_2 + \cdots + M_r \cdot y_r \cdot c_r.$$

é uma solução simultânea do sistema dado.

Primeiro observe que $M_i \equiv 0 \bmod m_k$ para $i \neq k$, pois, neste caso, $m_k \mid M_i$. O resultado é

$$x = M_1 \cdot y_1 \cdot c_1 + M_2 \cdot y_2 \cdot c_2 + \cdots + M_r \cdot y_r \cdot c_r \equiv M_k \cdot y_k \cdot c_k \bmod m_k.$$

Mas o inteiro y_k foi escolhido para satisfazer a congruência $M_k \cdot y \equiv 1 \bmod m_k$, o que força

$$x = c_k \cdot 1 \equiv c_k \bmod m_k.$$

Isto mostra que a solução para o sistema de congruências dado existe.

Quanto à unicidade, suponha que x' seja qualquer outro número inteiro que satisfaz estas congruências. Então,

$$x \equiv c_k \equiv x' \bmod m_k, \qquad k = 1, 2, \cdots, r$$

e logo $m_k \mid x - x'$ para cada valor de k. Como $(m_i, m_j) = 1$, o Corolário 2 do Teorema 2.4 que se encontra no livro BURTON (2016, p.22) diz que: Se $a \mid c$ e $b \mid c$, com $(a, b) = 1$, então $ab \mid c$, nos fornece o ponto crucial que $m_1.m_2.\cdots.m_r \mid x - x'$. Daí, $x \equiv x' \bmod m$. Com isso, o Teorema Chinês dos Restos está provado. □

Apesar do Teorema Chinês dos Restos ser uma ferramenta de resolução de Sistemas de Congruências Lineares prática e de fácil compreensão não é possível aplicá-lo em todos os Sistemas.

Veremos agora, uma proposição, que permite identificar se o Sistemas de Congruências Lineares admite solução ou não. Além de, descrever os passos para encontrá-la caso tenha.

Proposição 4.2. *O sistema de congruências*

$$\begin{cases} x & \equiv & c_1 \bmod m_1 \\ x & \equiv & c_2 \bmod m_2 \end{cases} \tag{4.3}$$

admite solução se, e somente se, $c_2 \equiv c_1 \bmod (m_1, m_2)$. *Além disso, dada uma solução* a *do sistema, um número* a' *é também uma solução se, e somente se,* $a' \equiv a \bmod [m_1, m_2]$.

Demonstração. O sistema (4.3) admite uma solução se, e somente se, existem $a, y, z \in \mathbb{Z}$ tais que $a - c_1 = ym_1$ e $a - c_2 = zm_2$. Assim, a existência de soluções do sistema é

equivalente à existência de soluções da equação Diofantina $ym_1 - zm_2 = c_2 - c_1$. Por sua vez, essa equação diofantina possui solução se, e somente se, (m_1, m_2) divide $c_2 - c_1$, o que equivale à $c_2 \equiv c_1 \bmod (m_1, m_2)$.

Suponhamos que a seja uma solução do sistema (4.3). Se a' é uma outra solução do sistema, então $a' \equiv c_1 \equiv a \bmod m_1$ e $a' \equiv c_2 \equiv a \bmod m_2$, o que, em vista da Proposição 3.9 item (b), implica que $a' \equiv a \bmod [m_1, m_2]$.

Por outro lado, se um número a' é tal que $a' \equiv a \bmod [m_1, m_2]$, então $a' \equiv a \equiv c_1 \bmod m_1$ e $a' \equiv a \equiv c_2 \bmod m_2$. Portanto, a' é solução do sistema (4.3). □

Daremos a seguir um algoritmo para determinar as soluções de um sistema da forma,

$$\begin{cases} x & \equiv & c_1 \bmod m_1 \\ x & \equiv & c_2 \bmod m_2 \end{cases}.$$

Sabemos, pelo *Algoritmo de Euclides Estendido*, que se $d = (a, b)$ então, existem números inteiros m e n tais que $ma + nb = d$. Como

$$\left(\frac{m_2}{(m_1, m_2)}, \frac{m_1}{(m_1, m_2)}\right) = 1,$$

segue que existem inteiros x_1 e $x_2 \in \mathbb{Z}$ tais que,

$$x_1 \frac{m_2}{(m_1, m_2)} + x_2 \frac{m_1}{(m_1, m_2)} = 1. \tag{4.4}$$

Mostraremos, a seguir, que

$$x = c_1 x_1 \frac{m_2}{(m_1, m_2)} + c_2 x_2 \frac{m_1}{(m_1, m_2)}. \tag{4.5}$$

é uma solução do sistema (4.3).

De (4.4) temos que,

$$\begin{aligned} x_1 \frac{m_2}{(m_1, m_2)} = 1 - x_2 \frac{m_1}{(m_1, m_2)} \quad &\Rightarrow \quad \frac{m_2}{(m_1, m_2)} \mid 1 - x_2 \frac{m_1}{(m_1, m_2)} \\ &\Rightarrow \quad x_2 \frac{m_1}{(m_1, m_2)} \equiv 1 \bmod \frac{m_2}{(m_1, m_2)}. \end{aligned}$$

Como

$$c_1 x_1 \frac{m_2}{(m_1, m_2)} \equiv 0 \bmod \frac{m_2}{(m_1, m_2)},$$

temos que

$$x \equiv c_2 x_2 \frac{m_1}{(m_1, m_2)} \bmod \frac{m_2}{(m_1, m_2)} \quad \Rightarrow \quad x \equiv c_2 \bmod \frac{m_2}{(m_1, m_2)}.$$

Analogamente, temos que

$$x \equiv c_1 \bmod \frac{m_1}{(m_1, m_2)}.$$

Como $\frac{m_i}{(m_1, m_2)}$ divide m_i, $i = 1, 2$, segue do item **a)** da Proposição 3.9 que

$$x \equiv c_1 \bmod m_1 \quad \text{e} \quad x \equiv c_2 \bmod m_2.$$

Ou seja, x é solução do sistema (4.3).

A Proposição 4.2 pode ser estendida para sistemas com n equações, onde $n > 2$. Este resultado é dado pelo Teorema 4.3 a seguir.

Teorema 4.3. *(Teorema Chinês dos Restos Generalizado) O sistema de congruências*

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

onde $i = 1, 2, \cdots, r$, *admite solução se, e somente se,* $c_i \equiv c_j \bmod (m_i, m_j), \forall i, j = 1, 2, \cdots, r$. *Neste caso, a solução é única módulo* $[m_1, \cdots, m_r]$.

Demonstração. Veja HEFEZ (2013, p.259). □

Vejamos o exemplo a seguir.

Exemplo 28. Resolvamos o sistema:

$$\begin{cases} x & \equiv & 2 \bmod 3 \\ x & \equiv & 3 \bmod 4 \\ x & \equiv & 4 \bmod 5 \\ x & \equiv & 2 \bmod 6. \end{cases}$$

Solução: Primeiro devemos verificar se o sistema de congruências admite solução, ou seja, se $c_i \equiv c_j \bmod (m_i, m_j), \forall i, j = 1, 2, \cdots, r$. Observe que, para a segunda e quarta equação do sistema, temos que $d = (4, 6) = 2$ e $3 \not\equiv 2 \bmod (4, 6)$, pois $d = 2 \nmid (3 - 2)$.

Portanto, o sistema não admite solução.

Veja no Capítulo 5 exemplos de soluções de Sistemas Lineares de Congruência.

Estudamos até aqui Congruência Lineares com uma varíavel, agora estudaremos Congruências Lineares com duas variáveis.

4.3 Resolução de Congruências Lineares com duas variáveis

Definição 4.4. Seja $m > 1$ um inteiro. Chamamos de congruência Linear com duas variáveis a toda equação da forma:

$$ax + by \equiv c \bmod m$$

onde a, b e c, são constantes inteiras e x, y são números inteiros procurados.

Definição 4.5. Uma solução da congruência $ax + by \equiv c \bmod m$ é um par $\begin{pmatrix} x \\ y \end{pmatrix}$ que satisfaz a equação.

Vamos, inicialmente, dar um critério para determinar se tais congruências admitem solução.

Proposição 4.3. *(Critério para existência de solução): A congruência linear $ax + by \equiv c \bmod m$, análogo ao Teorema 4.1, possui solução se, e somente se, o máximo divisor comum de a, b e m divide c, ou seja,*

$$ax + by \equiv c \bmod m \Leftrightarrow (a, b, m) \mid c.$$

Demonstração. Segue os mesmos passos da demonstração da Proposição 4.1. □

Pela Proposição 4.3 temos que se $(a, b, m) \nmid c$ então $ax + by \equiv c \bmod m$ não admite solução. Desta forma, no que segue, vamos considerar que $(a, b, m) \mid c$, ou seja, $ax + by \equiv c \bmod m$ admite pelo menos uma solução.

Uma pergunta que surge neste momento é: Quantas soluções tem a congruência $ax + by \equiv c \bmod m$?

Para facilitar a compreensão vamos analisar as situações a seguir

- **Caso 1:** $(a, m) = 1$.

  Suponha que $(a, m) = 1$. Escrevemos a congruência da forma,

  $$ax \equiv c - by \bmod m.$$

  O Corolário 4.1 garante uma única solução x para valor de y entre 0 e $m - 1$.

Mais especificamente, um número inteiro y é congruente módulo m a um único número do conjunto $S = \{0, 1, \cdots, m - 1\}$. Ou seja, que a menos de congruência, podemos considerar que y assume apenas os números de 0 a $m - 1$. Desta forma, a congruência $ax \equiv c - by \bmod m$ tem única solução módulo m para cada y entre 0 e $m - 1$. Portanto $ax + by \equiv c \bmod m$ admite exatamente m soluções.

- **Caso 2:** $(b, m) = 1$.

De modo análogo ao caso anterior, para cada x entre 0 e $m - 1$ existe uma única solução módulo m de $by \equiv c - ax \bmod m$.Portanto, $ax + by \equiv c \bmod m$ admite, também, exatamente m soluções.

- **Caso 3:** Caso Geral

Da congruência $ax + by \equiv c \bmod m$ temos que $ax \equiv c - by \bmod m$ ou $by \equiv c - ax \bmod m$. Consideremos primeiramente, que $ax \equiv c - by \bmod m$. Neste caso, a congruência admite solução se, e somente se, $d_1 \mid c - by$, onde $d_1 = (a, m)$.

Seja Q o conjunto dos y entre 0 e $m - 1$ tais que $d_1 \mid c - by$. Pelo Teorema 4.1, para cada $y \in Q$, existem exatamente d_1 soluções módulo m de $ax \equiv c - by \bmod m$, as quais podem ser obtidas a partir de uma solução particular x_0 da seguinte forma:

$$x_i = x_0 + i\frac{m}{d_1}, \quad i = 0, 1, \cdots, d_1 - 1.$$

Assim, as soluções de $ax + by \equiv c \bmod m$ são $\begin{pmatrix} x_i \\ y \end{pmatrix}, i = 0, 1, \cdots, d_1 - 1, y = 0, 1, \cdots, m - 1$.

Em particular, temos $|Q| \cdot d_1$ soluções módulo m da congruência, onde $|Q|$ é a quantidade de elemento de Q.

Consideremos agora, a congruência $by \equiv c - ax \bmod m$, qual admite solução se, e somente se, $d_2 \mid c - ax$, onde $d_2 = (b, m)$. De maneira análoga, seja P o conjunto dos x entre 0 e $m - 1$ tais que $d_2 \mid c - ax$. Pelo Teorema 4.1, para cada $x \in P$, existem d_2 soluções módulo m de $by \equiv c - ax \bmod m$ que podem ser escritas a partir de uma solução particular y_0:

$$y_i = y_0 + i\frac{m}{d_2}, \quad i = 0, 1, \cdots, d_2 - 1.$$

Assim, as soluções de $ax + by \equiv c \bmod m$ são $\begin{pmatrix} x \\ y_i \end{pmatrix}, i = 0, 1, \cdots, d_2 - 1, x = 0, 1, \cdots, m - 1$.

Em particular, temos $|P| \cdot d_2$ soluções módulo m da congruência, onde $|P|$ é a quantidade de elemento de P.

É importortante observar aqui que $|Q| \cdot d_1 = |P| \cdot d_2$.

Vejamos alguns exemplos.

Exemplo 29. Vamos resolver a congruência linear $7x + 4y \equiv 5 \bmod 12$.

Solução: Como $d = (7, 4, 12) = 1$ divide $c = 5$, temos que a congruência admite solução. Agora, vamos variar o valor de y entre 0 e 11 para encontrar os valores de x para os quais

$\begin{pmatrix} x \\ y \end{pmatrix}$ é solução da congruência: $7x \equiv 5 - 4y \bmod 12$,

$$
\begin{array}{llllll}
\text{para} & y = 0, & 7x \equiv 5 - 4 \cdot 0 \bmod 12 & \Leftrightarrow & 7x \equiv 5 \bmod 12 & \Leftrightarrow \quad x \equiv 11 \bmod 12 \\
\text{para} & y = 1, & 7x \equiv 5 - 4 \cdot 1 \bmod 12 & \Leftrightarrow & 7x \equiv 1 \bmod 12 & \Leftrightarrow \quad x \equiv 7 \bmod 12 \\
\text{para} & y = 2, & 7x \equiv 5 - 4 \cdot 2 \bmod 12 & \Leftrightarrow & 7x \equiv 9 \bmod 12 & \Leftrightarrow \quad x \equiv 3 \bmod 12 \\
\text{para} & y = 3, & 7x \equiv 5 - 4 \cdot 3 \bmod 12 & \Leftrightarrow & 7x \equiv 5 \bmod 12 & \Leftrightarrow \quad x \equiv 11 \bmod 12 \\
\text{para} & y = 4, & 7x \equiv 5 - 4 \cdot 4 \bmod 12 & \Leftrightarrow & 7x \equiv 1 \bmod 12 & \Leftrightarrow \quad x \equiv 7 \bmod 12 \\
\text{para} & y = 5, & 7x \equiv 5 - 4 \cdot 5 \bmod 12 & \Leftrightarrow & 7x \equiv 9 \bmod 12 & \Leftrightarrow \quad x \equiv 3 \bmod 12 \\
\text{para} & y = 6, & 7x \equiv 5 - 4 \cdot 6 \bmod 12 & \Leftrightarrow & 7x \equiv 5 \bmod 12 & \Leftrightarrow \quad x \equiv 11 \bmod 12 \\
\text{para} & y = 7, & 7x \equiv 5 - 4 \cdot 7 \bmod 12 & \Leftrightarrow & 7x \equiv 1 \bmod 12 & \Leftrightarrow \quad x \equiv 7 \bmod 12 \\
\text{para} & y = 8, & 7x \equiv 5 - 4 \cdot 8 \bmod 12 & \Leftrightarrow & 7x \equiv 9 \bmod 12 & \Leftrightarrow \quad x \equiv 3 \bmod 12 \\
\text{para} & y = 9, & 7x \equiv 5 - 4 \cdot 9 \bmod 12 & \Leftrightarrow & 7x \equiv 5 \bmod 12 & \Leftrightarrow \quad x \equiv 11 \bmod 12 \\
\text{para} & y = 10, & 7x \equiv 5 - 4 \cdot 10 \bmod 12 & \Leftrightarrow & 7x \equiv 1 \bmod 12 & \Leftrightarrow \quad x \equiv 7 \bmod 12 \\
\text{para} & y = 11, & 7x \equiv 5 - 4 \cdot 11 \bmod 12 & \Leftrightarrow & 7x \equiv 9 \bmod 12 & \Leftrightarrow \quad x \equiv 3 \bmod 12.
\end{array}
$$

Logo, para cada y de 0 a 11 temos uma única solução módulo 12 para a congruência $7x \equiv 5 - 4y \bmod 12$. Portanto, temos 12 soluções do problema inicial.

Exemplo 30. Resolvamos a congruência linear $3x + 4y \equiv 5 \bmod 8$.

Solução: Como $d = (3, 4, 8) = 1$ divide $c = 5$, temos que a congruência admite solução.

Para cada valor de y entre 0 e 7 fixo temos uma congruência da forma $ax \equiv c \bmod m$ onde $c = 5 - 4y$ e $a = 3$. Como $(3, 8) = 1$ temos pelo Corolário 4.1 que $3x \equiv 5 - 4y \bmod 8$ tem uma única solução para cada y fixado:

$$
\begin{array}{llllll}
\text{para} & y = 0, & 3x \equiv 5 - 4 \cdot 0 \bmod 8 & \Leftrightarrow & 3x \equiv 5 \bmod 8 & \Leftrightarrow \quad x \equiv 7 \bmod 8 \\
\text{para} & y = 1, & 3x \equiv 5 - 4 \cdot 1 \bmod 8 & \Leftrightarrow & 3x \equiv 1 \bmod 8 & \Leftrightarrow \quad x \equiv 3 \bmod 8 \\
\text{para} & y = 2, & 3x \equiv 5 - 4 \cdot 2 \bmod 8 & \Leftrightarrow & 3x \equiv 5 \bmod 8 & \Leftrightarrow \quad x \equiv 7 \bmod 8 \\
\text{para} & y = 3, & 3x \equiv 5 - 4 \cdot 3 \bmod 8 & \Leftrightarrow & 3x \equiv 1 \bmod 8 & \Leftrightarrow \quad x \equiv 3 \bmod 8 \\
\text{para} & y = 4, & 3x \equiv 5 - 4 \cdot 4 \bmod 8 & \Leftrightarrow & 3x \equiv 5 \bmod 8 & \Leftrightarrow \quad x \equiv 7 \bmod 8 \\
\text{para} & y = 5, & 3x \equiv 5 - 4 \cdot 5 \bmod 8 & \Leftrightarrow & 3x \equiv 1 \bmod 8 & \Leftrightarrow \quad x \equiv 3 \bmod 8 \\
\text{para} & y = 6, & 3x \equiv 5 - 4 \cdot 6 \bmod 8 & \Leftrightarrow & 3x \equiv 5 \bmod 8 & \Leftrightarrow \quad x \equiv 7 \bmod 8 \\
\text{para} & y = 7, & 3x \equiv 5 - 4 \cdot 7 \bmod 8 & \Leftrightarrow & 3x \equiv 1 \bmod 8 & \Leftrightarrow \quad x \equiv 3 \bmod 8.
\end{array}
$$

Como esperado, temos 8 soluções módulo 8 do problema inicial.

No exemplo a seguir, tivemos o cuidado de escolher uma congruência que apresentasse o valor de $d \neq d_1 \neq d_2$.

Exemplo 31. Vamos determinar a quantidade de soluções da congruência linear $2x+5y \equiv 3 \bmod 10$.

Solução: Como $d = (2, 5, 10) = 1$ divide $c = 3$, temos que a congruência admite solução.

Como $(a, m) = (2, 10) = 2 = d_1$ neste caso, $d_1 \neq 1$. Escrevemos a congruência da forma: $2x \equiv 3 - 5y \bmod 10$.

Vamos procurar os valores de $y \in \{0, 1, \cdots, 10\} = S$ tais que $d_1 = 2 \mid 3 - 5y \Rightarrow y \in Q = \{1, 3, 5, 7, 9\}$.

Para cada $y \in Q$ de acordo com o Teorema 4.1 temos 2 soluções módulo 10 para a congruência $2x \equiv 3 - 5y \bmod 10$. Logo, temos que a congruência $2x + 5y \equiv 3 \bmod 10$ tem $d_1 \cdot |Q| = 2 \cdot 5 = 10$ soluções módulo 10.

Observe que, o número de soluções da congruência independe de qual incógnita x ou y vamos isolar. Ou seja, se vamos reescrever a congruência da forma $2x \equiv 3-5y \bmod 10$ ou da forma $5y \equiv 3 - 2x \bmod 10$.

De fato, reescrevendo a congruência da forma: $5y \equiv 3 - 2x \bmod 10$, onde $(b, m) = (5, 10) = 5 = d_2$ neste caso, $d_2 \neq 1$. Neste caso, vamos procurar os valores de x entre 0 e 10 tais que $d_2 = 5 \mid 3 - 2x$, Ou seja, $x \in P = \{4, 9\}$.

Isso siginifica que, para cada $x \in P$ de acordo com o Teorema 4.1 temos 5 soluções módulo 10 para a congruência $5y + 2x \equiv 3 \bmod 10$. Logo, esta congruência tem $d_2 \cdot |P| = 5 \cdot 2 = 10$ soluções módulo 10.

Vejamos o exemplo a seguir, em que o valor de $d = d_1 \neq d_2$.

Exemplo 32. Vamos resolver a congruência linear $2x + 4y \equiv 6 \bmod 8$.

Solução: Como $d = (2, 4, 8) = 2$ divide $c = 6$, temos que a congruência admite solução.

Como $(a, m) = (2, 8) = 2 = d_1$ neste caso, $d_1 \neq 1$.

Reescreva a congruência na forma: $4y \equiv 6-2x \bmod 8$, onde $(b, m) = (4, 8) = 4 = d_2$ neste caso, $d_2 \neq 1$.

Assim, vamos procurar os valores de x entre 0 e 7 tais que $d_2 = 4 \mid 6-2x$. Obtemos que $x \in P = \{1, 3, 5, 7\}$.

Isso siginifica que, para cada $x \in P$ de acordo com o Teorema 4.1 temos $4 = (4, 8) = d_2$ soluções módulo 8 para a congruência $4y \equiv 6 - 2x \bmod 8$. Logo, temos que a congruência $4y \equiv 6 - 2x \bmod 8$ tem $d_2 \cdot |P| = 4 \cdot 4 = 16$ soluções módulo 8.

Vamos exibi-las.

- Para $x = 1$.

Temos que, $4y \equiv 6 - 2 \cdot 1 \bmod 8$, ou seja, $4y \equiv 4 \bmod 8$. Verifica-se, por inspeção direta, que $y_0 = 3$ é uma solução.

Pelo Teorema 4.1, $y_0 = 3$, $y_1 = 3 + 1\frac{8}{4} = 5$, $\quad y_2 = 3 + 2\frac{8}{4} = 7$, $\quad y_3 = 3 + 3\frac{8}{4} \equiv 1 \bmod 8$, são as únicas soluções módulo 8 da congruência $4y \equiv 4 \bmod 8$.

Portanto, quando $x = 1$ temos $y_0 = 3$, $y_1 = 5$, $y_2 = 7$, e $y_3 = 1$.

- Para $x = 3$.

Temos que, $4y \equiv 6 - 2 \cdot 3 \bmod 8$, ou seja, $4y \equiv 0 \bmod 8$. Verifica-se, por inspeção direta, que $y_0 = 2$ é uma solução.

Pelo Teorema 4.1, $y_1 = 2 + 1\frac{8}{4} = 4$, $\quad y_2 = 2 + 2\frac{8}{4} = 6$, $\quad y_3 = 2 + 3\frac{8}{4} \equiv 0 \bmod 8$, são as únicas soluções módulo 8 da congruência $4y \equiv 0 \bmod 8$.

Portanto, quando $x = 3$ temos $y_0 = 2$, $y_1 = 4$, $y_2 = 6$, e $y_3 = 0$.

- Para $x = 5$.

Temos que, $4y \equiv 6 - 2 \cdot 5 \bmod 8$, ou seja, $4y \equiv 4 \bmod 8$. Verifica-se, por inspeção direta, que $y_0 = 3$ é uma solução.

Pelo Teorema 4.1, $y_1 = 3 + 1\frac{8}{4}$, $\quad y_2 = 3 + 2\frac{8}{4}$, $\quad y_3 = 3 + 3\frac{8}{4}$, são as únicas soluções módulo 8 da congruência $4y \equiv 4 \bmod 8$.

Portanto, quando $x = 5$ temos $y_0 = 3$, $y_1 = 5$, $y_2 = 7$, e $y_3 = 1$.

- Para $x = 7$.

Temos que, $4y \equiv 6 - 2 \cdot 7 \bmod 8$, ou seja, $4y \equiv 0 \bmod 8$. Verifica-se, por inspeção direta, que $y_0 = 2$ é uma solução.

Pelo Teorema 4.1, $y_1 = 2 + 1\frac{8}{4}$, $\quad y_2 = 2 + 2\frac{8}{4}$, $\quad y_3 = 2 + 3\frac{8}{4}$, são as únicas soluções módulo 8 da congruência $4y \equiv 0 \bmod 8$.

Portanto, quando $x = 7$ temos $y_0 = 2$, $y_1 = 4$, $y_2 = 6$, e $y_3 = 0$.

Logo, as únicas soluções módulo 8 da congruência $2x + 4y \equiv 6 \bmod 8$ são:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 5 \end{pmatrix}, \begin{pmatrix} 1 \\ 7 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 3 \\ 6 \end{pmatrix}, \begin{pmatrix} 5 \\ 1 \end{pmatrix}, \begin{pmatrix} 5 \\ 3 \end{pmatrix},$$
$$\begin{pmatrix} 5 \\ 5 \end{pmatrix}, \begin{pmatrix} 5 \\ 7 \end{pmatrix}, \begin{pmatrix} 7 \\ 0 \end{pmatrix}, \begin{pmatrix} 7 \\ 2 \end{pmatrix}, \begin{pmatrix} 7 \\ 4 \end{pmatrix}, \begin{pmatrix} 7 \\ 6 \end{pmatrix}.$$

O próximo exemplo tem commo objetivo verificar se as soluções são as mesmas para a congruência $2x + 4y \equiv 6 \bmod 8$, do exemplo 32, ao escolhermos isolar a incógnita x ao invéz da incógnita y.

Exemplo 33. Neste exemplo vamos exibir as 16 soluções do exemplo anterior para o caso em que $(a, m) = (2, 8) = 2 = d_1$ neste caso, $d_1 \neq 1$, reescrevemos a congruência da forma: $2x \equiv 6 - 4y \bmod 8$.

Dessa forma, ao isolarmos a variável x devemos procurar os valores de y entre 0 e 7 tais que $d_1 = 2 \mid 6 - 4y$. Perceba que $2 \mid 2 \cdot (3 - 2y)$ para todo y. Logo, $Q = \{0, 1, \cdots, 7\}$.

Para cada $y \in Q$ de acordo com o Teorema 4.1 temos $2 = (2, 8)$ soluções módulo 8 para a congruência $2x \equiv 6 - 4y \bmod 8$. Logo, temos que a congruência $2x \equiv 6 - 4y \bmod 8$ tem $d_1 \cdot |Q| = 2 \cdot 8 = 16$ soluções módulo 8.

Vamos exibi-las.

- Para $y = 0$.

Temos que, $2x \equiv 6 - 4 \cdot 0 \bmod 8$, ou seja, $2x \equiv 6 \bmod 8$. Verifica-se, por inspeção direta, que $x_0 = 7$ é uma solução.

Pelo Teorema 4.1, $x_0 = 7, \quad x_1 = 7 + 1\frac{8}{2} \equiv 3 \bmod 8$, são as únicas soluções módulo 8 da congruência $2x \equiv 6 \bmod 8$.

Portanto, quando $y = 0$ temos $x_0 = 7$ e $x_1 = 3$.

- Para $y = 1$.

Temos que, $2x \equiv 6 - 4 \cdot 1 \bmod 8$, ou seja, $2x \equiv 2 \bmod 8$. Verifica-se, por inspeção direta, que $x_0 = 1$ é uma solução.

Pelo Teorema 4.1, $x_0 = 1, \quad x_1 = 1 + 1\frac{8}{2} \equiv 5 \bmod 8$, são as únicas soluções módulo 8 da congruência $2x \equiv 2 \bmod 8$.

Portanto, quando $y = 1$ temos $x_0 = 1$ e $x_1 = 5$.

- Para $y = 2$.

Temos que, $2x \equiv 6 - 4 \cdot 2 \bmod 8$, ou seja, $2x \equiv 6 \bmod 8$. Verifica-se, por inspeção direta, que $x_0 = 7$ é uma solução.

Pelo Teorema 4.1, $x_0 = 7, \quad x_1 = 7 + 1\frac{8}{2} \equiv 3 \bmod 8$, são as únicas soluções módulo 8 da congruência $2x \equiv 6 \bmod 8$.

Portanto, quando $y = 2$ temos $x_0 = 7$ e $x_1 = 3$.

- Para $y = 3$.

Temos que, $2x \equiv 6 - 4 \cdot 3 \bmod 8$, ou seja, $2x \equiv 2 \bmod 8$. Verifica-se, por inspeção direta, que $x_0 = 1$ é uma solução.

Pelo Teorema 4.1, $x_0 = 1, \quad x_1 = 1 + 1\frac{8}{2} \equiv 5 \bmod 8$, são as únicas soluções módulo 8 da congruência $2x \equiv 2 \bmod 8$.

Portanto, quando $y = 3$ temos $x_0 = 1$ e $x_1 = 5$.

- Para $y = 4$.

Temos que, $2x \equiv 6 - 4 \cdot 4 \bmod 8$, ou seja, $2x \equiv 6 \bmod 8$. Verifica-se, por inspeção direta, que $x_0 = 7$ é uma solução.

Pelo Teorema 4.1, $x_0 = 7, \quad x_1 = 7 + 1\frac{8}{2} \equiv 3 \bmod 8$, são as únicas soluções módulo 8 da congruência $2x \equiv 6 \bmod 8$.

Portanto, quando $y = 4$ temos $x_0 = 7$ e $x_1 = 3$.

- Para $y = 5$.

Temos que, $2x \equiv 6 - 4 \cdot 5 \bmod 8$, ou seja, $2x \equiv 2 \bmod 8$. Verifica-se, por inspeção direta, que $x_0 = 1$ é uma solução.

Pelo Teorema 4.1, $x_0 = 1, \quad x_1 = 1 + 1\frac{8}{2} \equiv 5 \bmod 8$, são as únicas soluções módulo 8 da congruência $2x \equiv 2 \bmod 8$.

Portanto, quando $y = 5$ temos $x_0 = 1$ e $x_1 = 5$.

- Para $y = 6$.

Temos que, $2x \equiv 6 - 4 \cdot 6 \bmod 8$, ou seja, $2x \equiv 6 \bmod 8$. Verifica-se, por inspeção direta, que $x_0 = 7$ é uma solução.

Pelo Teorema 4.1, $x_0 = 7, \quad x_1 = 7 + 1\frac{8}{2} \equiv 3 \bmod 8$, são as únicas soluções módulo 8 da congruência $2x \equiv 6 \bmod 8$.

Portanto, quando $y = 6$ temos $x_0 = 7$ e $x_1 = 3$.

- Para $y = 7$.

Temos que, $2x \equiv 6 - 4 \cdot 7 \bmod 8$, ou seja, $2x \equiv 2 \bmod 8$. Verifica-se, por inspeção direta, que $x_0 = 1$ é uma solução.

Pelo Teorema 4.1, $x_0 = 1, \quad x_1 = 1 + 1\frac{8}{2} \equiv 5 \bmod 8$, são as únicas soluções módulo 8 da congruência $2x \equiv 2 \bmod 8$.

Portanto, quando $y = 7$ temos $x_0 = 1$ e $x_1 = 5$.

Logo, as únicas soluções módulo 8 da congruência $2x + 4y \equiv 6 \bmod 8$ são:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 5 \end{pmatrix}, \begin{pmatrix} 1 \\ 7 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 3 \\ 6 \end{pmatrix}, \begin{pmatrix} 5 \\ 1 \end{pmatrix}, \begin{pmatrix} 5 \\ 3 \end{pmatrix},$$
$$\begin{pmatrix} 5 \\ 5 \end{pmatrix}, \begin{pmatrix} 5 \\ 7 \end{pmatrix}, \begin{pmatrix} 7 \\ 0 \end{pmatrix}, \begin{pmatrix} 7 \\ 2 \end{pmatrix}, \begin{pmatrix} 7 \\ 4 \end{pmatrix}, \begin{pmatrix} 7 \\ 6 \end{pmatrix}.$$

Assim fica claro que, o número de soluções da congruência independe de qual incógnita x ou y vamos isolar. Ou seja, se vamos reescrever a congruência da forma $2x \equiv 6 - 4y \bmod 8$ ou da forma $4y \equiv 6 - 2x \bmod 8$. Além disso, percebemos que o fato de $d = d_1 = d_2$, $d = d_1 \neq d_2$ ou $d \neq d_1 \neq d_2$ não altera a quantidade de soluções da congruência.

O próximo teorema apresenta uma condição para unicidade da solução.

4.4 Sistema de Congruências Lineares com duas variáveis

Teorema 4.4. *O Sistema de Congruências Lineares*

$$\begin{cases} ax + by \equiv r \bmod m \\ cx + dy \equiv s \bmod m \end{cases}$$

tem uma solução única módulo m sempre que $(ad - bc, m) = 1$.

Demonstração. Vamos multiplicar a congruência $ax+by \equiv r \bmod m$ por d, e a congruência $cx + dy \equiv s \bmod m$ por b.

$$\begin{cases} dax + dby \equiv dr \bmod m \\ bcx + bdy \equiv bs \bmod m \end{cases}$$

Ao subtrair as equações, obtemos

$$(ad - bc)x \equiv dr - bs \bmod m. \tag{4.6}$$

O pressuposto de que $(ad - bc, m) = 1$ garante que a congruência

$$(ad - bc)z \equiv 1 \bmod m$$

possua uma solução única, denote a solução por t. Quando a congruência (4.6) é multiplicada por t, obtemos

$$x \equiv (dr - bs)t \bmod m.$$

Um valor para y é encontrado com um processo de eliminação. Ou seja, multiplicar a congruência $ax + by \equiv r \bmod m$ por c, e a congruência $cx + dy \equiv s \bmod m$ por a.

$$\begin{cases} cax + cby \equiv cr \bmod m \\ acx + ady \equiv as \bmod m \end{cases}$$

Ao subtrair as equações, obtemos

$$(ad - bc)y \equiv as - cr \bmod m.$$

A multiplicação desta congruência por um certo s conduz a

$$y \equiv (as - cr)s \bmod m.$$

A solução do sistema está agora estabelecida e é única módulo m, pois t e s são únicos módulo m. □

Essa demonstração é importante porque nos dá a técnica de como resolver Sistema de Congruências Lineares com duas variáveis.

Exemplo 34. (Extraído do Livro do BURTON) Encontre as soluções do sistema de congruências

$$\begin{cases} 5x + 3y \equiv 1 \bmod 7 \\ 3x + 2y \equiv 4 \bmod 7. \end{cases}$$

Solução: Como $(5 \cdot 2 - 3 \cdot 3, 7) = (1, 7) = 1$, o sistema admite solução e é única módulo 7.

Multiplicando a primeira congruência pelo valor de $d = 2$, a segunda por $b = 3$, e subtrair a segunda congruência da primeira, obtemos

$$(5 \cdot 2 - 3 \cdot 3) \cdot x \equiv 2 \cdot 1 - 4 \cdot 3 \bmod 7 \Leftrightarrow x \equiv -10 \bmod 7.$$

Ao resolver a equação $x \equiv -10 \bmod 7$,

$$x \equiv (-10) + 7 \bmod 7 \Leftrightarrow x \equiv (-3) + 7 \bmod 7 \Leftrightarrow x \equiv 4 \bmod 7, \text{temos} \quad x = 7.$$

De maneira análoga, para deternimar o valor para y devemos multiplicar a primeira congruência pelo valor de $c = 3$, e a segunda pelo valor de $a = 5$ e subtrair a segunda equação de congruência da primeira, obtemos

$$(5 \cdot 2 - 3 \cdot 3) \cdot y \equiv 5 \cdot 4 - 3 \cdot 1 \bmod 7 \Leftrightarrow y \equiv 17 \bmod 7.$$

Ao resolver a equação $y \equiv 17 \bmod 7$,

$$y \equiv 17 \bmod 7 \Leftrightarrow y \equiv 17 - 7 \bmod 7 \Leftrightarrow y \equiv 10 - 7 \bmod 7 \Leftrightarrow y \equiv 3 \bmod 7, \text{temos} \quad y = 3.$$

Portanto, a solução única módulo 7 do sistema é $S = \begin{pmatrix} 4 \\ 3 \end{pmatrix}$.

5 Material de apoio- Técnicas de Resolução de Sistema de Congruências Lineares

A Teoria dos Números é, por natureza, um ramo da Matemática que exige um elevado nível de rigor e talvez por isso a maioria dos materiais que trata sobre o conteúdo de Sistema de Congruências Lineares é tratado de forma bem direta, com poucos exemplos práticos e um número inexpressivo de detalhes. Nesse sentido, buscamos neste capítulo elaborar um material de apoio que apresente soluções detalhadas (com todos os passos da resolução), explicativas (uma linguagem culta porém acessível) e relacionadas com os conceitos já estudados além daqueles que foram abordados no capítulo anterior.

Este material tem como objetivo auxiliar os professores da Formação Geral Básica que queiram se aprofundar nos conceitos de Teoria dos Números, para alunos da graduação que cursam da disciplina de Introdução a Teoria dos Números, para alunos da pós-graduação na disciplina de Aritmética e pode ainda ser direcionado a aqueles que têm um pouco de familiaridade com a Teoria dos Números.

Em uma busca de uma abordagem mais compreensível, que vise facilitar o acesso e dar uma visão geral do objeto de estudo, e em consonância com um dos objetivos que é utilizar de diferentes técnicas para resolver Sistema de Congruências Lineares que admite solução, dividiremos essas técnicas em tópicos. Dessa forma, queremos que o leitor ao finalizar a leitura deste material se sinta capaz de analisar e escolher a técnica mais eficiente e que melhor se adapte para resolver um Sistema de Congruências Lineares. E essa escolha é possível quando conhecemos todas elas e além disso, suas condições gerais e específicas. Lembrando que há possibilidade de usar mais de uma técnica em um mesmo problema.

Nesse contexto, a competência de número dois das competências Gerais da Educação Básica diz que:

> Exercitar a curiosidade intelectual e recorrer à abordagem própria das ciências, incluindo a investigação, a reflexão, a análise crítica, a imaginação e a criatividade, para investigar causas, elaborar e testar hipóteses, formular e resolver problemas e criar soluções (inclusive tecnológicas) com base nos conhecimentos das diferentes áreas,(BRASIL, 2017, p.09).

Essa competência trata do desenvolvimento do raciocínio, que deve ser feito por meio de várias estratégias, principalmente, a análise crítica e a busca por soluções criativas e inovadoras. É preciso desenvolver nos alunos a capacidade de questionar, de fazer escolhas e buscar diferentes soluções para um problema, aprender a explorar possibilidades. Muitas

vezes usamos e aplicamos um determinado conceito sem saber se de fato está de acordo com as condições de um teorema.

Este material contém a resolução de questões extraídas de diferentes fontes, de forma detalhada, seguindo todos os passos de resolução, com uma linguagem mais simples, porém rigorosa.

Apresentamos agora as diferentes técnicas de resolução de Sistema de Congruências Lineares com uma ou duas variáveis.

5.1 Resolução de Sistema de Congruências Lineares com uma variável

5.1.1 Técnica I- Redução do Sistema a uma única equação de congruência

O objetivo aqui é apresentar um método de reduzir um Sistema de Congruências Lineares da forma

$$\begin{cases} x & \equiv & c_1 \bmod m_1 \\ x & \equiv & c_2 \bmod m_2 \\ \vdots & & \\ x & \equiv & c_r \bmod m_r \end{cases} \tag{5.1}$$

onde $c_1, \cdots, c_k, m_1, \cdots, m_k$ são inteiros fixados, com $m_i > 0$ para todo $i = 1, 2, \cdots, r$, a uma única congruência.

Note que, pela Proposição 3.9 item (b) isto é possível desde que:

$$c_1 = c_2 = \cdots = c_r.$$

Desta forma, se para o sistema (5.1) tivermos que $m_i - c_i = k$ para todo $i = 1, \cdots r$, onde k é uma constate qualquer, então podemos obter um sistema compatível com a Proposição 3.9 item (b).

De fato, para isto, basta somar-se o número k em ambas equações do sistema de congruências.

$$\begin{cases} x & \equiv & c_1 \bmod m_1 \\ x & \equiv & c_2 \bmod m_2 \\ \vdots & & \\ x & \equiv & c_r \bmod m_r \end{cases} \Leftrightarrow \begin{cases} x+k & \equiv & c_1 + k \bmod m_1 \\ x+k & \equiv & c_2 + k \bmod m_2 \\ \vdots & & \\ x+k & \equiv & c_r + k \bmod m_r \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} x+k & \equiv & c_1 + k & \equiv 0 & \bmod m_1 \\ x+k & \equiv & c_2 + k & \equiv 0 & \bmod m_2 \\ \vdots & & & & \\ x+k & \equiv & c_r + k & \equiv 0 & \bmod m_r \end{cases} \Leftrightarrow \begin{cases} x+k & \equiv & 0 \bmod m_1 \\ x+k & \equiv & 0 \bmod m_2 \\ \vdots & & \\ x+k & \equiv & 0 \bmod m_r. \end{cases}$$

Logo, pela Proposição 3.9 item (b), temos uma única equação de congruência da forma $x + k \equiv 0 \bmod [m_1, m_2, \cdots, m_r]$, onde $i = 1, 2, \cdots, r$.

Portanto, as soluções do sistema é dado por $x + k = [m_1, m_2, \cdots, m_r] \cdot t$, onde $t \in \mathbb{Z}$.

De acordo, com a descrição acima podemos escrever uma sequência de passos a serem seguidos a fim de obter a solução do sistema caso exista.

Passo 1_{T_I}**:** Representar as informações do problema proposto por meio de um sistema da forma 5.1.

Passo 2_{T_I}**:** Verificar se $m_i - c_i = k$ para todo $i = 1, 2, \cdots, r$.

Passo 3_{T_I}**:** Somar k, obtendo $c_1 = c_2 = \cdots = c_r$. Para isto, basta somar-se o número k em ambas equações do sistema de congruências,

$$\begin{cases} x \equiv c_1 \bmod m_1 \\ x \equiv c_2 \bmod m_2 \\ \vdots \\ x \equiv c_r \bmod m_r \end{cases} \Leftrightarrow \begin{cases} x + k \equiv c_1 + k \bmod m_1 \\ x + k \equiv c_2 + k \bmod m_2 \\ \vdots \\ x + k \equiv c_r + k \bmod m_r \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} x + k \equiv c_1 + k \equiv 0 \bmod m_1 \\ x + k \equiv c_2 + k \equiv 0 \bmod m_2 \\ \vdots \\ x + k \equiv c_r + k \equiv 0 \bmod m_r \end{cases} \Leftrightarrow \begin{cases} x + k \equiv 0 \bmod m_1 \\ x + k \equiv 0 \bmod m_2 \\ \vdots \\ x + k \equiv 0 \bmod m_r. \end{cases}$$

Passo 4_{T_I}**:** Escrever a única solução equivalente ao sistema: $x + k \equiv 0 \bmod [m_1, m_2, \cdots, m_r]$, onde $i = 1, 2, \cdots, r$.

Passo 5_{T_I}**:** Resolver a congruência do **Passo** 4_{T_I}**:**

Vejamos alguns exemplos.

Exemplo 35. (Extraído do livro de Aritmética- Abramo Hefez) Ache todos os números inteiros que deixam restos 2, 3 e 4 quando divididos por 3, 4 e 5, respectivamente.

Solução: **Passo** 1_{T_I}**:** Seja N o número procurado. Sabemos que N é uma solução do seguinte sistema de congruências:

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 4 \\ x \equiv 4 \bmod 5. \end{cases}$$

Passo 2_{T_I}**:** Observe que, $x \equiv m - 1 \bmod m \quad \Leftrightarrow \quad x + 1 \equiv m \bmod m$, mas $m \equiv 0 \bmod m$, logo, $x + 1 \equiv 0 \bmod m, \forall m \in \mathbb{N}$. Portando, $k = 1$.

Passo 3_{T_I}**:** Somar $k = 1$ em todas as equações de congruência do sistema,

$$\begin{cases} x+1 \equiv 2+1 \bmod 3 \\ x+1 \equiv 3+1 \bmod 4 \\ x+1 \equiv 4+1 \bmod 5 \end{cases} \Leftrightarrow \begin{cases} x+1 \equiv 0 \bmod 3 \\ x+1 \equiv 0 \bmod 4 \\ x+1 \equiv 0 \bmod 5. \end{cases}$$

Passo 4_{T_I}**:** Pela Proposição 3.9 item (b), o sistema é equivalente à congruência $x+1 \equiv 0 \bmod [3,4,5]$. Como $[3,4,5] = 60$, temos que $x+1 \equiv 0 \bmod 60$.

Passo 5_{T_I}**:** As soluções são dadas por: $x+1 = 60\,t$, onde $t \in \mathbb{Z}$. A menor solução positiva ocorre quando $t = 1$, logo, $x+1 = 60 \cdot 1 \Rightarrow x = 60-1$. Portanto, $N = 59$.

Exemplo 36. (Extraído do livro de Aritmética- Abramo Hefez) Ache o menor número natural que deixa restos 1, 3 e 5 quando dividido por 5, 7 e 9, respectivamente.

Solução: **Passo** 1_{T_I}**:** Seja N o número procurado. Sabemos que N é uma solução do seguinte sistema de congruências:

$$\begin{cases} x \equiv 1 \bmod 5 \\ x \equiv 3 \bmod 7 \\ x \equiv 5 \bmod 9. \end{cases}$$

Passo 1_{T_I}**:** Observe que, $x \equiv m-4 \bmod m \quad \Leftrightarrow \quad x+4 \equiv m \bmod m$, mas $m \equiv 0 \bmod m$, logo, $x+4 \equiv 0 \bmod m, \forall m \in \mathbb{N}$.

Passo 3_{T_I}**:** Somar $k = 4$ em todas as equações de congruência do sistema,

$$\begin{cases} x+4 \equiv 1+4 \bmod 5 \\ x+4 \equiv 3+4 \bmod 7 \\ x+4 \equiv 5+4 \bmod 9 \end{cases} \Leftrightarrow \begin{cases} x+4 \equiv 0 \bmod 5 \\ x+4 \equiv 0 \bmod 7 \\ x+4 \equiv 0 \bmod 9. \end{cases}$$

Passo 4_{T_I}**:** Pela Proposição 3.9 item (b), o sistema é equivalente à congruência $x+4 \equiv 0 \bmod [5,7,9]$. Como $[5,7,9] = 315$, temos que $x+4 \equiv 0 \bmod 315$.

Passo 5_{T_I}**:** As soluções são dadas por: $x+4 = 315\,t$, onde $t \in \mathbb{Z}$. A menor solução positiva ocorre quando $t = 1$, logo, $x+4 = 315 \cdot 1 \Rightarrow x = 315-4$. Portanto, $N = 311$.

Exemplo 37. (Extraído do livro de Aritmética- Abramo Hefez) Dispomos de uma quantia de x reais menor do que 3000. Se distribuirmos essa quantia entre 11 pessoas, sobra um real; se a distribuirmos entre 12 pessoas, sobram dois reais e se a distribuirmos entre 13 pessoas, sobram 3 reais. De quantos reais dispomos?

Solução: **Passo** 1_{T_I}**:** Seja N o número procurado. Sabemos que N é uma solução do seguinte sistema de congruências, além disso $0 < N < 3000$:

$$\begin{cases} x \equiv 1 \bmod 11 \\ x \equiv 2 \bmod 12 \\ x \equiv 3 \bmod 13. \end{cases}$$

Passo 2_{T_I}**:** Observe que, $x \equiv m - 10 \bmod m \quad \Leftrightarrow \quad x + 10 \equiv m \bmod m$, mas $m \equiv 0 \bmod m$, logo, $x + 10 \equiv 0 \bmod m, \forall m \in \mathbb{N}$.

Passo 3_{T_I}**:** Somar $k = 10$ em todas as equações de congruência do sistema,

$$\begin{cases} x + 10 \equiv 1 + 10 \bmod 11 \\ x + 10 \equiv 2 + 10 \bmod 12 \\ x + 10 \equiv 3 + 10 \bmod 13 \end{cases} \Leftrightarrow \begin{cases} x + 10 \equiv 0 \bmod 11 \\ x + 10 \equiv 0 \bmod 12 \\ x + 10 \equiv 0 \bmod 13. \end{cases}$$

Passo 4_{T_I}**:** Pela Proposição 3.9 item (b), o sistema é equivalente à congruência $x + 10 \equiv 0 \bmod [11, 12, 13]$. Como $[11, 12, 13] = 1716$, temos que $x + 10 \equiv 0 \bmod 1716$.

Passo 5_{T_I}**:** As soluções são dadas por: $x + 10 = 1716\,t$, onde $t \in \mathbb{N}$. A menor solução positiva ocorre quando $t = 1$, logo, $x + 10 = 1716 \cdot 1 \Rightarrow x = 1716 - 10$. Portanto, $N = 1706$.

Exemplo 38. (Extraído do livro de Aritmética- Abramo Hefez) Ache o menor número natural que deixa restos 5, 4, 3, e 2 quando dividido por 6, 5, 4 e 3, respectivamente.

Solução: **Passo** 1_{T_I}**:** Seja N o número procurado. Sabemos que N é uma solução do seguinte sistema de congruências:

$$\begin{cases} x \equiv 5 \bmod 6 \\ x \equiv 4 \bmod 5 \\ x \equiv 3 \bmod 4 \\ x \equiv 2 \bmod 3. \end{cases}$$

Passo 2_{T_I}**:** Observe que, $x \equiv m - 1 \bmod m \quad \Leftrightarrow \quad x + 1 \equiv m \bmod m$, mas $m \equiv 0 \bmod m$, logo, $x + 1 \equiv 0 \bmod m, \forall m \in \mathbb{N}$.

Passo 3_{T_I}**:** Somar $k = 1$ em todas as equações de congruência do sistema,

$$\begin{cases} x + 1 \equiv 5 + 1 \bmod 6 \\ x + 1 \equiv 4 + 1 \bmod 5 \\ x + 1 \equiv 3 + 1 \bmod 4 \\ x + 1 \equiv 2 + 1 \bmod 3 \end{cases} \Leftrightarrow \begin{cases} x + 1 \equiv 0 \bmod 6 \\ x + 1 \equiv 0 \bmod 5 \\ x + 1 \equiv 0 \bmod 4 \\ x + 1 \equiv 0 \bmod 3. \end{cases}$$

Passo 4_{T_I}**:** Pela Proposição 3.9 item (b), o sistema é equivalente à congruência $x + 1 \equiv 0 \bmod [6, 5, 4, 3]$. Como $[6, 5, 4, 3] = 60$, temos que $x + 1 \equiv 0 \bmod 60$.

Passo 5_{T_I}**:** As soluções são dadas por: $x + 1 = 60\,t$, onde $t \in \mathbb{Z}$. A menor solução positiva ocorre quando $t = 1$, logo, $x + 1 = 60 \cdot 1 \Rightarrow x = 60 - 1$. Portanto, $N = 59$.

Exemplo 39. (Extraído do ENQ-2014.2) Em uma cesta contendo ovos, na contagem de dois em dois, de três em três, de quatro em quatro e de cinco em cinco, sobram 1, 2, 3 e 4 ovos, respectivamente. Qual é a menor quantidade de ovos que a cesta pode ter?

Solução: **Passo** 1_{T_I}**:** Seja N o número procurado. Sabemos que N é uma solução do seguinte sistema de congruências:

$$\begin{cases} x & \equiv & 1 \bmod 2 \\ x & \equiv & 2 \bmod 3 \\ x & \equiv & 3 \bmod 4 \\ x & \equiv & 4 \bmod 5. \end{cases}$$

Passo 2_{T_I}**:** Observe que, $x \equiv m-1 \bmod m \quad \Leftrightarrow \quad x+1 \equiv m \bmod m$, mas $m \equiv 0 \bmod m$, logo, $x+1 \equiv 0 \bmod m, \forall m \in \mathbb{N}$.

Passo 3_{T_I}**:** Somar $k=1$ em todas as equações de congruência do sistema,

$$\begin{cases} x+1 & \equiv & 1+1 \bmod 2 \\ x+1 & \equiv & 2+1 \bmod 3 \\ x+1 & \equiv & 3+1 \bmod 4 \\ x+1 & \equiv & 4+1 \bmod 5 \end{cases} \Leftrightarrow \begin{cases} x+1 & \equiv & 0 \bmod 2 \\ x+1 & \equiv & 0 \bmod 3 \\ x+1 & \equiv & 0 \bmod 4 \\ x+1 & \equiv & 0 \bmod 5. \end{cases}$$

Passo 4_{T_I}**:** Pela Proposição 3.9 item (b), o sistema é equivalente à congruência $x+1 \equiv 0 \bmod [2,3,4,5]$. Como $[2,3,4,5]=60$, temos que $x+1 \equiv 0 \bmod 60$.

Passo 5_{T_I}**:** As soluções são dadas por: $x+1=60\,t$, onde $t \in \mathbb{Z}$. A menor solução positiva ocorre quando $t=1$, logo, $x+1=60 \cdot 1 \Rightarrow x=60-1$. Portanto, $N=59$.

5.1.2 Técnica II- Substituição

Nesta técnica utilizaremos o método da substituição para resolver o sistema. Para isso, iremos reescrever quando necessário as equações de congruências por meio do Algoritmo de Euclides. Além disso, vamos utilizar a definição e as propriedades de congruências.

Vejamos o exemplo a seguir:

Exemplo 40. (Extraído do ENQ-2016.2) A secretaria de educação de um município recebeu uma certa quantidade de livros para distribuir entre as escolas do município. Sabe-se que a quantidade é superior a 1000, inferior a 2000, que se dividi-los entre 7 escolas sobram 4, entre 9 sobram 2 e entre 13 sobram 6. Encontre a quantidade de livros.

Solução: Seja N a quantidade de livros comprada pela secretaria. Além disso, $1000 < N < 2000$.

Vamos representar as informações dadas em um sistema.

$$\begin{cases} N & \equiv & 4 \bmod 7 \\ N & \equiv & 2 \bmod 9 \\ N & \equiv & 6 \bmod 13. \end{cases}$$

Neste exemplo o Sistema é composto por três equações, porém podemos aplicar essa técnica com duas ou mais equações de congruência.

Pela primeira equação modular segue que $N = 7k + 4$, com $k \in \mathbb{Z}$.

Substituindo o valor de N na segunda equação temos que,

$$N \equiv 2 \bmod 9$$

$$7k + 4 \equiv 2 \bmod 9$$

.

Somando 5 em ambos os lados, temos que

$$7k + 4 + 5 \equiv 2 + 5 \bmod 9$$

$$7k + 9 \equiv 7 \bmod 9$$

$$7k \equiv 7 \bmod 9$$

$$k \equiv 1 \bmod 9.$$

Logo,

$$k = 9t + 1.$$

Assim,

$$N = 7k + 4$$

$$N = 7(9t + 1) + 4$$

$$N = 63t + 11.$$

Substituindo essa informação na terceira equação segue que

$$N \equiv 6 \bmod 13$$

$$63t + 11 \equiv 6 \bmod 13$$

.

Somando 2 em ambos os lados, temos que

$$63t + 11 + 2 \equiv 6 + 2 \bmod 13$$

$$63t + 13 \equiv 8 \bmod 13$$

.

E como $63 = 13 \cdot 4 + 11$

$$11t \equiv 8 \bmod 13$$

.

Multiplicando essa equção por 6, temos que

$$66t \equiv 48 \bmod 13$$

Como $66 = 13 \cdot 5 + 1$ e $48 = 13 \cdot 3 + 9$

Logo,

$$t \equiv 9 \bmod 13.$$

Assim, segue que

$$t = 13w + 9$$

e

$$N = 63t + 11$$

$$N = 63(13w + 9) + 11$$

$$N = 819w + 578.$$

Como $1000 < N < 2000$, concluímos que a resposta é

$$1000 < 819w + 578 < 2000 \Rightarrow$$

$$1000 - 578 < 819w < 2000 - 578 \Rightarrow$$
$$\frac{422}{819} < w < \frac{1422}{819}, w \in \mathbb{N} \Rightarrow$$

$$0,52 < w < 1,74,$$

ou seja, $w = 1$ e

$$N = 819 \cdot 1 + 578,$$

Portanto, $N = 1397$.

5.1.3 Técnica III- Teorema Chinês dos Restos

Essa técnica é possível de ser utilizada em qualquer Sistema de Congruências Lineares da forma

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

onde $c_1, c_2, \cdots, c_k, m_1, m_2, \cdots, m_k$ são inteiros fixados, com $m_i > 0$ para todo $i = 1, 2, \cdots, r$, desde que atenda sua condição principal, ou seja, que os módulos sejam dois a dois primos entre si. Satisfeita essa condição podemos sim, utilizar o Teorema Chinês dos Restos.

Como esta técnica possui vários passos para chegar a solução, elaboramos um algoritmo de sua aplicação a fim de facilitar sua resolução.

5.1.3.1 Algoritmo da aplicação do Teorema Chinês dos Restos

Daremos a seguir os passos para encontrar uma solução particular de uma sistema de congruências lineares, quando este verifica as hipóteses do Teorema Chinês dos Restos acima.

Passo $1_{T_{III}}$**:** Construir inteiros $M, M_1, M_2, \cdots, M_n$, onde

$$M = m_1 \cdot m_2 \cdot \cdots \cdot m_k$$

e

$$M_1 = \frac{M}{m_1}, M_2 = \frac{M}{m_2}, \cdots, M_i = \frac{M}{m_i}, \cdots, M_n = \frac{M}{m_k}.$$

Passo $2_{T_{III}}$**:** Encontrar inteiros y_i.

Para cada $i = 1, 2, \cdots, k, (M_i, m_i) = 1$. Logo existe inteiros y_i, tais que:

$$\begin{aligned} &M_1 \cdot y_1 \equiv 1 \bmod m_1 \\ &M_2 \cdot y_2 \equiv 1 \bmod m_2 \\ &\vdots \\ &M_k \cdot y_k \equiv 1 \bmod m_k. \end{aligned}$$

Passo $3_{T_{III}}$**:** Determinar a solução particular.

A solução particular X é dada por:

$$X = M_1 \cdot y_1 \cdot c_1 + M_2 \cdot y_2 \cdot c_2 + \cdots + M_r \cdot y_r \cdot c_r \equiv M_k \cdot y_k \cdot c_k \bmod m_k.$$

Passo $4_{T_{III}}$**:** Determinar o conjunto solução.

Todas as demais soluções do sistema são congruentes a X módulo m. Logo o conjunto solução é dado por:

$$S = \{X + mt, t \in \mathbb{Z}.\}$$

Para começar resolveremos um exemplo de um Sistema que possui duas equações de congruências lineares.

Exemplo 41. (Extraído do ENQ-2020.1) Determine um número inteiro entre 1200 e 1400 que deixa restos 2 e 6 quando dividido, respectivamente, por 11 e 13.

Solução: Primeiro vamos montar o sistema de congruências lineares.

$$\begin{cases} x & \equiv & 2 \bmod 11 \\ x & \equiv & 6 \bmod 13. \end{cases}$$

Como (11, 13) = 1 (condição necessária), é possível aplicar o Teorema Chinês dos Restos para obter a solução geral que é única módulo m.

Passo $1_{T_{III}}$**:** Construir inteiros $M, M_1, M_2, \cdots, M_n$, onde $M = 11 \cdot 13 = 143$ e

$$M_1 = \frac{143}{11} = 13, \qquad M_2 = \frac{143}{13} = 11.$$

Passo $2_{T_{III}}$**:** Encontrar inteiros y_i. Para cada $i = 1, 2, \cdots, k, (M_i, m_i) = 1$, logo existe inteiros y_i, tais que:

$11 \cdot y_1 \equiv 1 \bmod 13$	$13 \cdot y_2 \equiv 1 \bmod 11$
$11 \cdot 1 \equiv 11 \bmod 13$	$13 \cdot 1 \equiv 2 \bmod 11$
$11 \cdot 2 \equiv 9 \bmod 13$	$13 \cdot 2 \equiv 4 \bmod 11$
$11 \cdot 3 \equiv 7 \bmod 13$	$13 \cdot 3 \equiv 6 \bmod 11$
$11 \cdot 4 \equiv 5 \bmod 13$	$13 \cdot 4 \equiv 8 \bmod 11$
$11 \cdot 5 \equiv 3 \bmod 13$	$13 \cdot 5 \equiv 10 \bmod 11$
$11 \cdot 6 \equiv 1 \bmod 13$	$13 \cdot 6 \equiv 1 \bmod 11.$

Portanto, $y_1 = 6$ e $y_2 = 6$.

Passo $3_{T_{III}}$**:** Determinar a solução particular.

A solução particular X é dada por:

$$X = M_1 \cdot y_1 \cdot c_1 + M_2 \cdot y_2 \cdot c_2 + \cdots + M_r \cdot y_r \cdot c_r \equiv M_k \cdot y_k \cdot c_k \bmod m_k.$$
$$X = 13 \cdot 2 \cdot 6 + 11 \cdot 6 \cdot 6 = 552 \equiv 123 \bmod 143.$$

Logo, 123 é uma solução, única módulo 143.

Passo $4_{T_{III}}$**:** Determinar o conjunto solução.

Todas as demais soluções do sistema são congruentes a 123 módulo 143. Logo o conjunto solução é dado por:

$$S = \{123 + 143t, t \in \mathbb{Z}.\}$$

Como queremos determinar uma solução inteira $X, 1200 < X < 1400$, temos que

$$1200 < 123 + 143t < 1400 \Rightarrow$$
$$1200 - 123 < 143t < 1400 - 123 \Rightarrow$$
$$\frac{1077}{143} < t \Rightarrow$$
$$7,5 < t, \text{ou seja}, t = 8 \text{ e}$$
$$X = 123 + 143 \cdot 8,$$
$$X = 1267.$$

Portanto, o valor de x que satisfaz simultaneamente as duas equações de congruência do sistema inicial é $x = 1267$.

Exemplo 42. (Extraído do Livro do EVES) "Um certo número desconhecido de coisas quando dividido por 3 deixa resto 2, por 5 resto 3 e por 7 resto 2. Qual é o (menor) número?
Solução: Primeiro vamos montar o sistema de congruências lineares.

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 5 \\ x \equiv 2 \bmod 7. \end{cases}$$

Como (3,5)=1, (3,7)=1 e (5,7) =1 (Condição necessária) podemos aplicar o Teorema Chinês dos Restos para obter a solução geral que é única módulo m.

Passo $1_{T_{III}}$**:** Construir inteiros $M, M_1, M_2, \cdots, M_n$, onde $M = 3 \cdot 5 \cdot 7 = 105$ e

$$M_1 = \frac{105}{3} = 35, \quad M_2 = \frac{105}{5} = 21, \quad M_3 = \frac{105}{7} = 15.$$

Passo $2_{T_{III}}$**:** Encontrar inteiros y_i.

Para cada $i = 1, 2, \cdots, k, (M_i, m_i) = 1$, logo existe inteiros y_i, tais que:

$35 \cdot y_1 \equiv 1 \bmod 3$	$21 \cdot y_2 \equiv 1 \bmod 5$	$15 \cdot y_3 \equiv 1 \bmod 7$
$35 \cdot 1 \equiv 2 \bmod 3$	$21 \cdot 1 \equiv 1 \bmod 5$	$15 \cdot 1 \equiv 1 \bmod 7.$
$35 \cdot 2 \equiv 1 \bmod 3$		

Portanto, $y_1 = 2, \quad y_2 = 1 \quad \text{e} \quad y_3 = 1.$

Passo $3_{T_{III}}$**:** Determinar a solução particular.

A solução particular X é dada por:

$$X = M_1 \cdot y_1 \cdot c_1 + M_2 \cdot y_2 \cdot c_2 + \cdots + M_r \cdot y_r \cdot c_r \equiv M_k \cdot y_k \cdot c_k \bmod m_k.$$
$$X = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 = 233 \equiv 23 \bmod 105.$$

Logo, 23 é uma solução, única módulo 105.

Passo $4_{T_{III}}$**:** Determinar o conjunto solução.

Todas as demais soluções do sistema são congruentes a 23 módulo 105. Logo o conjunto solução é dado por:

$$S = \{23 + 105t, t \in \mathbb{Z}\}$$

Exemplo 43. (Extraído do ENQ-2018.1) O objetivo desse problema é encontrar o número natural x, menor do que 1700 e que deixe restos 2, 2, 1 e 0 quando dividido por 5, 6, 7 e 11, respectivamente.

Solução: Primeiro vamos montar o sistema de congruências lineares.

$$\begin{cases} x \equiv 2 \bmod 5 \\ x \equiv 2 \bmod 6 \\ x \equiv 1 \bmod 7 \\ x \equiv 0 \bmod 11. \end{cases}$$

Como $(5,6) = 1, (5,7) = 1, (5,11) = 1, (6,7) = 1, (6,11) = 1$ e $(7,11) = 1$, (Condição necessária) é possível aplicar o Teorema Chinês dos Restos para obter a solução geral que é única módulo m.

Passo $1_{T_{III}}$**:** Construir inteiros $M, M_1, M_2, \cdots, M_n$, onde $M = 5 \cdot 6 \cdot 7 \cdot 11 = 2310$ e

$$M_1 = \frac{2310}{5} = 462, \quad M_2 = \frac{2310}{6} = 385, \quad M_3 = \frac{2310}{7} = 330, \quad M_4 = \frac{2310}{11} = 210.$$

Passo $2_{T_{III}}$**:** Encontrar inteiros y_i.

Para cada $i = 1, 2, \cdots, k, (M_i, m_i) = 1$, logo existe inteiros y_i, tais que:

$462 \cdot y_1 \equiv 1 \bmod 5$	$385 \cdot y_2 \equiv 1 \bmod 6$	$330 \cdot y_3 \equiv 1 \bmod 7$	$210 \cdot y_4 \equiv 1 \bmod 11$
$462 \cdot 1 \equiv 2 \bmod 5$	$385 \cdot 1 \equiv 1 \bmod 6$	$330 \cdot 1 \equiv 1 \bmod 7$	$210 \cdot 1 \equiv 1 \bmod 11.$
$462 \cdot 2 \equiv 4 \bmod 5$			
$462 \cdot 3 \equiv 1 \bmod 5$			

Portanto, $y_1 = 3, \quad y_2 = 1, \quad y_3 = 1 \quad$ e $\quad y_4 = 1.$

Passo $3_{T_{III}}$**:** Determinar a solução particular.

A solução particular X é dada por:

$$X = M_1 \cdot y_1 \cdot c_1 + M_2 \cdot y_2 \cdot c_2 + \cdots + M_r \cdot y_r \cdot c_r \equiv M_k \cdot y_k \cdot c_k \bmod m_k.$$

$$X = 462 \cdot 3 \cdot 2 + 385 \cdot 1 \cdot 2 + 330 \cdot 1 \cdot 1 + 210 \cdot 1 \cdot 0 = 3872 \equiv 1562 \bmod 2310.$$

Logo, 1562 é uma solução, única módulo 2310.

Passo $4_{T_{III}}$**:** Determinar o conjunto solução.

Todas as demais soluções do sistema são congruentes a 1562 módulo 2310. Logo o conjunto solução é dado por:

$$S = \{1562 + 2310t, t \in \mathbb{Z}.\}$$

5.1.4 Técnica IV- Teorema Chinês dos Restos Generalizado com duas equações de congruências

O objetivo dessa técnica é resolver sistema da forma

$$\begin{cases} x & \equiv & c_1 \bmod m_1 \\ x & \equiv & c_2 \bmod m_2 \end{cases}$$

onde $d = (m_1, m_2) \neq 1$.

E para facilitar a resolução desse sistema elaboramos um algoritmo com uma sequência de passos.

Passo $1_{T_{IV}}$**:** Verificar se o sistema admite solução, ou seja $(m_1, m_2) = d \mid (c_1 - c_2)$.

Passo $2_{T_{IV}}$**:** Determinar os valores de $a = \dfrac{m_2}{(m_1, m_2)}$ e $b = \dfrac{m_1}{(m_1, m_2)}$.

Passo $3_{T_{IV}}$**:** Aplicar o *Algoritmo de Euclides Estendido*, para determinar os inteiros x_1 e x_2 tais que

$$x_1 a + x_2 b = 1.$$

Passo $4_{T_{IV}}$**:** Determinar a solução através da fórmula:

$$x = c_1 x_1 a + c_2 x_2 b.$$

Exemplo 44. (Extraído do Livro do BURTON) Considere o sistema

$$\begin{cases} x & \equiv & 5 & \bmod 6 \\ x & \equiv & 7 & \bmod 15. \end{cases}$$

Solução: Note que, por verificação, o valor de x para o qual a equação $x \equiv 5 \bmod 6$ é satisfeita é $x = 11$ e para a equação $x \equiv 7 \bmod 15$, $x = 37$. Logo, separadamente cada congruência tem solução.

Por outro lado, pela Proposição 4.2, o sistema admite solução se, e somente se, $c_2 \equiv c_1 \bmod (m_1, m_2)$, e $7 \equiv 5 \bmod (6, 15)$. Como $(6, 15) = 3$, temos que $7 \not\equiv 5 \bmod 3$.

Portanto, o sistema não admite solução.

Exemplo 45. Resolvamos o sistema:

$$\begin{cases} x & \equiv & 1 & \mod 28 \\ x & \equiv & 3 & \mod 90. \end{cases}$$

Passo $1_{T_{IV}}$**:** Verificar se o sistema admite solução, ou seja $(m_1, m_2) = d \mid (c_1 - c_2)$.

Como $d = (m_1, m_2) = (90, 28) = 2$ divide $(3 - 1)$, temos que o sistema admite solução.

Passo $2_{T_{IV}}$**:** Determinar os valores de a e b.

$$a = \frac{90}{(90, 28)} = \frac{90}{2} = 45, \quad b = \frac{28}{(90, 28)} = \frac{28}{2} = 14.$$

Passo $3_{T_{IV}}$**:** Aplicar o *Algoritmo de Euclides Estendido*, para determinar os inteios x_1 e x_2 tais que

$$x_1 \cdot a + x_2 \cdot b = x_1 \cdot 45 + x_2 \cdot 14 = 1.$$

Aplicando o algoritmo de Euclides. Inicialmente, efetuamos a divisão $45 = 14 \cdot 3 + 3$ e colocamos os números envolvidos no seguinte diagrama:

	3	
45	14	
3		

A seguir, continuamos efetuando a divisão $14 = 3 \cdot 4 + 2$ e colocamos os números envolvidos no diagrama

	3	4
45	14	3
3	2	

Prosseguindo, enquanto for possível, teremos

	3	4	1	2
45	14	3	2	1
3	2	1	0	

até algum r_n dividir r_{n-1}. Assim, $(45, 14) = 1$, ou seja, o máximo divisor comum de 45 e 14 é o último resto não-nulo no processo de divisão.

Observe que, o *Algoritmo de Euclides* fornece-nos:

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ 2 &= 14 - 4 \cdot 3 \\ 3 &= 45 - 3 \cdot 14. \end{aligned}$$

Donde se segue que

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (14 - 4 \cdot 3) \\ &= 3 \cdot 5 - 1 \cdot 14 \\ &= (45 - 3 \cdot 14) \cdot 5 - 1 \cdot 14 \\ &= 5 \cdot 45 + (-16) \cdot 14. \end{aligned}$$

Portanto,

$$\begin{array}{rcll} r_n & = & (a, b) & = & x_1 a + x_2 b \\ 1 & = & (45, 14) & = & x_1 \cdot 45 + x_2 \cdot 14 \\ 1 & = & (45, 14) & = & 5 \cdot 45 + (-16) \cdot 14. \end{array}$$

Assim, $x_1 = 5$ e $x_2 = -16$.

Passo $4_{T_{IV}}$**:** Determinar a solução através da fórmula:

$$\begin{aligned} x &= c_1 x_1 a + c_2 x_2 b \\ x &= 1 \cdot 5 \cdot 45 + 3 \cdot (-16) \cdot 14 \\ x &= -447 \\ x &\equiv -447 \equiv 813 \bmod [28, 90]. \end{aligned}$$

Uma solução é, portanto, $x = 813$.

5.1.5 Técnica V- Utilizando mais de uma Técnica

O objetivo aqui não é apresentar uma nova técnica de resolução, mas sim de mostrar que é possível utilizar mais de uma das que foram estudadas para determinar a solução, caso exista, de um sistema.

Dessa forma, simplificamos o processo de resolução e com isso garantimos maior agilidade. Vale ressaltar que independe do número de equações de congruência que o sistema possui podemos utilizar mais de uma técnica no seu processo de encontrar a solução.

Veja o exemplo a seguir.

Exemplo 46. Resolvamos o sistema:

$$\begin{cases} x \equiv 1 \bmod 2 \\ x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 4 \\ x \equiv 4 \bmod 5 \\ x \equiv 5 \bmod 6 \\ x \equiv 6 \bmod 7 \\ x \equiv 7 \bmod 8 \\ x \equiv 2 \bmod 9 \end{cases}$$

Solução: Como $(2,4) = (2,6) = (2,8) = (4,6) = (6,8) = 2$, $(3,6) = (3,9) = 3$ e $(4,8) = 4$, ou seja, o mdc é diferente de 1 (Condição necessária), não é possível aplicar a Técnica III - (Teorema Chinês dos Restos) para obter a solução geral que é única módulo m. E caso fosse possível aplicar a Técnica III, teríamos muito trabalho para determinar a solução.

Observe que, para as sete primeiras equações de congruência do sistema, é possível usar a Técnica I - (Redução do Sistema a uma única equação de congruência), pois $x \equiv m-1 \bmod m \Leftrightarrow x+1 \equiv m \bmod m,$ mas $m \equiv 0 \bmod m$. Logo, $x+1 \equiv 0 \bmod m, \forall m \in \mathbb{N}$.

Assim,

$$\begin{cases} x+1 \equiv 1+1 \bmod 2 \\ x+1 \equiv 2+1 \bmod 3 \\ x+1 \equiv 3+1 \bmod 4 \\ x+1 \equiv 4+1 \bmod 5 \\ x+1 \equiv 5+1 \bmod 6 \\ x+1 \equiv 6+1 \bmod 7 \\ x+1 \equiv 7+1 \bmod 8 \\ x+7 \equiv 2+7 \bmod 9 \end{cases}$$

porém, a última equação de congruência não se enquadra nas condições desta técnica.

Dessa forma, aplicamos a Técnica I nas sete primeiras equações de congruência, e posteriormente escrevemos um novo sistema com a equação que representa a solução destas sete primeiras com a última equação so sistema original.

Temos que,

$$\begin{cases} x+1 \equiv 1+1 \bmod 2 \\ x+1 \equiv 2+1 \bmod 3 \\ x+1 \equiv 3+1 \bmod 4 \\ x+1 \equiv 4+1 \bmod 5 \\ x+1 \equiv 5+1 \bmod 6 \\ x+1 \equiv 6+1 \bmod 7 \\ x+1 \equiv 7+1 \bmod 8 \end{cases} \Leftrightarrow \begin{cases} x+1 \equiv 0 \bmod 2 \\ x+1 \equiv 0 \bmod 3 \\ x+1 \equiv 0 \bmod 4 \\ x+1 \equiv 0 \bmod 5 \\ x+1 \equiv 0 \bmod 6 \\ x+1 \equiv 0 \bmod 7 \\ x+1 \equiv 0 \bmod 8. \end{cases}$$

Pela Proposição 3.9 item (b), o sistema é equivalente à congruência $x+1 \equiv 0 \bmod [2,3,4,5,6,7,8]$. Como $[2,3,4,5,6,7,8] = 840$, temos que $x+1 \equiv 0 \bmod 840$.

Logo,

$$\begin{aligned} x+1 \equiv 0 \bmod 840 &\Leftrightarrow x+1-1 \equiv 0-1 \bmod 840 \\ &\Leftrightarrow x \equiv -1 \bmod 840 \\ &\Leftrightarrow x \equiv -1+840 \\ &\Leftrightarrow x \equiv 839 \bmod 840. \end{aligned}$$

Assim, a solução das sete primeiras equações de conguências do sistema é dado por:

$$x \equiv 839 \bmod 840.$$

Agora vamos escrever o novo sistema, ou seja,

$$\begin{cases} x & \equiv & 839 \bmod 840 \\ x & \equiv & 2 \bmod 9 \end{cases}$$

Como $d \neq 1$, ou seja, $d = (840, 9) = 3$ podemos usar a Técnica IV - (Teorema Chinês dos Restos Generalizado com duas equações de congruência).

Passo $1_{T_{IV}}$**:** Verificar se o sistema admite solução, ou seja $(m_1, m_2) = d \mid (c_1 - c_2)$.

Como $d = (m_1, m_2) = (840, 9) = 3$ divide $(839 - 2)$, temos que o sistema admite solução.

Os passos a seguir tem como objetivo determinar a solução do sistema.

Passo $2_{T_{IV}}$**:** Determinar os valores de a e b.

$$a = \frac{9}{(840, 9)} = \frac{9}{3} = 3, \quad b = \frac{840}{(840, 9)} = \frac{840}{3} = 280.$$

Passo $3_{T_{IV}}$**:** Aplicar o *Algoritmo de Euclides Estendido*, para determinar os inteiros x_1 e x_2, tais que

$$x_1 \cdot a + x_2 \cdot b = x_1 \cdot 3 + x_2 \cdot 280 = 1.$$

Aplicando o algoritmo de Euclides. Inicialmente, efetuamos a divisão $280 = 3 \cdot 93 + 1$ e colocamos os números envolvidos no seguinte diagrama:

	93	
280	3	
1		

A seguir, continuamos efetuando a divisão $3 = 1 \cdot 2 + 1$ e colocamos os números envolvidos no diagrama

	6	2
20	3	1
2	1	

Prosseguindo, enquanto for possível, teremos

	93	2	1
280	3	1	1
1	1	0	

até algum r_n dividir r_{n-1}. Assim, $(3, 280) = 1$, ou seja, o máximo divisor comum de 3 e 280 é o último resto não-nulo no processo de divisão.

Observe que, o *Algoritmo de Euclides* fornece-nos:

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ 1 &= 280 - 3 \cdot 93. \end{aligned}$$

Donde se segue que

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ &= 3 - 2 \cdot (280 - 3 \cdot 93) \\ &= 3 \cdot 187 - 2 \cdot 280 \\ &= 187 \cdot 3 + (-2) \cdot 280. \end{aligned}$$

Portanto,

$$\begin{array}{rcll} r_n & = & (a, b) & = x_1 a + x_2 b \\ 1 & = & (3, 280) & = x_1 \cdot 3 + x_2 \cdot 280 \\ 1 & = & (3, 280) & = 187 \cdot 3 + (-2) \cdot 280. \end{array}$$

Assim, $x_1 = 187$ e $x_2 = -2$.

Passo $4_{T_{IV}}$**:** Determinar a solução através da fórmula:

$$\begin{aligned} x &= c_1 x_1 a + c_2 x_2 b \\ x &= 839 \cdot 187 \cdot 3 + 2 \cdot (-2) \cdot 280 \\ x &= 469559. \end{aligned}$$

Uma solução é, portanto, $x = 469559$.

5.1.6 Técnica VI- Caso Geral

Um Sistema de Congruências Lineares é da forma:

$$\left\{ \begin{array}{rcl} a_1 x & \equiv & b_1 \bmod n_1 \\ a_2 x & \equiv & b_2 \bmod n_2 \\ \vdots & & \\ a_r x & \equiv & b_r \bmod n_r \end{array} \right. \tag{5.2}$$

onde $a_1, \cdots, a_r, b_1, \cdots, b_r$ e $n_1, \cdots, n_r$ são inteiros fixados, com $n_i > 0$ para todo $i = 1, 2, \cdots, r$.

Até o momento apresentamos técnicas de solução de alguns casos de sistemas na forma

$$\left\{ \begin{array}{rcl} x & \equiv & c_1 \bmod m_1 \\ x & \equiv & c_2 \bmod m_2 \\ \vdots & & \vdots \\ x & \equiv & c_r \bmod m_r \end{array} \right.$$

onde $c_1, \cdots, c_r$ e $m_1, \cdots, m_r$ são inteiros fixados, com $m_i > 0$ para todo $i = 1, 2, \cdots, r$.

O objetivo desta secçao é resolver, sempre que possível, um sistema da forma (5.2).

Para isto, apresentamos agora uma sequência de passos a ser seguidos.

Passo $1_{T_{VI}}$**:** Verificar se cada congruência possui solução ou seja, se o $(a_i, n_i) \mid b_i$ onde $i = 1, 2, \cdots, r$.

Observação: Caso uma das congruências do sistema não possua solução, então o sistema não possue solução. Caso contrário, utilizando da demonstração da Proposição 4.2, seguimos com os passo 2 e 3.

Passo $2_{T_{VI}}$**:** Calcular $d_i = (a_i, n_i)$ e dividir cada congruência por d_i. Obtendo uma congruência equivalente

$$a'x \equiv b' \bmod m, \text{ onde } (a', m) = 1.$$

Passo $3_{T_{VI}}$**:** Determinar os inversos de $a'_1, a'_2, \cdots, a'_r$, módulo $m_1, m_2, \cdots, m_r$ respectivamente. Em seguida, multiplicar cada congruência pelo inverso correspondente, reduzindo o sistema a um da forma

$$\begin{cases} x & \equiv & c_1 \bmod m_1 \\ x & \equiv & c_2 \bmod m_2 \\ \vdots & & \\ x & \equiv & c_r \bmod m_r. \end{cases}$$

onde $c_1, \cdots, c_r$ e $m_1, \cdots, m_r$ são inteiros fixados, com $m_i > 0$ para todo $i = 1, 2, \cdots, r$.

Passo $4_{T_{VI}}$**:** Utilizar uma das quatro técnicas estudadas neste capítulo para obter a solução do sistema, caso exista.

Vejamos alguns exemplos a seguir.

Exemplo 47. (Extraído do Livro do HEFEZ) Resolva o sistema:

$$\begin{cases} 3x & \equiv & 1 \bmod 7 \\ 5x & \equiv & 2 \bmod 11 \\ 4x & \equiv & 3 \bmod 13. \end{cases}$$

Solução: **Passo** $1_{T_{VI}}$**:** Observe que $a \neq 1$. Dessa forma, devemos verificar se cada congruência linear do sistema admite solução, ou seja,

- $3x \equiv 1 \bmod 7$.

  Como $d_1 = (3, 7) = 1$ divide 1. Logo, a congruência admite solução.

- $5x \equiv 2 \bmod 11$.

  Como $d_2 = (5, 11) = 1$ divide 2. Logo, a congruência admite solução.

- $4x \equiv 3 \bmod 13$.

  Como $d_3 = (4, 13) = 1$ divide 3. Logo, a congruência admite solução.

Como as congruências admitem solução, e o $d_i = (a_i, n_i) = 1$ podemos ir para o **Passo** $3_{T_{VI}}$, ou seja, transformar o sistema em um equivalente. Para isto, utilizamos a Proposição 4.2, ou seja, reduzir o sistema a um da forma $x \equiv c_i \bmod n_i$, para $i = 1, 2, 3$.

Assim, primeiro devemos determinar os inversos multiplicativos de 3,5 e 4, módulo 7,11 e 13, respectivamente:

$$\begin{cases} 3 \cdot 5 \equiv 1 \bmod 7 \\ 5 \cdot 9 \equiv 1 \bmod 11 \\ 4 \cdot 10 \equiv 1 \bmod 13 \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 \cdot 5 \bmod 7 \\ x \equiv 2 \cdot 9 \bmod 11 \\ x \equiv 3 \cdot 10 \bmod 13 \end{cases} \Leftrightarrow \begin{cases} x \equiv 5 \bmod 7 \\ x \equiv 18 \bmod 11 \\ x \equiv 30 \bmod 13. \end{cases}$$

Logo, o sistema inicial é equivalente ao sistema

$$\begin{cases} x \equiv 5 \bmod 7 \\ x \equiv 7 \bmod 11 \\ x \equiv 4 \bmod 13. \end{cases}$$

Passo $4_{T_{VI}}$**:** Utilizar uma das quatro técnicas estudadas neste capítulo para obter a solução do sistema, caso exista.

Como (7,11)=1, (7,13)=1 e (11,13) =1 (Condição necessária) podemos aplicar a Técnica III - (Teorema Chinês dos Restos) para obter a solução geral que é única módulo m.

Segue os passos para a aplicação do agoritmo do Teorema Chinês dos Restos.

Passo $1_{T_{III}}$**:** Construir inteiros $M, M_1, M_2, \cdots, M_n$, onde

$$M = 7 \cdot 11 \cdot 13 = 1001$$

e

$$M_1 = \frac{1001}{7} = 143, \quad M_2 = \frac{1001}{11} = 91, \quad M_3 = \frac{1001}{13} = 77.$$

Passo $2_{T_{III}}$**:** Encontrar inteiros y_i.

Para cada $i = 1, 2, \cdots, k, (M_i, m_i) = 1$, logo existe inteiros y_i, tais que:

$$\begin{array}{c|c|c|} 143 \cdot y_1 \equiv 1 \bmod 7 & 91 \cdot y_2 \equiv 1 \bmod 11 & 77 \cdot y_3 \equiv 1 \bmod 13 \\ 143 \cdot 5 \equiv 1 \bmod 7 & 91 \cdot 4 \equiv 1 \bmod 11 & 77 \cdot 12 \equiv 1 \bmod 13. \end{array}$$

Portanto, $y_1 = 5, \quad y_2 = 4 \quad$ e $y_3 = 12$.

Passo $3_{T_{III}}$**:** Determinar a solução particular.

A solução particular X é dada por:

$$X = M_1 \cdot y_1 \cdot c_1 + M_2 \cdot y_2 \cdot c_2 + \cdots + M_r \cdot y_r \cdot c_r \equiv M_k \cdot y_k \cdot c_k \bmod m_k.$$
$$X = 143 \cdot 5 \cdot 5 + 91 \cdot 4 \cdot 7 + 77 \cdot 12 \cdot 4 = 9819 \equiv 810 \bmod 1001.$$

Logo, 810 é uma solução, única módulo 1001.

Passo $4_{T_{III}}$**:** Determinar o conjunto solução.

Todas as demais soluções do sistema são congruentes a 810 módulo 1001. Logo o conjunto solução é dado por:

$$S = \{810 + 1001t, t \in \mathbb{Z}.\}$$

Exemplo 48. (Extraído do Livro do HEFEZ) Resolva o sistema:

$$\begin{cases} 3x & \equiv & 1 \bmod 5 \\ 4x & \equiv & 6 \bmod 14 \\ 5x & \equiv & 11 \bmod 11. \end{cases}$$

Solução: **Passo** $1_{T_{VI}}$**:** Observe que $a_i \neq 1$. Dessa forma, devemos verificar se cada congruência linear do sistema admite solução, ou seja,

- $3x \equiv 1 \bmod 5$.

  Como $d_1 = (3, 5) = 1$ divide 1. Logo, a congruência admite solução.

- $4x \equiv 6 \bmod 14$.

  Como $d_2 = (4, 14) = 2$ divide 6. Logo, a congruência admite solução.

- $5x \equiv 11 \bmod 11$.

  Como $d_3 = (5, 11) = 1$ divide 11. Logo, a congruência admite solução.

Passo $2_{T_{VI}}$**:** Calcular $d_i = (a_i, n_i)$ e dividir cada congruência por d_i. Obtendo uma congruência equivalente.

Observe que para as equações de congruências (1) e (3) do sistema o $d_1 = d_3 = (3, 5) = (5, 11) = 1$, mas para a segunda congruência, o $d_2 = (4, 14) = 2$. Dessa forma, devemos dividir a congruência por d_2, obtendo a equação equivalente

$$\frac{4x}{2} \equiv \frac{6}{2} \bmod \frac{14}{2} \Leftrightarrow 2x \equiv 3 \bmod 7.$$

Obtemos assim, o sistema

$$\begin{cases} 3x & \equiv & 1 \bmod 5 \\ 2x & \equiv & 3 \bmod 7 \\ 5x & \equiv & 11 \bmod 11. \end{cases}$$

Passo $3_{T_{VI}}$**:** Reduzir o sistema a um da forma $x \equiv c_i \bmod m_i$, onde $i = 1, 2, \cdots, r$. Para isso, devemos determinar os inversos de $3, 2$ e 5, módulo $5, 7$ e 11, respectivamente.

Assim,

$$\begin{cases} 3 \cdot 2 \equiv 1 \bmod 5 \\ 2 \cdot 4 \equiv 1 \bmod 7 \\ 5 \cdot 9 \equiv 1 \bmod 11 \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 \cdot 2 \bmod 5 \\ x \equiv 3 \cdot 4 \bmod 7 \\ x \equiv 11 \cdot 9 \bmod 11 \end{cases} \Leftrightarrow \begin{cases} x \equiv 2 \bmod 5 \\ x \equiv 12 \bmod 7 \\ x \equiv 99 \bmod 11. \end{cases}$$

Logo, o sistema inicial é equivalente ao sistema

$$\begin{cases} x \equiv 2 \bmod 5 \\ x \equiv 5 \bmod 7 \\ x \equiv 0 \bmod 11. \end{cases}$$

Passo $4_{T_{VI}}$**:** Utilizar uma das quatro técnicas estudadas neste capítulo para obter a solução do sistema, caso exista.

Como (5,7)=1, (5,11)=1 e (7,11) =1 (Condição necessária) podemos aplicar a Técnica III - (Teorema Chinês dos Restos) para obter a solução geral que é única módulo m.

Segue os passos para a aplicação do agoritmo do Teorema Chinês dos Restos.

Passo $1_{T_{III}}$**:** Construir inteiros $M, M_1, M_2, \cdots, M_n$, onde $M = 5 \cdot 7 \cdot 11 = 385$ e

$$M_1 = \frac{385}{5} = 77, \quad M_2 = \frac{385}{7} = 55, \quad M_3 = \frac{385}{11} = 35.$$

Passo $2_{T_{III}}$**:** Encontrar inteiros y_i.

Para cada $i = 1, 2, \cdots, k, (M_i, m_i) = 1$, logo existe inteiros y_i, tais que:

$$\begin{array}{c|c|c|} 77 \cdot y_1 \equiv 1 \bmod 5 & 55 \cdot y_2 \equiv 1 \bmod 7 & 35 \cdot y_3 \equiv 1 \bmod 11 \\ 77 \cdot 3 \equiv 1 \bmod 5 & 55 \cdot 6 \equiv 1 \bmod 7 & 35 \cdot 6 \equiv 1 \bmod 11 \end{array}$$

Logo, $y_1 = 3, \quad y_2 = 6 \quad$ e $\quad y_3 = 6$.

Passo $3_{T_{III}}$**:** Determinar a solução particular.

A solução particular X é dada por:

$$X = M_1 \cdot y_1 \cdot c_1 + M_2 \cdot y_2 \cdot c_2 + \cdots + M_r \cdot y_r \cdot c_r \equiv M_k \cdot y_k \cdot c_k \bmod m_k.$$

$$X = 77 \cdot 3 \cdot 2 + 55 \cdot 6 \cdot 5 + 35 \cdot 6 \cdot 0 = 2112 \equiv 187 \bmod 385.$$

Logo, 187 é uma solução, única módulo 385.

Passo $4_{T_{III}}$**:** Determinar o conjunto solução.

Todas as demais soluções do sistema são congruentes a 187 módulo 385. Logo o conjunto solução é dado por:

$$S = \{187 + 385t, t \in \mathbb{Z}\}.$$

Exemplo 49. Resolvamos o sistema

$$\begin{cases} 4x & \equiv & 10 & \mod 81 \\ 7x & \equiv & 19 & \mod 24. \end{cases}$$

Solução: **Passo** $1_{T_{VI}}$**:** Observe que $a_i \neq 1$. Dessa forma, devemos verificar se cada congruência linear do sistema admite solução, ou seja,

- $4x \equiv 10 \mod 81$.

  Como $d_1 = (4, 81) = 1$ divide 10. Logo, a congruência admite solução.

- $7x \equiv 19 \mod 24$.

  Como $d_2 = (7, 24) = 1$ divide 19. Logo, a congruência admite solução.

Como cada equação de congruência admite solução, então o sistema admite solução.

Passo $2_{T_{VI}}$**:** Calcular $d_i = (a_i, n_i)$ e dividir cada congruência por d_i. Obtendo uma congruência equivalente.

Como $d_1 = d_2 = 1$ e 1 divide qualquer número, as equações já estão na forma reduzida.

Passo $3_{T_{VI}}$**:** Transformar o sistema em um equivalente. Para isto, utilizaremos a Proposição 4.2, ou seja, reduzir o sistema a um da forma $x \equiv c_i \mod m_i$, para $i = 1, 2$.

Dessa forma, primeiro devemos determinar os inversos multiplicativos de 7 e 4, módulo 24 e 81, respectivamente:

$$\begin{cases} 4x & \equiv & 1 \mod 81 \\ 7x & \equiv & 1 \mod 24. \end{cases}$$

Assim,

$$\begin{cases} 4 \cdot 20 & \equiv & 1 \mod 81 \\ 7 \cdot 17 & \equiv & 1 \mod 24 \end{cases} \Leftrightarrow \begin{cases} x & \equiv & 10 \cdot 20 \mod 81 \\ x & \equiv & 19 \cdot 17 \mod 24 \end{cases} \Leftrightarrow \begin{cases} x & \equiv & 200 \equiv 38 \mod 81 \\ x & \equiv & 323 \equiv 11 \mod 24. \end{cases}$$

Logo, o sistema inicial é equivalente ao sistema

$$\begin{cases} x & \equiv & 38 \mod 81 \\ x & \equiv & 11 \mod 24. \end{cases}$$

Passo $4_{T_{VI}}$**:** Utilizar uma das quatro técnicas estudadas neste capítulo para obter a solução do sistema, caso exista.

Observe que não é possível utilizar a Técnica I, pois $(81-38) \neq (24-11)$, a Técnica III também não é possível utilizá-la, pois o $(m_1, m_2) \neq 1$. Neste caso, podemos utilizar a Técnica IV.

Passo $1_{T_{IV}}$**:** Verificar se o sistema admite solução, ou seja $(m_1, m_2) = d \mid (c_1 - c_2)$.

Como $d = (m_1, m_2) = (81, 24) = 3$ divide $(38 - 111)$, temos que o sistema admite solução.

Os passos a seguir tem como objetivo determinar a solução do sistema.

Passo $2_{T_{IV}}$**:** Determinar os valores de a e b.

$$a = \frac{24}{(81, 24)} = \frac{24}{3} = 8, \quad b = \frac{81}{(81, 24)} = \frac{81}{3} = 27.$$

Passo $3_{T_{IV}}$**:** Aplicar o *Algoritmo de Euclides Estendido*, para determinar os inteiros x_1 e x_2, tais que

$$x_1 \cdot a + x_2 \cdot b = x_1 \cdot 8 + x_2 \cdot 27 = 1.$$

Aplicando o algoritmo de Euclides. Inicialmente, efetuamos a divisão $27 = 8 \cdot 3 + 3$ e colocamos os números envolvidos no seguinte diagrama:

	3	
27	8	
3		

A seguir, continuamos efetuando a divisão $8 = 3 \cdot 2 + 2$ e colocamos os números envolvidos no diagrama

	3	2
27	8	3
3	2	

Prosseguindo, enquanto for possível, teremos

	3	2	1	2
27	8	3	2	1
3	2	1	0	

até algum r_n dividir r_{n-1}. Assim, $(8, 27) = 1$, ou seja, o máximo divisor comum de 8 e 27 é o último resto não-nulo no processo de divisão.

Observe que, o *Algoritmo de Euclides* fornece-nos:

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ 2 &= 8 - 2 \cdot 3 \\ 3 &= 27 - 3 \cdot 8. \end{aligned}$$

Donde se segue que

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (8 - 2 \cdot 3) \\ &= 3 \cdot 3 - 1 \cdot 8 \\ &= (27 - 3 \cdot 8) \cdot 3 - 1 \cdot 8 \\ &= (-10) \cdot 8 + 3 \cdot 27. \end{aligned}$$

Portanto,

$$\begin{array}{rcccl} r_n & = & (a,b) & = & x_1 a + x_2 b \\ 1 & = & (8,27) & = & x_1 \cdot 8 + x_2 \cdot 27 \\ 1 & = & (8,27) & = & (-10) \cdot 8 + 3 \cdot 27. \end{array}$$

Assim, $x_1 = -10$ e $x_2 = 3$.

Passo $4_{T_{IV}}$**:** Determinar a solução através da fórmula:

$$\begin{aligned} x &= c_1 x_1 a + c_2 x_2 b \\ x &= 38 \cdot (-10) \cdot 8 + 11 \cdot 3 \cdot 27 \\ x &= -2149 \\ x &\equiv -2149 \equiv 443 \bmod [81, 24]. \end{aligned}$$

Uma solução é, portanto, $x = 443$.

5.2 Resolução de Sistema de Congruências Lineares com Duas Variáveis

5.2.1 Técnica I- Redução a uma única equação de congruência com duas variáveis

O objetivo aqui é apresentar um método de reduzir um Sistema de Congruências Lineares da forma

$$\begin{cases} x + y &\equiv c_1 \bmod m_1 \\ x + y &\equiv c_2 \bmod m_2 \\ \vdots & \\ x + y &\equiv c_r \bmod m_r \end{cases} \tag{5.3}$$

onde $c_1, \cdots, c_k, m_1, \cdots, m_k$ são inteiros fixados, com $m_i > 0$ para todo $i = 1, 2, \cdots, r$, a uma única congruência.

Note que, pela Proposição 3.9 item (b) isto é possível desde que:

$$c_1 = c_2 = \cdots = c_r.$$

Desta forma, se para o sistema (5.3) tivermos que $m_i - c_i = k$ para todo $i = 1, \cdots r$, onde k é uma constate qualquer, então podemos obter um sistema compatível com a Proposição 3.9 item (b).

De fato, para isto, basta somar-se o número k em ambas equações do sistema de congruências.

$$\begin{cases} x+y &\equiv c_1 \bmod m_1 \\ x+y &\equiv c_2 \bmod m_2 \\ \vdots & \\ x+y &\equiv c_r \bmod m_r \end{cases} \Leftrightarrow \begin{cases} x+y+k &\equiv c_1+k \bmod m_1 \\ x+y+k &\equiv c_2+k \bmod m_2 \\ \vdots & \\ x+y+k &\equiv c_r+k \bmod m_r \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} x+y+k &\equiv c_1+k \equiv 0 \mod m_1 \\ x+y+k &\equiv c_2+k \equiv 0 \mod m_2 \\ \vdots & \\ x+y+k &\equiv c_r+k \equiv 0 \mod m_r \end{cases} \Leftrightarrow \begin{cases} x+y+k &\equiv 0 \bmod m_1 \\ x+y+k &\equiv 0 \bmod m_2 \\ \vdots & \\ x+y+k &\equiv 0 \bmod m_r. \end{cases}$$

Logo, pela Proposição 3.9 item (b), temos uma única equação de congruência da forma $x+y+k \equiv 0 \bmod [m_1, m_2, \cdots, m_r]$, onde $i = 1, 2, \cdots, r$.

Portanto, as soluções do sistema é dado por $x+y+k = [m_1, m_2, \cdots, m_r] \cdot t$, onde $t \in \mathbb{Z}$.

Exemplo 50. Encontre as soluções do sistema de congruências

$$\begin{cases} x+y &\equiv 2 \bmod 3 \\ x+y &\equiv 3 \bmod 4 \\ x+y &\equiv 4 \bmod 5. \end{cases}$$

Solução: Observe que, $x \equiv m-1 \bmod m \Leftrightarrow x+1 \equiv m \bmod m$, mas $m \equiv 0 \bmod m$. Logo, $x+1 \equiv 0 \bmod m, \forall m \in \mathbb{N}$.

Assim,

$$\begin{cases} x+y+1 &\equiv 2+1 \bmod 3 \\ x+y+1 &\equiv 3+1 \bmod 4 \\ x+y+1 &\equiv 4+1 \bmod 5 \end{cases} \Leftrightarrow \begin{cases} x+y+1 &\equiv 0 \bmod 3 \\ x+y+1 &\equiv 0 \bmod 4 \\ x+y+1 &\equiv 0 \bmod 5 \end{cases}$$

e pela Proposição 3.9 item (b), o sistema é equivalente à congruência $x+y+1 \equiv 0 \bmod [3,4,5]$. Como $[3,4,5] = 60$, temos que $x+y+1 \equiv 0 \bmod 60$.

Logo,

$$\begin{aligned} x+y+1 \equiv 0 \bmod 60 &\Leftrightarrow x+y+1-1 \equiv 0-1 \bmod 60 \\ &\Leftrightarrow x+y \equiv -1 \bmod 60 \\ &\Leftrightarrow x+y \equiv 59 \bmod 60. \end{aligned}$$

Para o sistema possuir solução a congruência $x + y \equiv 59 \bmod 60$ deve possuir solução.

Como $d = (1, 1, 60) = 1$ divide $c = 59$, temos que a congruência admite solução.

O Corolário 4.1 garante uma única solução x para cada um dos m valores incongruentes de y. Como $(a, m) = (1, 60) = 1$. Escrevemos a congruência da forma, $x \equiv 59 - y \bmod 60$.

Assim, para cada valor de y fixo temos uma congruência da forma $ax \equiv c \bmod m$ onde $c = 59 - y$ e como $(1, 60) = 1 \Rightarrow x \equiv 59 - y \bmod 59$ tem uma única solução para cada y fixado.

Lembre que um número inteiro y é congruente módulo m a um único número do conjunto $\{0, 1, \cdots, 59\}$. Ou seja, que a menos de congruência, podemos considerar que y assume apenas os números de 0 a 59.

Vamos exibir a solução para o caso $y = 0$ as demais seguem de forma análoga. Para $y = 0$, temos que $x \equiv 59 - 0 \bmod 60 \Leftrightarrow x \equiv 59 \bmod 60$. Logo, $x_0 = 59$.

Portanto, para cada $y \in \{0, 1, \cdots, 59\}$ temos uma solução incongruente a $x \equiv 59 - y \bmod 60$. Logo, temos 60 pares de soluções do problema inicial.

5.2.2 Técnica II- Módulos iguais

Essa técnica é semelhante a resolução de sistema de equações do 1º grau, com duas incógnitas, utilizando o método da adição. Este busca juntar as duas equações em uma única equação, eliminando uma das incógnitas. Para isso, é necessário que os coeficientes de uma das incógnitas sejam opostos, isto é, devem ter o mesmo valor e sinais contrários.

Se tratando de sistema de congruências com duas variáveis vamos utilizar o método desenvolvido na demonstração do Teorema 4.4 para obter a solução, quando houver. Para aplicar essa técnica devemos observar o módulo de cada equação de congruência, pois é necessário que os módulos sejam iguais.

Para facilitar a resolução de sistemas da forma

$$\begin{cases} ax + by & \equiv r \bmod m \\ cx + dy & \equiv s \bmod m \end{cases}$$

apresentamos a seguir uma sequência de passos.

Passo $1_{T_{II}}$**:** Verificar se o sistema admite solução, ou seja, $(ad - bc, m) = 1$.

Passo $2_{T_{II}}$**:** Multiplicar a primeira congruência do sistema por d, a segunda congruência por b, e subtrair a segunda equação de congruência da primeira. Obtém-se $(ad - bc)x \equiv dr - bs \bmod m$.

Passo $3_{T_{II}}$**:** Resolva a equação do **Passo** $2_{T_{II}}$ obtendo o valor de x.

Passo $4_{T_{II}}$**:** Para determinar o valor de y, devemos multiplicar a primeira congruência pelo valor de c, e a segunda pelo valor de a, e subtrair a segunda equação de congruência da primeira. Obtém-se $(ad - bc)y \equiv as - cr \bmod m$.

Passo $5_{T_{II}}$**:** Resolva a equação do **Passo** $4_{T_{II}}$ obtendo o valor de y.

Passo $6_{T_{II}}$**:** Escrever a solução do sistema $S = \begin{pmatrix} x \\ y \end{pmatrix}$.

Vejamos o exemplo a seguir:

Exemplo 51. (Extraído do Livro do BURTON) Encontre as soluções do sistema de congruências

$$\begin{cases} 3x + 4y & \equiv & 5 \bmod 13 \\ 2x + 5y & \equiv & 7 \bmod 13. \end{cases}$$

Solução: **Passo** $1_{T_{II}}$**:** Como $(3 \cdot 5 - 4 \cdot 2, 13) = (7, 13) = 1$, o sistema admite solução e é única módulo $m = 13$.

Passo $2_{T_{II}}$**:** Multiplicar a primeira congruência pelo valor de $d = 5$, a segunda por $b = 4$, e subtrair a segunda congruência da primeira.

$$(3 \cdot 5 - 4 \cdot 2) \cdot x \equiv 5 \cdot 5 - 4 \cdot 7 \bmod 13 \Leftrightarrow 7x \equiv -3 \bmod 13.$$

Passo $3_{T_{II}}$**:** Resolver a equação: $7x \equiv -3 \bmod 13$.

$$\begin{aligned} 7x \equiv -3 \bmod 13 &\Leftrightarrow 7x \cdot 2 \equiv (-3) \cdot 2 \bmod 13 \\ &\Leftrightarrow 14x \equiv -6 \bmod 13 \\ &\Leftrightarrow x \equiv 7 \bmod 13. \end{aligned}$$

Logo, o valor de $x = 7$.

Passo $4_{T_{II}}$**:** Determinar o valor para y. Multiplicar a primeira congruência pelo valor de $c = 2$, e a segunda pelo valor de $a = 3$ e subtrair a segunda equação de congruência da primeira.

$$(3 \cdot 5 - 4 \cdot 2) \cdot y \equiv 3 \cdot 7 - 2 \cdot 5 \bmod 13 \Leftrightarrow 7y \equiv 11 \bmod 13.$$

Passo $5_{T_{II}}$**:** Resolver a equação: $7y \equiv 11 \bmod 13$.

$$\begin{aligned} 7y \equiv 11 \bmod 13 &\Leftrightarrow 7y \cdot 2 \equiv 11 \cdot 2 \bmod 13 \\ &\Leftrightarrow 14y \equiv 22 \bmod 13 \\ &\Leftrightarrow y \equiv 9 \bmod 13. \end{aligned}$$

Logo, o valor de $y = 9$.

Passo $6_{T_{II}}$**:** Portanto, a solução única do sistema é $x \equiv 7 \bmod 13$ e $y \equiv 9 \bmod 13$, ou seja, $S = \begin{pmatrix} 7 \\ 9 \end{pmatrix}$.

5.2.3 Técnica III- Utilizando mais de uma Técnica

Nesta seção, nosso objetivo é mostrar que podemos utilizar a combinação de técnicas no processo de resolução de um Sistema de Congruências Lineares com duas variáveis.

Vejamos o exemplo a seguir.

Exemplo 52. Encontre as soluções do sistema de congruências, caso exista,

$$\begin{cases} x+y & \equiv & 5 \bmod 7 \\ x+y & \equiv & 6 \bmod 8 \\ 2x+3y & \equiv & 8 \bmod 56. \end{cases}$$

Solução: Observe que, nas duas primeiras equações de congruências podemos usar a Técnica I, para Sistema de Congruências Lineares com duas variáveis.

Note que, $x \equiv m-2 \bmod m \Leftrightarrow x+2 \equiv m \bmod m$, mas $m \equiv 0 \bmod m$. logo, $x+2 \equiv 0 \bmod m, \forall m \in \mathbb{N}$.

Daí,

$$\begin{cases} x+y+2 & \equiv & 5+2 \bmod 7 \\ x+y+2 & \equiv & 6+2 \bmod 8 \end{cases} \Leftrightarrow \begin{cases} x+y+2 & \equiv & 0 \bmod 7 \\ x+y+2 & \equiv & 0 \bmod 8 \end{cases}$$

e pela Proposição 3.9 item (b), o sistema é equivalente à congruência

$x+y+2 \equiv 0 \bmod [7,8]$. Como $[7,8]=56$, temos que $x+y+2 \equiv 0 \bmod 56$.

Logo,

$$\begin{aligned} x+y+2 \equiv 0 \bmod 56 &\Leftrightarrow x+y+2-2 \equiv 0-2 \bmod 56 \\ &\Leftrightarrow x+y \equiv -2+56 \bmod 56 \\ &\Leftrightarrow x+y \equiv 54 \bmod 56. \end{aligned}$$

Assim, a solução das duas primeiras equações de conguências do sistema é dado por: $x+y \equiv 54 \bmod 56$.

Agora, vamos escrever o novo sistema, ou seja,

$$\begin{cases} x+y & \equiv & 54 \bmod 56 \\ 2x+3y & \equiv & 8 \bmod 56. \end{cases}$$

Perceba que o novo sistema formado possui o mesmo módulo, logo podemos aplicar a Técnica II - (Módulos iguais) para resolvê-lo.

Passo $1_{T_{II}}$**:** Como $(1 \cdot 3 - 1 \cdot 2, 56) = (1, 56) = 1$, o sistema admite solução e é única módulo $m = 56$.

Passo $2_{T_{II}}$**:** Multiplicar a primeira congruência pelo valor de $d = 3$, a segunda por $b = 1$, e subtrair a segunda congruência da primeira.

$$(1 \cdot 3 - 1 \cdot 2) \cdot x \equiv 3 \cdot 54 - 1 \cdot 8 \bmod 56 \Leftrightarrow x \equiv 154 \bmod 56.$$

Passo $3_{T_{II}}$**:** Resolver a equação: $x \equiv 154 \bmod 56$.

$$\begin{aligned} x \equiv 154 \bmod 56 &\Leftrightarrow x \equiv 154 - 56 \bmod 56 \\ &\Leftrightarrow x \equiv 98 - 56 \bmod 56 \\ &\Leftrightarrow x \equiv 42 \bmod 56. \end{aligned}$$

Logo, o valor de $x = 42$.

Passo $4_{T_{II}}$**:** Determinar o valor para y. Multiplicar a primeira congruência pelo valor de $c = 2$, e a segunda pelo valor de $a = 1$ e subtrair a segunda equação de congruência da primeira.

$$(1 \cdot 3 - 1 \cdot 2) \cdot y \equiv 1 \cdot 8 - 2 \cdot 54 \bmod 56 \Leftrightarrow y \equiv -100 \bmod 56.$$

Passo $5_{T_{II}}$**:** Resolver a equação: $y \equiv -100 \bmod 56$.

$$\begin{aligned} y \equiv -100 \bmod 56 &\Leftrightarrow y \equiv -100 + 56 \bmod 56 \\ &\Leftrightarrow y \equiv -44 + 56 \bmod 56 \\ &\Leftrightarrow y \equiv 12 \bmod 56. \end{aligned}$$

Logo, o valor de $y = 12$.

Passo $6_{T_{II}}$**:** Portanto, a solução única do sistema é $x \equiv 42 \bmod 56$ e $y \equiv 12 \bmod 56$, ou seja, $S = \begin{pmatrix} 42 \\ 12 \end{pmatrix}$.

6 Considerações Finais

A Matemática é uma ciência fantástica, pois ela nos permite mesmo nesse momento pandêmico mostrar sua beleza. Vimos por meio dos noticiários a representação do número de casos de contaminação por covid-19 através de tabelas, gráficos e curvas que potencializaram escrever modelos matemáticos que permitem fazer projeções e isso possibilitou visualizar a real situação que estava ocorrendo no mundo.

Nessas tabelas tínhamos as informações como número de infectados, recuperados, óbitos, coeficiente de incidência, coeficiente de mortalidade e principalmente ocupação hospitalar.

Diante disso, foi possível além de verificar a rapidez que o vírus se propaga, identificar a deficiência do Sistema de Saúde Pública. E assim, os representantes do poder puderam tomar medidas restritivas como decretar o lockdown, aumentar a quantidade de leitos através dos Hospitais de campanha, abrir novos leitos de UTI, solicitar urgência pela imunização, calcular a quantidade de imunizante, solicitar urgência e tentar reduzir o tempo de fabricação, prever o tempo de imunização da população. Além disso, também foi possível acompanhar aos reflexos dessa situação na economia e como isso afetou de forma direta e indireta as famílias brasileiras.

E a Educação? foi afetada? O que mudou? Diante dessa situação, Escola, professores e alunos tiveram que se readaptar, reinventar, ressignificar de forma instantânea. Não pense que foi fácil até aqui. Muitas angustias, incertezas, ..., mas tenho certeza que em nenhum momento os professores desistiram, estiveram e estão sempre buscando fazer o melhor, mesmo com todas as dificuldades, seja, emocionais, financeiras e da própria escassez de material físico e informatizado.

Nesse panorama, destacamos não só a importância dessa Ciência, a Matemática, que mesmo em tempos remotos vem contribuindo com suas descobertas e criando novas ferramentas, mas também a importância de os professores permanecerem em formação contínua para que aperfeiçoem suas práticas pedagógicas. Desta maneira Delors *et al.* (1996) coloca que:

> A qualidade de ensino é determinada tanto ou mais pela formação contínua dos professores, do que pela sua formação inicial... A formação contínua não deve desenrolar-se, necessariamente, apenas no quadro do sistema educativo: um período de trabalho ou de estudo no setor econômico pode também ser proveitoso para aproximação do saber e do saber-fazer (DELORS *et al.*, 1996, p.160).

Nesse sentido, acreditamos que a nosso objetivo foi alcançado quando elaboramos um material de apoio que possibilite ao professor aprofundar seus conhecimentos sobre

Teoria dos Números, mais especificamente sobre aritmética dos Restos, no que diz respeito a Resolução de Sistemas de Congruências Lineares.

Neste material o leitor terá a oportunidade de conhecer com detalhes cada técnica de resolução, suas especificidades e como aplicar cada uma. Para escolher uma técnica é preciso fazer uma análise prévia, observar a forma em que o sistema está apresentado, ou seja, na forma completa, onde apresenta todos os coeficientes ou na forma reduzida (equivalente).

Para todas as técnicas o sistema precisa estar na forma reduzida, ou seja, o valor de a deve ser 1. E para transformar um sistema completo em um equivalente utilizamos várias ferramentas que foram enunciadas nos capítulos III e IV. Mas antes de transformá-lo, é necessário verificar se o sistema admite solução, pois se uma das equações de congruência não admite solução o próprio sistema também não possuirá. E quando não percebemos isso, é muito provável que mesmo não havendo solução realizamos diversos cálculos.

Nesse sentido, afim de evitar que façamos cálculos desnecessários, que elaboramos em cada técnica, uma sequência de passos que busque direcionar o leitor a não esquecer de nenhum detalhe importante que comprometa o desenvolvimento para se chegar a solução, caso exista, do sistema.

Com estes passos é possível também analisar qual a técnica melhor se adapta para cada sistema. Às vezes é possível utilizar apenas uma, mais de uma ou até mesmo fazer combinações de técnicas para se obter a solução de um sistema. Porém, dependendo da escolha o processo se torna mais trabalhoso e com isso menos ágil.

Neste material, também procuramos ressaltar a importância de se conhecer a ou as condições necessárias de cada técnica apresentada, pois a partir disso é possível escolher a mais eficiente e prática.

Finalizamos com a apresentação das técnicas de resolução de Sistema de Congruências Lineares com duas variáveis, ou seja, ao invés de apresentarmos uma solução para o sistema, apresentam pares de soluções, o que torna um diferencial para nosso trabalho.

Referências

BARBOSA, J. L. M. Geometria euclidiana plana. coleção do professor de matemática. **Rio de Janeiro: SBM**, 2006. Citado na página 33.

BOYER, C. B.; MERZBACH, U. C. **História da matemática**. [S.l.]: Editora Blucher, 2012. Citado 7 vezes nas páginas 21, 22, 23, 24, 25, 26 e 27.

BRASIL. **Base Nacional Comum Curricular**. [s.n.], 2017. Disponível em: <http://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf>. Citado 3 vezes nas páginas 29, 30 e 69.

BURTON, D. **Teoria elementar dos números .** [S.l.]: Grupo Gen-LTC, 2016. Citado 6 vezes nas páginas 21, 22, 23, 46, 55 e 56.

DELORS, J. *et al.* Relatório para a unesco da comissão internacional sobre educação para o século xxi. **Educação um tesouro a descobrir**, v. 6, 1996. Citado na página 99.

EVES, H. W. **Introdução à história da matemática**. [S.l.]: Editora Unicamp, 1995. Citado 7 vezes nas páginas 21, 22, 24, 25, 33, 54 e 55.

FILHO, A. L. d. S. **Teorema Chinês dos Restos**. Dissertação (Mestrado) — Universidade Federal do Maranhão, 2015. Citado na página 18.

GLAESER, G. Epistemologia dos números relativos. **Boletim GEPEM**, n. 57, jun. 2010. Disponível em: <https://periodicos.ufrrj.br/index.php/gepem/article/view/302>. Citado na página 24.

GLÓRIA, W. d. S. **Teorema Chinês dos Restos: ensino e aplicação**. Dissertação (Mestrado) — Universidade Federal do Amazonas, 2019. Citado na página 18.

GROENWALD, C. L. O.; SAUER, L. de O. Desenvolvendo o pensamento aritmético utilizando os conceitos da teoria dos números. **Acta Scientiae. Revista de Ensino de Ciências e Matemática**, v. 7, n. 1, p. 93–102, 2005. Citado na página 31.

HEFEZ, A. **Aritmética: Coleçao PROFMAT**. Rio de Janeiro: SBM, 2013. v. 1ª Ediçao. Citado 9 vezes nas páginas 25, 26, 34, 42, 43, 44, 51, 52 e 58.

JÚNIOR, C. C. B. **O Teorema Chinês dos Restos: uma abordagem voltada para olimpíadas de Matemática com aplicações em Criptografia RSA**. Dissertação (Mestrado) — Universidade Federal Rural de Pernambuco, 2020. Citado na página 18.

MEDEIROS, A.; MEDEIROS, C. Números negativos: uma história de incertezas. **Bolema-Boletim de Educação Matemática**, v. 7, n. 8, p. 49–59, 1992. Citado na página 25.

MOL, R. S. **Introdução à história da matemática**. [S.l.]: Belo Horizonte: CAED-UFMG, 2013. 140 p. Citado na página 21.

PRAZERES, S. B. d. **O Teorema Chinês dos Restos e a partilha de senhas**. Dissertação (Mestrado) — Universidade Federal Rural de Pernambuco, 2014. Citado na página 18.

REZENDE, M. R. **Re-significando a disciplina teoria dos números na formação do professor de matemática na licenciatura.2007**. 281 p. Tese (Doutorado em Educação) — Pontifícia Universidade Católica de São Paulo, 2007. Citado na página 29.

SALAZAR, M. S. **Rupturas no estatuto dos números negativos- o caso da Ingraterra**. Dissertação (Mestrado) — UFRJ: Universidade Federal do Rio de Janeiro, 2019. Citado na página 25.

SANTOS, A. d. **Teorema Chinês dos Restos e aplicações**. Dissertação (Mestrado) — Universidade Federal do Amazonas, 2017. Citado na página 18.

SBM, S. B. D. M. **Contribuição da SBM para a discussão dobre currículo de Matemática.** 2015. 8 p. Citado na página 30.

STRUIK, D. J.; GUERREIRO, J. S.; VIEIRA, M. J. **História concisa das matemáticas**. [S.l.]: Gradiva, 1992. Citado na página 24.