UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS FLORIANÓPOLIS
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

FRANKLIN PEDRO DA SILVA NETO

Criptografia RSA: Uma Proposta de Aplicação no Ensino Médio

Florianópolis
2025

FRANKLIN PEDRO DA SILVA NETO

Criptografia RSA: Uma Proposta de Aplicação no Ensino Médio

Dissertação submetida ao Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT da Universidade Federal de Santa Catarina para a obtenção do Grau de Mestre em Matemática. Com área de concentração no Ensino de Matemática.
Orientador: Prof. Felipe Lopes Castro, Dr.
Coorientador: Prof. Marcos André Braz Vaz, Dr.

Florianópolis
2025

Ficha catalográfica gerada por meio de sistema automatizado gerenciado pela BU/UFSC.
Dados inseridos pelo próprio autor.

da Silva Neto, Franklin Pedro
Criptografia RSA : Uma Proposta de Aplicação no Ensino Médio / Franklin Pedro da Silva Neto ; orientador, Felipe Lopes Castro, coorientador, Marcos André Braz Vaz, 2025.
92 p.

Dissertação (mestrado profissional) - Universidade Federal de Santa Catarina, Centro de Ciências Físicas e Matemáticas, Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Florianópolis, 2025.

Inclui referências.

1. Matemática. 2. Ensino de Matemática. 3. Teoria dos Números. 4. Aritmética Modular. 5. Criptografia RSA. I. Castro, Felipe Lopes. II. Vaz, Marcos André Braz. III. Universidade Federal de Santa Catarina. Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT. IV. Título.

FRANKLIN PEDRO DA SILVA NETO

Criptografia RSA: Uma Proposta de Aplicação no Ensino Médio

O presente trabalho em nível de mestrado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Profª. Maria Inez Cardoso Gonçalves, Drª.
Universidade Federal de Santa Catarina

Prof. Mario Rodolfo Roldan Daquilema, Dr.
Universidade Federal de Santa Catarina

Profª. Thaís Bardini Idalino, Drª.
Universidade Federal de Santa Catarina

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de Mestre em Matemática. Com área de concentração no Ensino de Matemática.

ICP-Edu
Documento assinado digitalmente
Sergio Tadao Martins
Data: 04/02/2026 09:32:51-0300
CPF: ***.598.118-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Dr Sérgio Tadao Martins
Coordenador do Programa

ICP-Edu
Documento assinado digitalmente
Felipe Lopes Castro
Data: 03/02/2026 16:10:51-0300
CPF: ***.060.710-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Felipe Lopes Castro, Dr.
Orientador

GOV.BR
Documento assinado digitalmente
MARCOS ANDRE BRAZ VAZ
Data: 03/02/2026 17:47:24-0300
CPF: ***.140.748-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Marcos André Braz Vaz, Dr.
Coorientador

Florianópolis, 2025.

Este trabalho é dedicado aos meus colegas de classe e aos meus queridos pais.

AGRADECIMENTOS

Primeiramente agradeço a minha família, que sempre me ajudou, me incentivou e me colaborou durante todo o mestrado. A todos meus colegas professores de matemática durante minha jornada, especialmente o mestre Alexsandro, que me incentivou a fazer o ENA em 2022 e o mestre Alex, que me ajudou enormemente durante o primeiro ano do mestrado. Ao orientador da dissertação, prof. Felipe Lopes Castro, que aceitou orientar minha dissertação, mesmo quando o tema já havia sido escolhido e o desenvolvimento já havia começado a ser escrito. Suas orientações foram fundamentais. Ao coorientador da dissertação, prof. Marcos André Braz Vaz, que orientou em todo o entorno da dissertação e auxiliou bastante em partes que eu certamente não conseguiria sozinho. Ao meu colega "sobrevivente"do PROFMAT, André, que colaborou nos estudos para o ENQ e nos estudos durante todo o segundo ano de mestrado. Aos membros da banca, prof. Thais, prof. Maria Inez e prof. Mário, por ter aceitado a avaliação dessa dissertação. Durante a reta final da escrita dessa dissertação, passei por uma grande redescoberta em minha vida e por uma mudança de paradigma. Agradeço a todos os meus amigos que me ajudaram a lidar com tudo isso, para que eu pudesse terminar e defender essa dissertação com a tranquilidade e seriedade necessárias. A todos os meus amigos e outros colegas, obrigado pela eventual ajuda!

"Cryptography without system integrity is like investing in an armored car to carry money between a customer living in a cardboard box and a person doing business on a park bench."

(Gene SPAFFORD, 1997)

RESUMO

Essa dissertação tem como objetivo o estudo da Criptografia RSA, com a produção de uma apostila voltada ao ensino médio. Para isso, são apresentados todos seus pré-requisitos: Divisibilidade e divisão euclidiana; máximo divisor comum e algoritmo de Euclides; equações diofantinas; números primos; congruências; Teorema de Euler e o Pequeno Teorema de Fermat; congruências lineares; teorema chinês dos restos.

Em seguida, aborda-se a criptografia, com o seu contexto histórico resumido, até chegarmos na atualidade, que é a criptografia RSA. Em relação a ela, são descritas todas as etapas para codificar e decodificar mensagens, além de ser feita a verificação do seu funcionamento e de possíveis situações onde sua segurança pode ser comprometida. A apostila produzida contém todos os conteúdos presentes na dissertação, de forma mais contextualizada.

Palavras-chave: Teoria dos Números. Aritmética Modular. Criptografia RSA.

ABSTRACT

This dissertation aims to study the RSA Criptography, with the development of a booklet, aimed to high school students. For that, it's presented all of its prerequisites: Divisibility and the Euclidean division; greater common divisor and the Euclidean algorithm; diophantine equations; prime numbers; congruences; Euler's Theorem and the Fermat's Little Theorem; linear congruences; the chinese remainder theorem.

Subsequently, the criptography is addressed, with its historical context summarized, until the present, which is the RSA criptography. About it, it's described all the stages to code and to decode messages, in addition to verify its operation and to see possible situations where the security may be compromised. The booklet developed contains all the contents presents in the dissertation, in a more contextualized way.

Keywords: Number Theory. Modular Arithmetic. RSA Criptography.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Em toda a história da criptografia, presente em Carneiro (2017), Singh (1999), entre outros, um dos métodos criptográficos mais recentes e atualmente o mais usado no dia-a-dia é a **Criptografia RSA**, que, de acordo com Severino Collier Coutinho (2015), *"[...] se trata do mais utilizado dos métodos de criptografia atualmente em uso"*. Esse método, dentre os métodos criptográficos, é um dos que mais usa conceitos matemáticos, pois é bem voltado a **Teoria dos Números**. Ainda de acordo com Severino Collier Coutinho (2015), *"[...] até os anos 1960, a teoria dos números, que é a parte da matemática mais utilizada nas aplicações à criptografia, era considerada quase que destituída de utilidade prática"*.

Criptografia é uma palavra que deriva do grego, junção das palavras *kryptos* (oculto, secreto) e *graphein* (escrever). Sobre isso:

> A Criptografia está silenciosamente presente na vida de muitas pessoas. A abordagem deste tema se mostra sobremaneira importante dada a sua vasta aplicação prática, além de uma crescente necessidade de enviar dados seguros de maneira segura, principalmente pela Internet. (OLIVEIRA LOPES; SILVEIRA LOPES, 2018)

Com relação a Teoria dos Números, Resende e Machado (2012) afirmam que a Teoria dos Números atende vários objetivos, dentre eles:

- "Tópicos de Teoria dos Números estão presentes na educação básica", principalmente os referentes aos números naturais e aos números inteiros.
- "A Teoria dos Números é um espaço propício para o desenvolvimento de ideias matemáticas relevantes relativas aos números naturais e algumas também estendidas aos inteiros, presentes na matemática escolar", principalmente os referentes a divisibilidade e aos números primos.
- "A Teoria dos Números é um campo propício para uma abordagem mais ampla da prova", pois permite aos estudantes trabalharem em um "território conhecido", que são os conteúdos relacionados aos números inteiros.

Apesar disso, a Teoria dos Números:

> "[...]é vista como uma componente curricular muito abstrata, sofisticada e sem muito espaço para as aplicações e o uso da criatividade e da inovação. Isso acaba gerando uma grande aversão nos alunos, fazendo com que acreditem que é algo difícil, distante da realidade e, muitas vezes, sem utilidades, onde quem aprende ou a compreende é considerado uma pessoa diferente" (OLIVEIRA LOPES; SILVEIRA LOPES, 2018).

Além disso:

> "A apresentação da Teoria dos Números de maneira usual e abstrata é, certamente, um dos motivos para as dificuldades no seu aprendizado. Muitas vezes, são utilizadas apenas simbologias e manipulações inerentes da linguagem matemática desconectadas de significados para os alunos." (OLIVEIRA LOPES; SILVEIRA LOPES, 2018)

Discutir a Teoria dos Números, especialmente a Aritmética Modular, no ensino básico é relevante porque "a Aritmética Modular veio a ocupar-se como uma classe mais vasta de problemas que surgiram naturalmente, a partir de muitos estudos, para facilitar suas aplicações na vida cotidiana das pessoas." (Pontes; Silva, L. M. da, 2020)

Como a Criptografia RSA usa muitos conteúdos relacionados à Aritmética Modular e à Teoria dos Números em geral e, além disso, como muitos dos conteúdos que fazem parte da aritmética modular não fazem parte do currículo presente na Base Nacional Comum Curricular (BNCC)[1], a proposta dessa dissertação é mobilizarmos conceitos relativos a Teoria dos Números e a Aritmética Modular com o intuito de compreendermos todos os detalhes referentes à Criptografia RSA. Isso deve ser feito de forma prática, pois "os problemas de Matemática desenvolvidos em sala de aula, muitas vezes, têm sido conduzidos de forma tradicional e sem correlação com o cotidiano, fato este que gera total desmotivação dos envolvidos no processo." (Pontes; Silva, L. M. da, 2020). Além disso, "[...]percebe-se a necessidade de se tratar o ensino de matemática de forma contextualizada e não apenas como um conjunto de exercícios obrigatórios e sem relação imediata com o dia a dia." (Pontes; Silva, L. M. da, 2020)

Para que essa mobilização de conceitos seja feita adequadamente, será produzida uma *apostila* contendo todos os conceitos preliminares e todos os detalhes que norteiam todas as áreas a serem trabalhadas.

O desenvolvimento da dissertação será dividido em três capítulos, com a apostila estando presente no apêndice dessa dissertação:

- O primeiro capítulo trata da Teoria dos Números, no que tange à divisibilidade, da divisão Euclidiana, do máximo divisor comum e do algoritmo de Euclides, das equações Diofantinas e dos números primos. O primeiro capítulo também trata da Aritmética Modular, no que tange à congruências, os teoremas de Euler e de Fermat, as congruências lineares e o teorema chinês dos restos. Este capítulo traz vários Teoremas, Proposições, Propriedades, Lemas e Corolários, todos devidamente demonstrados.
- O segundo capítulo trata da Criptografia no seu contexto histórico, com o passar dos séculos, até chegarmos a atualidade.
- O terceiro capítulo trata mais especificamente da Criptografia RSA, tendo presente o passo-a-passo necessário para saber como codificar e como decodificar uma mensagem por esse sistema.

1.1 JUSTIFICATIVA

Na graduação em matemática, geralmente a primeira fase (semestre) contém a disciplina/cadeira que contempla os conteúdos presentes na Teoria dos Números (na UFSC se chamava Fundamentos da Matemática e, atualmente, Fundamentos da Aritmética). A depen-

[1] A Base Nacional Comum Curricular é acessível em: <https://basenacionalcomum.mec.gov.br/>.

der do currículo do curso de matemática dessas universidades, essa cadeira pode incluir a Aritmética Modular ou não.

Pessoalmente, quando tive essa cadeira, achei bastante interessante, especialmente os conteúdos de aritmética modular, ao ponto de ter desejado ver esses conteúdos no ensino médio. Dez anos depois, já no PROFMAT, coube a mim fazer uma apresentação sobre a criptografia RSA e ao fazer a pesquisa e preparar a apresentação, também achei o conteúdo bastante interessante e também um conteúdo que pode tranquilamente ser passado e explicado para alunos do ensino básico (ensino médio principalmente). Mas o problema é que muitos dos conteúdos que são "pré-requisitos" para poder explicar a criptografia RSA são conteúdos que não estão presentes na BNCC, ou seja, normalmente esses alunos nunca verão esses conteúdos a não ser que eles escolham um curso na universidade que tenha alguma cadeira relacionada (como computação).

Então para que seja possível e viável fazer a apresentação e explicação da criptografia RSA com os alunos do ensino médio, é obrigatório ter que explicar os principais conteúdos da Teoria dos Números e todos os conteúdos da Aritmética Modular. Disso saiu a motivação para fazer essa dissertação. Não basta simplesmente passar a definição da criptografia RSA e seu passo-a-passo para os alunos sem nenhum tipo de preambulo e conteúdos prévios, é necessário passar tudo que é necessário para eles. Por causa disso, como produto educacional/pedagógico, será feita uma apostila, para que o professor(a) que quiser apresentar a criptografia RSA para seus alunos, tenha um material adequado e apropriado para servir de referência, contendo todos os conteúdos prévios necessários.

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Investigar o potencial pedagógico da Teoria dos Números e da Aritmética Modular como base para o ensino introdutório da Criptografia RSA, por meio do desenvolvimento de uma apostila didática voltada para estudantes da educação básica.

1.2.2 Objetivos Específicos

- Selecionar e organizar os conceitos fundamentais da Teoria dos Números e da Aritmética Modular que contribuam para a compreensão da Criptografia RSA.
- Elaborar um resumo da história da criptografia.
- Analisar e explicar a Criptografia RSA, com todos os passos necessários.
- Elaborar uma apostila didática que apresente os fundamentos da Criptografia RSA de forma acessível e contextualizada para estudantes da educação básica.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 REVISÃO SISTEMÁTICA

De acordo com Gil (2008) e Prodanov e De Freitas (2013), é importante e essencial que uma revisão sistemática da bibliografia com uma abordagem qualitativa utilize as plataformas digitais que produzem e publicam textos científicos.

Para fazermos tal revisão, foi utilizada a Análise Textual Discursiva (ATD), proposta por Moraes e Galiazzi (2006) e separada em três fases:

- Unitarização: Cada "resultado" é lapidado via extração de excertos relevantes ao tema.
- Categorização: Separar os conteúdos de análise, verificando as semelhanças e diferenças entre os temas.
- Comunicação: Exposição dos pontos descritos na categorização.

Para ser possível fazer a unitarização, foram utilizados o Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES)[1], o Google Acadêmico[2] e o portal *Scientific Electronic Library Online* (SCIELO)[3]. Foi inicialmente utilizado um recorte temporal de 5 anos (2019 até 2024), sendo ampliado conforme os resultados foram aparecendo. Essa pesquisa não se restringiu a artigos, sendo escolhidos Trabalhos de Conclusão de Curso (TCCs) e Dissertações[4].

A pesquisa inicial usou duas ou três das palavras-chaves a seguir: *Criptografia, RSA, Python*, com o uso da função busca avançada em cada banco de pesquisa. Apesar dessa dissertação e do produto educacional não ter uma seção específica voltada para o uso da linguagem *Python*, considerou-se o termo para busca pois esta linguagem é utilizada em aplicações da Criptografia RSA. Foram escolhidos os textos que mais tiveram similaridade com as palavras-chave descritas acima. Após os textos serem escolhidos, foi feita uma análise mais detalhada dos mesmos com a intenção de verificar a similaridade entre eles e ao tema de pesquisa.

Dos textos pesquisados, focando-se nos que tinham similaridade com o tema proposto: "Criptografia", "Criptografia RSA", "Software Python", "Aplicações em sala de aula", foram encontrados um certo número de textos, os quais foram divididos em:

- Artigos: 3
- TCCs: 2
- Dissertações: 6

Vamos denominá-los de T_1 até T_{11}, sendo que T_1 até T_3 serão artigos, T_4 e T_5 serão TCCs e T_6 até T_{11} serão as dissertações.

[1] O Portal de Períodicos da CAPES é acessível em <https://www.periodicos.capes.gov.br/>.
[2] O portal Google Acadêmico é acessível em <https:\scholar.google.com:.
[3] O portal SCIELO é acessível em <https://www.scielo.br/>.
[4] Tais dissertações foram extraídas de <https://profmat-sbm.org.br/dissertacoes/>.

Tabela 1 – Textos selecionados pelo autor

Nº	**Título**	**Autores**	**Tipo**	**Ano**
T_1	The power of the snake: number theory with Python	Markus Reitenbach	Artigo	2022
T_2	Criptografia: Uma possibilidade para o ensino de função inversa	Idemar Vizolli, Euvaldo de Souza Carvalho, Onésimo Rodrigues Pereira	Artigo	2019
T_3	Introdução da Criptografia no Ensino Médio e Fundamental utilizando Aritmética Modular	Luis Antonio da Silva Vasconcellos, João Fernando Montanher	Artigo	2022
T_4	Criptografia RSA: Uma proposta de interdisciplinaridade	Valdigley Ferreira Campos	TCC	2020
T_5	Fundamentos Matemáticos Aplicado a Alguns Métodos de Criptografia	Eugênio Carlos Rosa Rocha	TCC	2008
T_6	Aritmética com Python	Rogério da Silva Cavalcante	Dissertação	2018
T_7	Uso da Criptografia RSA no Ensino de Matemática	Alex Almeida Rosa	Dissertação	2023
T_8	O Estudo da Criptografia RSA no Ensino Básico com Auxílio de Softwares Computacionais	MARCEL CAVALCANTE CERQUEIRA	Dissertação	2016
T_9	Criptografia e algumas aplicações em sala de aula	Andresa Laurett da Silva	Dissertação	2021
T_{10}	Criptografia RSA para o Ensino Médio	Eliton Mendes Pedrosa Simes	Dissertação	2023
T_{11}	Divisibilidade e Congruência Modular	André Walter	Dissertação	2019

Fonte: Elaborado pelo autor.

Baseado nos três "campos" presentes nessa pesquisa: "Criptografia", "Python", "Ensino", foram obtidos as informações a seguir:

Tabela 2 – Campos de estudo dos textos selecionados pelo autor

Campo de Estudo	**Textos**
Criptografia	T_2, T_3, T_4, T_5, T_7, T_8, T_9, T_{10}, T_{11}
Python	T_1, T_6, T_8
Ensino	T_2, T_3, T_4, T_7, T_8, T_9, T_{10}

Fonte: Elaborado pelo autor.

Observando a Tabela 2, observa-se que muitos textos possuem mais de um campo de estudo em comum, sendo a maioria deles relacionando o campo "Criptografia" e com o campo "Ensino", mas apenas o texto T_8 possui os três campos de estudo em comum.

Baseada no tópico de "comunicação" da Análise Textual Descritiva, segue uma síntese de cada um desses textos, com ênfase na relação dos mesmos com o tema.

Com respeito ao T_1, Reitenbach (2022) mostra as inúmeras aplicações da Teoria dos Números que podem ser feitas através do software Python, na questão de divisão euclidiana, de mdc/mmc, de congruências, de inversos multiplicativos, do Teorema Chinês dos Restos, entre outros, sendo que todos (ou a maioria desses tópicos) são aplicados em criptografia, ou, nas palavras do autor, a criptografia é a *teoria dos números aplicada*.

Com respeito ao T_2, Vizolli, Souza Carvalho e Pereira (2019) mostra a relação intrínseca entre a criptografia RSA com o conceito de função inversa, até porque pode-se entender que se a codificação de uma mensagem é uma função, então, logicamente, sua decodificação é a sua função inversa.

Ademais, é um bom viés para se tratar com alunos de ensino médio no ensino de matemática, pois exime a necessidade de ter que ensiná-los todos os conceitos de aritmética modular.

Com respeito ao T_3, Silva Vasconcellos e Montanher (2022) passa todos os conceitos necessários de aritmética modular para mostrar as várias facetas em que ela é aplicada, como CPF, cartão de crédito, código de barras e criptografia, dando uma breve explicação do método RSA e descrevendo como essas aplicações podem ser feitas em sala de aula, tendo opções para o Fundamental II e para o Ensino Médio.

Com respeito ao T_4, Campos (2020) faz toda uma fundamentação teórica referente à aritmética modular, à criptografia em geral e a criptografia RSA mais especificamente, para, em seguida, propor um projeto interdisciplinar envolvendo este conteúdo usando alunos de vários cursos superiores que tenham uma disciplina de Teoria dos Números como parte de seu currículo, tais como Matemática, Engenharias, Computação, etc.

Essa proposta de projeto interdisciplinar envolve uma dinâmica feita em grupos, onde cada grupo é responsável por uma etapa da criptografia, que vai desde gerar as chaves usadas, codificar uma frase, tentar "quebrar" tal código para, no fim, fazer a decodificação correta.

Com respeito ao T_5, Rocha (2008) descreve muitos dos métodos criptográficos existen-

tes, tais como: métodos matriciais, métodos que envolvem permutação, métodos utilizando cifras, métodos utilizando a aritmética modular (RSA incluso), entre outros. Na explicação de alguns métodos mais antigos, o autor ressalta que atualmente, com o advento dos computadores, esses métodos ficaram meio "ultrapassados", pois um computador avançado consegue quebrar esse código com relativa facilidade, mas são úteis num viés didático.

O autor ainda mostra toda a questão envolvendo números primos e como determinar números primos grandes, para tornar os métodos criptográficos que utilizem tais números, cada vez mais difíceis de serem quebrados.

Com respeito ao T_6, Cavalcante (2018) traz toda uma introdução à linguagem de programação Python, explicando como que essa linguagem é concebida e fundamentada, com explicação sobre suas estruturas e como realizar procedimentos matemáticos. Além disso, o autor visa trazer uma aplicação dessa linguagem com alguns tópicos relacionados a Aritmética, que, segundo o próprio autor, "[...] a lógica transita naturalmente entre a computação e a matemática, mostrando desta maneira uma interdisciplinariedade nata entre esses assuntos".

Tais aplicações envolvem a divisão euclidiana, a representação de números em bases diferentes, o conceito de MDC e de números primos. Em cada um desses tópicos, o autor realiza uma revisão teórica bem fundamentada para, na sequência, mostrar como tais tópicos são usados na linguagem Python.

Com respeito ao T_7, Rosa (2023), tal como muitos dos textos anteriores, faz toda uma contextualização geral sobre a criptografia (RSA inclusa), desde suas origens, seus fundamentos, seus preâmbulos, como codificar e decodificar, sua eficiência, suas aplicações, entre outros. Como proposta pedagógica, o autor propõe uma sequência didática que utiliza recursos computacionais via aplicativos de *smartphone* que auxiliem em muitos procedimentos, tais como aplicativos que auxiliem a realizar cálculos que envolvem aritmética modular, aplicativos que respondem se determinado número é primo ou não, aplicativos que permitem gerar números primos grandes e aplicativos que permitem conhecer e usar outros métodos criptográficos existentes. O autor também, além da sequência didática, propõe um minicurso sobre aritmética modular para auxiliar os integrantes nesse curso (os estudantes) sobre esse conteúdo. A sequência didática, além de utilizar os aplicativos acima descritos, utiliza outros recursos (filme, crivos criptográficos em papel, entre outros) para mostrar de forma bem didática e detalhada tudo que tange a criptografia.

Com respeito ao T_8, Cerqueira (2016) também realiza toda uma fundamentação teórica sobre teoria dos números e sobre aritmética modular e toda uma contextualização sobre a criptografia RSA. Focando na proposta pedagógica, o autor apresenta uma proposta pedagógica composta de cinco momentos. Usando uma proposta construtivista, o autor propõe nesses momentos fazer todo um contexto histórico da criptográfica e sua utilização em vários momentos da história geral, mostrar a Cifra de César (o primeiro instrumento criptográfico), com aplicação no software *Geogebra*, fazer uma explicação do conteúdo de aritmética modular, porque é essencial ter essa noção para aprender a criptografia RSA.

Sobre essa criptografia, o autor apresenta o conteúdo através da resolução de alguns problemas, em que cada problema representa uma "etapa" da criptografia. No último momento, o autor propõe alguns problemas envolvendo passos da criptografia que envolvem a linguagem de programação *Python*.

Com respeito ao T_9, Andresa Laurett da Silva (2021) também se propõe a fazer uma revisão teórica sobre a teoria dos números e a criptografia. A autora também se propõe a pôr na revisão elementos de álgebra linear e de álgebra abstrata (anéis e grupos). Estes conteúdos são importantes para a explicação de alguns métodos criptográficos que a autora apresenta mais para a frente no seu trabalho. Deste modo, a autora de fato faz uma fundamentação teórica de tudo o que é necessário para o pleno entendimento de todos os métodos criptográficos que foram apresentados.

Tais métodos envolvem transformações lineares, transformações de dígrafos, sistemas simétricos, sistemas assimétricos, no que se inclui o RSA e o Logaritmo Discreto. No que tange as aplicações propostas pela autora para o primeiro ano do ensino médio, a mesma se propõe no uso da criptografia como tema motivador para o conteúdo de funções, principalmente pela função inversa, até porque, como dito antes, se a codificação é uma função, a decodificação é a sua função inversa. Para o segundo ano, a autora propõe atividades que utilizem o conceito de permutação e o conceito de probabilidade, para explicar principalmente os métodos de substituição e transposição. Em cada uma das duas propostas, a autora aplica uma atividade avaliativa e realiza a análise dessas atividades, com opiniões dos alunos.

Com respeito ao T_{10}, Simes (2023) desenvolve a fundamentação teórica de forma bem completa, colocando contexto histórico, apresentando os diversos métodos criptográficos, descrevendo a parte relevante ao conteúdo presente na Teoria dos Números e na aritmética modular, além de fazer uma explicação bem conceituada sobre todo o passo-a-passo da criptografia RSA e explicar a garantia e a segurança do funcionamento da mesma.

Quanto à proposta didática, o autor apresenta uma sequência didática muito bem formatada, diagramada e sistematizada. Cada aula (das 6 propostas) tem todo um desenvolvimento, com a metodologia e com atividades propostas. Foi feita também uma análise dos resultados das atividades que foram entregues pelos alunos. O autor fez algo deveras interessante, que foi aplicar a mesma sequência didática para alunos dos anos do ensino médio (1º, 2º e 3º). Em todos os casos, o autor montou tabelas para mostrar a porcentagem de questões acertadas (totalmente e parcialmente) dos alunos, com uma consolidação dos dados feita ao final.

Com respeito ao T_{11}, Walter (2019) foca num conteúdo ora "ignorado" nos outros textos presentes nessa revisão: na parte da divisibilidade. O autor faz toda uma fundamentação teórica do conteúdo, com apresentação de proposições, teoremas e propriedades, todas demonstradas formalmente. O autor também teoriza praticamente todos os conteúdos sobre a Teoria dos Números (mdc, primos, equações Diofantinas lineares e não-lineares, além da aritmética modular).

O autor, ao final do trabalho, apresenta algumas discussões que apareceram em ques-

tões de Divisibilidade e de Equações Diofantinas nos vestibulares. Bem, segundo ele, são "Vestibulares", mas na prática só tem questões do vestibular de uma instituição (Instituto Militar de Engenharia), sendo que existem muitas outras questões de ENEM (Exame Nacional do Ensino Médio), de vestibular ou de olimpíadas que envolvem esses conteúdos, embora as questões presentes estejam bem respondidas e com fácil entendimento.

3 CONSTRUINDO UM MATERIAL PEDAGÓGICO (APOSTILA)

Sob a perspectiva dos estudos realizados anteriormente e mediante a necessidade dos alunos em aprofundarem mais os conceitos presentes no desenvolvimento, foi elaborado o produto educacional, em forma de apostila, para que seja utilizado em sala de aula. O material presente no anexo desse trabalho é de livre acesso a todos que desejarem e/ou precisarem. O propósito dessa apostila é de mostrar todos os conceitos preliminares da criptografia RSA de forma simples, fácil de entender, para que não haja problemas em executar os passos da codificação.

3.1 DO PÚBLICO ALVO

Essa apostila é sugerida para o ensino médio, para ser usada em sala de aula, preferencialmente por alunos do terceiro ano do ensino médio. Embora muitos dos conteúdos presentes na apostila sejam conteúdos vistos no ensino fundamental II, outros conteúdos são conteúdos que não são vistos no ensino médio e por isso, é necessária uma maior "maturidade" por parte dos leitores.

A utilização e aplicação dessa apostila pode ser usada em turmas de 1º e 2º ano, caso o professor deseje, para usar alguns dos conceitos apresentados ou para trazer uma forma mais simplificada desses conceitos, mesmo que não seja o objetivo principal dessa apostila.

3.2 DOS ASSUNTOS ABORDADOS

A apostila contém um prefácio, além de 4 capítulos:

1) Teoria dos Números
2) Aritmética Modular
3) Criptografia
4) Criptografia RSA

Em cada capítulo, os conteúdos serão semelhantes aos presentes no desenvolvimento, embora mais simplificado, sem as demonstrações e com exemplos e exercícios de fixação.

No capítulo 1, **Teoria dos Números**, serão tratados os conteúdos de divisibilidade, da divisão euclidiana, do máximo divisor comum e do algoritmo de Euclides, das equações diofantinas e dos números primos.

No capitulo 2, **Aritmética Modular**, serão tratados os conteúdos de congruências, os teoremas de Euler e de Fermat, as congruências lineares e o teorema chinês dos restos.

No capítulo 3, **Criptografia**, será tratado todo o contexto histórico da criptografia com o passar dos séculos, até chegarmos a atualidade.

No capítulo 4, **Criptografia RSA**, será tratado, passo-a-passo, como codificar e como decodificar uma mensagem por esse sistema.

Conforme dito acima, todos os capítulos terão exercícios de fixação, com as respostas dos mesmos presentes no final da apostila.

3.3 DA METODOLOGIA E DA APLICAÇÃO

A metodologia escolhida é a de apresentar o conteúdo presente na apostila de forma expositiva e dialogada, com explicações e resolução dos exercícios.

Essa explicação, principalmente do capítulo 1 da apostila, é importante de ser feita corretamente, pois ela é necessária para os próximos conteúdos, que não estão presentes no currículo do ensino médio e por isso deve ser tratado com mais cautela por parte do professor.

A proposta para os capítulos 1 e 2 da apostila é de ser aplicado em três ou quatro aulas, a depender do nível de entendimento dos alunos, sendo duas aulas voltadas à explicação do conteúdo presente, e uma ou duas aulas voltadas a resolução dos exercícios presentes na apostila. Cada professor que for aplicar pode, se quiser, trazer exercícios que não estejam presentes na apostila.

Como o capítulo 3 só contém o contexto histórico da criptografia, o professor pode optar por deixar como tarefa a leitura desse capítulo e posterior discussão em sala de aula, ou ler e explicar o conteúdo presente em sala de aula junto com os alunos.

O capítulo 4 é melhor aplicado seguindo a dinâmica presente no capítulo com os alunos, que facilitará o entendimento acerca da criptografia RSA por parte dos alunos. O ideal é que a sequência presente no capítulo seja respeitada, para que não tenha nenhum problema na decodificação da mensagem.

4 DESENVOLVIMENTO

4.1 DIVISIBILIDADE

Definição 4.1. Dados dois números inteiros a e b, dizemos que a *divide* b, e escrevemos $a \mid b$, se existir $c \in \mathbb{Z}$ tal que $b = a \cdot c$. De forma simbólica

$$a \mid b \iff \exists c \in \mathbb{Z}, b = a \cdot c.$$

Quando $a \mid b$, também dizemos que:

- a é divisor de b;
- a divide b;
- a é fator de b; e
- b é múltiplo de a.

Observação 4.2. Para todo $a \in \mathbb{Z}$, como $a = a \cdot 1$, logo tem-se que $1 \mid a$ e $a \mid a$. Também vale que $a \mid 0$, para todos $a \in \mathbb{Z}$, pois $0 = a \cdot 0$.

4.1.1 Propriedades da Divisibilidade

Proposição 4.3. *Sejam a,b,$c \in \mathbb{Z}$, então as seguintes propriedades são válidas:*

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

b) *Se $a \mid b$, então $ac \mid bc$.*

c) *Se $a, b \in \mathbb{N}$, $a \mid b$ e $b \mid a$, então $a = b$.*

d) *Se $a \mid b$ e $c \mid d$, então $ac \mid bd$.*

e) *Se $a \mid (b + c)$ e $a \mid b$, então $a \mid c$.*

f) *Se $a \mid (b - c)$ e $a \mid b$, então $a \mid c$.*

g) *Se $a \mid b$ e $a \mid c$, então $a \mid \alpha b + \beta c$, para quais $\alpha, \beta \in \mathbb{Z}$.*

h) *Se $a \mid b$, então $|a| \leq |b|$.*

Demonstração. **a)** Se $a \mid b$, então existe $k \in \mathbb{Z}$, tal que $b = a \cdot k$.

Por outro lado, se $b \mid c$ então existe $l \in \mathbb{Z}$, tal que $c = b \cdot l$.

Logo, $c = b \cdot l = (a \cdot k) \cdot l$. Reorganizando, obtemos $c = a \cdot (k \cdot l)$, ou seja, chamando $k \cdot l$ de m, $c = a \cdot m$, o que implica em $a \mid c$.

b) Se $a \mid b$ então $b = a \cdot k$, para algum $k \in \mathbb{Z}$. Multiplicando os dois lados da igualdade por $c \in \mathbb{Z}$, obtemos $b \cdot c = (a \cdot k) \cdot c$. Reorganizando, obtemos $b \cdot c = (a \cdot c) \cdot k$. Ou seja, $ac \mid bc$.

c) Se $a \mid b$ então existe $c \in \mathbb{N}$ tal que $b = a \cdot c$. Se $b \mid a$ então existe $k \in \mathbb{N}$ tal que $a = b \cdot k$.

Ou seja, $b = a \cdot c = (b \cdot k) \cdot c = b \cdot (k \cdot c)$, ou seja, $k \cdot c = 1$. Como ambos são naturais, temos que $c = 1$ e $k = 1$. Portanto, $a = b$.

d) Se $a \mid b$ então existe $k \in \mathbb{Z}$ tal que $b = a \cdot k$ e se $c \mid d$ então existe $l \in \mathbb{Z}$ tal que $d = c \cdot l$. Pegando as duas desigualdades e multiplicando uma pela outra, obtemos $b \cdot d = a \cdot k \cdot c \cdot l$. Reorganizando, obtemos $b \cdot d = a \cdot c \cdot (k \cdot l)$. Portanto, $a \cdot c \mid b \cdot d$.

e) Se $a \mid b + c$ então existe $k \in \mathbb{Z}$ tal que $b + c = a \cdot k$. Ainda, se $a \mid b$, então existe $l \in \mathbb{Z}$ tal que $b = a \cdot l$. Substituindo b na primeira igualdade, obtemos $a \cdot l + c = a \cdot k$. Ou seja, $c = a \cdot k - a \cdot l = a \cdot (k - l)$. Como k e l são inteiros, então $k - l$ também é inteiro. Portanto $c = a \cdot (k - l)$ e $a \mid c$.

f) Se $a \mid b - c$ então existe $k \in \mathbb{Z}$ tal que $b - c = a \cdot k$. Ainda, se $a \mid b$, então existe $l \in \mathbb{Z}$ tal que $b = a \cdot l$. Substituindo b na primeira igualdade, obtemos $a \cdot l - c = a \cdot k$. Ou seja, $c = a \cdot l - a \cdot k = a \cdot (l - k)$. Como l e k são inteiros, então $l - k$ também é inteiro. Portanto $c = a \cdot (l - k)$ e $a \mid c$.

g) Como $a \mid b$, então existe $k \in \mathbb{Z}$ tal que $b = a \cdot k$. Como $a \mid c$, então existe $l \in \mathbb{Z}$ tal que $c = a \cdot l$. Multiplicando ambos os lados da primeira igualdade por α e multiplicando ambos os lados da segunda igualdade por β, obtemos $\alpha b = \alpha \cdot a \cdot k$ e $\beta \cdot c = \beta \cdot a \cdot l$. Se somarmos essas duas igualdades, obtemos

$$\alpha \cdot b + \beta \cdot c = \alpha \cdot a \cdot k + \beta \cdot a \cdot l = a(\alpha \cdot k + \beta \cdot l)$$

Portanto, $a \mid \alpha b + \beta c$.

h) Como $a \mid b$ então existe $l \in \mathbb{Z}$ tal que$b = a \cdot l$. Se tomarmos os módulos em ambos os lados da igualdade, obtemos $|b| = |a| \cdot |l|$. Como $a \neq 0$ e $b \neq 0$, por definição, temos que $l \neq 0$, logo, $|l|$ deve ser maior ou igual a 1, $|l| \geq 1$. Portanto, $|a| \leq |b||l| = |b|$.

□

4.1.2 Divisão Euclidiana

Para mostrarmos que a divisão Euclidiana é válida, precisamos do Princípio da Boa Ordenação e da Propriedade Arquimediana.

Definição 4.4. Seja S um subconjunto de $\mathbb{N}$. Um número $a \in \mathbb{N}$ é chamado de *menor elemento* de S, se satisfaz:

i) $a \in S$; e

ii) $a \leq x$ para todo $x \in S$.

Observação 4.5. Se S tem um menor elemento, então esse elemento é único. De fato, se a e a' são dois elementos que satisfazem i) e ii) então:

- $a \leq a'$ (pois a é menor elemento)
- $a' \leq a$ (pois a' é menor elemento).
  Assim, segue que $a = a'$.

Sabendo disso, temos o *Principio da Boa Ordenação*.

Princípio 4.6 (Principio da Boa Ordenação)**.** *Todo subconjunto não-vazio do conjunto dos números naturais admite um elemento menor.*

Proposição 4.7 (Propriedade Arquimediana em $\mathbb{Z}$). *Dados $a, b \in \mathbb{Z}$, com $a > 0$ e $b \neq 0$, então existe $n \in \mathbb{N}$ tal que*

$$n \cdot a \geq b.$$

Demonstração. [1] Vamos supor que a afirmação não é verdadeira, de modo que para todo natural n, $n \cdot a < b$. Logo, o conjunto:

$$S = \{b - na \mid n \in \mathbb{N}\}$$

é formado apenas por números naturais. Pelo Principio 4.6 (PBO), S possui menor elemento, digamos, $m = \min(S)$. Como $m \in S$, existe um $n_0 \in \mathbb{N}$ tal que $m = b - n_0 a$. Por outro lado, o elemento $m_1 = b - (n_0 + 1)a$ pertence a S, pois S contém todos os elementos dessa forma. Além disso,

$$m_1 = b - (n_0 + 1)a = b - n_0 a - a = m - a < m$$

pois $a > 0$. Assim $m_1 \in \mathbb{N}$ e $m_1 < m$, o que contraria o fato de m se o menor elemento de S. Assim, temos que $n \cdot a \geq b$. □

Teorema 4.8 (Divisão Euclidiana). *Sejam a,$b \in \mathbb{Z}$, com $b \neq 0$. Então existem* únicos *números inteiros q e r tais que:*

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

Na divisão Euclidiana de a por b, a é chamado *dividendo*, b é chamado *divisor*, q é chamado *quociente* e r é chamado de *resto*.

Demonstração. Precisamos provar duas coisas: Que esses dois números inteiros **existem** e que eles são **únicos**.

Existência: Considere o conjunto

$$S = \{a - b \cdot q; q \in \mathbb{Z}\} \cap \mathbb{N}.$$

Como $b \neq 0$, pela Propriedade Arquimediana (Proposição 4.7) existe $n \in \mathbb{N}$ tal que $b \cdot n > -a$. Multiplicando por -1, obtemos que $b \cdot (-n) < a$, assim $a - b \cdot (-n) > 0$. Portanto, S é um subconjunto de $\mathbb{N}$ não-vazio e, pelo Princípio da Boa Ordenação (Proposição 4.6), existe $r \in S$ elemento menor, ou seja, tal que

$$r \leq x, \text{ para todo } x \in S$$

Como $r \in S$, existe $q \in \mathbb{Z}$ tal que $r = a - qb$. Assim, $a = bq + r$, com $r \geq 0$. Vamos verificar que r satisfaz a propriedade desejada.

[1] Retirado de (Vieira, 2020)

Suponhamos (*por absurdo*) que $r \geq |b|$, assim $r' = r - |b| \geq 0$ e, como $b \neq 0$, $r' < r$. Como $a = b \cdot q + r$, logo

$$r' = r - |b| = (a + b \cdot q) - |b| = a - b \cdot \left(\frac{|b|}{b} - q \right).$$

Deste modo, $r' \in S$ e $r' < r$, o que é um absurdo, pois r é o elemento menor de S. Assim nossa suposição é falsa e, portanto, $r < |b|$.

Unicidade: Suponha que existam q_1, q_2, r_1 e r_2 tais que

$$a = b \cdot q_1 + r_1, \text{ com } 0 \leq r_1 < |b|$$

e

$$a = b \cdot q_2 + r_2, \text{ com } 0 \leq r_2 < |b|$$

Vamos provar que $r_1 = r_2$ e $q_1 = q_2$.

Assim, temos que $-|b| < -r_1 \leq r_2 - r_1 \leq r_2 < |b|$. Ou seja, $|r_2 - r_1| < |b|$.

Mas, da suposição inicial, $bq_1 + r_1 = bq_2 + r_2$, o que é equivalente a $b(q_1 - q_2) = r_2 - r_1$. Colocando módulos dos dois lados, obtemos:

$$|b||q_1 - q_2| = |r_2 - r_1| < |b|$$

Como $|b| > 0$, cancelando $|b|$, obtemos que $|q_1 - q_2| < 1$. Essa desigualdade só é possível quando $q_1 = q_2$. Consequentemente, $r_2 - r_1 = b(q_1 - q_2) = 0$ e, portanto, $r_1 = r_2$. □

4.2 MÁXIMO DIVISOR COMUM

Vamos definir o que é o Máximo Divisor Comum e depois demonstrar que ele de fato existe e é único.

Definição 4.9. Sejam a,$b \in \mathbb{Z}$. Chamamos de *Máximo Divisor Comum* (ou MDC), o maior divisor comum desses dois inteiros, ou seja, o MDC de a e b é um número d que satisfaz:

1. $d \geq 0$.
2. $d \mid a$ e $d \mid b$.
3. Se $d' \mid a$ e $d' \mid b$ então $d' \mid d$.

Denotaremos o MDC entre a e b por $\mathrm{mdc}(a, b)$.

Proposição 4.10. *Dados a,b,$c \in \mathbb{Z}$. Então temos que:*

1. *Se $a \mid b$ e $b \neq 0$, então $|a| \leq |b|$.*
2. $\mathrm{mdc}(0,a) = |a|$.
3. $\mathrm{mdc}(1,a) = 1$.
4. *$a \mid b$ e $a \neq 0$, então* $\mathrm{mdc}(a,b) = a$.

Demonstração.

1. Como $a \mid b$, logo $|a| \mid |b|$. Deste modo, existe $n \in \mathbb{N}$ tal que $|a| \cdot n = |b|$. Como $b \neq 0$, logo $n \neq 0$. Assim, $1 \leq n$ e, multiplicando por $|a|$, segue que $|a| \leq |a| \cdot n$, ou seja, $|a| \leq |b|$.

   Assim, de fato, o MDC entre dois números não nulos é o *maior* divisor comum.

2. Pela definição de mdc, o $\mathrm{mdc}(0,a)$ deve ser um número que divida 0 e divida a. Qualquer inteiro a divide 0. Então, dado a, os divisores de a são também divisores de 0. O maior divisor de a é $|a|$, ou seja, $\mathrm{mdc}(0,a) = |a|$.

3. Pela definição de mdc, o $\mathrm{mdc}(1,a)$ deve ser um número que divida 1 e divida a. Os únicos divisores de 1 é ± 1. O número 1 divide qualquer inteiro a, mas o único inteiro que divide 1 é o próprio número 1. Portanto, $\mathrm{mdc}(1,a) = 1$.

4. De fato, se $a \mid b$, temos que $|a|$ é um divisor comum de a e b, e se c é um divisor comum de a e b, então c divide $|a|$, o que mostra que $|a|$ é igual a $\mathrm{mdc}(a,b)$. □

Vamos agora demonstrar que esse MDC de fato existe.

Teorema 4.11 (Existência do MDC). *Dados quaisquer dois inteiros a e b, existe um número natural d que é o máximo divisor comum de a e de b.*

Demonstração. Se $a = 0$ ou $b = 0$, por Proposição 4.10 sabemos quem é $\mathrm{mdc}(a, b)$.

Se $a, b \neq 0$, então consideramos o conjunto $L = \{ax + by \mid x,y \in \mathbb{Z}\} \cap \mathbb{N}^*$. Se, por exemplo, fizermos $x = a$ e $y = b$ então $a^2 + b^2$ pertence a L e, portanto, L não é vazio. Pelo Princípio da Boa Ordenação (Proposição 4.6), L tem menor elemento d. Vamos mostrar que d é o máximo divisor comum de a e b.

- Temos que d é maior do que zero.
- Como d pertence à L, então podemos escrever $d = ax_0 + by_0$, com x_0 e y_0 inteiros. Aplicando o algoritmo da divisão, temos que

  $$a = dq + r, \text{ com } 0 \leq r < d$$

  e daí

  $$a = (ax_0 + by_0)q + r$$

  ou ainda,

  $$r = a(1 - qx_0) + b(-y_0q)$$

  Logo, $r = 0$ ou $r \in L$. Como $r < d$ e d é o menor elemento de L, logo $r \notin L$ e, então, $r = 0$, o que implica que $a = dq$ e, portanto, $d \mid a$.

  Analogamente, prova-se que $d \mid b$.

- Seja d' um número inteiro tal que $d' \mid a$ e $d' \mid b$, então $a = x_1d'$, para algum $x_1 \in \mathbb{Z}$ e $b = y_1d'$, para algum $y_1 \in \mathbb{Z}$. Como $d = ax_0 + by_0$, então $d = (x_1d')x_0 + (y_1d')y_0 = (x_1x_0)d' + (y_1y_0)d' = d'(x_1x_0 + y_1y_0)$. Com isso, $d = d'(x_1x_0 + y_1y_0)$ e $d' \mid d$.

Isso finaliza a demonstração. □

Definição 4.12. Dois números a,$b \in \mathbb{Z}$ são considerados **coprimos** (ou **primos entre si**) se $\mathrm{mdc}(a,b) = 1$.

Lema 4.13. *(Lema de Euclides) Sejam a e b inteiros com $b \neq 0$, q e r respectivamente o quociente e o resto da divisão de a por b, isto é,*

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

Então

$$\mathrm{mdc}(a,b) = \mathrm{mdc}(b,r), \text{ ou } \mathrm{mdc}(a,b) = \mathrm{mdc}(b, a - bq)$$

Demonstração. [2]

Suponha $d = \mathrm{mdc}(a,b)$. Vamos mostrar que $d = \mathrm{mdc}(b,r)$. De fato,

- Como $d = \mathrm{mdc}(a,b)$, logo $d \mid a$ e $d \mid b$, então segue das propriedades da divisibilidade que, $d \mid (a - bq)$, ou seja, $d \mid r$.

  Assim d é um divisor comum de b e r;

- Seja d' um inteiro, tal que $d' \mid b$ e $d' \mid r$, logo $d' \mid (bq + r)$, assim $d' \mid a$. Como $d = \mathrm{mdc}(a,b)$ e d' é divisor comum de a e b, segue da definição de MDC, que $d' \mid d$.

□

Esse lema é importante para desenvolvermos um algoritmo que permita calcular o MDC entre dois números grandes.

O próximo teorema é também importante para o algoritmo mencionado acima.

Teorema 4.14 (de Bézout[3]). *Sejam a_1,a_2,...,a_n números inteiros. Defina o conjunto:*

$$S = \left\{ \sum_{i=1}^{n} a_i x_i \;\middle|\; x_i \in \mathbb{Z}, 1 \leq i \leq n \right\}$$

Se $d = \mathrm{mdc}(a_1,a_2,\ldots,a_n)$, então S é igual ao conjunto dos múltiplos de d. Como caso particular, existem u_1,u_2,...,$u_n \in \mathbb{Z}$ tais que

$$d = a_1u_1 + a_2u_2 + \cdots + a_nu_n$$

Demonstração. [4] Vamos chamar de $\mathcal{D}$ o conjunto de todos os múltiplos de d. Como $d \geq 0$, $\mathcal{D} = \{0, d, 2d, 3d, \ldots\}$. Precisamos provar que $\mathcal{D} \subseteq S$ e $S \subseteq \mathcal{D}$.

Como d é o MDC de a_1,a_2,...,a_n então $d \mid a_1$, $d \mid a_2$, ..., $d \mid a_n$. Por uma propriedade da divisibilidade, podemos afirmar que $d \mid a_1x_1 + a_2x_2 + \cdots + a_nx_n$, para quaisquer x_1,x_2,...,$x_n \in \mathbb{Z}$. Com isso, temos que $S \subseteq \mathcal{D}$.

[2] Retirado de BEZERRA et al. (2018)

[3] *Étienne Bézout* foi um matemático francês do Século XVIII, especializado em Aritmética e em Geometria Algébrica

[4] Demonstração baseada no escrito em Neto (2012)

Para mostrar a outra inclusão, note que S contém inteiros positivos, pois, escolhendo $x_1 = a_1$ e $x_2 = x_3 = \cdots = x_n = 0$, concluímos que $a_1^2 \in S$. Como S contém inteiros positivos, vamos chamar de d' o menor desses inteiros positivos, que existe pelo Princípio da Boa Ordenação (Proposição 4.6). Se mostrarmos que $d' = d$, teremos mostrado a outra inclusão.

Afirmação: $d' \mid a_1,a_2,\ldots,a_n$.

De fato, como $d' \in S$, $d' = a_1u_1 + a_2u_2 + \cdots + a_nu_n$, para $u_1,u_2,\ldots,u_n \in \mathbb{Z}$. Agora, tome $a_1 = d'q + r$, com $q,r \in \mathbb{Z}$ e $0 \leq r < d'$. Então:

$$\begin{aligned} r &= a_1 - d'q \\ &= a_1 - (a_1u_1 + a_2u_2 + \cdots + a_nu_n)q \\ &= a_1(1 - u_1q) + a_2(-u_2q) + \cdots + a_n(-u_nq) \end{aligned}$$

Ou seja, $r \in S$. Como d' é o menor inteiro positivo de S, o fato de $0 < r < d'$ seria uma contradição. Logo, $r = 0$ e com isso, $d' \mid a_1$. Analogamente, prova-se que $d' \mid a_2,\ldots,a_n$.

Como d' é um divisor comum de $a_1,a_2,\ldots,a_n$, para mostrarmos que $d' = d$, note que como d' é o menor inteiro positivo de S então, $d' \leq d$. Se mostrarmos que $d' \geq d$, teremos a igualdade desejada.

Temos que $a_1 = dq_1,a_2 = dq_2,\ldots,a_n = dq_n$, com $q_1,q_2,\ldots,q_n \in \mathbb{Z}$. Ou seja,

$$\begin{aligned} d' &= a_1u_1 + a_2u_2 + \cdots + a_nu_n \\ &= dq_1u_1 + dq_2u_2 + \cdots + dq_nu_n \\ &= d(a_1u_1 + a_2u_2 + \cdots + a_nu_n), \end{aligned}$$

ou seja, $0 < d \mid d'$. Com isso, $d' \geq d$ e $d = d'$. Isso mostra que $\mathcal{D} \subseteq S$ e, portanto, que $\mathcal{D} = S$. □

Com isso, existem $u_1,u_2,\ldots,u_n \in \mathbb{Z}$ tais que

$$d = a_1u_1 + a_2u_2 + \cdots + a_nu_n$$

Vamos ver alguns resultados adicionais sobre o mdc.

Proposição 4.15. *Dados $a,b \in \mathbb{Z}$. Então temos que*

1. *Dado $n \in \mathbb{N}$, $\mathrm{mdc}(na,nb) = n \cdot \mathrm{mdc}(a,b)$.*
2. *Se $a \neq 0$ ou $b \neq 0$, então os números $\dfrac{a}{\mathrm{mdc}(a,b)}$ e $\dfrac{b}{\mathrm{mdc}(a,b)}$ são coprimos, ou seja,*

$$\mathrm{mdc}\left(\frac{a}{\mathrm{mdc}(a,b)},\frac{b}{\mathrm{mdc}(a,b)}\right) = 1$$

3. *(Lema de Gauss) Se $a \mid bc$ e $\mathrm{mdc}(a,b) = 1$ então $a \mid c$.*

4. *Se* $a \mid c$, $b \mid c$ *e* $\mathrm{mdc}(a,b) = 1$ *então* $ab \mid c$.

Demonstração. 1. Considere o conjunto $L = \{ax + by \mid x,y \in \mathbb{Z}\}$. Vimos no Teorema de Bézout (Proposição 4.14) que em L existem números positivos, sendo $d = \mathrm{mdc}(a,b)$ o menor deles. Vamos agora considerar o conjunto $L' = \{(na)x + (nb)y \mid x,y \in \mathbb{Z}\}$, onde $n \in \mathbb{N}$.

   Mas $L' = \{n(ax + by) \mid x,y \in \mathbb{Z}\}$, ou seja, $L' = n \cdot L$. Como L admite menor elemento positivo (d), L' também admite (d'), e como $L' = nL$, logo $d' = nd$. Por outro lado, pela definição de L', temos que $d' = \mathrm{mdc}(na,nb)$. Portanto, temos que $\mathrm{mdc}(na, nb) = n \cdot \mathrm{mdc}(a,b)$.

2. Como $a \neq 0$ ou $b \neq 0$, logo $\mathrm{mdc}(a, b) \neq 0$, assim pelo item anterior, temos que

$$\begin{aligned}\mathrm{mdc}(a,b) &= \mathrm{mdc}\left(\mathrm{mdc}(a,b) \cdot \frac{a}{\mathrm{mdc}(a,b)}, \mathrm{mdc}(a,b) \cdot \frac{b}{\mathrm{mdc}(a,b)}\right) \\ &= \mathrm{mdc}(a,b) \cdot \mathrm{mdc}\left(\frac{a}{\mathrm{mdc}(a,b)}, \frac{b}{\mathrm{mdc}(a,b)}\right),\end{aligned}$$

   deste modo

$$\mathrm{mdc}\left(\frac{a}{\mathrm{mdc}(a,b)}, \frac{b}{\mathrm{mdc}(a,b)}\right) = 1$$

3. (Retirado de Vieira (2020)) Da hipótese que $a \mid bc$, existe $k \in \mathbb{Z}$ tal que $bc = ak$. Como $\mathrm{mdc}(a,b) = 1$ então pelo Teorema de Bézout (Proposição 4.14), existem $x,y \in \mathbb{Z}$ tais que $ax + by = 1$. Multiplicando ambos os lados por c, obtemos

$$c = acx + bcy = acx + aky = a(cx + ky),$$

   o que implica em $a \mid c$.

4. (Retirado de Severino Colier Coutinho (1997)) Se $b \mid c$ então existe $t \in \mathbb{Z}$ tal que $c = bt$. Mas como $a \mid c$, logo $a \mid bt$, então, como $\mathrm{mdc}(a,b) = 1$, segue da afirmação anterior que $a \mid t$. Assim, existe $k \in \mathbb{Z}$ tal que $t = ak$.

   Portanto, $c = bt = b(ak) = (ba)k = (ab)k$. Isso significa que $ab \mid c$. □

Agora vamos ver dois algoritmos para obtenção do mdc de dois naturais a e b. O primeiro, chamado **Algoritmo de Euclides**, nos permite calcular o mdc de quaisquer dois naturais. Já o segundo, chamado de **Algoritmo de Euclides Estendido**, nos permite, além de calcular o $d = \mathrm{mdc}(a,b)$, encontrar dois inteiros x e y tal que $ax + by = d$ (Teorema de Bézout).

4.2.1 Algoritmo de Euclides

Esse algoritmo está presente no Livro VII de Os Elementos.

Algoritmo 4.16 (Algoritmo de Euclides). Queremos calcular $\mathrm{mdc}(a,b)$. Suponhamos, Sem Perda de Generalidade (SPG), que $b \leq a$. Se tivermos $b \mid a$, já vimos que $\mathrm{mdc}(a,b) = b$. Então, vamos supor que $b \nmid a$ (logo $b \neq a$).

Pela divisão Euclidiana, existem q_1,$r_1 \in \mathbb{N}$ tais que:

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

Disso, temos duas situações:

- Ou $r_1 \mid b$, o que implica em $r_1 = \mathrm{mdc}(b,r_1)$, e, pelo Lema de Euclides, $\mathrm{mdc}(a,b) = \mathrm{mdc}(b,r_1)$ (algoritmo termina!).
- Ou $r_1 \nmid b$, o que nesse caso podemos repetir o passo anterior e fazer a divisão euclidiana de b por r_1:
$$b = r_1q_2 + r_2 \text{ com } 0 < r_2 < r_1$$

Novamente temos duas situações:

- Ou $r_2 \mid r_1$, o que implica em $r_2 = \mathrm{mdc}(r_1,r_2)$, e, pelo Lema de Euclides, $\mathrm{mdc}(a,b) = \mathrm{mdc}(b,r_1 = \mathrm{mdc}(r_1,r_2)$ (algoritmo termina!).
- Ou $r_2 \nmid r_1$, o que nesse caso podemos repetir o passo anterior e fazer a divisão euclidiana de r_1 por r_2.
$$r_1 = r_2q_3 + r_3 \text{ com } 0 < r_3 < r_2$$

Esse processo deve ser continuado até achar um par r_n,r_{n-1} onde se tenha $r_n \mid r_{n-1}$. Isso sempre irá acontecer pois, caso contrário, teríamos uma sequência de números naturais $b > r_1 > r_2 > \cdots > 0$, que não possui menor elemento, o que fere o Principio da Boa Ordenação. Logo, para algum n, teremos $r_n \mid r_{n-1}$, implicando em

$$\mathrm{mdc}(a,b) = \mathrm{mdc}(b,r_1) = \mathrm{mdc}(r_1,r_2) = \cdots = \mathrm{mdc}(r_{n-1},r_n) = r_n$$

Observação 4.17. Um modo "seguro" de se obter o $\mathrm{mdc}(a,b)$, sem deixar nenhum passo faltando é realizar o algoritmo até que o **resto** da divisão euclidiana seja igual a **zero**. Quando isso acontecer, o resto da divisão euclidiana **anterior** será o mdc.

Exemplo 4.18. Aplique o algoritmo de Euclides para calcular $\mathrm{mdc}(639,234)$.

Resolução. Vamos fazer as divisões sucessivas:

$$\begin{cases} 639 = 234 \times 2 + 171 \\ 234 = 171 \times 1 + 63 \\ 171 = 63 \times 2 + 45 \\ 63 = 45 \times 1 + 18 \\ 45 = 18 \times 2 + 9, \end{cases}$$

Como $9 \mid 18$, logo $\mathrm{mdc}(639,234) = 9$. □

Utilizando esse algoritmo, é possível, usando ele "de trás para frente", obter dois números x,y tais que $ax + by = \mathrm{mdc}(a,b)$. Um método de encontrarmos **diretamente** esses números x,y estará presente no **Algoritmo de Euclides Estendido.**

4.2.2 Algoritmo de Euclides Estendido

Este algoritmo, publicado pela primeira vez em 1963 por *D.E. Knuth* (ver Knuth (1997)), calcula, ao mesmo tempo, o mdc de dois números inteiros a e b e determina inteiros x e y tal que $ax + by = \mathrm{mdc}(a,b)$.[5]

Algoritmo 4.19 (Algortimo de Euclides Estendido, de Knuth)**.** Novamente podemos supor, SPG, que $b < a$. Para calcular $\mathrm{mdc}(a,b)$ montamos a matriz:

$$A = \begin{bmatrix} b & 1 & 0 \\ a & 0 & 1 \end{bmatrix}$$

Efetuando-se a divisão euclidiana entre a e b, temos $a = bq_1 + r_1$. O primeiro passo do algoritmo consiste em diminuir da segunda linha q_1 vezes a primeira linha, obtendo a matriz:

$$A_1 = \begin{bmatrix} b & 1 & 0 \\ a - bq_1 & -q_1 & 1 \end{bmatrix} = \begin{bmatrix} b & 1 & 0 \\ r_1 & -q_1 & 1 \end{bmatrix}$$

Efetuando-se agora a divisão euclidiana entre b e r_1, temos $b = r_1q_2 + r_2$. O segundo passo do algoritmo consiste em diminuir da primeira linha q_2 vezes a segunda linha, obtendo a matriz:

$$A_2 = \begin{bmatrix} b - q_2r_1 & 1 + q_1q + 2 & -q_2 \\ a - bq_1 & -q_1 & 1 \end{bmatrix} = \begin{bmatrix} r_2 & 1 + q_1q_2 & -q_2 \\ r_1 & -q_1 & 1 \end{bmatrix}$$

O processo repete-se, seguindo esses dois passos, reproduzindo o algoritmo de Euclides efetuado, agora, sobre as duas linhas da matriz, até obtermos no final uma matriz B, da forma:

$$B = \begin{bmatrix} d & y & x \\ 0 & k & l \end{bmatrix} \text{ ou } B = \begin{bmatrix} 0 & k & l \\ d & y & x \end{bmatrix}$$

Nessas matrizes, $d = \mathrm{mdc}(a,b)$ e x e y são inteiros tais que $d = ax + by$.

Justificativa. A explicação desse fato não é difícil se interpretarmos matricialmente as operações elementares sobre as linhas das matrizes. A matriz A é formada por dois blocos:

$$A = \left[\begin{array}{c|cc} b & 1 & 0 \\ a & 0 & 1 \end{array}\right]$$

[5] Esse algoritmo, na forma matricial, foi retirado de Hefez (2016)

No primeiro passo do algoritmo, obtemos a matriz A_1. O que foi feito foi multiplicar, à esquerda, cada bloco da matriz A pela matriz:

$$M_1 = \begin{bmatrix} 1 & 0 \\ -q_1 & 1 \end{bmatrix}$$

obtendo a matriz:

$$A_1 = M_1 A = \left[\begin{array}{c|c} M_1 \cdot \begin{bmatrix} b \\ a \end{bmatrix} & M_1 \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{array} \right]$$

No segundo passo do algoritmo, obtemos a matriz A_2. O que foi feito foi multiplicar, à esquerda, os blocos da matriz A_1 pela matriz:

$$M_2 = \begin{bmatrix} 1 & -q_2 \\ 0 & 1 \end{bmatrix}$$

obtendo a matriz:

$$A_2 = M_2 M_1 A = M_2 A_1 = \left[\begin{array}{c|c} M_2 M_1 \cdot \begin{bmatrix} b \\ a \end{bmatrix} & M_2 M_1 \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{array} \right]$$

Continuando esse processo, obteremos uma matriz B, que é resultante do produto da matriz M pela matriz A, sendo que M é a matriz resultante de $M_n M_{n-1} \dots M_2 M_1$. Ou seja:

$$B = MA = \left[\begin{array}{c|c} M \cdot \begin{bmatrix} b \\ a \end{bmatrix} & M \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{array} \right]$$

Supondo que

$$B = \left[\begin{array}{c|cc} d & y & x \\ 0 & k & l \end{array} \right]$$

Para vermos que $d = ax + by$, basta verificarmos que:

$$\begin{bmatrix} d \\ 0 \end{bmatrix} = M \cdot \begin{bmatrix} b \\ a \end{bmatrix} = \begin{bmatrix} y & x \\ k & l \end{bmatrix} \begin{bmatrix} b \\ a \end{bmatrix} = \begin{bmatrix} by + ax \\ kb + la \end{bmatrix}$$

donde $d = \mathrm{mdc}(a,b) = ax + by$.

O caso onde

$$B = \left[\begin{array}{c|cc} 0 & k & l \\ d & y & x \end{array} \right]$$

é análogo. □

Exemplo 4.20. Fizemos anteriormente $\mathrm{mdc}(639,234)$ via algoritmo de Euclides. Vamos refazer via o algoritmo estendido, seguindo os procedimentos explicados anteriormente.

Resolução.

$$\begin{bmatrix} 234 & 1 & 0 \\ 639 & 0 & 1 \end{bmatrix} \Longrightarrow \begin{bmatrix} 234 & 1 & 0 \\ 639-2\cdot 234 & -2 & 1 \end{bmatrix} = \begin{bmatrix} 234 & 1 & 0 \\ 171 & -2 & 1 \end{bmatrix}$$
$$\Longrightarrow \begin{bmatrix} 234-1\cdot 171 & 1-1\cdot(-2) & 0-1\cdot 1 \\ 171 & -2 & 1 \end{bmatrix} = \begin{bmatrix} 63 & 3 & -1 \\ 171 & -2 & 1 \end{bmatrix}$$
$$\Longrightarrow \begin{bmatrix} 63 & 3 & -1 \\ 171-2\cdot 63 & -2-2\cdot 3 & 1-2\cdot(-1) \end{bmatrix} = \begin{bmatrix} 63 & 3 & -1 \\ 45 & -8 & 3 \end{bmatrix}$$
$$\Longrightarrow \begin{bmatrix} 63-1\cdot 45 & 3-1\cdot(-8) & -1-1\cdot 3 \\ 45 & -8 & 3 \end{bmatrix} = \begin{bmatrix} 18 & 11 & -4 \\ 45 & -8 & 3 \end{bmatrix}$$
$$\Longrightarrow \begin{bmatrix} 18 & 11 & -4 \\ 45-2\cdot 18 & -8-2\cdot 11 & 3-2\cdot(-4) \end{bmatrix} = \begin{bmatrix} 18 & 11 & -4 \\ 9 & -30 & 11 \end{bmatrix}$$
$$\Longrightarrow \begin{bmatrix} 18-2\cdot 9 & 11-2\cdot(-30) & -4-2\cdot 11 \\ 9 & -30 & 11 \end{bmatrix} = \begin{bmatrix} 0 & 71 & -26 \\ 9 & -30 & 11 \end{bmatrix}$$

Logo $\mathrm{mdc}(639{,}234) = 9$ e $9 = 639\cdot(11) + 234\cdot(-30)$. □

4.3 EQUAÇÕES DIOFANTINAS

Esse nome é uma homenagem a *Diofanto de Alexandria*, matemático Grego do século III. É considerado um dos matemáticos mais influentes de sua época e considerado o pai da Álgebra e da Teoria dos Números.

Definição 4.21. Uma *equação diofantina* é qualquer equação polinomial que tenha coeficientes inteiros, com uma ou mais incógnitas.

Quando a equação é da forma:

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

A equação é chamada de *equação diofantina linear*, onde a_1,a_2,...,a_n são números inteiros, b também é, chamado de *termo independente* e $x_1,\ldots,x_n$ são as incógnitas.

Exemplo 4.22. A equação $3a + 5b - 6c + d = 13$ é um exemplo de equação diofantina linear e a equação $x^2 - 2y^3 = 1$ é um exemplo de equação diofantina não-linear.

Vamos focar nossos estudos com as equações diofantinas lineares com duas incógnitas.

4.3.1 Equações Diofantinas Lineares com duas incógnitas

Vamos ver como são esses tipos de equações com o seguinte *problema*[6]:

[6] retirado e adaptado de BEZERRA et al. (2018)

Exemplo 4.23. Um jogo eletrônico tem o seguinte funcionamento: A máquina exibe um número inteiro positivo, que corresponde a pontuação exata que o jogador deverá marcar para vencer a partida. Os pontos são marcados cada vez que o jogador abate um invasor, que o fica desafiando na tela. Existem dois tipos de invasores: os marcianos (na cor vermelha), valendo cada um 14 pontos e os jupiterianos (na cor verde), com o valor individual de 10 pontos. Suponha que você vai participar deste jogo e a máquina lhe exibe o número 420. De quantas maneiras você pode vencer o jogo? Quantos invasores de cada cor você deverá abater?

Deveremos procurar saber qual o número de marcianos e qual o número de jupiterianos que devem ser abatidos de modo a chegar exatamente nessa pontuação. Denotaremos, respectivamente por x e y essas quantidades. Relacionando as variáveis temos a equação: $14x + 10y = 420$.

Esse é um exemplo de uma equação diofantina linear com duas incógnitas. As perguntas que devemos nos fazer aqui são as seguintes: *Tem solução essa equação? Se sim, o número de soluções é finito ou infinito?*

Para responder a essas questões, vamos demonstrar o teorema abaixo:

Teorema 4.24. *Uma equação diofantina da forma* $ax + by = c$ *tem solução se, e só se, tivermos* $\mathrm{mdc}(a,b) \mid c$.

Demonstração. Considere $d = \mathrm{mdc}(a,b)$.

($\Longrightarrow$) A equação $ax + by = c$ tem solução, ou seja, existem $x_0,y_0 \in \mathbb{Z}$ tal que $ax_0 + by_0 = c$. Como $d = \mathrm{mdc}(a,b)$, então $d \mid a$ e $d \mid b$. Pela Propriedade f da divisibilidade (cf. Proposição 4.3), para quaisquer inteiros x,y temos que $d \mid ax + by$.

Em particular, existe $k \in \mathbb{Z}$ tal que $ax_0 + by_0 = dk$. Isso significa que $c = dk$ e, logo, $d \mid c$. Em outras palavras, $\mathrm{mdc}(a,b) \mid c$.

($\Longleftarrow$) Como $d \mid c$, então existe $k \in \mathbb{Z}$ tal que $c = dk$. Além disso, sabemos pelo Teorema de Bézout (Proposição 4.14) que existem x_0,y_0 inteiros tais que $ax_0 + by_0 = d$. Dessa equação, se multiplicarmos ambos os lados por k, obteremos $a(kx_0) + b(ky_0) = dk$, ou seja, $a(kx_0) + b(ky_0) = c$. Portanto, a equação diofantina tem solução. □

Agora que já sabemos quais as condições para uma equação diofantina da forma $ax + by = c$ ter solução, vamos ver como determinar a solução geral dela.

Proposição 4.25. *Se* (x_0,y_0) *é uma solução particular da equação diofantina* $ax + by = c$, *então sua solução geral é dada por*

$$\left(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t\right),$$

onde $t \in \mathbb{Z}$ *e* $d = \mathrm{mdc}(a,b)$.

Demonstração. [7]

[7] Baseado em BEZERRA et al. (2018)

O **conjunto solução** da equação diofantina pode ser definido por:

$$S = \left\{(u,v) \in \mathbb{Z}^2 \;\middle|\; au + bv = c\right\}$$

Defina o conjunto

$$T := \left\{\left(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t\right) \;\middle|\; t \in \mathbb{Z}\right\}$$

Se mostrarmos que $S = T$, resolveremos nosso problema. Para mostrarmos isso, teremos que mostrar a dupla inclusão: $T \subseteq S$ e $S \subseteq T$.

- $(T \subseteq S)$

  Seja $\left(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t\right) \in T$. Então

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

  Logo, $\left(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t\right) \in S$ e, portanto $T \subseteq S$.

- $(S \subseteq T)$

  Tome $(u,v) \in S$. Como (x_0,y_0) é uma solução particular, então $au + bv = c$ e também $ax_0 + by_0 = c$.

  Com isso, $au + by = ax_0 + by_0$ e, logo, $au - ax_0 = by_0 - bv$. Desse modo $a(u - x_0) = b(y_0 - v)$ e, segue que, $\frac{a}{d}(u - x_0) = \frac{b}{d}(y_0 - v)$.

  Segue que, $\frac{a}{d}$ divide $\frac{b}{d}(y_0 - v)$. Mas, pela Proposição 4.15, item 2, $\mathrm{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Logo, pela Proposição 4.15, item 3, segue que $\frac{a}{d}$ divide $(y_0 - v)$.

  Então existe $t \in \mathbb{Z}$ tal que $y_0 - v = \frac{a}{d}t$, assim $v = y_0 - \frac{a}{d}t$. Voltando para a igualdade $a(u - x_0) = b(y_0 - v)$, substituindo o v obtido nela, temos

  $$a(u - x_0) = b\left(y_0 - y_0 + \frac{a}{d}t\right) = \frac{b}{d}at,$$

  assim temos que

  $$u - x_0 = \frac{b}{d}t$$

  e, portanto,

  $$u = x_0 + \frac{b}{d}t$$

  Logo $(u,v) = \left(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t\right)$ e, com isso, $(u,v) \in T$. Logo, $S \subseteq T$.

  Conclui-se que $S = T$, ou seja, o conjunto solução da equação diofantina é

  $$S = \left\{\left(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t\right) \;\middle|\; t \in \mathbb{Z}\right\}$$ □

Ou seja, sabendo de uma solução particular da equação diofantina, é possível definir todas as soluções.

Vamos agora voltar para o problema mostrado no início da seção: Resolver $14x+10y = 420$.

Em algumas equações diofantinas é possível determinar uma solução particular apenas observando a equação. Caso isso não seja possível, se deve resolver a equação $ax + by = d$, com $d = \text{mdc}(a,b)$ e então multiplicar os valores obtidos por $\frac{c}{d}$.

Para achar valores que resolvem a equação, basta aplicar o **Algoritmo de Euclides Estendido**.

Resolução do Exemplo 4.23. Como $\text{mdc}(14,10) = 2$, vamos achar uma solução particular de $14x + 10y = 2$.

$$\begin{bmatrix} 10 & 1 & 0 \\ 14 & 0 & 1 \end{bmatrix} \implies \begin{bmatrix} 10 & 1 & 0 \\ 14-1\cdot 10 & 0-1\cdot 1 & 1-1\cdot 0 \end{bmatrix} = \begin{bmatrix} 10 & 1 & 0 \\ 4 & -1 & 1 \end{bmatrix}$$
$$\implies \begin{bmatrix} 10-2\cdot 4 & 1-2\cdot(-1) & 0-2\cdot 1 \\ 4 & -1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 3 & -2 \\ 4 & -1 & 1 \end{bmatrix}$$
$$\implies \begin{bmatrix} 2 & 3 & -2 \\ 4-2\cdot 2 & -1-2\cdot(3) & 1-2\cdot(-2) \end{bmatrix} = \begin{bmatrix} 2 & 3 & -2 \\ 0 & -7 & 5 \end{bmatrix}$$

Pelo algoritmo, uma solução particular é $(-2,3)$, ou seja, $14\cdot(-2) + 10\cdot 3 = 2$. Como $\frac{420}{2} = 210$, então multiplicando a equação nos dois lados por 210, obtemos:

$$14\cdot(-420) + 10\cdot(630) = 420$$

Com isso, $(-420,630)$ é uma solução particular de $14x + 10y = 420$. Com isso, a solução geral é dada por:

$$S = \{(-420 + 5t, 630 - 7t) \mid t \in \mathbb{Z}\}$$

Mas, nem todas as soluções nos interessam, pois queremos as soluções que sejam inteiros não-negativos (não deve existir uma quantidade negativa de invasores destruídos). Assim, devemos impor a condição

$$-420 + 5t \geq 0 \qquad \text{e} \qquad 630 - 7t \geq 0$$

Resolvendo essas inequações, obtemos $t \geq 84$ e $t \leq 90$.

Como $t \in \mathbb{Z}$, então $t = 84,85,86,87,88,89,90$. Para saber as soluções, precisamos substituir os valores de t acima na solução geral, obtendo:

- Para $t = 84$ temos a solução $(-420 + 5\cdot 84, 630 - 7\cdot 84) = (0, 42)$
- Para $t = 85$ temos a solução $(-420 + 5\cdot 85, 630 - 7\cdot 85) = (5, 35)$
- Para $t = 86$ temos a solução $(-420 + 5\cdot 86, 630 - 7\cdot 86) = (10, 28)$

- Para $t = 87$ temos a solução $(-420 + 5 \cdot 87, 630 - 7 \cdot 87) = (15, 21)$
- Para $t = 88$ temos a solução $(-420 + 5 \cdot 88, 630 - 7 \cdot 88) = (20, 14)$
- Para $t = 89$ temos a solução $(-420 + 5 \cdot 89, 630 - 7 \cdot 89) = (25, 7)$
- Para $t = 90$ temos a solução $(-420 + 5 \cdot 90, 630 - 7 \cdot 90) = (30, 0)$

Assim, para ganhar o jogo, deve-se fazer as combinações acima de marcianos e jupiterianos destruidos, respectivamente. □

4.4 NÚMEROS PRIMOS

Baseado no conteúdo presente em Hefez (2016).

Definição 4.26. Dado um número inteiro positivo p, com $p > 1$, ele é dito ser *primo* se seus únicos divisores positivos são 1 e p.

Todo número inteiro $n > 1$ que não é primo é dito ser *composto*.

Proposição 4.27. *Dados p,q primos e $a \in \mathbb{Z}$. Então:*

1. *Se $p \mid q$, então $p = q$*
2. *Se $p \nmid a$, então $\mathrm{mdc}(p,a) = 1$*

Demonstração. Ambas as afirmações decorrem diretamente da definição.

Para o primeiro item, se $p \mid q$ então, como q é primo, $p = 1$ ou $p = q$. Como p é primo, segue da definição que $p > 1$. Logo, $p = q$.

Para o segundo item, se tivermos $\mathrm{mdc}(p,a) = d$, $d \neq 1$, temos, pela definição de mdc, que $d \mid p$ e $d \mid a$. Portanto, como p é primo, $d = p$ ou $d = 1$. Mas $d \neq p$, pois, pela hipótese, $p \nmid a$. Portanto, $d = 1$. □

Um resultado muito importante sobre números primos será mostrado a seguir.

Lema 4.28 (Lema de Euclides - Primos). *Sejam a,b,$p \in \mathbb{Z}$, com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração. Se $p \mid a$, não há nada a se fazer.

Vamos supor que $p \nmid a$ e mostrar que $p \mid b$. Ora, se $p \nmid a$, então da Proposição 4.27, segue que $\mathrm{mdc}(a,p) = 1$. Disso e da hipótese, $p \mid ab$, segue, do Lema de Gauss (ver Proposição 4.15) que $p \mid b$. □

Iremos ver dois corolários antes de demonstrarmos o Teorema principal dessa seção. A demonstração desses dois corolários são baseados no conteúdo presente em Vieira (2020). O primeiro deles generaliza o Lema anterior.

Corolário 4.29. *Se p é primo e $p \mid a_1 a_2 \ldots a_n$, com $n \geq 1$, então $p \mid a_i$, para algum $i = 1, \ldots, n$.*

Demonstração. Vamos provar via indução sobre o número de fatores.

Para $n = 1$, nada a se fazer, o resultado segue imediatamente.

Para $n = 2$, é o Proposição 4.28.

Suponhamos agora o resultado válido para $n \geq 1$ (hipótese de indução).

Se para $p \mid a_1a_2 \cdots a_na_{n+1}$, temos que $p \mid (a_1a_2 \ldots a_n)a_{n+1}$. Sege do caso $n = 2$, que $p \mid (a_1a_2 \ldots a_n)$ ou $p \mid a_{n+1}$.

Se $p \mid a_{n+1}$, temos o resultado. Se $p \mid (a_1a_2 \ldots a_n)$, então, por hipótese de indução, $p \mid a_i$ para algum $i = 1, \ldots, n$. □

Corolário 4.30. *Se p,q_1,q_2, $\ldots$,q_r são números primos e $p \mid q_1q_2 \ldots q_r$, então $p = q_i$, para algum $i = 1,2, \ldots, r$.*

Demonstração. $p \mid q_1q_2 \ldots q_r$, então, pelo Corolário 4.29, $p \mid q_i$ para algum $i = 1, \ldots, r$. Como p e q_i são primos, segue de Proposição 4.27, que $p = q_i$. □

Podemos agora partir para o **Teorema Fundamental da Aritmética**.

Teorema 4.31 (Teorema Fundamental da Aritmética (TFA)). *Todo número natural a, maior do que 1, pode ser escrito de forma* única*, a menos da ordem dos fatores, como um produto de números primos. De outra forma, isso significa que a pode ser escrito da forma*

$$a = p_1p_2 \cdots p_n,$$

onde $n \in \mathbb{N}$, $n \geq 1$, e p_1, p_2, $\ldots$, p_n são números primos, não necessariamente distintos.

Demonstração. Precisamos provar duas coisas: A *Existência* e a *Unicidade*.

- (*Existência*) Vamos provar a existência via contradição (baseado em (Loveless, 2011))

  Suponha que existe um natural n, $n > 1$ que não pode ser expresso como um produto de primos. Pelo PBO, há um menor elemento, $n_0 > 1$ que não pode ser expresso como um produto de primos.

  n_0 não pode ser primo pois, caso contrário, ele seria sua própria fatoração em primos, e nós estamos assumindo que n_0 não admite fatoração em primos. Ou seja, n_0 é composto. Isso significa que n_0 contém algum divisor a, $1 < a < n_0$. Ou seja, $n_0 = a \cdot b$, com $1 < b < n_0$. Como n_0 é o menor exemplo que não pode ser expresso como um produto de primos e a e b são menores que n_0, então a e b devem ter forma fatorada. Então, podemos expressar a,b da forma $a = p_1p_2p_3 \ldots p_u$ e $b = q_1q_2q_3 \ldots q_v$, com p_i e q_j números primos ($i = 1, \ldots, u$ e $j = 1, \ldots, v$). Mas isso significa que $n_0 = ab = p_1p_2 \ldots p_uq_1q_2 \ldots q_v$ é um produto de primos. Mas isso é uma contradição, pois assumimos que n_0 não pode ser expresso como um produto de primos. Consequentemente nossa suposição inicial estava incorreta.

  Portanto, todos os $n \in \mathbb{N}$, $n > 1$ podem ser expressos como um produto de números primos.

- (*Unicidade*) Suponhamos

$$a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m, \tag{1}$$

sendo p_1,p_2,$\dots$,p_n,q_1,q_2,$\dots$,q_m todos números primos. Então $p_1 \mid q_1 q_2 \dots q_m$ e, por Proposição 4.30, $p_1 = q_j$, para algum $j = 1, \dots, m$. SPG, suponha $p_1 = q_1$. Pela lei do cancelamento, a igualdade (1) é equivalente a

$$p_2 \dots p_n = q_2 \dots q_m.$$

Da mesma forma, $p_2 = q_j$, para algum $j = 2, \dots, m$. Assumindo que $p_2 = q_2$, obtemos:

$$p_3 \dots p_n = q_3 \dots q_m.$$

Continuando com esse processo, como queremos mostrar que $m = n$, vamos assumir $n > m$ ou $n < m$ para chegarmos em contradições. Assumindo $n > m$, fazendo esse processo m vezes, obtemos que:

$$1 = p_{m+1} \dots p_n,$$

o que é impossível de acontecer. Agora, assumindo $n < m$, fazendo esse processo n vezes, obtemos que:

$$1 = q_{n+1} \dots p_m,$$

o que também é uma impossibilidade. Portanto, temos que $m = n$ e $q_i = p_i$ para cada $i = 1, \dots, n$. □

Vamos demonstrar agora um teorema que mostra que existem infinitos números primos: (demonstração retirada de Severino Collier Coutinho (2015))

Teorema 4.32. *Se $\mathcal{P}$ é um conjunto finito de números primos, então existe um primo que não pertence a $\mathcal{P}$.*

Antes da demonstração, um adendo: O enunciado desse teorema é mais parecido com o enunciado presente dos *Elementos* de Euclides, ao invés do enunciado mais popularmente atribuído a ele: *"Existem infinitos números primos"*. Segundo Severino Collier Coutinho (2015), a tradução quase literal do grego do enunciado presente no *Elementos* é: *"há mais números primos do que qualquer quantidade proposta de primos"*.

Demonstração. Para demonstrar o teorema, o que mostraremos é que, dado um conjunto finito qualquer $\mathcal{P}$ de primos, tem que existir um primo fora de $\mathcal{P}$.

Digamos que $\mathcal{P} = \{p_1, \dots, p_s\}$, é um conjunto finito formado apenas por números primos e consideremos o número $\mathcal{N} = p_1 \dots p_s$, que é igual ao produto de todos os primos em $\mathcal{P}$. Como $\mathcal{N}$ e $\mathcal{N} + 1$ não podem ter nenhum fator próprio comum, um primo que divide $\mathcal{N}$ não pode dividir $\mathcal{N} + 1$. Mas, todos os primos em $\mathcal{P}$ dividem $\mathcal{N}$, logo nenhum primo em

$\mathcal{P}$ pode dividir $\mathcal{N}+1$. Contudo, pelo Teorema Fundamental da Aritmética (Proposição 4.31), $\mathcal{N}+1$ tem que ter algum fator primo. Como estes fatores não podem dividir $\mathcal{N}$, então são primos que não pertencem a $\mathcal{P}$, provando assim o que queríamos. □

Com isso, existem infinitos números primos.

A fatoração de um número não é feita somente pelo TFA. Se o número for muito grande, essa tarefa se torna muito extenuante. Existem, felizmente, outros métodos de se encontrar sua fatoração (chamados de métodos de fatoração ou de algoritmos de fatoração). Uma delas será vista agora.

4.4.1 Método de Fermat

A explicação é baseada no conteúdo presente em Nucci e Grosch (2009). A demonstração desse método é baseada na demonstração presente em Severino Colier Coutinho (1997).

Esse é um dos métodos mais elementares que existem. Ele funciona baseado na propriedade a seguir.

Proposição 4.33. *Se um número ímpar n for composto, então ele pode ser escrito na forma $n = a^2 - b^2$, com a e b inteiros positivos.*

Assim, n pode ser fatorado como $n = (a+b)(a-b)$ e, com isso, $(a+b)$ e $(a-b)$ serão fatores de n.

Mas como determinar esses números a e b? Na prática é o seguinte:

Algoritmo 4.34. Dado n um número inteiro ímpar.

1. Considere $a = [\sqrt{n}]$.[8]
2. Calcule $b = \sqrt{a^2 - n}$.
3. Verificar se b é um número inteiro.
    - Se b for inteiro, ótimo, encontramos a e b e determinamos nossos fatores.
    - Se b não for inteiro, aumentamos o valor de a em uma unidade e repetimos as etapas 2 e 3.

Se a for incrementado sem sucesso até que ele seja igual a $\dfrac{n+1}{2}$, então n será primo.

Exemplo 4.35. Vamos testar esse método para um n composto, $n = 1717$

Resolução. Vamos determinar a: $a = [\sqrt{1717}] = [41{,}43] = 41$. Vamos verificar se b é inteiro: $b = \sqrt{a^2 - n} = \sqrt{1681 - 1717} = \sqrt{-36}$. Como b não é inteiro, devemos incrementar a, ou seja, testarmos para $a + 1 = 42$. Devemos fazer isso quantas vezes forem necessárias até encontrarmos b inteiro. A tabela contém todas as iterações a partir do 42.

[8] Dado um número real α denotamos por $[\alpha]$ o maior número inteiro que é menor do que ou igual a α. A função $[\ \ ]$ é chamada de *função parte inteira* ou *função piso*.

a	$b = \sqrt{a^2 - 1717}$	a	$b = \sqrt{a^2 - 1717}$
42	6,8557	51	29,7321
43	11,4891	52	31,4165
44	14,7986	53	33,0454
45	17,5499	54	34,6266
46	19,9749	55	36,1666
47	22,1810	56	37,6699
48	24,2280	57	39,1408
49	26,1534	58	40,5826
50	27,9821	59	42

Após todos esses passos, encontramos nosso b inteiro. Como $a = 59$ e $b = 42$, podemos encontrar nossos fatores: $(a + b) = 59 + 42 = 101$ e $(a - b) = 59 - 42 = 17$, que são os fatores de 1717.

Exemplo 4.36. Vamos testar esse método agora para $n = 2209$.

Resolução. Como $\sqrt{2209} = 47$, logo $a = 47$ e, assim, $b = 0$ e, deste modo, $a + b = a - b$. De fato,

a	$b = \sqrt{a^2 - 2209}$
47	0

Assim $a = 47$ e $b = 0$. Com isso, $(a + b) = 47$ e $(a - b) = 47$, que são os fatores de n. Com isso, n é um quadrado perfeito. □

Observação 4.37. No exemplo anterior n era um quadrado perfeito. Nesse caso, sempre temos que $a = \sqrt{n}$ e, portanto, $b = 0$.

Assim, $a - b = a$ e $a + b = a$, logo $n = a \cdot a$.

Vamos agora demonstrar esse método:

Demonstração. Queremos demonstrar o funcionamento desse método para qualquer n inteiro. Precisamos considerar separadamente o que ocorre quando n é composto e quando n é primo. No primeiro caso, precisamos mostrar que existe um inteiro x tal que $x > [\sqrt{n}]$ (parte inteira de $\sqrt{n}$) tal que $\sqrt{x^2 - n}$ é um número inteiro menor que $\frac{n+1}{2}$. Isso significa que, se n for composto, o método para antes de chegar a $\frac{n+1}{2}$. Se n for primo, então temos que verificar que o único valor de x possível será $\frac{n+1}{2}$.

Vamos supor que n pode ser fatorado da forma $n = ab$, onde $a \leq b$. Queremos achar inteiros positivos x e y tais que $n = x^2 - y^2$. Em outras palavras:

$$n = ab = (x - y)(x + y) = x^2 - y^2$$

Como $x - y \leq x + y$, isso sugere que $a = x - y$ e $b = x + y$. Temos o sistema de equações:

$$\begin{cases} x - y = a \\ x + y = b \end{cases}$$

Que, ao ser resolvido, teremos $x = \dfrac{a+b}{2}$ e $y = \dfrac{b-a}{2}$. Fazendo a verificação:

$$\left(\frac{b+a}{2}\right)^2 - \left(\frac{b-a}{2}\right)^2 = \frac{b^2+2ab+a^2}{4} - \left(\frac{b^2-2ab+a^2}{4}\right) = \frac{4ab}{4} = ab = n \quad (2)$$

Note que x e y são inteiros positivos mas estão representados em forma de fração. Precisamos nos assegurar que eles são de fato inteiros.

Lembremos que n deve ser ímpar, o que faz com que a e b, seus fatores, também sejam ímpares. Com isso, $a + b$ e $b - a$ são, por consequência, pares, e com isso, $\dfrac{a+b}{2}$ e $\dfrac{b-a}{2}$ são inteiros, como deve ser.

Agora podemos verificar para n primo e para n composto. Para n primo, ele é imediato:

Se n for primo, então só podemos ter $a = 1$ e $b = n$, ou vice-versa, isso faz com que $x = \dfrac{n+1}{2}$ e $y = 0$, que é o único valor possível para x se ele for primo.

Resta agora considerarmos n composto. Se $a = b$, então o método já acaba no primeiro passo. Então, supondo que n e composto e não é um quadrado perfeito, teremos $1 < a < b < n$. Nesse caso, o método irá parar quando forem satisfeitas as desigualdades:

$$[\sqrt{n}] \leq \frac{a+b}{2} < \frac{n+1}{2} \quad (3)$$

que serão demonstradas.

Observando a desigualdade da direita, $\dfrac{a+b}{2} < \dfrac{n+1}{2}$, ele é equivalente a $a+b < n+1$. Para mostrar que ela é sempre válida, precisamos reduzir ela até chegarmos numa desigualdade "trivial" ou "óbvia". Substituindo $n = ab$ na ultima desigualdade, obtemos $a + b < ab + 1$. Subtraindo $b + 1$ de ambos os membros, obtemos $a + b - b - 1 < ab + 1 - b - 1 \Rightarrow a - 1 < ab - b$. Já que $a > 1$, ainda podemos dividir $a - 1$ em ambos os lados, para obtermos $\dfrac{a-1}{a-1} < \dfrac{b(a-1)}{a-1} \Rightarrow 1 < b$. Com isso, chegamos a $b > 1$ que é a desigualdade "óbvia" que procuramos, já que $1 < a < b < n$. Com isso, a desigualdade da direita é válida.

Vamos observar agora a desigualdade da esquerda. Como $[\sqrt{n}] \leq \sqrt{n}$, então precisamos verificar que $\sqrt{n} \leq \dfrac{a+b}{2}$. Elevando ambos os membros ao quadrado, temos que a desigualdade acima é equivalente à $n \leq \dfrac{(a+b)^2}{4}$, ou seja, $\dfrac{(a+b)^2}{4} - n \geq 0$. Precisamos mostrar que essa desigualdade é válida. Observando a igualdade em ((2)), temos $\dfrac{(b+a)^2}{4} - \dfrac{(b-a)^2}{4} = n$, ou seja,

$$\frac{(b+a)^2}{4} - n = \frac{(b-a)^2}{4}$$

Como $a < b$ e como já foi mostrado que $\frac{b-a}{2}$ é inteiro, então $\frac{(b-a)^2}{4} > 0$, ou seja, $\frac{(b+a)^2}{4} - n \geq 0$. Com isso, a desigualdade da esquerda é válida. Com isso, $[\sqrt{n}] \leq \frac{a+b}{2} < \frac{n+1}{2}$ é válido.

Voltando ao método, a variável x começa com o valor $[\sqrt{n}]$ e vai sendo incrementada uma unidade por iteração. Assim, a desigualdade ((3)) nos garante que, se n for composto, chegaremos a $\frac{a+b}{2}$ antes de chegarmos à $\frac{n+1}{2}$. Quando $x = \frac{a+b}{2}$, temos que

$$y^2 = \frac{(b+a)^2}{4} - n = \frac{(b-a)^2}{4}$$

Por ((2)). Atingindo essa iteração, o método irá parar, e com isso, iremos obter os fatores a e b. Portanto, se n é composto, então o método irá parar sempre antes de $x = \frac{n+1}{2}$, com os fatores de n sendo determinados.

□

4.5 ARITMÉTICA MODULAR

4.5.1 Congruências

Esta seção é baseado no conteúdo presente em Carneiro (2017) e DOMINGUES (2021).

Antes de chegarmos na definição principal dessa unidade (congruências), precisamos definir o que é uma relação de equivalência.

Definição 4.38. Seja X um conjunto onde está definido uma relação, que denotaremos por $\sim$. Essa relação é chamada de *relação de equivalência* se, para quaisquer elementos de X (digamos a,b,c), as seguintes propriedades são satisfeitas:

Reflexiva : $a \sim a$.

Simétrica : Se $a \sim b$, então $b \sim a$.

Transitiva : Se $a \sim b$ e $b \sim c$, então $a \sim c$.

Agora vamos definir uma **congruência**:

Definição 4.39. Seja n um número inteiro positivo. Dizemos que dois inteiros a e b são *congruentes módulo* n se $a - b$ for um múltiplo de n. Sua notação é dada por $a \equiv b \pmod{n}$. Ou seja,

$$a \equiv b \pmod{n} :\Longleftrightarrow a - b = k \cdot n, \text{ com } k \in \mathbb{Z}$$

Proposição 4.40. *Congruência módulo n é uma relação de equivalência em $\mathbb{Z}$.*

Demonstração. Vamos provar cada propriedade da definição de relação de equivalência.

Reflexiva Por definição, $a \equiv a \pmod{n}$ equivale a dizer que $a - a$ é múltiplo de n, o que é verdade pois, $a - a = 0$ e 0 é múltiplo de qualquer inteiro.

Simétrica: Se $a \equiv b \pmod{n}$, então $a - b$ é múltiplo de n. Mas, por outro lado, $b - a = -(a - b)$, que também é um múltiplo de n. Ou seja, $b \equiv a \pmod{n}$.

Transitiva: Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, significa que $a - b = k \cdot n, k \in \mathbb{Z}$ e $b - c = l \cdot n, l \in \mathbb{Z}$. Se somarmos essas igualdades, obtemos outro múltiplo de n e com isso $(a - b) + (b - c) = a - c$ também será múltiplo de n. Portanto, $a \equiv c \pmod{n}$.

Ou seja, a congruência é de fato uma relação de equivalência. □

4.5.1.1 Propriedades das Congruências

Proposição 4.41. *A congruência módulo n, para $n > 1$, segue as seguintes propriedades, para quaisquer $a, b, c, d \in \mathbb{Z}$:*

1. *Temos que $a \equiv b \pmod{n}$ se, e somente se, a e b possuem o mesmo resto na divisão por n.*
2. *(*Compatibilidade com soma e produto*) Se $a \equiv b \pmod{n}$ então temos $a \pm c \equiv b \pm c \pmod{n}$ e $ac \equiv bc \pmod{n}$.*
3. *Se temos $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$ então temos $a \pm c \equiv b \pm d \pmod{n}$ e $ac \equiv bd \pmod{n}$.*
4. *Se $a \equiv b \pmod{n}$, então $a^r \equiv b^r \pmod{n}$, para todo $r \in \mathbb{Z}, r \geq 1$.*
5. *(*Lei do cancelamento aditivo*) Se $a + c \equiv b + c \pmod{n}$, então $a \equiv b \pmod{n}$.*
6. *Se $ac \equiv bc \pmod{n}$, então $a \equiv b \left(\mathrm{mod} \frac{n}{\mathrm{mdc}(c,n)}\right)$.*
7. ***(Lei do cancelamento multiplicativo)** Se $ac \equiv bc \pmod{n}$ e $\mathrm{mdc}(c,n) = 1$ então $a \equiv b \pmod{n}$.*

Demonstração. • (Propriedade 1) ($\Longrightarrow$) Pela definição de congruência, $a - b = kn$, ou seja, $a = b + kn$, para algum $k \in \mathbb{Z}$. Se formos realizar a divisão euclidiana de b por n, temos que $b = nq + r$, com $0 \leq r \leq n$. Com isso:

$$a = b + kn = nq + kn + r = n(q + k) + r.$$

Ou seja, como $0 \leq r \leq n$, r também será o resto da divisão euclidiana de a por n.

($\Longleftarrow$) Temos que a e b deixam mesmo resto na divisão por n, ou seja, existem quocientes q e q', de modo que:

$$a = nq + r \text{ e } b = nq' + r$$

Disso segue que $a - nq = b - nq'$, ou seja, $a - b = n(q - q')$. Isso significa que $a \equiv b \pmod{n}$. □

- (Propriedade 2) Pela definição de congruência, $a - b = kn$, para algum $k \in \mathbb{Z}$. Essa igualdade é equivalente a

$$a - b \pm c \mp c = kn, k \in \mathbb{Z} \implies (a \pm c) - (b \pm c) = kn.$$

Ou seja, $a \pm c \equiv b \pm c \pmod{n}$. Quanto a segunda afirmação, da igualdade anterior, $a - b = kn$, ao multiplicarmos "c" $\in \mathbb{Z}$ em ambos os lados, obtemos:

$$c(a - b) = c(kn) \implies ac - bc = n(ck)$$

Ou seja, $ac \equiv bc \pmod{n}$. □

- (Propriedade 3) Das duas congruências, temos que $a - b = kn$, para algum $k \in \mathbb{Z}$ e $c - d = ln$, para algum $l \in \mathbb{Z}$. Se formos "somar" as duas igualdades, obtemos:

$$(a - b) + (c - d) = kn + ln \implies (a + c) - (b + d) = (k + l)n$$

Ou seja, $a + c \equiv b + d \pmod{n}$. O caso da subtração é análogo, ou seja, $a \pm c \equiv b \pm d \pmod{n}$.

Para demonstrar a segunda afirmação, vamos fazer o seguinte: A primeira congruência, $a \equiv b \pmod{n}$ é equivalente, pela Propriedade 2, a $ac \equiv bc \pmod{n}$. A segunda congruência, $c \equiv d \pmod{n}$, é equivalente, pela propriedade 2, a $bc \equiv bd \pmod{n}$. Pela transitividade, concluímos que $ac \equiv bd \pmod{n}$. □

- (Propriedade 4) Vamos provar por indução:

Base de Indução Como $r \geq 1$, então $a^1 \equiv b^1 \pmod{n}$ que equivale a nossa hipótese inicial, que é $a \equiv b \pmod{n}$.

Hipótese de Indução: Vamos supor que $a^r \equiv b^r \pmod{n}$.

Passo de Indução: Da hipótese de indução, $a^r \equiv b^r \pmod{n}$ e da hipótese inicial, $a \equiv b \pmod{n}$, podemos aplicar a **propriedade 3** e fazer o produto dessas duas congruências, obtendo:

$$a^r \cdot a \equiv b^r \cdot b \pmod{n}$$

O que equivale a:

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

Com isso, fica provado por indução que $a^r \equiv b^r \pmod{n}$, para todo $r \in \mathbb{Z}, r \geq 1$. □

- (Propriedade 5) Da hipótese, $a + c \equiv b + c \pmod{n}$. Pela definição de congruência, temos $(a+c)-(b+c) = kn$, para algum $k \in \mathbb{Z}$, mas $(a+c)-(b+c) = a-b+c-c = a+b$. Com isso, temos a igualdade $a - b = kn$, o que equivale a $a \equiv b \pmod{n}$. □

- (Propriedade 6) Por uma proposição anterior, $\frac{n}{\text{mdc}(c,n)}$ e $\frac{c}{\text{mdc}(c,n)}$, são coprimos. Então $ac \equiv bc \pmod{n} \iff n \mid (b-a)c \iff \frac{n}{\text{mdc}(c,n)} \mid (b-a)\frac{c}{\text{mdc}(c,n)} \iff$ $\iff \frac{n}{\text{mdc}(c,n)} \mid (b-a) \iff a \equiv b \left(\text{mod}\frac{n}{\text{mdc}(c,n)}\right)$. □
- (Propriedade 7) Decorre diretamente da Propriedade 6, bastando substituir o $\text{mdc}(c,n)$ por 1.

□

Vamos aplicar essas propriedades num exemplo:

Exemplo 4.42. Determine o resto de 3^{333} por 25.

Resolução. Precisamos achar um número x tal que $3^{333} \equiv x \pmod{25}$. Vamos calcular as primeiras potências de 3 para determinarmos um bom ponto de partida:

$$\begin{cases} 3^1 \equiv 3 \pmod{25} \\ 3^2 \equiv 9 \pmod{25} \\ 3^3 \equiv 2 \pmod{25} \\ 3^4 \equiv 6 \pmod{25} \\ 3^5 \equiv -7 \pmod{25} \end{cases}$$

Dessas primeiras potências, um bom ponto de partida para nós começarmos é a congruência $3^3 \equiv 2 \pmod{25}$. Como queremos 3^{333}, podemos aplicar a Propriedade 4, e reescrever essa congruência como:

$$3^{333} \equiv (3^3)^{111} \equiv 2^{111} \pmod{25}.$$

Agora, pela transitividade, temos que $2^{111} \equiv x \pmod{25}$, então precisamos lidar com essa potência 2^{111}. Vamos fazer a mesma coisa feita com as potências de 3:

$$\begin{cases} 2^1 \equiv 2 \pmod{25} \\ 2^2 \equiv 4 \pmod{25} \\ 2^3 \equiv 8 \pmod{25} \\ 2^4 \equiv 16 \pmod{25} \\ 2^5 \equiv 7 \pmod{25} \\ 2^6 \equiv 14 \pmod{25} \\ 2^7 \equiv 3 \pmod{25} \\ 2^8 \equiv 6 \pmod{25} \\ 2^9 \equiv 12 \pmod{25} \\ 2^{10} \equiv -1 \pmod{25}. \end{cases}$$

Dessas potências acima, um bom candidato é $2^{10} \equiv -1 \pmod{25}$. Como queremos 2^{111}, podemos aplicar a Propriedade 4 e reescrever essa congruência como:

$$2^{111} \equiv 2^{10 \cdot 11} \equiv (2^{10})^{11} \equiv (-1)^{11} \equiv -1 \pmod{25}.$$

Como temos $2^{110} \equiv -1 \pmod{25}$, pela Propriedade 2, temos que $2^{110} \cdot 2 \equiv -1 \cdot 2 \pmod{25}$, o que é equivalente a $2^{111} \equiv -2 \pmod{25}$. Como nosso resto deve ser positivo, note que $-2 \equiv 23 \pmod{25}$, pois $-2 - 23 = -25 = 25 \cdot (-1)$.

Concluindo, o resto da divisão de 3^{333} por 25 é 23. □

4.5.2 Sistemas Completos de Restos

Como a congruência é uma relação de equivalência sobre $\mathbb{Z}$, então, para todo $n > 0$, fica determinada sobre o conjunto dos inteiros, através da relação de congruência, uma quantidade n de partições de $\mathbb{Z}$, chamadas *classes de equivalência*.

Cada classe de equivalência, chamada de *classe residual* módulo n é definida como:

$$[a] = \{x \in \mathbb{Z} \,;\, x \equiv a \pmod{n}\}.$$

Para $n = 3$, há três classes residuais que são:

Exemplo 4.43. Para $n = 3$, há três classes residuais, que são:

$$[0] = \{a \in \mathbb{Z} \,;\, x \equiv 0 \pmod{3}\} \quad \rightarrow \text{é múltiplo de } 3$$
$$[1] = \{a \in \mathbb{Z} \,;\, x \equiv 1 \pmod{3}\} \quad \rightarrow \text{deixa resto 1 quando dividido por 3}$$
$$[2] = \{a \in \mathbb{Z} \,;\, x \equiv 2 \pmod{3}\} \quad \rightarrow \text{deixa resto 2 quando dividido por 3}$$

Observação 4.44. Dada uma classe residual módulo n, dois elementos que pertencem a uma mesma classe são congruentes módulo n e dois elementos de classes diferentes não são congruentes módulo n.

Demonstração. Dados as classes residuais $[a]$, $[b]$, e os números inteiros $x, y \in \mathbb{Z}$.

Se $x, y \in [a]$, então $x \equiv a \pmod{n}$ e $y \equiv a \pmod{n}$. Como a congruência é uma relação transitiva, logo $x \equiv y \pmod{n}$.

Se $x \in [a]$ e $y \in [b]$, com $[a] \neq [b]$. Como $x \in [a]$ e $y \in [b]$, logo $x \equiv a \pmod{n}$ e $y \equiv b \pmod{n}$. Supondo que $x \equiv y \pmod{n}$, então da transitividade da congruência, $a \equiv b \pmod{n}$. Segue que todo elemento de $[a]$ está em $[b]$, e vice-versa. Portanto, $[a] = [b]$, o que é uma contradição. Deste modo, $x \not\equiv y \pmod{n}$. □

Definição 4.45. Um conjunto de n inteiros, com $n > 0$, forma um *sistema completo de restos módulo* n (SCR) se quaisquer dois desses números (distintos) não são congruentes módulo n.

Em outras palavras, o conjunto $\{a_1, a_2, \ldots, a_n\}$ é um SCR módulo n se, e somente se, $a_1, \ldots, a_n$ geram n classes distintas, $[a_1], [a_2], \ldots, [a_n]$.

Exemplo 4.46. Por exemplo, o conjunto $I_{n-1} = \{0,1,2,\ldots,n-1\}$ é um SCR módulo n pois, se tivermos $k,l \in I_{n-1}$ de modo que $0 \leq k < l < n$, então temos $0 < l - k < n$, e com isso, $k \not\equiv l \pmod{n}$.

Definição 4.47. O conjunto de todas as classes residuais módulo n é denotado por Z_n. Ele é definido da forma:

$$\mathbb{Z}_n = \{[a_1],[a_2],\ldots,[a_{n-1}]\}$$

Em $\mathbb{Z}_n$ podemos definir duas operações:

1. Adição: $[a] + [b] \coloneqq [a + b]$
2. Multiplicação: $[a] \cdot [b] \coloneqq [a \cdot b]$

Exemplo 4.48. Em $\mathbb{Z}_6 = \{[0],[1],[2],[3],[4],[5]\}$, temos:

- $[3] + [4] = [3 + 4] = [7] = [1]$
- $[0] + [5] = [0 + 5] = [5]$
- $[3] \cdot [4] = [3 \cdot 4] = [12] = [0]$
- $[5] \cdot [5] = [5 \cdot 5] = [25] = [1]$

Proposição 4.49 (Propriedades de $\mathbb{Z}_n$). *Dado $n > 1$, as propriedades a seguir são válidas, para quaisquer $a, b, c, d \in \mathbb{Z}$:*

Propriedades da Adição

Associatividade $([a] + [b]) + [c] = [a] + ([b] + [c])$

Comutatividade $[a] + [b] = [b] + [a]$

Elemento Neutro *Existe $z \in \mathbb{Z}_n$ tal que* $[a] + z = z + [a] = [a]$

Elemento Oposto ou Simétrico *Para cada $a \in \mathbb{Z}$ existe $\tilde{a} \in \mathbb{Z}_n$* $[a] + \tilde{a} = z$

Propriedades da Multiplicação

Associatividade $([a] \cdot [b]) \cdot [c] = [a] \cdot ([b] \cdot [c])$

Comutatividade $[a] \cdot [b] = [b] \cdot [a]$

Elemento Neutro *Existe $e \in \mathbb{Z}_n$ tal que* $[a] \cdot e = e \cdot [a] = [a]$

Distributividade em relação à adição $[a] \cdot ([b] + [c]) = [a][b] + [a][c]$

Multiplicação por zero $[a] \cdot z = z$

Demonstração.

Propriedades da Adição

(Associatividade) $([a] + [b]) + [c] = [(a + b) + c] = [a + (b + c)] = [a] + [(b + c)] = [a] + ([b] + [c])$.

(Comutatividade) $[a] + [b] = [a + b] = [b + a] = [b] + [a]$.

(Elemento Neutro) Considere $z \coloneqq [0]$, assim temos que $[a]+z = [a]+[0] = [a+0] = [a]$.

(Elemento Oposto) Dado $a \in \mathbb{Z}$, considere $\tilde{a} \coloneqq [-a]$, assim temos que $[a] + \tilde{a} = [a] + [-a] = [a - a] = [0] = z$.

Propriedades da Multiplicação

(Associatividade) $([a] \cdot [b]) \cdot [c] = [(a \cdot b) \cdot c] = [a \cdot (b \cdot c)] = [a] \cdot [(b \cdot c)] = [a] \cdot ([b] \cdot [c])$.

(Comutatividade) $[a] \cdot [b] = [a \cdot b] = [b \cdot a] = [b] \cdot [a]$

(Elemento Neutro) Considere $e \coloneqq [1]$, assim temos que $[a] \cdot e = [a] \cdot [1] = [a \cdot 1] = [a]$.

(Distributividade em relação à adição) $[a] \cdot ([b] + [c]) = [a] \cdot [b + c] = [a \cdot (b + c)] = [ab + ac] = [ab] + [ac] = [a][b] + [a][c]$.

(Multiplicação por zero) $[a] \cdot z = [a] \cdot [0] = [a \cdot 0] = [0]$. □

Definição 4.50. Dizemos que um elemento $x \in \mathbb{Z}_n$ é invertível se existir $y \in \mathbb{Z}_n$ tal que $x \cdot y = [1]$.

Nesse caso, dizemos que y é o inverso de x em $\mathbb{Z}_n$, e denotamos $y \overset{not}{=} x^{-1}$.

Vamos ver agora uma proposição que caracteriza bem como são definidos os elementos *invertíveis* de Z_n.

Proposição 4.51. *Um elemento* $[a]$ *de* Z_n *é invertível se, e somente se,* $\mathrm{mdc}(a,n) = 1$.

Demonstração. ($\Longrightarrow$) Se $[a]$ é invertível, então existe $[b]$ em Z_n tal que $[a \cdot b] = [1]$. Ou seja, $a \cdot b \equiv 1 \pmod{n}$, isto é, existe t inteiro tal que, $a \cdot b - 1 = n \cdot t$, ou seja, $a \cdot b + n \cdot (-t) = 1$. Assim a equação diofantina linear $ax + ny = 1$ tem solução. Segue de Proposição 4.24 que $\mathrm{mdc}(a, n) \mid 1$ e, com isso, temos que $\mathrm{mdc}(a,n) = 1$.

($\Longleftarrow$) Se temos $\mathrm{mdc}(a,n) = 1$, então de Proposição 4.14 existem inteiros b e t tais que $a \cdot b + n \cdot t = 1$. Isso pode ser reescrito como $a \cdot b - 1 = n \cdot (-t)$, o que implica $a \cdot b \equiv 1 \pmod{n}$. Da definição de classe residual, temos que $[a] \cdot [b] = [a \cdot b] = [1]$. □

4.5.3 Função Totiente de Euler

O conteúdo apresentado nesta seção é baseado no conteúdo presente em Vieira (2020).

Definição 4.52. Para cada inteiro $n \geq 1$, indiquemos por $\varphi(n)$ a quantidade de números de inteiros positivos menores ou iguais a n que são relativamente primos (co-primos) com n.

A função φ assim definida é chamada de *Função de Euler* (ou Função Totiente de Euler).

Dado n, consideramos o conjunto

$$A_n = \{m \in \mathbb{N} \mid 1 \leq m \leq n \text{ e } \mathrm{mdc}(m,n) = 1\},$$

assim temos que $\varphi(n) \coloneqq \#(A_n)$.[9]

OBS: Uma outra definição para $\varphi(n)$ seria o número de inteiros positivos que admitem inverso módulo n.

[9] Dado um conjunto X, denotamos por $\#(X)$ (ou simplesmente $\#X$) a cardinalidade do conjunto X.

Exemplo 4.53. Para $n = 20$, os inteiros positivos menores do que 20 e co-primos com ele são $1,3,7,9,11,13,17,19$. Assim, $\varphi(20) = 8$.

Queremos estabelecer uma fórmula que nos permita calcular $\varphi(n)$, para qualquer n. Começamos observando o que acontece quando n é primo.

Proposição 4.54. *Dado $n \in \mathbb{Z}$, com $n > 1$, temos que n é primo se, e somente se, $\varphi(n) = n - 1$.*

Demonstração. ($\Longrightarrow$) Se n é primo, então todos os números estritamente menores do que ele são co-primos com n. Ou seja, $\varphi(n) = n - 1$.

($\Longleftarrow$) Temos que $\varphi(n) = n - 1$. Suponha, por absurdo, que n é composto. Ou seja, n possui um divisor d tal que $1 < d < n$. Isso significa que entre os números $1,2,\ldots,n$, existem ao menos dois inteiros que não co-primos com n, sendo d e o próprio n. Por causa disso, $\varphi(n) \leq n - 2$, o que é um absurdo, pois $\varphi(n) = n - 1$. Logo, n é primo. □

Agora que sabemos o valor de $\varphi(n)$ quando n é primo, encontraremos um modo de determinar $\varphi(n)$, para qualquer n (por maior que ele seja), bastando obter a fatoração de n em potências de primos (via Teorema Fundamental da Aritmética, cf. Proposição 4.31). Para isso, precisamos provar alguns resultados.

Teorema 4.55. *Dados p um número primo e $k \geq 1$, então*

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

Demonstração. É fácil ver que $\mathrm{mdc}(n,p^k) = 1$ se, e somente se $p \nmid n$ pois, se $\mathrm{mdc}(n,p^k) = 1$ então n e p^k não tem fatores em comum. Mas como o único fator primo de p^k é o próprio p então n e p não tem fatores em comum, o que implica em $p \nmid n$. Por outro lado, se $p \nmid n$, então p não é um fator primo de n, ou seja, $\mathrm{mdc}(n,p) = 1$. Como p^k só tem p como fator primo, então $\mathrm{mdc}(n,p^k)$ também será igual a 1.

Por exclusão vamos contar quantos múltiplos de p temos de 1 até p^k.

Note que entre 1 e p^k existem p^{k-1} números que são múltiplos de p, que são

$$1p,2p,3p,\ldots,(p^{k-1})p.$$

O conjunto $\{1,2,\ldots,p^k\}$ tem exatamente p^k elementos e, desses, p^{k-1} não são co-primos com p^k. Deste modo, o conjunto $\{1,2,\ldots,p^k\}$ contém exatamente $p^k - p^{k-1}$ números que são co-primos com p^k. Portanto,

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

Precisamos demonstrar um lema importante antes do próximo teorema.

Lema 4.56. *Dados inteiros a,b e c, temos que $\mathrm{mdc}(a,bc) = 1$ se, e somente se, $\mathrm{mdc}(a,b) = 1$ e $\mathrm{mdc}(a,c) = 1$.*

Demonstração. ($\Longrightarrow$) Suponhamos $\mathrm{mdc}(a,bc) = 1$ e $d = \mathrm{mdc}(a,b)$. Logo, $d \mid a$ e $d \mid b$ e, por isso, $d \mid a$ e $d \mid bc$. Consequentemente, $d \mid \mathrm{mdc}(a,bc) = 1$, o que implica em $d = 1$. Analogamente, se considerarmos $d' = \mathrm{mdc}(a,c)$, mostra-se da mesma forma que $d' = 1$.

($\Longleftarrow$) Tome $d = \mathrm{mdc}(a,bc)$ e suponha que $d > 1$. Assim, existe um primo p tal que $p \mid d$. Como $d \mid a$ e $d \mid bc$, segue, por transitividade, que $p \mid a$ e $p \mid bc$. Sendo p primo, $p \mid b$ ou $p \mid c$. Se $p \mid b$, como $p \mid a$, $p \mid \mathrm{mdc}(a,b) = 1$, o que impossível de acontecer. Analogamente, se $p \mid c$, chegamos na mesma impossibilidade. Logo, $\mathrm{mdc}(a,bc) = 1$. □

Essa propriedade acima pode ser generalizada.

Corolário 4.57. *Dados números inteiros* $a,a_1,a_2,\ldots,a_n$*, temos que* $\mathrm{mdc}(a,a_1a_2\ldots a_n) = 1$ *se, e somente se,* $\mathrm{mdc}(a,a_i) = 1$*, para todo* $i = 1,\ldots,n$.

Demonstração. Segue direto do Proposição 4.56, por indução. □

Podemos agora demonstrar o próximo teorema.

Teorema 4.58. *Se* m *e* n *são números naturais tais que* $\mathrm{mdc}(m,n) = 1$*, então*

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

Demonstração. Vamos montar uma tabela formada pelos números inteiros de 1 até $m\,n$, que tem a seguinte forma:

1	2	$\ldots$	r	$\ldots$	m
$m+1$	$m+2$	$\ldots$	$m+r$	$\ldots$	$2m$
$2m+1$	$2m+2$	$\ldots$	$2m+r$	$\ldots$	$3m$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
$(n-1)m+1$	$(n-1)m+2$	$\ldots$	$(n-1)m+r$	$\ldots$	nm

Pela definição da função φ, $\varphi(mn)$ é o número de inteiros dessa tabela que são co-primos com mn. Pelo Proposição 4.56, calcular esse número equivale a determinar o número de inteiros que são co-primos com m e com n.

Pelo Lema de Euclides (Proposição 4.13), $\mathrm{mdc}(qm + r,m) = \mathrm{mdc}(r,m)$. Assim, os números da r-ésima coluna são co-primos com m se, e somente se, r é co-primo com m. Consequentemente, apenas um número $\varphi(m)$ de colunas contém inteiros co-primos com m, e todo primeiro número de cada coluna é co-primo com m.

Queremos agora mostrar que em cada uma dessas $\varphi(m)$ colunas citadas acima, existem exatamente $\varphi(n)$ inteiros que são co-primos com n, concluindo que existem $\varphi(m)\varphi(n)$ números na tabela que são co-primos com m e n.

Os números da r-ésima coluna são $r, m + r, 2m + r, \ldots, (n-1)m + r$.

Afirmação: Estes números são incongruentes dois a dois, módulo n. De fato, se tivermos $k_1m + r \equiv k_2m + r \pmod{n}$, onde $0 \leq k_1 < k_2 < n$, então teremos $k_1m \equiv k_2m \pmod{n}$. Como temos $\mathrm{mdc}(m,n) = 1$, então podemos eliminar m dessa congruência, obtendo

$k_1 \equiv k_2 \pmod{n}$, ou seja, $n \mid k_2 - k_1$, o que é impossível de acontecer, pois de $0 \leq k_1 < k_2 < n$ temos que $0 < k_2 - k_1 < n$. Com isso, temos que

$$k_1 m + r \not\equiv k_2 m + r \pmod{n}, \text{ se } k_1 \neq k_2, \text{ com } 0 \leq k_1 < k_2 < n.$$

Como temos n elementos na r-ésima coluna da tabela, segue do Algoritmo da Divisão, os números da r-ésima coluna da tabela anterior são congruentes, módulo n, a $0,1,\ldots,n-1$, em alguma ordem. Mais ainda, se $s \equiv t \pmod{n}$, então $\mathrm{mdc}(s,n) = \mathrm{mdc}(t,n)$.

Isso nos mostra que a quantidade de números na r-ésima coluna que são co-primos com n é igual a quantidade de elementos do conjunto $\{0,1,2,\ldots,n-1\}$ que são co-primos com n, ou seja, temos $\varphi(n)$ números na r-ésima coluna que são co-primos com n.

Como temos $\varphi(m)$ colunas da tabela onde estão exatamente todos os co-primos com m e, em cada uma dessas colunas, temos exatamente $\varphi(n)$ números que são co-primos com n. Segue do Proposição 4.56 a quantidade de números na tabela que são co-primos com mn é $\varphi(m)\varphi(n)$. Concluindo, temos que $\varphi(mn) = \varphi(m)\varphi(n)$. □

Podemos generalizar esse teorema:

Corolário 4.59. *Se $n_1,n_2,\ldots,n_k$ são números inteiros positivos co-primos dois-a-dois ($\mathrm{mdc}(n_i,n_j) = 1, i \neq j$), então*

$$\varphi(n_1 n_2 \cdots n_k) = \varphi(n_1)\varphi(n_2)\cdots\varphi(n_k).$$

Demonstração. Vamos demonstrar via indução sobre k.

(**Base de Indução**) Se $k = 2$, nada a se fazer pois acabou de ser demonstrado.

(**Hipótese de Indução**) Suponha que o resultado é válido para um número $k \geq 2$.

(**Passo de Indução**) Agora, tome $n_1,n_2,\ldots,n_k,n_{k+1}$ inteiros positivos dois-a-dois co-primos, então, por Proposição 4.57, temos que $\mathrm{mdc}(n_1 n_2 \ldots n_k, n_{k+1}) = 1$. Com isso, temos que:

$$\begin{aligned}\varphi(n_1 n_2 \ldots n_k n_{k+1}) &= \varphi((n_1 n_2 \ldots n_k) n_{k+1}) \\ &\overset{\star}{=} \varphi(n_1 n_2 \ldots n_k)\varphi(n_{k+1}) \\ &\overset{*}{=} (\varphi(n_1)\varphi(n_2)\ldots\varphi(n_k))\varphi(n_{k+1}),\end{aligned}$$

onde em $\star$ foi usada a base de indução e em $*$ foi usado a hipótese de indução. O que prova o passo de indução. □

Podemos agora, provar um resultado que generaliza o Teorema 4.55 e obter uma formula para $\varphi(n)$, para qualquer inteiro $n > 1$.

Teorema 4.60. *Dado um número inteiro $n > 1$, seja $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ sua fatoração em primos, então*

$$\begin{aligned}\varphi(n) &= \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right)\ldots\left(p_r^{k_r} - p_r^{k_r-1}\right) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right).\end{aligned} \tag{4}$$

Demonstração. Sabemos que a função φ é multiplicativa, se os fatores são co-primos (Proposição 4.55). Como $\mathrm{mdc}\left(p_i^{k_i},p_j^{k_j}\right) = 1$, para $i \neq j$, então, segue do Corolário 4.59 que

$$\varphi(n) = \varphi(p_1^{k_1})\varphi(p_2^{k_2})\ldots\varphi(p_r^{k_r}).$$

Pelo Teorema 4.55,

$$\varphi(p_i^{k_i}) = p_i^{k_i} - p_i^{k_i-1} = p_i^{k_i}\left(1-\frac{1}{p_i}\right)$$

para cada $i = 1,\ldots,r$. Com isso,

$$\begin{aligned}\varphi(n) &= \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right)\ldots\left(p_r^{k_r} - p_r^{k_r-1}\right)\\ &= p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_r}\right)\\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_r}\right)\end{aligned}$$

□

Seguindo essa expressão acima, podemos calcular a função φ para qualquer número composto, bastando saber sua fatoração em primos.

Exemplo 4.61. Calcule $\varphi(86.400)$.

Resolução. A fatoração em primos é $86.400 = 2^7 \cdot 3^3 \cdot 5^2$. Então, pela Expressão (4), temos que

$$\begin{aligned}\varphi(86.400) &= 86.400\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 86.400\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)\\ &= 86.400 \cdot \frac{4}{15} = 5.760 \cdot 4 = \mathbf{23.040}\end{aligned}$$

□

Lema 4.62. *Seja a um inteiro tal que $\mathrm{mdc}(a,n) = 1$. Se $a_1,a_2,\ldots,a_{\varphi(n)}$ são os inteiros positivos menores do que n e co-primos com n então*

$$aa_1,aa_2,\ldots,aa_{\varphi(n)}$$

são congruentes módulo n a $a_1,a_2,\ldots,a_{\varphi(n)}$, em alguma ordem.

Demonstração. Iremos mostrar inicialmente que o conjunto $aa_1,aa_2,\ldots,aa_{\varphi(n)}$ é um sistema completo de restos módulo $\varphi(n)$. Se não fosse, teríamos $aa_i \equiv aa_j \pmod n$, para $i \neq j$, então, como $\mathrm{mdc}(a,n) = 1$, o fator a pode ser cancelado, o que teríamos $a_i \equiv a_j \pmod n$, ou seja, $n \mid a_i - a_j$, o que é impossível, pois $1 \leq a_i,a_j \leq n-1$ e $a_i \neq a_j$.

Agora, como $\mathrm{mdc}(a,n) = 1$ e $\mathrm{mdc}(a_i,n) = 1$, para $i = 1,\ldots,\varphi(n)$, segue da Proposição 4.56, que $\mathrm{mdc}(aa_i,n) = 1$.

Vimos anteriormente que o conjunto $I_{n-1} = \{0,1,2,\ldots,n-1\}$ é um SCR módulo n, então para cada aa_i, existe um único inteiro b, com $0 \leq b < n$, tal que $aa_i \equiv b \pmod n$. Como $\mathrm{mdc}(b,n) = \mathrm{mdc}(aa_i,n) = 1$, b deve obrigatoriamente ser um dos inteiros $a_1,a_2,\ldots,a_{\varphi(n)}$. Logo, $aa_i \equiv a_j \pmod n$, para algum $j = 1,\ldots,\varphi(n)$. □

Com esse lema demonstrado, podemos enunciar e demonstrar o Teorema de Euler:

Teorema 4.63 (Teorema de Euler). *Sejam a e n inteiros, com $n \geq 1$ e $\mathrm{mdc}(a,n) = 1$. Então*

$$a^{\varphi(n)} \equiv 1 \pmod{n} \tag{5}$$

Demonstração. Vamos considerar $n > 1$ ($n = 1$ é imediato). Considere $a_1,a_2,\ldots,a_{\varphi(n)}$ os inteiros positivos menores do que n que são co-primos com n. Como $\mathrm{mdc}(a,n) = 1$, segue do Proposição 4.62 que $aa_1,aa_2,\ldots,aa_{\varphi(n)}$ são congruentes módulo n a $a_1,a_2,\ldots,a_{\varphi(n)}$, em alguma ordem. Logo, se multiplicarmos todas estas congruências, obtemos:

$$(aa_1)(aa_2)\ldots(aa_{\varphi(n)}) \equiv a_1a_2\ldots a_{\varphi(n)} \pmod{n}$$

ou seja,

$$a^{\varphi(n)}(a_1a_2\ldots a_{\varphi(n)}) \equiv a_1a_2\ldots a_{\varphi(n)} \pmod{n}. \tag{6}$$

Como $\mathrm{mdc}(a_i,n) = 1$, para todo $i = 1,\ldots,\varphi(n)$, segue, em decorrência do Proposição 4.56 que $\mathrm{mdc}(a_1a_2\ldots a_{\varphi(n)},n) = 1$. Por causa disso, é possível cancelar o fator $a_1a_2\ldots a_{\varphi(n)}$ na congruência e, assim, temos

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$ □

Uma consequência direta desse teorema será elencado a seguir. Apesar de ser considerado um teorema, sua demonstração é bem direta.

Teorema 4.64 (Pequeno Teorema de Fermat). *Seja p primo e $a \in \mathbb{Z}$ de modo que $p \nmid a$. Então*

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

Demonstração. Como p é primo, então $\varphi(p) = p - 1$. Como $p \nmid a$, então $\mathrm{mdc}(a,p) = 1$. Substituindo $\varphi(n)$ na expressão do Teorema de Euler (Proposição 4.63), segue que

$$a^{p-1} \equiv 1 \pmod{p}.$$ □

Exemplo 4.65. Determine o resto da divisão de 3^{2026} por 8.

Resolução. Como $\mathrm{mdc}(3,8) = 1$, o Teorema de Euler pode ser usado. Como $\varphi(8) = 4$, segue que:

$$3^4 \equiv 1 \pmod{8}$$

Efetuando a divisão euclidiana de 2026 por 4, obtemos: $2026 = 4 \cdot 506 + 2$, ou seja, elevando ambos os membros da congruência por 506, obtemos:

$$3^{2024} \equiv 3^{4\cdot 506} \equiv \left(3^4\right)^{506} \equiv 1^{506} \equiv 1 \pmod{8}$$

Como $3^2 \equiv 1 \pmod{8}$, segue que

$$3^{2026} \equiv 3^{2024+2} \equiv 3^{2024} \cdot 3^2 \equiv 1 \cdot 1 \pmod{8}$$

Portanto, o resto da divisão de 3^{2026} por 8 é igual a 1. □

4.6 CONGRUÊNCIAS LINEARES

O que são congruências lineares? Pense numa equação do primeiro grau, com coeficientes inteiros e com incógnita x, do tipo $ax + c = d$. Essa equação pode ser reescrita da forma $ax = d - c$. Chamando "$d - c$" de b, obtemos $ax = b$. Congruências Lineares é o equivalente a essa equação mostrada, só que usando congruências. Numa equação como a acima, só existe uma solução. No caso das congruências lineares, isso nem sempre acontece. O conteúdo apresentado nesta seção está conforme Vieira (2020).

Definição 4.66. Dados a, b e n inteiros, com $a \neq 0$ e $n > 1$, uma congruência da forma

$$ax \equiv b \pmod{n}$$

é chamada uma *congruência linear*, onde x é uma incógnita.

Queremos determinar todas as soluções, caso elas existam, de uma congruência linear da forma $ax \equiv b \pmod{n}$, ou seja, achar todos os x_0 inteiros de modo que $ax_0 \equiv b \pmod{n}$.

Um caso especial de congruência linear são os dos inversos módulo n, visto na Proposição 4.51. Dado um inteiro a, um outro inteiro b é o inverso módulo n de a se $ab \equiv 1 \pmod{n}$. Conforme visto na Proposição 4.51, o elemento a só possui inverso módulo n se $\mathrm{mdc}(a,n) = 1$.

Vamos ver agora como resolver uma congruência linear, ou seja, encontrar e descrever o seu conjunto solução.

Teorema 4.67. *A congruência linear $ax \equiv b \pmod{n}$ tem solução inteira se, e somente se, $\mathrm{mdc}(a,n) \mid b$.*

Demonstração. ($\Rightarrow$) Seja x_0 uma solução de $ax \equiv b \pmod{n}$ e seja $d = \mathrm{mdc}(a,n)$. Assim, $ax_0 - b = kn$, para algum $k \in \mathbb{Z}$, o que é equivalente a $b = ax_0 - kn$. Como $d \mid a$ e $d \mid n$, então $d \mid b$, ou seja, $\mathrm{mdc}(a,n) \mid b$.

($\Leftarrow$) Vamos supor que $\mathrm{mdc}(a,n) \mid b$, então sendo $d = \mathrm{mdc}(a,n)$, temos que $b = dt$, para algum $t \in \mathbb{Z}$, e, ainda, pelo Teorema de Bézout (Proposição 4.14), existem inteiros r e s tais que

$$d = ar + sn.$$

De $b = dt$, obtemos $b = (ar + sn)t = art + snt$, o que implica em $b - a(rt) = (st)n$. Isso significa que $a(rt) \equiv b \pmod{n}$. Logo $x_0 = rt$ é uma solução de $ax \equiv b \pmod{n}$. □

Vimos a condição de existência de solução de uma congruência linear. Vamos agora caracterizar todas as soluções de dada congruência linear.

Teorema 4.68. *Seja x_0 uma solução particular da congruência linear $ax \equiv b \pmod{n}$. Então, todas as soluções dessa congruência serão da forma*

$$x = x_0 + \frac{n}{d} \cdot k,$$

com $k \in \mathbb{Z}$ *e* $d = \text{mdc}(a,n)$.

Demonstração. Como $ax_0 \equiv b \pmod{n}$, logo $ax_0 = b + \lambda n$, para algum $\lambda \in \mathbb{Z}$. Queremos mostrar que, para cada inteiro k, $x = x_0 + \frac{n}{d}k$ é uma solução da congruência linear. De fato,

$$ax = a\left(x_0 + \frac{n}{d} \cdot k\right) = ax_0 + a \cdot \frac{n}{d} \cdot k = (b + \lambda n) + \frac{ak}{d} \cdot n = b + \left(\lambda + \frac{ak}{d}\right) n.$$

Como $d \mid a$, logo $\frac{ak}{d} \in \mathbb{Z}$, temos que $ax \equiv b \pmod{n}$, para $x = x_0 + \frac{n}{d}k$ e qualquer z inteiro.

Mostramos que todo inteiro da forma $x_0 + \frac{n}{d}k$ é solução da congruência linear, agora falta mostrar que toda solução da congruência linear é dessa forma.

Agora, tome $\tilde{x} \in \mathbb{Z}$ tal que $a\tilde{x} \equiv b \pmod{n}$. Como já temos $ax_0 \equiv b \pmod{n}$, segue, por transitividade, que $a\tilde{x} \equiv ax_0 \pmod{n}$. Assim, pela Proposição 4.41 (item 6), temos que $x_0 \equiv \tilde{x} \left(\text{mod}\frac{n}{d}\right)$, ou seja,

$$\tilde{x} = x_0 + \frac{n}{d}t,$$

com $k \in \mathbb{Z}$. □

Existem soluções de $ax \equiv b \pmod{n}$ que são incongruentes duas a duas módulo n. Essas ocorrem em um número **finito** e elas são obtidas da expressão $x = x_0 + \frac{n}{d} \cdot k$, com $k = 0, 1, 2, \ldots, d-1$. Isso nos leva à proposição seguinte:

Proposição 4.69. *Dada a congruência* $ax \equiv b \pmod{n}$. *Se ela tiver soluções, então a quantidade de soluções que são duas a duas incongruentes, módulo* n, *é igual a* $d = \text{mdc}(a,n)$. *Essas soluções serão da forma:*

$$x_0, \quad x_0 + \frac{n}{d}, \quad x_0 + \frac{2n}{d}, \ldots, \quad x_0 + \frac{(d-1)n}{d}, \tag{7}$$

em que x_0 *é uma solução particular qualquer da congruência.*

Demonstração. Pelo Proposição 4.68, para cada inteiro k, temos que

$$x = x_0 + \frac{n}{d} \cdot k$$

é solução de $ax \equiv b \pmod{n}$. O que queremos mostrar é que

$$\left(x_0 + \frac{n}{d} \cdot k_1\right) \not\equiv \left(x_0 + \frac{n}{d} \cdot k_2\right) \pmod{n},$$

para $0 \leq k_1 < k_2 \leq d-1$. De fato, nessas condições, se

$$\left(x_0 + \frac{n}{d} \cdot k_1\right) \equiv \left(x_0 + \frac{n}{d} \cdot k_2\right) \pmod{n}$$

então

$$\frac{n}{d} \cdot k_1 \equiv \frac{n}{d} \cdot k_2 \pmod{n}.$$

Pela Proposição 4.41 (item 6),

$$k_1 \equiv k_2 \left(\mathrm{mod}\frac{n}{d_1}\right),$$

onde $d_1 = \mathrm{mdc}\left(\frac{n}{d},n\right)$. Como $\frac{n}{d}$ divide n, temos que $d_1 = \frac{n}{d}$ e, com isso,

$$\frac{n}{d_1} = \frac{n}{\frac{n}{d}} = d.$$

Portanto

$$k_1 \equiv k_2 \pmod{d},$$

ou seja, $d \mid k_2 - k_1$, o que é uma contradição, pois $0 \leq k_1 < k_2 \leq d-1$ e, logo, $0 < k_2 - k_1 \leq k_2 < d$. Consequentemente, as soluções são duas a duas incongruentes, módulo n.

Ainda nos falta mostrar que qualquer solução de $ax \equiv b \pmod{n}$, da forma $x = x_0 + \frac{n}{d} \cdot k$, é congruente módulo n a uma das soluções apresentadas em (7). Fazendo a divisão de n por d pelo Algoritmo da Divisão, temos $k = dq + r$, com $0 \leq r \leq d-1$. Assim

$$x \equiv x_0 + \frac{n}{d} \cdot k \equiv x_0 + \frac{n}{d}(dq + r) \equiv x_0 + nq + r \cdot \frac{n}{d} \equiv x_0 + r \cdot \frac{n}{d} \pmod{n}.$$

Portanto $x_0 + r \cdot \frac{n}{d}$ é congruente, módulo n, a uma das soluções apresentadas em (7). □

Uma decorrência imediata dessa proposição é o corolário seguinte:

Corolário 4.70. *Se* $\mathrm{mdc}(a,n) = 1$*, então a congruência linear* $ax \equiv b \pmod{n}$ *só terá* uma solução*, módulo* n*. Qualquer outra solução será congruente, módulo* n*, a solução encontrada.*

Corolário 4.71. *Seja* $x_0 \in \mathbb{Z}$ *uma solução particular qualquer da congruência linear* $ax \equiv b \pmod{n}$*, denotando por* $n' = \frac{n}{\mathrm{mdc}(a,n)}$*, temos que um número inteiro* m *é solução de* $ax \equiv b \pmod{n}$ *se, e somente se,* m *é solução de* $x \equiv x_0 \pmod{n'}$*.*

Mais ainda, a congruência linear $x \equiv x_0 \pmod{n'}$*, tem solução única (módulo* n'*).*

Definição 4.72. Duas congruências lineares que possuem as mesmas soluções, são ditas *congruências lineares equivalentes*.

Agora que já sabemos quando uma congruência linear terá soluções, qual é a caracterização dessas soluções e quantas soluções duas a duas incongruentes, módulo n, existem, resta-nos saber *como resolver* uma congruência linear $ax \equiv b \pmod{n}$.

Observação 4.73. Dado $d = \mathrm{mdc}(a,n)$, como a congruência linear tem solução, logo $d \mid b$. Precisamos primeiramente usar o Algoritmo de Euclides Estendido para obter inteiros r e s tais que $d = ar + ns$. Como $d \mid b$, logo existe t inteiro tal que $b = dt$, então $x_0 = rt$ é uma solução de $ax \equiv b \pmod{n}$. Consequentemente, sua solução geral será

$$x = x_0 + \frac{n}{d}k,$$

com $k \in \mathbb{Z}$ e $d = \text{mdc}(a,n)$. Além disso,

$$x_0, \quad x_0 + \frac{n}{d}, \quad x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}$$

são as soluções da congruência linear que são duas a duas incongruentes, módulo n.

Vamos mostrar dois exemplos para ver como funciona.

Exemplo 4.74. Resolver as congruências lineares a seguir.

a) $6x \equiv 15 \pmod{21}$

b) $18x \equiv 60 \pmod{16}$

Resolução. **a)** $6x \equiv 15 \pmod{21}$

Nesse caso, $d = \text{mdc}(6,21) = 3$ e $3 \mid 15, 15 = 3 \cdot 5, t = 5$, logo essa congruência tem solução. Para achar uma solução particular, devemos achar r e s tal que

$$6r + 21s = 3$$

Usando o algoritmo de Euclides estendido, obtemos $6 \cdot (-3) + 21 \cdot 1 = 3$, ou seja, $r = -3$. Com $r = -3$ e $t = 5$, temos que $x_0 = rt = (-3) \cdot 5 = -15$ é uma sol. particular da congruência.

Sua solução geral é $x = -15 + \frac{21}{3}k = -15 + 7k$, com $k \in \mathbb{Z}$. Como $d = 3$, temos três soluções incongruentes, módulo 21, que são

$$-15, \quad -15 + \frac{21}{3} = -8, \quad \text{e} \quad -15 + \frac{42}{3} = -1.$$

Se quisermos apenas soluções positivas, temos que -15, -8 e -1 são congruentes modulo 21 a 6, 13 e 20, respectivamente.

Obs. Poderíamos ter obtido as soluções positivas diretamente, sabendo que $-15 \equiv 6 \pmod{21}$, aonde a solução geral seria $x = 6 + 7k$, e as três soluções incongruentes seriam 6, 13 e 20, como encontramos anteriormente.

b) $18x \equiv 60 \pmod{16}$

Nesse caso, $d = \text{mdc}(18,16) = 2$ e $2 \mid 60, 60 = 2 \cdot 30, t = 30$, logo essa congruência tem solução. Para achar uma solução particular, devemos achar r e s tal que

$$18r + 16s = 2$$

Usando o algoritmo de Euclides estendido, obtemos $18 \cdot 1 + 16 \cdot (-1) = 2$, ou seja, $r = 1$. Com $r = 1$ e $t = 30$, temos que $x_0 = rt = (1) \cdot 30 = 30$ é uma sol. particular da congruência, com $30 \equiv 14 \pmod{16}$.

Sua solução geral é $x = 14 + \frac{16}{2}k = 14 + 8k, \quad k \in \mathbb{Z}$. Como $d = 2$, temos **duas** soluções incongruentes módulo 16, que são

$$14 \quad \text{e} \quad 14 + \frac{16}{2} = 22.$$

Como $22 \equiv 6 \pmod{16}$, as duas soluções incongruentes são 6 e 14. □

4.6.1 Sistemas de Congruências Lineares

Como já sabemos determinar a solução de uma congruência linear, nos convém saber como determinar soluções de sistemas de congruências lineares, que, tal como em sistemas de equações lineares, consiste em resolver simultaneamente duas (ou mais) congruências lineares.

Exemplo 4.75. Considere o sistema:

$$\begin{cases} x \equiv 4 \pmod 7 \\ x \equiv 9 \pmod{15} \end{cases}$$

Resolução. Resolver esse sistema significa determinar todos os inteiros x que satisfazem ambas as congruências. Podemos achar uma solução geral via o método da substituição, que funciona de modo semelhante ao usado para resolver sistemas de equações lineares.

Da primeira congruência, obtemos $x = 7y + 4$, com $y \in \mathbb{Z}$. Como esse valor de x deve satisfazer a segunda congruência também, devemos substituir esse x na segunda congruência, obtendo $7y + 4 \equiv 9 \pmod{15}$, o que equivale em $7y \equiv 5 \pmod{15}$. Como $\mathrm{mdc}(7{,}15) = 1$ e $1 \mid 5$, essa congruência tem solução inteira. Resolvendo da forma vista na seção anterior, se obtém $y = 5 + 15k$, com $k \in \mathbb{Z}$. Agora, substituindo esse valor de y em $x = 7y + 4$, obtemos:

$$x = 7(5 + 15k) + 4 = 35 + 105k + 4 = 105k + 39$$

Ou seja, a solução geral desse sistema é $x = 39 + 105k$, com $k \in \mathbb{Z}$. □

Caso fosse um sistema de 3 ou 4 congruências, o ideal, por evitar confusão de incógnita, usar a incógnita k somente na última congruência.

Esse método não é o único, e nem é recomendado em sistemas de 3 ou mais congruências. Outro método será descrito na sequência.

Observação 4.76. No contexto da Proposição 4.71, as congruências lineares $ax \equiv b \pmod n$ e $x \equiv x_0 \pmod{n'}$ são equivalentes.

Se o objetivo for determinar todas as soluções de uma congruência linear, basta considerar a sua congruência linear "mônica" equivalente.

4.6.1.1 Teorema Chinês dos Restos

De acordo com Ing (2003), "o problema mais antigo envolvendo restos foi descoberto num tratado chinês do século III d.C chamado de *Sun Ji Suanjing*, cuja tradução é *O Clássico Matemático de Sun Zi*, de autor desconhecido". O problema envolvendo restos neste tratado é chamado atualmente de **Teorema Chinês dos Restos**.

O problema, encontrado no Capítulo 3, página 26 do *Sun Ji Suanjing*, diz o seguinte:

> *Agora há um número desconhecido de objetos.*
> *Se os contarmos de três em três, resta 2;*
> *Se os contarmos de cinco em cinco, resta 3;*
> *Se os contarmos de sete em sete, resta 2.*
> *Encontre o número de objetos.*

Ao lado do problema, o autor de *Sun Ji Suanjing* trouxe a resposta:

> *Resposta: 23.*
> *Método: Se contarmos de três em três e o resto for 2, anote 140.*
> *Se contarmos de cinco em cinco e o resto for 3, anote 63.*
> *Se contarmos de sete em sete e o resto for 2, anote 30.*
> *Some os valores para obter 233 e subtraia 210 para encontrar a resposta.*
> *Se contarmos de três em três e o resto for 1, anote 70.*
> *Se contarmos de cinco em cinco e o resto for 1, anote 21.*
> *Se contarmos de sete em sete e o resto for 1, anote 15.*
> *Quando [um número] excede 106, o resultado é obtido subtraindo 105.*

De acordo com Ing (2003), desde a antiguidade houveram muitas pesquisas envolvendo o *Teorema Chinês dos Restos* e atualmente este teorema foi sistematizado ao ponto de ser encontrado facilmente em muitos livros de matemática. O teorema em si será demonstrado um pouco mais adiante.

De um modo geral, nossa intenção é resolver sistemas de congruências da forma

$$\begin{cases} a_1 x \equiv b_1 & (\mathrm{mod}\ n_1) \\ a_2 x \equiv b_2 & (\mathrm{mod}\ n_2) \\ \quad \vdots & \\ a_k x \equiv b_k & (\mathrm{mod}\ n_k) \end{cases} \tag{8}$$

Para que esse sistema tenha solução, é necessário que cada uma das k congruências tenha solução, ou seja, $d_i \mid b_i$, para cada $i = 1, \ldots, k$, conforme o Proposição 4.67. Mas, essa condição não é suficiente pois, um sistema pode não ter solução mesmo que cada congruência tenha solução.

Exemplo 4.77. O sistema de congruências lineares

$$\begin{cases} x \equiv 2 & (\mathrm{mod}\ 4) \\ x \equiv 1 & (\mathrm{mod}\ 2) \end{cases}$$

não tem solução, pois todas as soluções da primeira congruência são números pares, enquanto que todas as soluções da segunda congruência são números ímpares.

Vamos começar com um lema que nos permite expressar um sistema equivalente ao presente em (8), com as congruências sendo da forma $x \equiv c_i \pmod{m_i}$, para todo $i = 1, \ldots, k$. Essas duas congruências serão *equivalentes*, ou seja, terão as mesmas soluções.

Lema 4.78. *A congruência linear $ax \equiv b \pmod{n}$, em que $d = \mathrm{mdc}(a,n)$, com $d \mid b$ é* ***equivalente*** *a*

$$x \equiv rb^* \pmod{m},$$

sendo $b = b^*d$, $d = ar + sn$ e $n = md$.

Demonstração. Como $d \mid a$, $d \mid n$ e $d \mid b$, logo existem a^*, m e b^* números inteiros tais que $a = a^*d$, $b = b^*d$ e $n = md$. Assim, temos que

$$ax \equiv b \pmod{n} \iff a^*dx \equiv b^*d \pmod{md}.$$

Pela Proposição 4.41 (item 7), obtemos

$$a^*x \equiv b^* \pmod{m} \tag{9}$$

Sendo $d = ar + sm$, segue que $d = a^*dr + smd = d(a^*r + sm)$, ou seja, $1 = a^*r + sm$. Logo,

$$ra^* \equiv 1 \pmod{m}.$$

Pegando a congruência em (9) e multiplicando por r, obtemos

$$ra^*x \equiv rb^* \pmod{m},$$

ou seja,

$$x \equiv rb^* \pmod{m},$$

o que prova a primeira parte.

Reciprocamente, se $x \equiv rb^* \pmod{m}$, então, como $ra^* \equiv 1 \pmod{m}$, temos $xra^* \equiv rb^* \pmod{m}$. Por outro lado, como $1 = a^*r + sm$, isso equivale em $\mathrm{mdc}(r,m) = 1$ (já que a^* e s são inteiros). Isso nos permite cancelar o fator r da última congruência (via Proposição 4.41 (item 7)), obtendo $xa^* \equiv b^* \pmod{m}$. Multiplicando por d, temos que $xa^*d \equiv b^*d \pmod{md}$, ou seja, $ax \equiv b \pmod{n}$. □

Esse lema foi demonstrado pois, caso tenhamos uma congruência da forma $x \equiv b \pmod{n}$, a sua solução geral é obtida diretamente, da forma $x = kn + b, k \in \mathbb{Z}$.

De acordo com o Lema 4.78, o sistema presente em (8) é equivalente a um sistema da forma:

$$\begin{cases} x \equiv c_1 & \pmod{m_1} \\ x \equiv c_2 & \pmod{m_2} \\ \quad \vdots & \\ x \equiv c_k & \pmod{m_k} \end{cases} \tag{10}$$

Esse sistema pode ser resolvido pelo teorema a seguir (que da o nome dessa subseção).

Teorema 4.79 (Teorema Chinês dos Restos). *Sejam $m_1,m_2,\ldots,m_k$ números naturais tais que $\mathrm{mdc}(m_i,m_j)=1$, para todo $i\neq j$. Então, o sistema de congruências lineares presente em* (10) *possui uma solução, que é única módulo $m=m_1m_2\cdots m_k$.*

Demonstração. Precisamos provar duas coisas: A **existência** de uma solução e a **unicidade** módulo m, dessa solução.

(*Existência*) Sendo $m=m_1m_2\ldots m_k$, defina M_i é o produto de todos os inteiros $m_1,m_2,\ldots,m_k$, excluindo m_i, ou seja,

$$M_i=m_1m_2\ldots m_{i-1}m_{i+1}\ldots m_k=\frac{m}{m_i}.$$

Já que $\mathrm{mdc}(m_i,m_j)=1$, para $i\neq j$, temos que os m_i's são distintos entre si e além disso, eles não tem fatores primos em comum, ou seja, M_1 e m_1 são co-primos, M_2 e m_2 são coprimos, ..., M_k e m_k são coprimos. Ou seja, para todo $i=1,2,\ldots,k$, temos que $\mathrm{mdc}(M_i,m_i)=1$. Pelo Proposição 4.14 (Bézout), existem inteiros r_i e s_i tais que:

$$r_iM_i+s_im_i=1, \tag{11}$$

para cada $i=1,\ldots,k$. Considerando

$$x_0\coloneqq\sum_{i=1}^{k}c_ir_iM_i=c_1r_1M_1+c_2r_2M_2+\cdots+c_kr_kM_k,$$

vamos mostrar que x_0 é uma solução do sistema dado. Para $i\neq j$, temos então que $M_j\equiv 0 \pmod{m_i}$, pois $m_i \mid M_j$. Logo, $c_jr_jM_j\equiv 0 \pmod{m_i}$ de modo que

$$x_0\equiv\sum_{i=1}^{k}c_ir_iM_i\equiv c_1r_1M_1+c_2r_2M_2+\cdots+c_kr_kM_k\equiv c_ir_iM_i \pmod{m_i},$$

para cada i.

Por outro lado, da Equação (11), temos que $r_iM_i\equiv 1 \pmod{m_i}$, para cada $i=1,\ldots,k$. Daí, $c_ir_iM_i\equiv c_i \pmod{m_i}$ e, por transitividade, $x_0\equiv c_i \pmod{m_i}$ para todo i. Isso mostra que x_0 é uma solução para o sistema.

(*Unicidade*) Seja y_0 uma outra solução do sistema, $y_0\equiv c_i \pmod{m_i}$, para cada $i=1,\ldots,k$. Desse modo, $x_0\equiv y_0 \pmod{m_i}$, isto é, $m_i \mid x_0-y_0$. Como temos $\mathrm{mdc}(m_i,m_j)=1$, quando $i\neq j$, então, da Proposição 4.15 (item 4), $m=m_1m_2\ldots m_k$ divide x_0-y_0, ou seja, $x_0\equiv y_0 \pmod{m}$, o que prova a unicidade de solução módulo m.

Portanto, a solução geral do sistema é:

$$x=x_0+km,$$

para todo $k\in\mathbb{Z}$. □

Vamos resolver o problema mostrado no início da seção e, então, resolver um exemplo adicional.

Exemplo 4.80. Determine a solução do sistema de congruências lineares a seguir via o Teorema Chinês dos Restos.

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

Resolução. Uma vez que $\mathrm{mdc}(3,5) = \mathrm{mdc}(3,7) = \mathrm{mdc}(5,7) = 1$, o teorema pode ser usado. Como $m_1 = 3$, $m_2 = 5$, $m_3 = 7$, então

$$m = 3 \cdot 5 \cdot 7 = 105, \qquad M_1 = \frac{m}{m_1} = 35, \qquad M_2 = \frac{m}{m_2} = 21 \quad \text{e} \quad M_3 = \frac{m}{m_3} = 15.$$

Vamos determinar agora inteiros r_i e s_i tais que $r_i M_i + s_i m_i = 1$, para $i = 1,2,3$. Temos:

$$\begin{aligned} 1 &= (-1) \cdot 35 + 3 \cdot 12 \implies r_1 = -1 \\ 1 &= 1 \cdot 21 + 5 \cdot (-4) \implies r_2 = 1 \\ 1 &= 1 \cdot 15 + 7 \cdot (-2) \implies r_3 = 1 \end{aligned}$$

Como $c_1 = 2, c_2 = 3$ e $c_3 = 2$, podemos determinar x_0, como segue.

$$\begin{aligned} x_0 &= c_1 r_1 M_1 + c_2 r_2 M_2 + c_3 r_3 M_3 \\ &= 2 \cdot (-1) \cdot 35 + 3 \cdot 1 \cdot 21 + 2 \cdot 1 \cdot 15 \\ &= -70 + 63 + 30 \qquad\qquad = 23 \end{aligned}$$

Portanto, $x_0 = 23$ e a solução geral do sistema é:

$$x = 23 + 105k,$$

para todo $k \in \mathbb{Z}$. Verificando, $23 = 3 \cdot 7 + 2$, $23 = 5 \cdot 4 + 3$, $23 = 7 \cdot 3 + 2$. □

Exemplo 4.81 (Han Xin[10])**.** Um general conta o número de soldados sobreviventes de uma batalha alinhando-os sucessivamente em linhas de certos tamanhos. Toda vez, ele conta o número de soldados que faltam para completar uma linha inteira. O general, antes da batalha, dispunha de 1.200 soldados. Depois da batalha, tivemos:

- 3 soldados restantes se alinharmos em linhas de cinco soldados.
- 3 soldados restantes se alinharmos em linhas de seis soldados.
- 1 soldado restante se alinharmos em linhas de sete soldados.
- Nenhum soldado restante se alinharmos em linhas de onze soldados.

Quantos soldados sobreviveram à batalha?

[10] Baseado nas pesquisas realizadas por Hui (1265)

Solução. Resolver esse problema significa resolver o sistema:

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 3 \pmod 6 \\ x \equiv 1 \pmod 7 \\ x \equiv 0 \pmod{11} \end{cases}$$

Vamos resolvê-lo do mesmo jeito que o exemplo anterior.

Uma vez que $\text{mdc}(5,6) = \text{mdc}(5,7) = \text{mdc}(5,11) = \text{mdc}(6,7) = \text{mdc}(6,11) = \text{mdc}(7,11) = 1$, o teorema pode ser usado. Como $m_1 = 5$, $m_2 = 6$, $m_3 = 7$, $m_4 = 11$, então $m = 5 \cdot 6 \cdot 7 \cdot 11 = 2310$ e

$$M_1 = \frac{m}{m_1} = 462 \qquad M_2 = \frac{m}{m_2} = 385 \qquad M_3 = \frac{m}{m_3} = 330 \qquad M_4 = \frac{m}{m_4} = 210$$

Vamos determinar agora inteiros r_i e s_i tais que $r_i M_i + s_i m_i = 1$ para $i = 1,2,3,4$. Temos:

$$\begin{aligned} 1 &= 3 \cdot 462 + 5 \cdot (-277) \implies r_1 = 3 \\ 1 &= 1 \cdot 385 + 6 \cdot (-64) \implies r_2 = 1 \\ 1 &= 1 \cdot 330 + 7 \cdot (-47) \implies r_3 = 1 \\ 1 &= 1 \cdot 210 + 11 \cdot (-19) \implies r_4 = 1 \end{aligned}$$

Como $c_1 = 3, c_2 = 3$, $c_3 = 1$ e $c_4 = 0$, podemos determinar x_0:

$$\begin{aligned} x_0 &= c_1 r_1 M_1 + c_2 r_2 M_2 + c_3 r_3 M_3 + c_4 r_4 M_4 \\ &= 3 \cdot 3 \cdot 462 + 3 \cdot 1 \cdot 385 + 1 \cdot 1 \cdot 330 + 0 \cdot (1) \cdot 210 \\ &= 4158 + 1175 + 330 = 5643 \end{aligned}$$

Portanto, $x_0 = 5643 \equiv 1023 \pmod{2310}$ e a solução geral do sistema é:

$$x = 1023 + 2310k, \text{ para todo } k \in \mathbb{Z}. \qquad \square$$

4.7 CRIPTOGRAFIA

A palavra *Criptografia* vem do grego, da fusão das palavras *kryptos* (que significa secreto ou oculto) e *graphein* (que significa escrita ou escrever), ou seja, de um modo bem simplista, criptografia significa *Escrita em Códigos*. De acordo com Singh (1999), "o intuito da criptografia não é ocultar a existência de uma mensagem, mas esconder seu significado."

Esse ato de "esconder" tem um nome: Codificação. E o ato de "descobrir" o conteúdo dessa mensagem tem outro nome: Decodificação.

Ainda de acordo com Carneiro (2017), codificadores e decodificadores travam uma batalha, e tal batalha inspirava muitas descobertas científicas, com os codificadores criando códigos cada vez mais fortes enquanto que os decodificadores buscam encontrar fraquezas nesses códigos que os permitiam desvendá-los. Tal batalha acelerou o desenvolvimento da tecnologia, incluindo os computadores mais modernos.

Singh (1999) descreve um **código** como "uma substituição de palavras ou frases", enquanto o mesmo descreve uma **cifra** como "uma substituição de letras". Por causa disso, **cifrar** significa "misturar uma mensagem usando uma cifra" enquanto que **codificar** significa "misturar uma mensagem usando um código". Os termos **encriptar** e **decriptar** envolvem a codificação e decodificação de ambos, códigos e cifras. A **cifragem** pode ser entendida como uma função que "recebe" uma mensagem qualquer e "devolve" a mensagem encriptada. Enquanto que a **decifragem** pode ser entendida como sua função inversa, ou seja, ela "recebe" a mensagem encriptada e "devolve" a mensagem original.

Vamos descrever brevemente as principais técnicas de codificação presentes na codificação **clássica**. Todo o conteúdo presente é baseado em Carneiro (2017). Maioria dos métodos que serão descritos são de cifras simétricas, que usam a mesma chave para cifrar e decifrar. O RSA é um exemplo de cifra que não é simétrica.

4.7.1 Cifras de Transposição

Esse tipo de cifra consiste em embaralhar as letras das mensagens, gerando um anagrama da mensagem. Embora essa cifra seja bem difícil de ser decifrada por um interceptador, ela também será bem difícil de ser decifrada pelo destinatário, a não ser que esse embaralhamento siga um acordo previamente estabelecido entre as partes, o que deve ser feito em segredo.

Há dois métodos relativamente simples que usam essa técnica. Um deles é a transposição via "Cerca de Ferrovia". Trata-se de escrever uma mensagem em uma sequência de diagonais, alterando-as de forma a deixá-las em linhas alternadas, onde o texto cifrado é formado pela sequência de letras na linha superior seguida pela sequência de letras na linha inferior.

Exemplo 4.82. Vejamos um exemplo: Se a mensagem original é "DEPOIS DE AMANHÃ", essa mensagem na cerca de ferrovia seria da forma:

Figura 1 – Cerca de Ferrovia

D		P		I		D		A		A		H	
	E		O		S		E		M		N		A

Fonte: Elaborado pelo autor.

Portanto, a mensagem cifrada é "DPIDAAHEOSEMNA".

Para recuperar a mensagem, o caminho contrário deve ser feito, o que torna um processo bastante vulnerável.

Um outro método pode ser usado, esse um pouco mais seguro, que usa um "método retangular" (segundo Carneiro (2017)).

Primeiramente, é definida uma *chave*, que é uma palavra qualquer, assim é montada uma tabela com quantidade de colunas igual a quantidade de letras da chave. Na primeira linha da tabela são adicionadas as letras da chave, uma em cada célula e na ordem de escrita. Na segunda linha da tabela, abaixo de cada letra da chave, é colocado um número que indica a ordem dessa letra, considerando a ordem alfabética. Em seguida, a partir da terceira linha da tabela, escreve-se a mensagem a ser cifrada letra por letra, linha após linha, preenchendo todas as células da tabela. Caso haja células vazias na última linha, normalmente se coloca o símbolo do jogo da velha (#).

Para cifrar a mensagem, é retirada a sequência das letras das colunas na ordem crescente das letras da chave.

Exemplo 4.83. Vejamos um exemplo: Se a mensagem original é "DEPOIS DE AMANHÃ" e a chave é "QUATRO", a tabela retangular será da forma:

Figura 2 – Método Retangular.

Chave	**Q**	**U**	**A**	**T**	**R**	**O**
Ordem	**3**	**6**	**1**	**5**	**4**	**2**
Mensagem	**D**	**E**	**P**	**O**	**I**	**S**
	D	**E**	**A**	**M**	**A**	**N**
	H	**A**	#	#	#	#

Fonte: Elaborado pelo autor.

A mensagem cifrada será "PA#SN#DDHIA#OM#EEA".

Para decifrar a mensagem, o receptor faz o processo inverso, ou seja, o receptor deve escrever em colunas e decodificar em linhas.

4.7.2 Cifra de Substituição

Esse tipo de cifra consiste em trocar uma letra ou conjunto de letras por outras letras, símbolos e/ou números. Um dos métodos de criptografar mensagens mais antigos que existem é a chamada "Cifra de César". Segundo o autor, para produzir o texto cifrado, Júlio César substituía cada letra do alfabeto por outra que fica três posições adiante no alfabeto (A $\rightarrow$ D, B $\rightarrow$ E, etc). Se seguirmos essa lógica, a mensagem "DEPOIS DE AMANHÃ" seria cifrada em "GHSRLVDPDQKD".

Podemos interpretar essa cifra via Aritmética Modular: Por exemplo, se a letra "A" representasse o número 0, então a cifra como descrita acima seria congruente módulo 26 a $\phi + 2$, sendo ϕ o número que representa determinada letra. Pegando a letra Z, representada pelo número 25, ela seria levada pela cifra a $25 + 2 = 27$, só que 27 é congruente a 1 módulo 26, ou seja, a letra Z seria levada pela cifra pelo equivalente ao número 1, que é a letra B.

Esse método é um dos mais antigos, mas também um dos mais rápidos de serem decifrados. Se soubermos que foi usada a Cifra de César, como há somente 25 (26-1) valores possíveis para as chaves, levaríamos pouco tempo para quebrar o código. Esses 25 valores compõem o **espaço de chaves** dessa cifra. Espaço de chaves é um conjunto com todas as chaves possíveis de quebrarem uma cifra. Quanto menor esse conjunto, mais fácil ele é de ser quebrado via força bruta.

Outra cifra de substituição é a **Cifra de Substituição Monoalfabética**, onde cada um dos caracteres da mensagem original é substituído por outro caractere, baseado numa tabela pré-estabelecida ou de acordo com uma chave, que nesse caso será um número que indica quantas posições deve-se avançar no alfabeto para obter o texto cifrado.

Embora esse método seja mais "complexo" que a Cifra de César, ele ainda é fácil de ser quebrado. Isso porque, no alfabeto, cada letra tem uma "frequência" fixa em que elas são geralmente usadas. Uma tabela presente em Severino Collier Coutinho (2015) contém essas frequências:

Figura 3 – Tabela das Frequências das Letras em Português

Letra	%	Letra	%	Letra	%	Letra	%
A	11,64	G	1,30	N	5,05	T	4,34
B	1,04	H	1,28	O	10,73	U	4,64
C	3,88	I	6,18	P	2,52	V	1,70
D	4,10	J	0,40	Q	1,20	X	0,21
E	12,57	L	2,78	R	6,53	Z	0,47
F	1,02	M	4,75	S	7,81		

Fonte: Severino Collier Coutinho (2015)

Assim, apenas analisando a frequência de cada símbolo na mensagem, podemos descobrir a que letra correspondem os símbolos mais frequentes.

Com o tempo, essa cifra foi ficando cada vez mais ineficiente e sendo quebrada cada vez mais facilmente. Coube aos criptógrafos criarem uma cifra mais resistente à quebra.

Uma dessas cifras é a **Cifra de Substituição Polialfabética**, que passou por muitos intelectuais para ser aperfeiçoada gradativamente. Entre esses intelectuais, estavam o abade alemão *Johannes Trithemius (1462-1516)*, o cientista italiano *Giovanni Porta (1535-1615)* e

o diplomata Francês *Blaise de Vigenère (1523-1596)*. Este último chegou a misturar as ideias dos três para formar uma nova cifra, coerente e poderosa. Essa cifra, portanto, ficou conhecida como **Cifra de Vigenère**.

Em 1586, Vigenère publica um tratado sobre a escrita secreta, chamada *Traicté des chiffres*, que descreve seu método: Uma matriz 26×26 com 26 alfabetos, chamada tabela de Vigenère ou **Tabula Recta**.

Figura 4 – Tabula Recta

		Letra da Mensagem																								
		A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Letra da palavra-chave	**A**	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fonte: Produzido pelo autor.

Portanto, para enviar uma mensagem por esse método deve ser feito o seguinte: escreve-se a palavra-chave sobre a mensagem original repetidamente até que cada letra da mensagem original fique associada a uma determinada letra da palavra-chave. A letra da mensagem cifrada será onde se intercepta a letra da palavra-chave (linha da tabela acima) com a letra da mensagem original (coluna da tabela acima) e, dessa forma, se prossegue até concluir a cifragem.

Por exemplo: Se a mensagem for "DEPOIS DE AMANHÃ" e a palavra-chave for "COISA" então a cifragem fica da forma:

Tabela 3 – Codificação cifra de Vigenère

Palavra-Chave	C	O	I	S	A	C	O	I	S	A	C	O	I	S
Mensagem Original	D	E	P	O	I	S	D	E	A	M	A	N	H	A
Mensagem Cifrada	F	S	X	G	I	U	R	M	S	M	C	B	P	S

Fonte: Produzido pelo autor.

Para decifrar a mensagem, se procede de modo parecido. Essa cifra é imune à análise de frequência, a letra com mais frequência na mensagem cifrada nem sempre irá representar a mesma letra na mensagem original. E descobrir a chave é um processo quase que literalmente impossível, pois a palavra-chave pode ser qualquer palavra no dicionário ou uma palavra inventada.

Outra cifra foi inventada pelo arquiteto italiano *Leon Alberti (1404-1472)*, que foi a primeira cifra a ter uma máquina criptográfica, que é o disco de cifra, chamado de *"Disco de Alberti"*:

Figura 5 – Disco de Alberti

Fonte: (Wikipédia, 2025)

Esse disco foi construído da seguinte maneira: Alberti tomou dois círculos de cobre com uma pequena diferença de diâmetro entre eles e escreveu um alfabeto ao longo da borda de cada círculo. Em seguida, colocou-se o círculo menor no interior do círculo maior de modo que uma agulha passada pelos dois centros seja usada como eixo comum. Os círculos podiam girar independentemente, de modo que os dois alfabetos mudavam suas posições relativas e assim eram usados para cifrar a mensagem. O alfabeto do círculo maior representava a mensagem original enquanto que o alfabeto do círculo menor representava a mensagem cifrada. Cada letra na mensagem original era extraída do círculo maior com a correspondente no círculo menor, sendo esta a letra na mensagem cifrada.

4.7.3 Criptografia nos séculos XIX e XX

Em 1830 houve um avanço na área de comunicação com a invenção do telégrafo e do código Morse, ambos inventados por *Samuel Morse (1791-1872)*. O código Morse foi a primeira representação binária (ponto e traço) do alfabeto com grande aplicação. Após suas respectivas invenções, o código e o telégrafo chegaram a exercer um importante papel na comunicação em geral. Mas havia preocupação quanto à segurança e à sigilosidade das mensagens enviadas, isso porque a mensagem escrita em código Morse era entregue ao operador do telégrafo, que a lia antes de transmiti-lá adiante. Para evitar que segredos sentimentais, comerciais, importantes, etc, de serem revelados ao operador, uma solução adotada foi cifrar essas mensagens antes de passá-las ao operador. Com a estabilidade do código Morse, o interesse de se quebrar a cifra de Vigenère foi diminuindo com o tempo. Mas existiram duas pessoas que contribuíram a esse "interesse": Babbage e Kasiski.

Charles Babbage (1791-1871) foi um matemático e inventor inglês mais conhecido por conceber a primeira ideia de um computador. Entre outras obras, Babbage ficou inreressado na cifra de Vigenère e de como quebrá-la.

Trabalhando paralelamente a Babbage, o oficial da reserva do exército prussiano, *Friedrich Wilhelm Kasiski (1805-1881)*, publicou em 1863 um trabalho, cujo nome era *"Die Geheimschriften und die Dechiffer-Kunst"* (A Escrita Secreta e a Arte de Decifrá-la, tradução nossa) que descreve uma técnica de como quebrar a cifra de Vigenère, conhecida como "Teste de Kasiski". Essa publicação acabou dando os créditos da quebra da cifra de Vigenère somente a Kasiski e não se sabe ao certo por que Babbage não chegou a publicar seu trabalho sobre a quebra da cifra (foram encontrados documentos após sua morte). Há uma teoria para isso, porém: Segundo relatos, Babbage descobriu a quebra logo depois do início da Guerra da Criméia (1853-1856), e essa descoberta deu aos britânicos uma vantagem sobre os russos, e isso pode ser significado que, Babbage provavelmente tenha sido "obrigado" a manter em segredo o seu trabalho pela segurança britânica.

Graças à descoberta de Babbage e Kasiski, a cifra de Vigenère não era mais segura e não houve nenhum avanço no sentido de novas cifras na segunda metade do século XIX. Nesse período de insegurança, na virada do século, o físico italiano *Guglielmo Marconi (1874-1937)* realizou um feito poderoso para a comunicação: A transmissão via **rádio**. Esse equipamento era capaz de transmitir e receber pulsos elétricos a uma distância de até $2{,}5Km$ com a vantagem de não haver a necessidade de um fio para transportar a mensagem entre o emissor e o receptor. Tal invenção encantou os militares, que sentiram ao mesmo tempo euforia e medo. De uma forma, a comunicação via rádio permitiu que generais mantivessem contato com seus batalhões independentemente de seus movimentos. Mas essa facilidade de comunicação também significava que essa mensagem poderia chegar aonde não deveria, a chamada **interceptação**. Por causa disso, era necessário uma codificação confiável para que terceiros, ao interceptar as mensagens, não conseguissem decifrá-las.

Toda essa indefinição acerca da comunicação via rádio foi posta em prova na *Primeira*

Guerra Mundial (1914-1918), onde as nações envolvidas queriam utilizar esse poder do rádio, mas não conseguiam garantir sua segurança. Não houve nenhum avanço na criptografia nesse período, no sentido de se criarem cifras que sejam difíceis de serem quebradas. Por mais que houvesse essa insegurança, a quantidade de mensagens transmitidas pelo rádio durante a Guerra foi enorme e todas corriam risco de serem interceptadas.

No período entre guerras, a procura por um sistema eficiente e seguro que possa ser usado nos conflitos seguintes continuou. Isso, felizmente, aconteceu com os criptográficos deixando de usar lápis e papel e passando a explorar a tecnologia da época. Na década de 1920, o engenheiro alemão *Arthur Scherbius (1878-1929)* desenvolveu uma máquina criptográfica que era uma versão elétrica do Disco de Alberti. Ele patentou essa máquina e deu a ela o nome de **Enigma**. Essa invenção se tornaria o mais complicado sistema de cifragem da história e a partir de 1926, o exército alemão passou a desfrutar desse sistema.

Com a *Segunda Guerra Mundial (1939-1945)*, os alemães acreditavam que a máquina Enigma teria um papel vital na vitória do Eixo, mas isso não aconteceu. Uma equipe de milhares de matemáticos trabalhava anonimamente para conseguir quebrar a máquina Enigma, entre eles *Alan Turing (1912-1954)*. Antes de trabalhar nessa equipe, Turing era professor de matemática em Cambridge, onde, em 1937, publicou um trabalho científico intitulado *"On Computable Numbers"* (Sobre Números Computáveis, tradução nossa), onde descreve uma máquina imaginária que poderia efetuar de forma automática os processos que são desenvolvidos por um matemático. Essas máquinas, chamadas de "Máquinas de Turing", foram as precursoras dos primeiros computadores, que surgiram décadas depois.

Em 1939, Turing recebe um convite da Escola de Cifras e Códigos do Governo da Inglaterra para se tornar um **Criptoanalista** (especialista em quebrar cifras), e interrompe sua carreira em Cambridge. Essa escola tinha sede na Mansão Bletchley Park e seu único objetivo era quebrar as chaves da máquina Enigma.

Os ingleses já tinham uma réplica da máquina Enigma, mas não conseguiam decifrar as mensagens cifradas porque o segredo era saber como a máquina era ajustada, pois a chave permanecia em segredo. Essa busca pela quebra da cifra continuou até que Turing, seguindo os caminhos do matemático polonês *Marian Rejewski (1905-1980)*, que havia quebrado uma versão mais simples da máquina Enigma, e em conjunto com os outros pesquisadores em Bletchley Park, conseguiram quebrar a versão atual e mais avançada da Enigma, o que alterou o curso da guerra[11].

4.7.4 Criptografia pós-guerra: Diffie-Hellman e RSA

Após a segunda guerra, o uso da tecnologia e dos computadores pasou a ser cada vez mais presente na criptografia e na criptoanálise. Começando com a *máquina Colossus*, os criptoanalistas continuaram a desenvolver tecnologias computacionais para auxiliá-los na

[11] Estima-se que isso antecipou o término da guerra em três anos.

quebra de todas as cifras, enquanto que os criptógrafos começaram a contra-atacar, usando os computadores para desenvolver cifras mais complexas.

Essas cifras podem ser divididas em **cifras simétricas e cifras assimétricas**.

Sobre as cifras simétricas, BURNETT (2002) diz que "*Nessa abordagem, um algoritmo utiliza uma **chave** para converter as informações naquilo que se parece com bits aleatórios. Assim, o mesmo algoritmo utiliza a mesma chave para recuperar os dados originais.*"

Sobre as cifras assimétricas:

> *Esse esquema utiliza duas chaves diferentes. Mesmo estando relacionadas entre si — elas são parceiras — elas são significativamente diferentes. O relacionamento é matemático; o que uma chave encripta a outra chave decripta. Na criptografia simétrica, a mesma chave é utilizada para encriptar e decriptar. Se utilizar uma outra chave qualquer para decriptar, o resultado será algo sem sentido. Mas com a criptografia assimétrica, a chave que é utilizada para encriptar os dados não é utilizada para decriptá-los; apenas a parte correspondente pode. (BURNETT, 2002)*

A imagem abaixo ajuda a mostrar essa diferença:

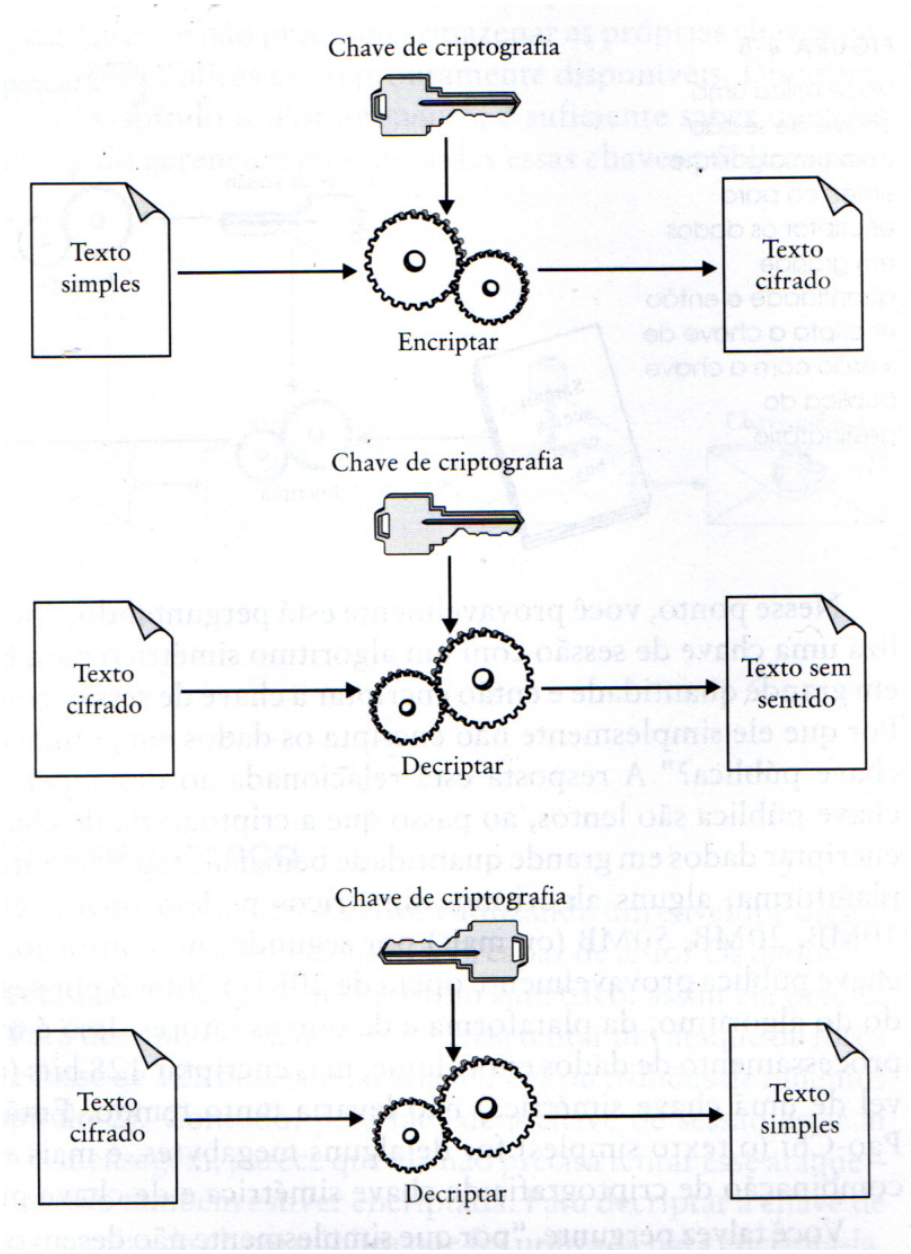

Figura 6 – Diferenças entre as cifras simétrica e assimétrica

Na década de 1960, os computadores ficaram mais poderosos, em maior quantidade e mais baratos. O que era algo que somente o governo e os militares teriam, agora estava presente também em empresas, e com isso as cifragens ficaram cada vez mais difundidas. Um dos fatores que determinam a "força" de uma cifra é a quantidade de chaves possíveis, o seu **espaço de chaves**. Quanto maior for esse conjunto, maior será o número de possibilidades e, consequentemente, o tempo para encontrar a chave certa será maior, via força bruta.

Quando duas pessoas querem conversar "em segredo", essas pessoas tinham que combinar entre elas uma chave. O problema é que, a não ser que essa chave seja combinada numa conversa pessoal, essa chave teria que ser combinada via computador ou via outro método, e a chance dessa chave ser interceptada ou roubada era relativamente alta. Esse problema é chamado de *Problema da Distribuição de Chaves*. Um dos criptógrafos interessados em resolver

esse problema era *Whitfield Diffie (1944-presente)*, graduado pelo Instituto de Tecnologia de Massachussets (MIT). Em 1974, em uma palestra apresentada por ele sobre as suas tentativas em resolver o problema da distribuição de chaves, ele acaba conhecendo outro criptógrafo, *Martin Hellman (1945-presente)*. Os dois acabaram por trabalhar juntos para tentar resolver o problema da distribuição de chaves. Mais tarde se junta a eles o pesquisador *Ralph Merkle (1952-presente)*. A ideia trabalhada por eles era a ligação entre a criptografia e a teoria dos números, que atualmente é uma ligação irreversível. Ela pode ser exemplificada na seguinte situação.

Exemplo 4.84 (Retirado de Hefez (2016))**.** João e Maria querem trocar entre si uma chave secreta por telefone. Eles escolhem, em comum acordo, dois números naturais a e m, e os tornam públicos. João escolhe outro número natural α_J e o mantém secreto. Com esse número ele calcula o **único** número $\beta_j < m$ tal que $a^{\alpha_J} \equiv \beta_J \pmod{m}$, e o envia para Maria. Maria, por sua vez, escolhe um número natural α_M, também mantendo-o secreto, e com ele calcula o único número $\beta_M < m$ tal que $a^{\alpha_M} \equiv \beta_M \pmod{m}$ e o envia para João.

Em seguida, João calcula $\beta_M^{\alpha_J}$, obtendo:

$$\beta_M^{\alpha_J} \equiv (a^{\alpha_M})^{\alpha_J} \equiv a^{\alpha_M \alpha_J} \equiv \alpha \pmod{m},$$

com $\alpha < m$.

Por sua vez, Maria calcula $\beta_J^{\alpha_M}$, obtendo:

$$\beta_J^{\alpha_M} \equiv (a^{\alpha_J})^{\alpha_M} \equiv a^{\alpha_J \alpha_M} \equiv \alpha \pmod{m},$$

com $\alpha < m$.

Pronto! Está trocada a chave secreta (α) entre João e Maria. São públicas as informações a,m,β_J,β_M e são secretas as informações α_J, que só João conhece, α_M, que só Maria conhece e α, que ambos conhecem.

Exemplo 4.85. Pegue a situação acima e considere $a = 52$ e $m = 271$. Além disso, João escolhe $\alpha_J = 5$ e Maria escolhe $\alpha_M = 7$. Qual será a chave secreta?

João faz o seguinte cálculo para determinar β_J e enviá-lo a Maria:

$$52^2 \equiv 2704 \equiv 265 \pmod{271}$$
$$52^4 \equiv 265^2 \equiv 36 \pmod{271}$$
$$52^7 = 52^4 \times 52^2 \times 52 \equiv 36 \times 265 \times 52 \equiv 496080 \equiv 150 \pmod{271}.$$

Logo, $\beta_J = 150$. Por sua vez, Maria faz a seguinte conta para determinar β_M e enviá-lo a João:

$$52^5 = 52^4 \times 52 \equiv 36 \times 52 \equiv 246 \pmod{271}.$$

Logo, $\beta_M = 246$. Para determinar a chave α, João tem que reduzir $\beta_M^{\alpha_J} = 246^7$ módulo 271. Logo,

$$246^2 = 60516 \equiv 83 \pmod{271}$$

$$246^4 = 246^2 \times 246^2 \equiv 83 \times 83 \equiv 114 \pmod{271}$$
$$246^7 = 246^4 \times 246^2 \times 246 \equiv 114 \times 83 \times 246 \equiv 33 \pmod{271}$$

João encontra então $\alpha = 33$.

Agora é a vez de Maria calcular o resíduo de $\beta_J^{\alpha_M} = 150^5$ módulo 271. Mas, $150^2 = 22500 \equiv 7 \pmod{271}$, logo

$$150^5 = 150^2 \times 150^2 \times 150 = 7 \times 7 \times 150 \equiv 33 \pmod{271}$$

encontrando também, como era de se esperar, $\alpha = 33$.

O sucesso deste método reside no fato de ser difícil descobrir qualquer dos três números α_J, α_M ou α, conhecendo apenas os dados públicos a, m, β_J e β_M. De fato, dado $x \in \mathbb{N}$, relativamente fácil calcular o resto da divisão de a^x por m, mas é difícil fazer o caminho oposto, ou seja, dado $y \in \mathbb{N}$ é difícil encontrar $x \in \mathbb{N}$ tal que y é o resto da divisão de a^x por m. Os restos da divisão de a^x por m, ao variar x, comportam-se de modo caótico. Assim, dado y, para resolver em x a equação $a^x \equiv y \pmod{m}$ é necessário construir a tabela dos valores da função

$$\mathbb{N} \to \mathbb{Z}_m$$
$$x \to [a^x]$$

o que pode ser computacionalmente inviável, dependendo de uma boa escolha de a e de m.

Todos os métodos descritos até agora (exceto o método acima) são de cifras simétricas, já descrita anteriormente. O contrário desse método é o método de cifras assimétricas, também já descrita anteriormente. Essa distinção é o que torna essa cifra tão especial, que revolucionaria o mundo da criptografia, no sentido assimétrico. No sentido simétrico, há o AES (Advanced Standard Encription), que é simétrico e é utilizado para grandes transferências de dados. Para mais detalhes sobre o AES, veja (Daemen; Rijmen, 2002). Diffie e Hellman tinham convencido o mundo que o problema de distribuição de chaves havia solução mas nunca conseguiram tornar em realidade a cifra assimétrica. **O método exemplificado acima resolve esse problema no caso particular de troca entre duas pessoas de cada vez**.

Essa "corrida" foi vencida por um trio de pesquisadores:

- *Ron **R**ivest (1947-presente)*
- *Adi **S**hamir (1952-presente)*
- *Leonard **A**dleman (1945-presente)*

Rivest e Shamir eram os responsáveis pelas ideias e pela formalização das mesmas, enquanto que Adleman era o responsável em detectar falhas nas ideias de Rivest e Shamir, garantindo que eles não perdessem tempo em ideias que não chegariam a lugar nenhum. A primeira versão foi feita em abril de 1977 e a versão final foi publicada em setembro de 1977 (disponível em <`https://people.csail.mit.edu/rivest/Rsapaper.pdf`>. Rivest

foi quem fez essa descoberta, com a contribuição de Shamir e de Adleman, aos quais citou na sua primeira versão. Adleman não concordou em ser considerado um dos autores pois não foi ele quem fez a descoberta e sim quem identificava as falhas. Após discussão, Adleman concorda em ser citado como o terceiro autor. E assim esse método acabou sendo chamado de **RSA** (Rivest, Shamir e Adleman), tornando-se a cifra mais influente da criptografia moderna e hoje mais conhecida como criptografia de chave pública.

Na seção seguinte, iremos entrar bem em detalhes nesse método.

4.8 CRIPTOGRAFIA RSA

Tudo (ou quase tudo) o que foi visto nas seções anteriores será usado nessa seção, para mostrarmos como que a criptografia RSA funciona e como descrever ela. Além de mostrar esse funcionamento, precisamos ver se de fato ela é segura. O conteúdo presente é baseado em Severino Colier Coutinho (1997).

4.8.1 Pré-Codificação

Para codificarmos uma mensagem, é necessário fazer um procedimento preliminar para podermos fazer a codificação, que é converter a mensagem em uma sequência de números.

Suponhamos, para simplificar, que a mensagem original é um texto onde não há números, apenas palavras, e no qual todas as letras são maiúsculas. Portanto, em última análise, a mensagem é constituída pelas letras que formam as palavras e pelos espaços entre palavras. Chamaremos esta primeira etapa de pré-codificação, para distingui-la do processo de codificação propriamente dito.

Na pré-codificação, convertemos as letras em números usando a seguinte tabela de conversão:

Tabela 4 – Pré-codificação na criptografia RSA.

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Fonte: Severino Collier Coutinho (2015)

O espaço entre duas palavras será substituído pelo número 99, quando for feita a conversão. Por exemplo, a frase "AMO GATOS" é convertida no número

$$10\ 22\ 24\ 99\ 16\ 10\ 29\ 24\ 28$$

Observe que precisamos fazer cada letra corresponder a um número de, pelo menos, dois algarismos para evitar ambiguidades. Se fizéssemos A corresponder ao número 1, B ao 2

, e assim por diante, não teríamos como saber se 19 representa "AI" ou "S", já que esta última é a décima nona letra do alfabeto.

Antes de continuar, precisamos determinar os parâmetros do sistema RSA que vamos usar. Estes parâmetros são dois primos distintos, que vamos denotar por p e q. Escolhidos esses primos p e q, faça $n = p \cdot q$. A parte final da pré-codificação consiste em separar a mensagem original em blocos, onde cada bloco deve ser menor que o número n e não pode começar com 0. Por exemplo, se escolhermos $p = 13$ e $q = 23$, teremos $n = 299$. A mensagem acima convertida em números seria dividida nos blocos abaixo:

$$102 - 224 - 99 - 16 - 102 - 92 - 42 - 8$$

Note que essa divisão dos blocos não é única, mesmo que se tome o cuidado de não começar nenhum bloco com o número 0. Além disso, nenhum desses blocos representam uma unidade linguística (da tabela), ou seja, é quase que literalmente impossível decifrar essa mensagem pelo método de frequência.

Por exemplo, a frase "O alcance da república é imenso" convertida em números, seria:

$$24\ 99\ 10211210231214\ 99\ 1310\ 99\ 271425301121181210\ 99\ 14\ 182214232824$$

Se formos fazer a divisão em blocos, teríamos algo do tipo:

$$\cdots - 102 - 112 - \cdots - 30 - 112 - 118 - \ldots$$

Dois blocos representados pelo número 112, mas que foram gerados por sequências de letras diferentes. O primeiro através da sequência "LC" e o segundo através da sequência "BL".

4.8.2 Codificação

Para codificarmos a mensagem, precisamos de n, o produto dos primos definido na pré-codificação, e de um número inteiro positivo e que seja invertível módulo $\varphi(n)$, ou seja, $\mathrm{mdc}(e, \varphi(n)) = 1$. Como visto anteriormente, já que n é um produto de primos p e q, distintos, então:

$$\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1) \cdot (q-1)$$

O par (n,e) é chamado de *chave de codificação* do sistema RSA que estamos usando. Supondo que já submetemos a mensagem à pré-codificação, temos uma sequência de números que, como na seção anterior, chamaremos de blocos. Codificaremos cada bloco separadamente. A mensagem codificada será a sequência dos blocos codificados. Isto é muito importante porque, depois de codificados, os blocos não podem mais ser reunidos de modo a formar um longo número.

Então, se a chave de codificação for um par (n,e), como codificar um bloco b qualquer? Por construção, b deve ser menor que n. Denotando o bloco codificado por $\mathbf{C}(b)$, ele é calculado

da forma:

$$\mathbf{C}(b) = \text{ resto da divisão de } b^e \text{ por } n$$

Em termos de aritmética modular, $\mathbf{C}(b) \equiv b^e \pmod{n}$, com $0 \leq \mathbf{C}(b) < n$.

Vamos retornar ao nosso caso: $p = 13$ e $q = 23$, logo $n = 299$. Com isso, $\varphi(n) = 12 \cdot 22 = 264$. Precisamos agora encontrar um valor para e, sabendo que e é invertível, módulo 264. Uma forma simples de encontrar esse número é encontrar o menor primo que não divide 264, esse número é o número 5. Assim, o primeiro bloco da mensagem a ser codificada, 102, será codificado como o resto da divisão de 102^5 por 299. Vamos fazer as contas:

$$102^5 \equiv 102^2 \cdot 102^2 \cdot 102 \equiv 238 \cdot 238 \cdot 102 \equiv 133 \cdot 102 \equiv 13.566 \equiv 111 \pmod{299}$$

Codificando toda a mensagem, bloco a bloco, obtemos:

$$\begin{aligned}
224^5 &\equiv (-75)^5 \equiv (-75)^2 \cdot (-75)^2 \cdot 224 \equiv 243^2 \cdot 224 \equiv 146 \cdot 224 \equiv 113 \pmod{299} \\
99^5 &\equiv (99)^3 \cdot (99)^2 \equiv 44 \cdot 233 \equiv 86 \pmod{299} \\
16^5 &\equiv (16^2)^2 \cdot 16 \equiv (-43)^2 \cdot 16 \equiv 55 \cdot 16 \equiv 282 \pmod{299} \\
102^5 &\equiv 111 \pmod{299} \\
92^5 &\equiv (92^2)^2 \cdot 92 \equiv 92^2 \cdot 92 \equiv 92 \cdot 92 \equiv 92 \pmod{299} \\
42^5 &\equiv (42^2)^2 \cdot 42 \equiv 269^2 \cdot 42 \equiv 3 \cdot 42 \equiv 126 \pmod{299} \\
8^5 &\equiv 8^3 \cdot 8^2 \equiv 213 \cdot 64 \equiv 177 \pmod{299}
\end{aligned}$$

Portanto, a mensagem codificada será:

$$111 - 113 - 86 - 282 - 111 - 92 - 126 - 177$$

4.8.3 Decodificação

Com a mensagem codificada, iremos ver agora como o procedimento para **decodificarmos** essa mensagem, bloco por bloco. Do que precisamos? Do número n e do inverso de e, módulo $\varphi(n)$, o qual chamaremos de d. Esse par (n,d) é chamado de **par de decodificação**. Se a for um bloco da mensagem codificada, então $\mathbf{D}(a)$ será o resultado do processo de decodificação. Tal como na codificação, $\mathbf{D}(a)$ é calculado da forma:

$$\mathbf{D}(a) = \text{ resto da divisão de } a^d \text{ por } n$$

Em termos de aritmética modular, $\mathbf{D}(a) \equiv a^d \pmod{n}$, com $0 \leq \mathbf{D}(a) < n$.

Tendo em posse os valores de e e de $\varphi(n)$, é relativamente simples encontrarmos d, basta usar o algoritmo de Euclides estendido (cf. Seção 4.2.2). Por outro lado, se queremos decodificar um bloco já codificado, o esperado é que o resultado seja o bloco original, ou seja, $\mathbf{D}(\mathbf{C}(b)) = b$. Precisamos ver cuidadosamente que isso é realmente verdade e isso será feito na próxima seção.

No exemplo atual, temos $n = 299$ e $e = 5$. Vamos aplicar o algoritmo de Euclides estendido para calcularmos d. Lembremos que d é o inverso de e módulo $\varphi(n) = 264$, ou seja, no nosso caso, $5d \equiv 1 \pmod{264}$, o que equivale a $5d - 264k = 1$, logo $5d + 264(-k) = 1$. Nem precisamos fazer todo o procedimento pois $264 = 5 \cdot 53 - 1$, donde $1 = 264 \cdot (-1) + 5 \cdot 53$, ou seja, $d = 53$. Assim, para podermos decodificar o bloco 111 da mensagem codificada, precisamos calcular a forma reduzida de 111^{53}, módulo 299. Efetuar a conta 111^{53} de maneira direta (sem auxílio do computador) é um procedimento bem longo, para não dizer impossível. Felizmente, podemos usar o Teorema Chinês dos Restos e o Pequeno Teorema de Fermat para aliviar as contas.

Como $299 = 13 \cdot 23$, podemos encontrar os resíduos de 111^{53} módulo 13 e módulo 23, respectivamente. Como $\varphi(13) = 12$ e $\varphi(23) = 22$, podemos usar o Pequeno Teorema de Fermat para calcularmos os resíduos. Começando pelo resíduo módulo 13:

$$\begin{aligned} 111^{12} &\equiv 1 \pmod{13} \\ (111^{12})^4 &\equiv 1^4 \pmod{13} \\ 111^{48} &\equiv 1 \pmod{13} \\ 111^{53} &\equiv 111^5 \pmod{13} \end{aligned}$$

Vamos lidar com o 111^5 agora. Como $111 \equiv 7 \pmod{13}$, então $111^2 \equiv 49 \equiv 10 \pmod{13}$, logo $111^4 \equiv 100 \equiv 9 \pmod{13}$. Deste modo $111^5 \equiv 63 \equiv 11 \pmod{13}$, portanto, por transitividade, $111^{53} \equiv 11 \pmod{13}$.

Vamos encontrar o resíduo módulo 23 agora:

$$\begin{aligned} 111^{22} &\equiv 1 \pmod{23} \\ (111^{22})^2 &\equiv 1^2 \pmod{23} \\ 111^{44} &\equiv 1 \pmod{23} \\ 111^{53} &\equiv 111^9 \pmod{23} \end{aligned}$$

Vamos lidar com o 111^9 agora. Como $111 \equiv 19 \pmod{23}$, então $111^2 \equiv 361 \equiv 16 \pmod{23}$, logo $111^4 \equiv 256 \equiv 3 \pmod{23}$. Deste modo, $111^8 \equiv 9$ e $111^9 \equiv 171 \equiv 10 \pmod{23}$, portanto, por transitividade, $111^{53} \equiv 10 \pmod{23}$.

Dos dois resultados obtidos, $111^{53} \equiv 11 \pmod{13}$ e $111^{53} \equiv 10 \pmod{23}$, eles são correspondentes ao sistema:

$$\begin{cases} x \equiv 11 \pmod{13} \\ x \equiv 10 \pmod{23} \end{cases}$$

O que é possível de se resolver via Teorema Chinês dos Restos (cf. Seção 4.6.1.1).

Considerando $c_1 = 11$, $c_2 = 10$, $m_1 = 13$, $m_2 = 23$, $M_1 = 23$ e $M_2 = 13$, como $\mathrm{mdc}(m_1, M_1) = 1$ e $\mathrm{mdc}(m_2, M_2) = 1$, então precisamos expressar 1 como combinação linear de 13 e 23, essencialmente resolvendo a eq. Diofantina $13x + 23y = 1$. Vamos resolver via

algoritmo de Euclides estendido:

$$\begin{bmatrix} 13 & 1 & 0 \\ 23 & 0 & 1 \end{bmatrix} \Longrightarrow \begin{bmatrix} 13 & 1 & 0 \\ 23-1\cdot 13 & -1 & 1 \end{bmatrix} \Longrightarrow \begin{bmatrix} 13 & 1 & 0 \\ 10 & -1 & 1 \end{bmatrix} \Longrightarrow$$
$$\Longrightarrow \begin{bmatrix} 13-1\cdot 10 & 1-1\cdot(-1) & 0-1\cdot 1 \\ 10 & -1 & 1 \end{bmatrix} \Longrightarrow \begin{bmatrix} 3 & 2 & -1 \\ 10 & -1 & 1 \end{bmatrix} \Longrightarrow$$
$$\Longrightarrow \begin{bmatrix} 3 & 2 & -1 \\ 10-3\cdot 3 & -1-3\cdot 2 & 1-3\cdot(-1) \end{bmatrix} \Longrightarrow \begin{bmatrix} 3 & 2 & -1 \\ 1 & -7 & 4 \end{bmatrix} \Longrightarrow$$
$$\Longrightarrow \begin{bmatrix} 3-3\cdot 1 & 2-3\cdot(-7) & -1-3\cdot 2 \\ 1 & -7 & 4 \end{bmatrix} \Longrightarrow \begin{bmatrix} 0 & 23 & -7 \\ 1 & -7 & 4 \end{bmatrix}$$

Portanto, $x = -7$ e $y = 4$, logo $1 = 13 \cdot (-7) + 23 \cdot 4$ e, desse modo,

$$11 = 13 \cdot (-77) + 23 \cdot (44) \quad \text{e} \quad 10 = 13 \cdot (-70) + 23 \cdot (40).$$

Portanto, uma solução do sistema é:

$$X_0 = 23 \cdot 44 + 13 \cdot (-70) = 1012 - 910 = 102$$

Portando o bloco 111, ao ser decodificado, retorna o bloco 102, o que era o esperado. Ao invés de fazermos esses mesmos cálculos demorados para os outros blocos, iremos mostrar que esse método de codificação e de decodificação de fato funciona.

4.8.4 Funcionamento

Como foi mostrado nos cálculos anteriores, nós tínhamos um bloco pré-codificado (102), que codificado retornou o bloco 111 e que decodificado retornou o bloco 102 novamente. O método exposto acima só será útil se o que aconteceu nos cálculos de fato acontecer com **qualquer** bloco. Digamos que temos um sistema RSA de parâmetros p e q, onde $n = pq$. Então para codificarmos, precisamos de "n" e "e", e para decodificarmos, precisamos de "n" e "d". Na notação que usamos anteriormente, precisamos mostrar que se temos um bloco b, $0 \leq b \leq n-1$, então $\mathbf{D}(\mathbf{C}(b)) = b$.

Na verdade só precisamos mostrar que $\mathbf{D}(\mathbf{C}(b)) \equiv b \pmod{n}$ pois, ambos os números $\mathbf{D}(\mathbf{C}(b))$ e b estão no intervalo entre 0 e $n-1$, e eles só serão congruentes módulo n se forem iguais. Isso é o motivo de, na pré-codificação, os blocos serem formados de forma a cada bloco ser menor que n e que esses blocos tenham que ficar separados mesmo após a codificação.

Da definição de $\mathbf{D}$ e de $\mathbf{C}$ temos que

$$\mathbf{D}(\mathbf{C}(b)) \equiv (b^e)^d \equiv b^{ed} \pmod{n} \tag{12}$$

Porém d é o inverso de e módulo $\varphi(n)$, ou seja, $ed = 1 + k\varphi(n), k \in \mathbb{Z}$. Como d e e são inteiros maiores do que 2 e $\varphi(n) > 0$, então $k > 0$. Substituindo ed em (12), temos:

$$b^{ed} \equiv b^{1+k\varphi(n)} \equiv (b^{\varphi(n)})^k b \pmod{n}$$

Como $b^{\varphi(n)} \equiv 1 \pmod{n}$, pelo Teorema de Euler, nos resta $b^{ed} \equiv b \pmod{n}$. Portanto, $\mathbf{D}(\mathbf{C}(b)) \equiv b \pmod{n}$, o que resolveria nossa demonstração, mas, para podermos usar o Teorema de Euler, estaríamos assumindo que $\mathrm{mdc}(b,n) = 1$, o que não necessariamente é verdade. Para evitarmos isso, teremos que demonstrar sem usar o Teorema de Euler.

Para isso, lembre-se que $n = pq$ em que p e q são primos distintos. Vamos calcular a forma reduzida de b^{ed} módulo p e módulo q (são análogos). Vamos começar com a forma reduzida de b^{ed}, módulo p.

Sabemos que existe $k \in \mathbb{Z}$ tal que $ed = 1 + k\varphi(n)$, mas como $\varphi(n) = (p-1)(q-1)$ então $ed = 1 + k(p-1)(q-1)$. Logo:

$$b^{ed} \equiv b \cdot (b^{p-1})^{k(q-1)} \pmod{p}$$

Parece ser o momento para usarmos o Pequeno Teorema de Fermat, mas para isso, precisamos analisar se p divide b.

- Caso p não divida b, então $b^{p-1} \equiv 1 \pmod{p}$, pelo Pequeno Teorema de Fermat, o que implica em $b^{ed} \equiv b \pmod{p}$.
- Caso p divida b, então $b \equiv 0 \pmod{p}$ e a congruência é imediatamente verificada, pois $b^{ed} \equiv 0 \equiv b \pmod{p}$.

Analogamente, mostra-se que $b^{ed} \equiv b \pmod{q}$. Com isso, temos que $b^{ed} - b$ é divisível tanto por p quanto por q. Como p e q são primos distintos, então $\mathrm{mdc}(p,q) = 1$. Pela Proposição 4.15, item 4, temos que pq divide $b^{ed} - b$. Como $n = pq$, concluímos que $b^{ed} \equiv b \pmod{n}$, para qualquer inteiro b. Isto encerra a demonstração que o método funciona, ou seja, que $\mathbf{D}(\mathbf{C}(b)) = b$.

4.8.5 Segurança

Como já sabemos, a criptografia RSA é uma criptografia de *chave pública*, onde a chave de codificação, (n,e) é acessível a qualquer usuário. A segurança do RSA depende da dificuldade de se calcular d quando n e e são conhecidos. Como nós vimos anteriormente, d é o inverso de e módulo $\varphi(n)$, e, para obtê-lo, teríamos que aplicar o algoritmo de Euclides estendido. Mas, para obtermos $\varphi(n)$, teríamos que fatorar n para obtermos p e q. O segredo para "quebrarmos" o código é conseguirmos fatorar n. Por isso, o ideal é que n seja um número grande, pois não existe um algoritmo rápido de fatoração que permita "quebrar" n em dois fatores, independentemente da quantidade de algarismos de n.

Embora não exista uma demonstração de que quebrar o RSA e fatorar n sejam problemas equivalentes, ou seja, que provar um significa provar o outro, ou vice-versa, geralmente se acredita nessa conjectura, como afirma Rivest e Kaliski (2003).

Mas se uma fatoração difícil/impossível de n é o segredo para assegurar a segurança do RSA, *como escolher* os primos p e q? De acordo com Severino Colier Coutinho (1997), é

compreensível que, se ambos os números forem pequenos, é fácil fatorar n. Ainda, se ambos forem grandes mas $\mid p - q \mid$ for pequeno, também será fácil fatorar n usando o *Algoritmo de Fermat* (cf. Seção 4.4.1).

O sistema RSA está em uso faz-se muitos anos e uma escolha adequada de primos p e q torna o sistema muito seguro. Além desse, existem outros métodos, em que a fatoração se torna possível se $p-1$ ou $q-1$ tiverem fatores primos pequenos, chamado de método *p-1 de Pollard* (cf. Capítulo A), e um método em que a fatoração se torna possível se $p+1$ ou $q+1$ tiverem fatores primos pequenos, chamado método de *p+1 de Williams*.

De acordo com Singh (1999), normalmente, para uso pessoal, uma chave deve ter tamanho da ordem 10^{231} aproximadamente, com 231 algarismos, ou seja, os primos p e q deveriam ter, por exemplo, 110 e 121 algarismos, respectivamente. Para importantes transações bancárias, esse número seria ainda maior, da ordem 10^{308} aproximadamente, ou seja, com 308 algarismos. Com o passar do tempo, essas ordens irão aumentar, mas, para valores suficientemente grandes de p e de q, o RSA é invencível... por enquanto.

Não sabemos o que o futuro nos reserva, mas é possível que, em alguma época no futuro, alguém encontre um modo rápido de fatorar qualquer n, o que tornaria o RSA inútil. Mas até agora não existe nenhum método de fatoração realmente rápida, além do que, matemáticos acreditam que fatorar números grandes é uma tarefa *inerentemente difícil*. Por enquanto, o RSA é seguro. Não se sabe por quanto tempo. Quem sabe até o dia em que os computadores quânticos forem completamente desenvolvidos.

5 CONSIDERAÇÕES FINAIS

Nessa dissertação, foram selecionados e organizados todos os tópicos fundamentais da Teoria dos Números e da Aritmética Modular para que se tivesse uma melhor compreensão da Criptografia RSA. Em respeito a história da criptografia e dos sistemas criptográficos, foi realizado um resumo da história da criptografia, da antiguidade até os dias atuais. Como o enfoque é na criptografia RSA, foi realizada uma explicação, em passo a passo, de como essa criptografia funciona, no sentido de codificar uma mensagem e decodificar a mensagem codificada. Foi ressaltado o funcionamento dessa cifra e suas principais preocupações em relação à sua segurança.

Como produto educacional, uma apostila foi realizada, contendo todos os fundamentos necessários para se compreender a criptografia RSA, de uma forma acessível e contextualizada. São apresentados exemplos e mais de 30 exercícios propostos com suas resoluções constando em um apêndice, de uso exclusivo do professor. Recomenda-se a aplicação da apostila para alunos do ensino médio, podendo ser adaptada para outros níveis de ensino de acordo com a estratégia do professor aplicador.

Futuramente, uma evolução natural dessa pesquisa será elaborar e organizar uma sequência didática adequada para a aplicação da apostila em sala de aula, levando em consideração o contexto da escola e dos alunos. Além disso, outra evolução natural será aliar a teoria presente na dissertação à aplicações usando linguagens de programação (*Python*, *C++*, etc), além de realizar pesquisas em outros métodos criptográficos, mais complexos que o RSA, tais como o logaritmo discreto e as teorias baseadas em computação quântica, como por exemplo: (Shor, 1997), (Jr., 2023), (Dullius, 2001), entre outros. Aliado a isso, a apostila poderá ser reformulada ao ponto de incluir esses métodos, aumentando também sua complexidade.

Como a apostila ainda está em sua versão inicial, ela não passou por uma avaliação formal (*feedback*) de professores de escolas públicas ou particulares. Esse retorno é fundamental para verificar se os conteúdos estão realmente adequados ao nível do ensino médio e se os exercícios podem ser resolvidos pelos alunos, tanto em sala de aula, com o apoio do professor, quanto de forma autônoma em casa. É sempre essencial considerar o contexto específico de cada escola e de seus estudantes, de modo que a apostila seja acessível ao maior número possível de alunos e também de professores.

Todo o conteúdo presente nesta dissertação e no produto educacional busca auxiliar em futuras investigações acerca da criptografia RSA e da criptografia em geral, bem como incentivar o interesse de estudantes por essa área do conhecimento. Paralelamente a isso, a leitura e as interlocuções dos leitores poderão contribuir para um maior aprofundamento em pesquisas nesta área, e isso é muito importante.

REFERÊNCIAS

BARNABÉ, Vinícius Cardoso. **Uma introdução aos métodos de fatoração de inteiros de Fermat e Pollard**. Dourados, MS: [s.n.], jan. 2009. Orientadora: Profa. MSc. Adriana Betânia de Paula Molgora.

BEZERRA, Maria de Nazaré Carvalho et al. **Teoria dos números: um curso introdutório**. [S.l.]: Editora Universitária da Assessoria de Educação a Distância-EditAedi, 2018.

BURNETT, STEVEN. **Criptografia e segurança: o guia oficial RSA**. [S.l.]: Gulf Professional Publishing, 2002.

CAMPOS, Valdigley Ferreira. **CRIPTOGRAFIA RSA: UMA PROPOSTA DE INTERDISCIPLINARIDADE**. 2020. B.S. thesis – IFSC.

CARNEIRO, Framilson José Ferreira. **Criptografia e Teoria dos números**. [S.l.]: Rio de Janeiro: Editora Ciência Moderna Ltda., 2017.

CAVALCANTE, Rogério da Silva. Aritmética com Python, 2018.

CERQUEIRA, Marcel Cavalcante. O estudo da criptografia RSA no ensino básico com auxílio de softwares computacionais. Universidade Federal de Alagoas, 2016.

COUTINHO, Severino Colier. **Números inteiros e criptografia RSA**. [S.l.]: IMPA, 1997.

COUTINHO, Severino Collier. Criptografia. **Rio de Janeiro, Programa de Iniciação Científica da OBMEP (PIC-OBMEP)**, 2015.

DAEMEN, Joan; RIJMEN, Vincent. **The design of Rijndael**. [S.l.]: Springer, 2002. v. 2.

DOMINGUES, Hygino Hugueros. **Fundamentos da aritmética**. [S.l.]: Florianópolis: Editora da UFSC, 2021.

DULLIUS, Maria Madalena. **O problema do logaritmo discreto**. 2001. Diss. (Mestrado) – Universidade Federal do Rio Grande do Sul, Porto Alegre, RS, Brasil. Dissertação (Mestrado), Instituto de Matemática. Orientador: Vilmar Trevisan. Disponível em: `https://lume.ufrgs.br/bitstream/handle/10183/118185/000271720.pdf?sequence=1`.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. [S.l.]: 6. ed. Ediitora Atlas SA, 2008.

HEFEZ, Abramo. **Aritmética**. [S.l.]: Rio de Janeiro: SBM, 2016.

HUI, Yang. **Xiangjie Jiuzhang Suanfa**. [S.l.]: Unknown, 1265. Inclui a história de Han Xin contando soldados, associada ao Teorema Chinês dos Restos.

ING, Law Huong. The History of The Chinese Remainder Theorem. **Mathematical Medley**, 2003.

JR., Robert L. Singleton. Shor's Factoring Algorithm and Modular Exponentiation Operators. **Quanta**, v. 12, p. 41–130, 2023. Preprint arXiv:2306.09122. Disponível em: `https://arxiv.org/pdf/2306.09122`.

KNUTH, Donald Ervin. **The art of computer programming**. [S.l.]: Pearson Education, 1997. v. 3.

LOVELESS, Andy. **The Fundamental Theorem of Arithmetic**. Seattle, WA, USA, 2011. Lecture notes for Math 300 – Introduction to Mathematical Reasoning. Disponível em: `https://sites.math.washington.edu/~aloveles/Math300Summer2011/FundamentalTheoremOfArithmetic.pdf`.

MORAES, Roque; GALIAZZI, Maria do Carmo. Análise textual discursiva: processo reconstrutivo de múltiplas faces. **Ciência & Educação (Bauru)**, SciELO Brasil, v. 12, p. 117–128, 2006.

NETO, Antônio Caminha Muniz. **Tópicos de Matemática Elementar Volume 5: Teoria dos Números**. [S.l.]: Rio de Janeiro: SBM, 2012.

NUCCI, Higor H. P.; GROSCH, Gustavo R. **Um estudo teórico e prático dos métodos de fatoração de inteiros de Fermat e Pollard p-1**. Dourados, MS: [s.n.], jan. 2009. Orientadora: Profa. MSc. Adriana Betânia de Paula Molgora.

OLIVEIRA LOPES, Gabriela Lucheze de; SILVEIRA LOPES, Jaques. Criptografia: a evolução histórica e seu potencial como ferramenta no ensino de teoria dos números nos cursos de licenciatura em matemática. **Universidade Federal do Rio Grande do Norte. V Conedu-congresso nacional de educação**, 2018.

PONTES, Edel Alexandre Silva; SILVA, Luciano Martins da. Aritmética modular na interpretação de sistemas codificados no processo de ensino e aprendizagem de matemática. **Revista de Ciência e Inovação**, v. 5, n. 1, 2020.

PRODANOV, Cleber Cristiano; DE FREITAS, Ernani Cesar. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico-2ª Edição**. [S.l.]: Editora Feevale, 2013.

REITENBACH, Markus. The power of the snake: number theory with Python. **International Journal of Mathematical Education in Science and Technology**, Taylor & Francis, v. 53, n. 12, p. 3484–3490, 2022.

RESENDE, Marilene Ribeiro; MACHADO, Silvia Dias Alcântara. O ensino de matemática na licenciatura: a disciplina Teoria Elementar dos Números. **Educação Matemática Pesquisa Revista do Programa de Estudos Pós-Graduados em Educação Matemática**, v. 14, n. 2, p. 257–278, 2012.

RIVEST, Ronald L.; KALISKI, Burt. The RSA Problem. **Technical Report, MIT / RSA Laboratories**, dez. 2003. Pré-publicação. Disponível em: `https://people.csail.mit.edu/rivest/pubs/RK03.prepub.pdf`.

ROCHA, Eugênio Carlos Rosa. Fundamentos matemáticos aplicado a alguns métodos de criptografia. Florianópolis, SC, 2008.

ROSA, Alex Almeida da. **Uso da Criptografia RSA no Ensino de Matemática**. 2023. Tese (Doutorado).

SHOR, Peter W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. **SIAM Journal on Computing**, Society for Industrial e Applied Mathematics, v. 26, n. 5, p. 1484–1509, 1997. Preprint disponível em: `https://arxiv.org/pdf/quant-ph/9508027`.

SILVA, Andresa Laurett da. Criptografia e algumas aplicações em sala de aula, 2021.

SILVA VASCONCELLOS, Luis Antonio da; MONTANHER, João Fernando. Introdução da Criptografia no Ensino Médio e Fundamental utilizando Aritmética Modular. **CQD-Revista Eletrônica Paulista de Matemática**, 2022.

SIMES, Eliton Mendes Pedrosa. **Criptografia RSA para o Ensino Médio**. 2023. Tese (Doutorado).

SINGH, Simon. **The code book**. [S.l.]: Doubleday New York, 1999. v. 7.

VIEIRA, Vandenberg Lopes. **Um curso básico em teoria dos números**. [S.l.]: Editora Livraria da Física, 2020.

VIZOLLI, Idemar; SOUZA CARVALHO, Euvaldo Euvaldo de; PEREIRA, Onésimo Rodrigues. CRIPTOGRAFIA: UMA POSSIBILIDADE PARA O ENSINO DE FUNÇÃO INVERSA. **REAMEC-Rede Amazônica de Educação em Ciências e Matemática**, v. 7, n. 1, p. 196–212, 2019.

WALTER, André. **Divisibilidade e congruência modular**. 2019.

WIKIPÉDIA. Disco de Alberti. In*:* WIKIPÉDIA: a enciclopédia livre. [S.l.]: Wikimedia, 2025.

APÊNDICE A – MÉTODO $p-1$ DE POLLARD

Quando estamos tratando da Criptografia RSA, será importante verificarmos se os primos escolhidos não sejam tais que o seu produto seja fatorado ("quebrado") facilmente. Uma das formas já foi vista no desenvolvimento, que é o *Método de Fermat*. Outra das formas em que isso acontece é se, dado um primo p, $p-1$ seja um número relativamente fácil de se fatorar (chamado de *suave*). Esse método detalha como fatorar um número caso isso aconteça.

Esse método foi desenvolvido por *John M. Pollard* em 1974. Existem duas formas de realizarmos a fatoração por esse método, uma via *exponencial* e uma via *fatorial*. Em ambas, o método é baseado no conceito de que se existe pelo menos um primo p na fatoração de n, tal que $p-1$ é um produto de primos relativamente pequenos. Vamos ver essas duas vias. Esse conteúdo é baseado no conteúdo presente em Barnabé (2009) e Nucci e Grosch (2009).

Algoritmo A.1 (Método de Pollard via exponencial)**.** Dado um número n que desejamos fatorar e um número limitante B, nós procuramos fatores de n.

Para tal, sejam p um número primo, k um número inteiro positivo tais que $p^k < B$, e a um número inteiro com $1 < a < [\sqrt{n}] + 1$.[1]

Determinamos r o resto da divisão de a^{p^k} por n, assim $a^{p^k} \equiv r \pmod{n}$. Deste modo, temos que $\mathrm{mdc}(r-1, n)$ é um fator de n.

Se $\mathrm{mdc}(r-1, n) \neq 1, n$, então $\mathrm{mdc}(r-1,n)$ é um fator não-trivial de n.

Testamos todos os possíveis valores de p e k, se $\mathrm{mdc}(r-1, n)$ resultar sempre em 1, então precisamos aumentar o valor de B, se $\mathrm{mdc}(r-1,n)$ resultar em n, escolhemos um valor diferente para a.

Exemplo A.2. Vamos tentar fatorar pelo método acima para $n = 143$.

Resolução. Vamos escolher $B = 7$, com isso $p = 2{,}3{,}5$. Como $\lfloor\sqrt{143}\rfloor + 1 = 12 + 1 = 13$, vamos escolher $a = 3$. Com a definido, os expoentes k serão, respectivamente, $2{,}1{,}1$. Vamos verificar os valores de r.

- Para $p = 2$, $k = 2$, temos que $3^{2^2} \equiv 3^4 \equiv 81 \pmod{143}$. Assim, $mdc(r-1,n) = mdc(80{,}143) = 1$. Não era o que queríamos, então, vamos pegar o próximo primo.
- Para $p = 3$, $k = 1$ e $3^{3^1} \equiv 3^3 \equiv 27 \pmod{143}$. Então, $mdc(r-1,n) = mdc(26{,}143) = 13$. Como foi diferente de 1 e de 143, então 13 é um dos fatores. De fato, $143 = 13 \times 11$.

□

Para fatorarmos pela via fatorial, supõe-se que n tem um fator primo p tal que $p-1$ tenha apenas primos pequenos em sua fatoração. Se n não tiver um fator p primo nessas condições, então o método não é eficiente. Seja $\tilde{k}$ o menor inteiro positivo tal que $p-1$ divide $\tilde{k}!$. Como $p-1$ tem apenas primos pequenos na fatoração, então $\tilde{k}$ será pequeno, o que facilita o cálculo.

[1] Aqui, $\lfloor x \rfloor$ é a função *parte inteira* ou função *piso*, que retorna o maior inteiro que é menor ou igual a x.

O Pequeno Teorema de Fermat é utilizado para justificar esse método (cf. Proposição 4.64): Se p é primo e $a \in \mathbb{Z}$ de modo que $p \nmid a$, então $a^{p-1} \equiv 1 \pmod{p}$.

Portanto, se $p-1$ divide $\tilde{k}!$, podemos dizer que $\tilde{k}! = (p-1) \cdot q$, para algum $q \in \mathbb{Z}$. Assim

$$a^{\tilde{k}!} = a^{(p-1)q} \equiv \left(a^{(p-1)}\right)^q \equiv 1^q \equiv 1 \pmod{p},$$

o que significa que p divide $a^{\tilde{k}!} - 1$.

Chamando de M o menor valor inteiro não-negativo que seja congruente a $a^{\tilde{k}!} - 1$ módulo n (ou seja, M é o resto de $a^{\tilde{k}} - 1$ por n), como p divide n (por hipótese) e n divide $M - (a^{\tilde{k}!} - 1)$, logo p divide $M - (a^{\tilde{k}!} - 1)$. Mais ainda, como p divide $a^{\tilde{k}!} - 1$, temos que p divide M. Assim, $\mathrm{mdc}(M, n)$ será um fator de n maior do que ou igual a p.

Para encontrar um divisor de n é preciso calcular $d = \mathrm{mdc}(M,n)$, que é possível via algoritmo de Euclides. Para que d não seja um divisor trivial ($d = 1$ ou $d = n$), é necessário que M não seja nulo, que é o caso onde o próprio n não divide $a^{\tilde{k}} - 1$, o que é provável quando n tem divisores primos bem grandes.

Na prática, para se usar esse método devemos calcular $a^{k!}$ módulo n, para $k = 1, 2, \ldots, \tilde{k} - 1$, e então calcular $\mathrm{mdc}(M_k,n)$, onde M_k é o resto de $a^{k!} - 1$ por n. Podemos fazer isso através de exponenciação modular. Para encontrar o menor valor de $a^{k!}$ módulo n fixamos $r_1 = a^1$ e usaremos a seguinte sequência de cálculos:

$$r_2 \equiv (r_1)^2 \pmod{n}, \quad r_3 \equiv (r_2)^3 \pmod{n}, \ldots, \quad r_k \equiv (r_{k-1})^k \pmod{n}.$$

Pois $a^{(n+1)!} = a^{(n+1)n!} = \left(a^{n!}\right)^{(n+1)}$.

Algoritmo A.3 (Método de Pollard via fatorial)**.** Dado n um número inteiro positivo, que desejamos fatorar, consideramos a um número inteiro positivo coprimo com n e a sequência $a^{1!}-1, a^{2!}-1, \ldots, a^{k!}-1, \ldots$. Considerando M_k o menor inteiro positivo tal que $M_k \equiv a^{k!}-1 \pmod{n}$, temos que $\mathrm{mdc}(M_k, n)$ será um divisor de n.

Vamos ver um exemplo.

Exemplo A.4. Vamos utilizar esse método para $n = 50.851$, com $a = 2$.

Resolução. Vamos fazer o passo a passo. Para cada M_k encontrado, testamos $\mathrm{mdc}(M_k - 1,n)$. Se esse mdc é 1, passamos para o próximo. Caso contrário, encontramos nosso fator.

$$\begin{aligned}
r_1 \equiv 2^1 \equiv 2 \pmod{50.851} &\implies \mathrm{mdc}(1,50.851) = 1 \\
r_2 \equiv (r_1)^2 \equiv 2^2 \equiv 4 \pmod{50.851} &\implies \mathrm{mdc}(3,50.851) = 1 \\
r_3 \equiv (r_2)^3 \equiv 4^3 \equiv 64 \pmod{50.851} &\implies \mathrm{mdc}(63,50.851) = 1 \\
r_4 \equiv (r_3)^4 \equiv 64^4 \equiv 16.777.216 \equiv 47.237 \pmod{50.851} &\implies \mathrm{mdc}(47.236,50.851) = 241
\end{aligned}$$

Para $k = 4$, obtemos um fator de 50.851 que é 241. Ao fazer a divisão, obtemos o outro fator, que é 211.

Desse modo, encontramos um divisor de 50.851 em apenas 4 passos. □