William Debon Pereira

FUNDAMENTOS DA ARITMÉTICA: PROPRIEDADES NATURAIS E ELEMENTARES DAS CONGRUÊNCIAS

Rio Grande, Rio Grande do Sul, Brasil

Dezembro, 2020

William Debon Pereira

FUNDAMENTOS DA ARITMÉTICA: PROPRIEDADES NATURAIS E ELEMENTARES DAS CONGRUÊNCIAS

Trabalho de Conclusão de Curso, Matemática Licenciatura, submetido por William Debon Pereira junto ao Instituto de Matemática, Estatística e Física da Universidade Federal do Rio Grande.

Universidade Federal do Rio Grande - FURG

Instituto de Matemática, Estatística e Física - IMEF

Curso de Matemática Licencitura

Orientador: Prof.ª Dr.ª Grasiela Martini

Coorientador: Prof. Dr. Eneilson Campos Fontes

Rio Grande, Rio Grande do Sul, Brasil

Dezembro, 2020

Grandiosamente dedico este trabalho à minha família e, em especial, aos meus pais (José Pereira e Fernanda Debon), pois sempre me apoiaram com minhas escolhas na vida. Posteriormente, à minha professora, orientadora, "psicóloga" e grande amiga Grasiela Martini bem como minha melhor amiga Lisiane Coutinho, visto que elas cederam seu tempo para poder escutar meus desabafos pessoais nos momentos em que mais precisava de alguém que não fosse de minha família. Brilhantemente, encerro está dedicatória à mulher cujas iniciais estão ocultas nessa pequena passagem por ela me fazer conhecer o amor e meu outro eu que jazia escondido em minh'alma.

Agradecimentos

Desde já, gostaria de registrar meus sinceros agradecimentos a Deus, pois sem Ele não seríamos nada. Se hoje cheguei onde estou foi porque o Senhor cuidou de mim nas horas de solidão, tristeza, alegria e felicidade; e, por sua intervenção, estou realizando um dos meus maiores sonhos. Foi Ele quem expurgou os males que habitavam em mim, obliterou os pensamentos sobrecarregados de tristeza e facultou aqueles cheios de felicidade. É por meio dEle que confesso meus anseios mais doloridos, pois Ele é o único que aguenta escutar tamanho peso. Nem meus amigos e família aguentariam desmensurado e demasiado fardo de ouvir-me lamuriar sobre meu passado, presente e por que não o futuro? Tenho plena certeza que Ele irá me ajudar com a nova jornada que virá!

Agradeço imensamente aos meus pais, José da Silva Pereira e Fernanda Asevedo Debon, e ao meu irmão, Charles Debon Pereira, por terem me apoiado com a escolha do meu curso e todo carinho que me forneceram durante todos os dias desde meu nascimento. Inclusive, sou grato aos meus avôs maternos, Aldivo Debon e Neuza Regina Debon, e minha avó paterna, Marinha Pereira, que sempre me deram muito amor e suporte emocional (infelizmente, não conheci meu avô paterno por já ter partido deste plano terreno quando vim a este mundo, mas tenho certeza que do céu ele transmitiu boas vibrações). Sem todos eles não teria chão para prosseguir e muito menos mente para suportar todas as intempéries da vida.

Sou grato também a todos os meus amigos pelo apoio imensurável e pela amizade incondicional além de terem me ajudado durante minhas crises existenciais, pois eles sempre me deram total suporte quando necessitei. Também recordo das belas e boas conversas filosóficas que faziam-me refletir sobre a vida, bem como os momentos brincalhões para descontrair. Dentre meus amigos, posso citar: Lisiane da Costa (Lisi), Bruno Oleiro, Lucas da Silva, Roger Braga, Andressa Machado, Richard Pinto, Ana Carolina Félix, Andressa Martins, Jéssica da Cruz, Murilo Paz, Andrielly de Souza (Lely), Victória Motta, Maribel Santos, Daniel Jacques, Iriel Freitas e Jaíne Silva. Peço desculpas caso tenha esquecido de mencionar alguém porque são tantos para agradecer, mas já fica aqui registrado meu muito obrigado!

Aos meus orientadores, Prof.ª Dr.ª Grasiela Martini e Prof. Dr. Eneilson Fontes, agradeço de coração por terem me aceitado como orientando e também por me aturarem durante estes últimos anos. São pessoas adoráveis e sempre me ajudaram nos momentos difíceis me escutando e dando total suporte/apoio. Sempre me lembrarei dos nossos encontros a tarde para discutirmos sobre Álgebra e Teoria de Grafos, pois permitiram debates e conhecimentos incríveis. Quero ainda agradecer a todos os professores que

passaram pela minha vida, em especial aqueles que me ensinaram Matemática, pois cada um me constituiu como o cidadão que sou hoje.

Por fim, a todos aqueles que conviveram e convivem comigo; e me apoiaram nesta trajetória, meus sinceros agradecimentos!

"Uma psique perturbada é incapaz de absorver, como uma [psique] sossegada, as essências do ambiente, pois um pensamento desorientado desencadeia a desordem mental impossibilitando o indivíduo do raciocínio primordial, seu próprio raciocínio."
(William Debon Pereira, 2016)

Resumo

O presente trabalho tem por objetivo expor a teoria, bem como os resultados fundamentais, da Aritmética dos Restos ou também chamada Aritmética Modular (ramo da Matemática que estuda as relações e operações entre os restos das divisões entre dois números inteiros). Este assunto está centrado dentro do conceito de congruência que, por sua vez, envolve diretamente as ideias sobre divisibilidade dos números inteiros. É interessante compreender a Aritmética dos Restos, pois possibilita perceber e inferir determinadas propriedades para os números inteiros. Além do mais, apresenta-se no decorrer deste trabalho uma atividade didática realizada com estudantes dos três níveis de Ensino completamente conectada com a Aritmética Modular. A referida atividade teve como intuito proporcionar um espaço de aprendizagem deste objeto matemático que é a congruência utilizando apenas operações básicas.

Palavras-chaves: Aritmética Modular, Restos Aritméticos, Congruências.

Abstract

The present work has for purpose to expose the theory, as well as the fundamental results, of the Arithmetic of Remainders or also called Modular Arithmetic (branch of Mathematics that studies the relations and operations between the remainders of the divisions between two integers numbers). This subject is centered on the concept of congruence, which, in turn, directly involves the ideas about divisibility in the integer numbers. It is interesting to comprehend arithmetic about the remainders because it's possible to perceive and infer certain properties to the integer numbers. Furthermore, it presents in this work a didactic activity that was realized with students in the three stages of Teaching completely associate with the Modular Arithmetic. The referred activity has gotten as purpose to provide a space of learning mathematical object that is the congruence using only basic operations.

Key-words: Modular Arithmetic, Arithmetics Remainders, Congruences.

Lista de ilustrações

Figura 1 – Primeiro problema. 53
Figura 2 – Resolução do 1º problema por um estudante do Ensino Fundamental, Médio e Superior da esquerda para a direita. 55
Figura 3 – Solução do 1º problema de um aluno do Ensino Superior 56
Figura 4 – Segundo problema. 57
Figura 5 – Resolução do item (a) do segundo problema por um aluno do Ensino Fundamental, Médio e Superior da esquerda para a direita. 58
Figura 6 – Resolução do item (c) do segundo problema por um aluno do Ensino Fundamental, Médio e Superior da esquerda para a direita. 59
Figura 7 – Resposta da primeira questão de um aluno do Ensino Médio e de dois do Ensino Superior de cima para baixo. 60
Figura 8 – Resposta da segunda questão de dois alunos do Ensino Médio (esquerda) e do Ensino Superior (direita). 61
Figura 9 – Retângulo de comprimento $\frac{p}{2}$ e largura $\frac{q}{2}$. 97
Figura 10 – Retângulo $ABCD$ com os pontos internos. 98
Figura 11 – Retângulo $ABCD$ com sua diagonal. 98

Sumário

Introdução **11**

1 PRÉ-REQUISITOS **13**
1.1 Divisibilidade em $\mathbb{Z}$ **13**
1.1.1 Múltiplos e Divisores 13
1.1.2 Divisão Euclidiana 16
1.1.3 Máximo Divisor Comum - MDC 18
1.1.4 Mínimo Múltiplo Comum - MMC 25
1.2 Números Primos **27**
1.2.1 Números primos 28
1.3 Equações Diofantinas **33**
1.3.1 Equações diofantinas lineares 34

2 ARITMÉTICA MODULAR **38**
2.1 Congruências **38**
2.1.1 Congruências 39
2.1.2 Sistema Completo de Resíduos 50
2.2 Atividade Didática **51**
2.2.1 Metodologia 52
2.2.2 Objetivos 52
2.2.3 Aplicação 53
2.2.4 Algumas considerações 62

3 CONGRUÊNCIAS LINEARES **64**
3.1 Equações de Congruências Lineares **64**
3.1.1 Equações de Congruências Lineares 65
3.2 Alguns Teoremas Clássicos da Aritmética **69**
3.2.1 Teorema de Euler 70
3.2.2 Teorema de Wilson 77
3.2.3 Teorema Chinês dos Restos 78

4 CONGRUÊNCIAS QUADRÁTICAS **81**
4.1 Congruências quadráticas **81**
4.1.1 Congruências quadráticas $x^2 \equiv a\ (mod\ p)$ 81
4.1.2 Símbolo de Legendre 86
4.2 Lei da Reciprocidade Quadrática Gaussiana **92**

5 CONCLUSÃO 101

REFERÊNCIAS 102

ANEXOS 103

ANEXO A – SITUAÇÕES-PROBLEMAS 104

ANEXO B – QUESTIONÁRIO E CALENDÁRIOS 108

Introdução

Em um determinado período na história da humanidade, o homem precisou construir um sistema numérico para poder quantificar os objetos ao seu redor. Sendo assim, surgiu o mais natural conjunto para suprir tal necessidade; o conhecido conjunto dos números naturais ($\mathbb{N}$). Neste conjunto, o homem concebeu as operações básicas/essenciais (soma, subtração, multiplicação e divisão) e, até mesmo, explorou suas propriedades.

Conforme o tempo passava, surgiu um certo empecilho com a subtração nos números naturais, pois, como resolver o cálculo de $2-3$? Para responder a este questionamento, era fundamental a construção de outro conjunto, no qual a operação de subtração fosse fechada (isto é, operando quaisquer dois elementos deste conjunto, então obtém-se um outro elemento também pertencente ao mesmo [conjunto]). Logo, surgiu o conjunto dos números inteiros ($\mathbb{Z}$), onde contas como, $2-3$, fossem solucionadas.

Todas essas descobertas/criações não foram o ápice do que podia ser encontrado e, à vista disto, movido pela curiosidade do novo, o homem aprofundou seu conhecimento através dos estudos das propriedades que esses conjuntos carregavam bem como ampliaram ainda mais outros ramos da Matemática. Refletindo sobre estas descobertas do ser humano, reunimos e apresentamos neste trabalho, baseando-se no conjunto dos números inteiros (pois $\mathbb{N} \subset \mathbb{Z}$), fundamentos matemáticos necessários para entendermos, a posteriori, o conceito de congruência (tema principal deste texto como um todo).

O referido conceito de congruência é uma ideia matemática centrada na relação entre dois números inteiros com respeito ao resto de suas divisões quando estes são divididos por outro número inteiro. Cabe destacar que o introdutor deste princípio foi o matemático alemão Johann Carl Friedrich Gauss (1777-1855) quando este publicou, com seus 24 anos de idade, o livro intitulado *Disquisitiones Arithmeticae* composto de 7 capítulos.

No que tangencia a aplicabilidade dessa noção, podemos pautar os fenômenos cíclicos como, por exemplo, as horas de um relógio, os dias do ano e, também, a passagem do Cometa Haley pela terra. É possível determinar/prever estes fatores/acontecimentos conhecendo apenas algumas informações. Além disso, dentro da Matemática, as congruências proporcionam uma notação mais sofisticada para demonstrarmos os testes de divisibilidade dos números inteiros (conjunto de regras que permite saber quando um número inteiro é ou não divisível por outro número inteiro).

Nesse sentido, separamos o presente trabalho em quatro capítulos dos quais reunimos os principais resultados para compreendermos mais sobre as congruências. Salientamos ainda que baseamos/fundamentamos nosso texto nas seguintes obras literárias: (GOMES; SILVA, 2018), (HEFEZ, 2009), (DOMINGUES, 1991) e (SANTOS, 2020).

A seguir, faremos uma sucinta descrição/apresentação de cada um dos capítulos para que o leitor possa, de forma organizada, compreender a diagramação e como foram divididos os assuntos neste trabalho.

No Capítulo 1, procuramos abordar alguns dos conceitos mais elementares da Aritmética como a divisibilidade dos números inteiros, os números primos e as equações diofantinas lineares (conceitos totalmente interligados às congruências). Além disso, apresentaremos as demonstrações de teoremas cruciais para podermos prosseguir com nossos estudos dentre os quais estão: Divisão Euclidiana - que fornece uma igualdade entre números inteiros não divisíveis por outro; e o Teorema de Bézout - que, além de mostrar a existência do máximo divisor comum (mdc) entre dois números inteiros não simultaneamente nulos, proporciona escrever o mesmo como uma combinação linear de outros dois números inteiros.

As congruências, principal tema deste trabalho, são definidas precisamente no Capítulo 2 juntamente com os mais relevantes resultados que o versa. Além do mais, trouxemos uma atividade didática que foi realizada em três níveis de ensino (Fundamental, Médio e Superior) e, esta, possui relação direta com o tema deste capítulo.

Na sequência, Capítulo 3, passamos a adentrar no universo das equações de congruências lineares, já que expande nossas possibilidades de resolver problemas envolvendo congruências. Nesta parte, discutiremos a existência de solução destes objetos de estudo e formas de solucioná-las. Também apresentaremos as demonstrações dos Teoremas de Euler e Wilson e do Teorema Chinês dos Restos - resultados importantes para a Teoria dos Números porque revelam expressões que evidenciam a relação entre os números inteiros.

Por último, mas não menos, trataremos, no Capítulo 4, a respeito das congruências quadráticas para darmos continuidade ao que foi discutido no capítulo que a este antecede. Aqui, procuramos estabelecer o Símbolo de Legendre que proporciona informações sobre a existência de soluções das congruências quadráticas. Ademais, enunciaremos e demonstraremos a Lei da Reciprocidade Quadrática de Gauss que fornece uma igualdade entre dois Símbolos de Legendre seguindo determinadas hipóteses.

Reforçamos, neste momento, que o leitor esteja familiarizado com os conjuntos dos números inteiros e saiba as propriedades básicas referente as operações elementares neste conjunto. Isto facilitará o entendimento de algumas passagens nas demonstrações dos resultados aqui apresentados.

1 Pré-requisitos

Neste capítulo, iremos apresentar/elencar diversos conceitos preliminares que serão inescusáveis para compreendermos os conceitos de congruências. Para isto, nos baseamos nas seguintes literaturas: (DOMINGUES, 1991), (GOMES; SILVA, 2018), (HEFEZ, 2009) e (SANTOS, 2020).

1.1 Divisibilidade em $\mathbb{Z}$

O conjunto dos números inteiros possui uma vasta gama de propriedades com as operações de adição e multiplicação como, por exemplo, associatividade, existência de elemento neutro e comutatividade. Além disso, sabemos que todos os números inteiros com a operação de adição possuem simétrico, enquanto que para a operação de multiplicação isto não é verdade, pois dado o número inteiro 2, por exemplo, não existirá um número inteiro a tal que $2 \cdot a = 1$. De fato, se existisse $a \in \mathbb{Z}$ tal que $2 \cdot a = 1$ teríamos que $2 \cdot a = (1 + 1) \cdot a = a + a = 1$. Além disso, o antecessor de a será $a - 1 = a - (a + a) = a - a - a = -a$ gerando um absurdo, visto que entre a e $-a$ existe o número 0.

A partir disso, observamos que não é possível estabelecer uma operação de divisão de forma similar à utilizada para definir subtração. Entretanto, através da relação de divisibilidade, que iremos definir no decorrer dessa seção, conseguimos expressar um número inteiro - que não é necessariamente divisível por um outro número inteiro - numa igualdade envolvendo as operações de soma e multiplicação.

Iniciaremos esta seção apresentando os conceitos de números múltiplos e divisores elencando suas principais propriedades. Em seguida, enunciaremos um resultado importantíssimo para os números inteiros (Divisão Euclidiana) e, por fim, finalizaremos definindo máximo divisor comum e mínimo múltiplo comum bem como enunciando e provando os seus resultados mais relevantes para este trabalho.

1.1.1 Múltiplos e Divisores

Os conceitos de números múltiplos e divisores estão inteiramente interligados, pois um completa o outro e vice-versa. Além disso, convém mencionar que eles são fundamentais para começarmos nossas compreensões sobre divisibilidade no conjunto dos números inteiros, visto que suas estruturas são as mais elementares/essenciais.

Definição 1.1.1. Dados $a, b \in \mathbb{Z}$, dizemos que a divide b quando existir algum $c \in \mathbb{Z}$ tal que $b = c \cdot a$. Além disso, chamamos a de divisor, b de dividendo e c de quociente.

Para indicarmos que a divide b, iremos denotar tal fato como $a|b$ enquanto que, se a não divide b, denotaremos por $a \nmid b$. Ressaltamos também que no caso de a dividir b, às vezes, é oportuno escrevermos que a é divisor de b ou b é divisível por a ou ainda b é múltiplo de a em vista do fato dos conceitos de números múltiplos e divisores estarem associados. Vejamos alguns exemplos para ilustrar o que acabamos de definir.

Exemplo 1.1.2. Sejam os números inteiros 25 e 3.350. Observe que $25|3.350$, pois existe $c \in \mathbb{Z}$, a saber $c = 134$, de forma que $3.350 = 134 \cdot 25$.

Exemplo 1.1.3. Consideremos os números inteiros -36 e 5.292. Note que 5.292 é múltiplo de -36, ou seja, $(-36)|5.292$ porque existe $c \in \mathbb{Z}$, a saber $c = -147$, tal que $5.292 = (-147) \cdot (-36)$.

Exemplo 1.1.4. Sejam os números inteiros -25 e -1.256. Repare que para $c = 50$ e $c = 51$, temos $50 \cdot (-25) = -1.250$ e $51 \cdot (-25) = -1275$, respectivamente. Como entre dois números inteiros consecutivos não há nenhum outro número inteiro, decorre na inexistência de $c \in \mathbb{Z}$ tal que $-1.256 = c \cdot (-25)$. Portanto, $(-25) \nmid 1.256$.

Observação 1.1.5. Veja que $0|0$, pois dado qualquer número inteiro c a sentença $0 = c \cdot 0$ é satisfeita. Contudo, é falso que, para qualquer $b \in \mathbb{Z}^*$, $0|b$, porque não existe nenhum $c \in \mathbb{Z}$ que torne a igualdade $b = c \cdot 0$ verdadeira e assim, pela notação fixada anteriormente, temos que $0 \nmid b$.

Proposição 1.1.6. Sejam $a, b, c \in \mathbb{Z}$. Então,

i) $a|0$, $1|a$ e $a|a$;

ii) $a|b \iff |a| \Big| |b|$;

iii) se $a|b$ e $b|c$, então $a|c$;

iv) se $a|b$ e $b|a$, então $a = \pm b$;

v) se $a \Big| |b|$, então $a|b$.

Demonstração. Segue abaixo a prova de cada um dos itens.

i) Basta observar que: $0 = 0 \cdot a$, $a = a \cdot 1$ e $a = 1 \cdot a$.

ii) Se $a|b$, então existe $c \in \mathbb{Z}$ tal que $b = c \cdot a$. Tomando o módulo de b, segue que $|b| = |c \cdot a| = |c| \cdot |a|$, logo $|a|$ divide $|b|$. Por outro lado, se $|a|$ divide $|b|$, então existe $c \in \mathbb{Z}$ de forma que $|b| = c \cdot |a|$. Além disso, sabemos que $|b| = b$, se $b \geqslant 0$, ou $|b| = -b$, se $b < 0$. De mesma forma, $|a| = a$ (se $a \geqslant 0$) ou $|a| = -a$ (se $a < 0$). Sendo assim, se $a \geqslant 0$ e $b \geqslant 0$, então $b = c \cdot a$, assim $a|b$. No caso em que $a < 0$ e $b \geqslant 0$, temos que $b = c \cdot (-a) = (-c) \cdot a$, assim $a|b$. Analogamente mostra-se para os casos ($a \geqslant 0$ e $b < 0$) e ($a < 0$ e $b < 0$).

iii) Note que do fato de $a|b$ e $b|c$ irão existir $q, r \in \mathbb{Z}$ tais que $b = q \cdot a$ e $c = r \cdot b$. Assim, substituindo b na segunda igualdade, obtemos $c = r \cdot (q \cdot a) = (r \cdot q) \cdot a$, ou seja, $a|c$.

iv) Se $a|b$ e $b|a$, então sabemos que existem $q, r \in \mathbb{Z}$ tais que $b = q \cdot a$ e $a = r \cdot b$. Assim, $a = r \cdot (q \cdot a) \Leftrightarrow a = (r \cdot q) \cdot a \Leftrightarrow 1 = r \cdot q$. Dessa última igualdade, podemos concluir que $q = r = 1$ ou $q = r = -1$ donde vemos que $a = \pm b$.

v) Por hipótese, existe $c \in \mathbb{Z}$ tal que $|b| = c \cdot a$. Atente que $|b| = b$, se $b \geqslant 0$, ou $|b| = -b$, se $b < 0$. Se $b \geqslant 0$, temos $b = c \cdot a$, isto é, $a|b$. No caso em que $b < 0$, temos $-b = c \cdot a \Leftrightarrow b = (-c) \cdot a$, ou seja, $a|b$. □

A partir de agora, iremos escrever o produto de dois números inteiros a e b não mais como $a \cdot b$, mas como ab para não sobrecarregarmos a notação (salvo os casos em que lidamos com números propriamente ditos, pois pode causar confusão em vista que, por exemplo, 52 é o número cinquenta e dois e não 5 multiplicado por 2).

Proposição 1.1.7. Dados $a, b, c, d \in \mathbb{Z}$, então se $a|b$ e $c|d$ temos que $ac|bd$.

Demonstração. Se $a|b$ e $c|d$, então existem dois números inteiros q, r tais que $b = qa$ e $d = rc$. Com isso, temos que $bd = (qa)(rc) = (qr)(ac)$, isto é, $ac|bc$. □

Proposição 1.1.8. Sejam $a, b, c \in \mathbb{Z}$. Se $a|b$ e $a|c$, então para todo número inteiro x e y temos que $a|(bx + cy)$.

Demonstração. Por hipótese, temos que existem dois números inteiros q, r tais que $b = qa$ e $c = ra$. Agora, vamos multiplicar essas duas igualdades pelos números inteiros x e y, respectivamente, obtendo assim $bx = (qa)x$ e $cy = (ra)y$. Por fim, vamos ter que $bx + cy = (qa)x + (ra)y$ e, organizando os termos, ficamos com $bx + cy = (qx + ry)a$ donde concluí-se $a|(bx + cy)$. □

Proposição 1.1.9. Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Se $a|b$, então $|a| \leqslant |b|$.

Demonstração. De fato, como $a|b$ temos que existe $c \in \mathbb{Z}$ tal que $b = ca$. Assim, tomando o módulo de b, temos $|b| = |ca| = |c||a|$. Observe que $c \neq 0$ porque $b \neq 0$ e, daí, $|c| \neq 0 \Rightarrow |c| \geqslant 1$. Do fato de $|c| \geqslant 1$, vai existir $r \in \mathbb{Z}_+$ tal que $|c| = 1 + r$ donde segue que $|b| = (1 + r)|a| = |a| + |a|r$ ou melhor dizendo $|a| \leqslant |b|$. □

Comentário 1.1.10. Esta última proposição nos evidência que o módulo do dividendo é sempre igual ou maior do que o módulo do divisor. Inclusive, é possível, de forma análoga, provar que se o número inteiro b puder ser escrito como $b = ca$, com $a, c \in \mathbb{Z}$ e $b \neq 0$, então $|c| \leqslant |b|$ ou, em outras palavras, se $a|b$ com $b \neq 0$, então o módulo do quociente de b por a é no máximo $|b|$.

Diante da definição e dos resultados exibidos nessa subseção, estamos prontos para falar da Divisão Euclidiana, que discorrerá sobre a divisão dos números inteiros que não são, necessariamente, divisíveis por outro inteiro.

1.1.2 Divisão Euclidiana

Nesse tópico, vamos apresentar um dos resultados mais relevantes para o estudo de divisibilidade dos números inteiros como também para as congruências, a Divisão Euclidiana. Contudo, antes de entrarmos em detalhes deste resultado, iremos abordar de forma sucinta a história do matemático cujo nome esta presente no resultado. Ressaltamos que os próximos 5 parágrafos foram baseados nos seguintes trabalhos: (HEFEZ, 2009) e (LUCHETTA, 2008).

Esse resultado foi abordado por Euclides de Alexandria em sua obra denominada *Os Elementos*, onde o resultado é enunciado sem uma demonstração e trabalha exclusivamente no universo dos números naturais.

Sobre a vida de Euclides, pouco se sabe porque não existem muitas informações sobre o local de nascimento e causa da morte, por exemplo. Contudo, estima-se que ele viveu por volta do século III a.C. e foi um matemático (considerado "Pai da Geometria") que não estabeleceu muitos resultados, porém foi quem organizou/sistematizou a lógica de apresentação e rigor dentro da Matemática que, provavelmente, jamais foi alcançado anteriormente.

Algumas das obras escritas por Euclides são: *Os dados*, *Divisões de figuras*, *Os fenômenos*, *Óptica* e *Os Elementos*. Esses registros científicos são os mais antigos materiais gregos parcialmente conservados e existentes após *A esfera* de Autólico (outro matemático grego).

O trabalho desenvolvido por Euclides em *Os Elementos* é fundamental até os dias atuais porque é uma fonte de pesquisa para organizar a teoria sobre os números e a Geometria. Convém salientar ainda que esse material é constituído por treze livros, que estão divididos da seguinte maneira: Os seis primeiros volumes abordam o ramo da Geometria na perspectiva plana, os volumes VII, VIII e IX são voltados para a área da Aritmética, o volume X aborda os segmentos de retas incomensuráveis; e, por fim, os últimos 3 volumes trazem a Geometria dos sólidos.

Depois de Euclides, o campo da Matemática que trata dos números e operações entre eles (Aritmética) acaba se estratificando por cerca de 5 séculos até que Diofanto de Alexandria ressurge com seus estudos sobre equações no universo dos números racionais e inteiros. Cabe mencionar que as equações de estudo de Diofanto são chamadas de equações diofantinas em homenagem a este matemático (saberemos mais informações sobre este matemático e suas equações na Seção 1.3).

Antes de enunciarmos e provarmos o resultado da Divisão Euclidiana, vamos enunciar outros dois resultados que se fazem necessários para mostrarmos o resultado principal. Ressaltamos que nosso objetivo não será demonstrar estes outros dois [resultados] e, por isto, ao leitor que tiver curiosidade de saber como é a demonstração dos mesmos, aconselhamos que busquem no livro (HEFEZ, 2009).

Teorema 1.1.11 (Princípio do Menor Inteiro)**.** Seja X um subconjunto não-vazio do conjunto $\mathbb{Z}$ dos números inteiros. Se X admite cota inferior em $\mathbb{Z}$, então X possui um menor elemento (ou elemento mínimo).

Proposição 1.1.12 (Princípio de Arquimedes)**.** Dados os números inteiros a e b quaisquer, com $b \neq 0$, então existe um número inteiro n tal que $nb > a$.

Estamos prontos para entender a Divisão Euclidiana!

Teorema 1.1.13 (Divisão Euclidiana)**.** Sejam a e b números inteiros quaisquer com $b \neq 0$, então existem dois únicos números inteiros q e r de forma que $a = bq + r$, com $0 \leqslant r < |b|$.

Demonstração. Iremos dividir a prova do teorema nas seguintes duas etapas: Existência e Unicidade.

Existência: Consideremos o conjunto $X = \{a - bx;\ x \in \mathbb{Z} \ \wedge \ a - bx \geqslant 0\}$. Pelo Princípio de Arquimedes 1.1.12, existe $n \in \mathbb{Z}$ tal que $(-b)n > -a$ e, assim, $a - bn > 0$. Logo, temos que $a - bn \in X$, ou seja, $X \neq \emptyset$. Além disso, note que X é limitado inferiormente por números negativos e, pelo Princípio do Menor Inteiro 1.1.11, existe um menor elemento em X, digamos r. A partir disso, existe $q \in \mathbb{Z}$ tal que $r = a - bq$ além de $r \geqslant 0$ (pois $r \in X$). Mostraremos que $r < |b|$. De fato, se $r \geqslant |b|$, então vai existir $s \in \mathbb{N}$ tal que $r = |b| + s$, com $0 \leqslant s < r$. Entretanto, isso contradiz o fato de r ser o menor elemento uma vez que $s = a - b(q + 1)$ (se $b \geqslant 0$) ou $s = a - b(q - 1)$ (se $b < 0$), isto é, $s \in X$, com $s < r$. Portanto, existem os números inteiros q e r tais que $a = bq + r$, com $0 \leqslant r < |b|$.

Unicidade: Suponhamos que existam os números inteiros q, r, q_1 e r_1 tais que $a = bq + r$, com $0 \leqslant r < |b|$, e $a = bq_1 + r_1$, com $0 \leqslant r_1 < |b|$. Observe que $r = a - bq$ e $r_1 = a - bq_1$, logo $r - r_1 = b(q_1 - q)$. Além disso, obtemos das desigualdades que $-|b| < r - r_1 < |b|$. Então, $r - r_1 = 0$ porque é o único múltiplo de b naquele intervalo e com isso segue $r = r_1$. Assim, $0 = b(q_1 - q)$ e, como $b \neq 0$, temos $q = q_1$. □

Os números inteiros a, b, q e r são chamados de dividendo, divisor, quociente e resto, respectivamente. Observemos alguns exemplos os quais aplicamos o teorema acima.

Exemplo 1.1.14. Dados os números inteiros 2.345 e -6. Note que aplicando a Divisão Euclidiana de -6 em 2.345 existem os únicos números inteiros -390 e 5 de forma que $2.345 = (-6)(-390) + 5$.

Exemplo 1.1.15. Sejam os números inteiros -6.185 e -50. Observe que existem e são únicos os números inteiros 124 e 15 tal que $-6.185 = (-50)(124) + 15$.

Comentário 1.1.16. Repare que o fato de $b \neq 0$ é crucial para que o teorema seja válido porque se $b = 0$, então $r = a$ e q seria um inteiro qualquer. Isto torna inconsistente a existência de $0 \leqslant r < |b|$ e a unicidade do próprio q.

Comentário 1.1.17. Quando o resto da divisão entre dois números inteiros for nulo, então temos que um desses dois números é múltiplo do outro. De fato, dados $a, b \in \mathbb{Z}$ com $b \neq 0$, então existem $q, r \in \mathbb{Z}$ tal que $a = bq + r$ e $0 \leqslant r < |b|$. Se $r = 0$ temos $a = bq + 0 = bq = qb \Rightarrow b|a$. Por outro lado, se $b|a \Rightarrow \exists q \in \mathbb{Z}$ tal que $a = qb = bq = bq + 0$ e, assim, basta tomar $r = 0$.

Comentário 1.1.18. Outro fato interessante, que surge do Teorema 1.1.13, é em relação a distribuição dos números inteiros, visto que a partir da Divisão Euclidiana de um inteiro a por 2, por exemplo, temos que $a = 2k+r$, com $0 \leqslant r < 2$ e $k \in \mathbb{Z}$. Assim, as possibilidades de a são $a = 2k$ ou $a = 2k + 1$. Neste caso, podemos construir os conjuntos abaixo:

$$\begin{aligned} \{a = 2k; k \in \mathbb{Z}\} &= \{..., -8, -6, -4, -2, 0, 2, 4, 6, 8, ...\} \\ \{a = 2k + 1; k \in \mathbb{Z}\} &= \{..., -9, -7, -5, -3, -1, 1, 3, 5, 7, 9, ...\} \end{aligned}$$

Observe que esses conjuntos são disjuntos, ou seja, sua interseção é vazia e ainda a reunião é o conjunto dos números inteiros, logo dizemos que estes conjuntos formam uma partição do conjunto $\mathbb{Z}$. Além disso, à esta partição, chamamos o primeiro conjunto de *conjunto dos números pares* e o segundo de *conjunto dos números ímpares*.

1.1.3 Máximo Divisor Comum - MDC

Agora estamos interessados em saber se existe um número inteiro positivo pertencente ao conjunto dos divisores de outros dois números inteiros, não ambos nulos, tal que esse elemento seja o maior possível e que, por sua vez, divida esses dois números inteiros simultaneamente. Se existir esse elemento, então vamos chamar ele de *máximo divisor comum* entre esses dois números inteiros.

Definição 1.1.19. Sejam $a, b \in \mathbb{Z}$ não simultaneamente nulos. O máximo divisor comum entre os números inteiros a e b é o maior inteiro positivo d que satisfaz as seguintes condições:

i) $d|a$ e $d|b$;

ii) Se existir $d_1 \in \mathbb{Z}$ tal que $d_1|a$ e $d_1|b$, então $d_1|d$.

Em vez de ficarmos escrevendo os termos "máximo divisor comum entre os números inteiros a e b", iremos escrever $mdc(a, b)$ para indicar tal fato. A seguir, veremos um exemplo.

Exemplo 1.1.20. Consideremos os números inteiros 8 e -16. Listando o conjunto de divisores desses números, que denotaremos por $D(8)$ e $D(-16)$ (respectivamente), obtemos $D(8) = \{\pm 1, \pm 2, \pm 4, \pm 8\}$ e $D(-16) = \{\pm 1, \pm 2, \pm 4, \pm 8, \pm 16\}$. Os divisores em comum entre 8 e -16 vão ser ± 1, ± 2, ± 4 e ± 8. Diante disso, vemos que o maior divisor positivo e comum a esses números será o 8 e, portanto, $mdc(8, -16) = 8$ porque $8|8$, $8|(-16)$ e quaisquer um dos demais divisores comuns vão dividir 8.

Observação 1.1.21. O $mdc(0, 0)$ não está definido, visto que qualquer inteiro divide 0 como visto no item (i) da Proposição 1.1.6.

Proposição 1.1.22. Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. Assim, temos que:

i) $mdc(a, b)$ é único;

ii) $mdc(a, b) = mdc(b, a)$;

iii) $mdc(a, b) = mdc(|a|, |b|)$;

iv) $mdc(a, 1) = 1$;

v) se $a \neq 0 \Rightarrow mdc(a, 0) = |a|$;

vi) se $a \neq 0$ e $a|b$, então $mdc(a, b) = |a|$.

Demonstração. Segue abaixo a prova de cada um dos itens.

i) Suponhamos que $mdc(a, b) = d$ e $mdc(a, b) = d_1$. Pela Definição 1.1.19, segue que $d|a$, $d|b$, $d_1|a$ e $d_1|b$. Inclusive, $d|d_1$ e o mesmo ocorre para d_1, ou seja, $d_1|d$. Assim, pelo item (iv) da Proposição 1.1.6 e do fato de $d > 0$, segue que $d = d_1$.

ii) Consideremos que $mdc(a, b) = d$ e $mdc(b, a) = d_1$. Sendo assim, $d|a$, $d|b$, $d_1|a$ e $d_1|b$. Inclusive, $d|d_1$ do mesmo modo que $d_1|d$. Portanto, segue do item (iv) da Proposição 1.1.6 e do fato de $d > 0$ que $d = d_1$.

iii) Suponhamos que $mdc(a, b) = d$. Logo, $d|a$ e $d|b$. Daí, existem $q, r \in \mathbb{Z}$ tal que $a = qd$ e $b = rd$. Tomando o módulo de a e b, temos $|a| = |qd| = |q||d| = |q|d \Rightarrow d\Big||a|$ e $|b| = |rd| = |r||d| = |r|d \Rightarrow d\Big||b|$. Agora, suponhamos que $d_1\Big||a|$ e $d_1\Big||b|$. Pelo item (v) da Proposição 1.1.6, $d_1|a$ e $d_1|b$. A partir disso, pela segunda condição da definição de máximo divisor comum $d_1|d$. Portanto, $d = mdc(a, b) = mdc(|a|, |b|)$.

iv) Se $d = mdc(a, 1)$, então $d|a$ e $d|1$. Como $d|1$ e $1|d$, segue do item (iv) da Proposição 1.1.6 que $d = \pm 1$. Pelo fato de $d > 0$, temos $d = 1$.

v) Seja $d = mdc(a, 0)$. Note que $mdc(a, 0) = mdc(|a|, 0)$, logo basta mostrar para o caso $a > 0$. Atente que $d|a$ e $d|0$. Além disso, $a|a$ e $a|0$. Portanto, pelo segundo item da definição de máximo divisor comum, segue que $a|d$, mas $d|a$ concluindo que $d = a$.

vi) Pela propriedade (iii), podemos supor $a > 0$ sem perder a generalidade do resultado. Suponhamos $d = mdc(a, b)$, então $d|a$ e $d|b$. Além disso, sabemos que $a|a$ e, por hipótese, $a|b$. Pelo segundo item da definição de máximo divisor comum, $a|d$. Portanto, $a = d$. □

Observação 1.1.23. Repare que a partir da propriedade (iii) da Proposição 1.1.22, podemos inferir que $mdc(a, b) = mdc(-a, -b) = mdc(-a, b) = mdc(a, -b) = mdc(|a|, |b|)$.

Exemplo 1.1.24. Sabemos, pelo Exemplo 1.1.20, que $mdc(8, -16) = 8$. Daí, pela observação que acabamos de ver, tem-se que $8 = mdc(8, -16) = mdc(8, 16)$. Inclusive, podemos simplesmente aplicar o item (vi) da Proposição 1.1.22 uma vez que $8|16$ e concluir que $mdc(8, -16) = mdc(8, 16) = 8$ sem que necessitássemos analisar o conjunto de divisores desses números e verificar o maior divisor positivo e comum a eles.

Exemplo 1.1.25. O $mdc(-50, -1) = mdc(50, 1) = 1$, pois basta aplicar o item (iv) da Proposição 1.1.22.

Comentário 1.1.26. Sabemos calcular o máximo divisor comum entre dois números inteiros quando são satisfeitas as hipóteses da Proposição 1.1.22 ou listando os divisores de ambos os números e verificando o maior divisor comum. Contudo, nem sempre estamos dentro das hipóteses da referida proposição ou é muito trabalhoso listar os divisores de dois números, quando estes são grandes. Diante disso, como calcular, por exemplo, $mdc(852, -458)$? Isto é o que iremos ver no segmento desta subseção.

Enunciaremos e provaremos a seguir um teorema muito importante para o máximo divisor comum, visto que até então não provamos sua existência. Nós trabalhamos com esse conceito na hipótese de se existir então são satisfeitas tais propriedades, mas agora esse teorema irá definitivamente mostrar que o máximo divisor comum sempre existe além de evidenciar que é possível escrevê-lo como uma combinação linear. O referido teorema é chamado de Teorema de Bézout por conta do matemático Étienne Bézout, que provou o análogo do resultado para polinômios.

Étienne Bézout foi um matemático francês que nasceu na cidade de Nemours no ano de 1730 e morreu em 1783 na comuna de Avon ainda na França. Seu principal trabalho foi *Théorie générale des équations algébriques* (em portugês: Teoria geral das equações algébricas) e sua publicação aconteceu no ano de 1779 em Paris. (MACHADO, 2013).

Embora Bézout não tenha demonstrado o resultado para os números inteiros e sim para o caso mais geral (polinômios), é sabido que Claude Gaspard Bachet de Méziriac

(1581 - 1638), que foi outro matemático francês, provou para os números inteiros tal relação. (BERTONE, 2014).

Teorema 1.1.27 (Teorema de Bézout)**.** Dados $a, b \in \mathbb{Z}$ não simultaneamente nulos, então existem os números inteiros x e y tais que $mdc(a, b) = ax + by$.

Demonstração. Vamos dividir a prova deste teorema em três casos.
(1º caso): Se $a = 0$ e $b \neq 0$, então sabemos que $mdc(0, b) = |b|$. Com isso, basta tomar um inteiro qualquer x e $y = 1$, se $b > 0$, ou um inteiro qualquer x e $y = -1$, se $b < 0$, para assim obtermos a combinação linear desejada.
(2º caso): Quando $a \neq 0$ e $b = 0$ a prova é análoga ao caso anterior.
(3º caso): Se a e b são números inteiros não nulos. Vamos considerar o seguinte conjunto auxiliar: $X = \{ax + by;\ ax + by > 0\ \wedge\ x, y \in \mathbb{Z}\}$. Repare que $X \neq \emptyset$ porque se $a > 0$, então $0 < a \cdot 1 + b \cdot 0$, mas caso $a < 0$ atente que $0 < a \cdot (-1) + b \cdot 0$. Observe que X possui cotas inferiores em $\mathbb{Z}$ (números negativos) e, através do Princípio do Menor Inteiro 1.1.11, X possui um menor elemento. Digamos que $d = min\ X$, onde $min\ X$ quer dizer o elemento mínimo de X. Como $d \in X$, então existem $x_o, y_o \in \mathbb{Z}$ tais que:

$$d = ax_o + by_o. \tag{1.1}$$

Agora, precisamos apenas mostrar que $d = mdc(a, b)$. É claro que $d > 0$ (pois $d \in X$). Assim, vamos aplicar o Teorema 1.1.13 aos números inteiros a e d. Sendo assim, existem únicos $q, r \in \mathbb{Z}$ tais que:

$$a = dq + r;\ 0 \leqslant r < |d| = d. \tag{1.2}$$

Diante das Equações (1.1) e (1.2), obtemos:

$$\begin{aligned} r &= a - dq \\ &= a - (ax_o + by_o)q \\ &= a - ax_oq - by_oq \\ &= a(1 - x_oq) + b(-y_oq). \end{aligned}$$

Da igualdade acima, percebe-se que $r \in X$, já que r é uma combinação linear de a e b além de ser maior do que ou igual à zero. Daí, como $0 \leqslant r < d$ e $d = min\ X$ não podemos ter $r \neq 0$. Logo, $r = 0$ fazendo com que $a = dq \Rightarrow d|a$. De forma análoga, prova-se que $d|b$. Inclusive, se $d_1|a$ e $d_1|b$, pela Proposição 1.1.8, temos $d_1|(ax_o + by_o) = d$. Portanto, segue que $d = mdc(a, b)$. □

Lema 1.1.28. Os elementos do conjunto $X = \{ax + by;\ x, y \in \mathbb{Z}\}$ são divisíveis pelo $mdc(a, b)$.

Demonstração. Suponhamos que $mdc(a,b) = d$, então $d|a$ e $d|b$. Disso, segue pela Proposição 1.1.8 que $d|(ax+by)$ para quaisquer $x, y \in \mathbb{Z}$. Isto completa a demonstração, pois qualquer combinação linear dos números inteiros a e b estão em X e são múltiplos de $d = mdc(a,b)$. □

Lema 1.1.29. Os múltiplos do $mdc(a,b)$ são elementos de $X = \{ax + by;\ x, y \in \mathbb{Z}\}$.

Demonstração. Seja $d = mdc(a,b)$. Então, pelo Teorema 1.1.27 existem $x, y \in \mathbb{Z}$ tais que $d = ax + by$. Multiplicando d por um número inteiro q qualquer, temos que $dq = (ax+by)q = (ax)q + (by)q = a(xq) + b(yq)$. Portanto, segue que $dq \in X$. □

Teorema 1.1.30. Sejam os números inteiros a e b ambos não simultaneamente nulos. Então o conjunto dos múltiplos de $mdc(a,b)$ é igual ao conjunto $X = \{ax+by;\ x, y \in \mathbb{Z}\}$.

Demonstração. Consequência imediata dos Lemas 1.1.28 e 1.1.29. □

Proposição 1.1.31. Sejam os números inteiros a e b não simultaneamente nulos. Se $a = bq + r$, então $mdc(a,b) = mdc(b,r)$.

Demonstração. Seja $d = mdc(a,b)$. Queremos mostrar que $d = mdc(b,r)$. Do fato de d ser o máximo divisor comum de a e b, segue que $d|a$ e $d|b$. Por hipótese, $a = bq + r$ e, assim, podemos reescrever a igualdade como $r = a - bq$. Como $d|a$ e $d|b$ segue da Proposição 1.1.8 que $d|(a - bq) = r$. Suponhamos agora que existe um inteiro d_1 tal que $d_1|b$ e $d_1|r$. Precisamos mostrar que $d_1|d$. De fato, como fizemos para descobrir que $d|r$, descobrimos que $d_1|(bq+r) = a$. Com isso, temos que $d_1|a$ e $d_1|b$, então pela definição de máximo divisor comum, $d_1|d$. Isso mostra que $d = mdc(b,r)$. □

Exemplo 1.1.32. Vamos calcular o $mdc(15,6)$. Aplicando a Divisão Euclidiana de 15 por 6, existem os únicos números inteiros 2 e 3 tais que $15 = 6 \cdot 2 + 3$. Logo, pela Proposição 1.1.31, $mdc(15,6) = mdc(6,3)$ e, por sua vez, como $mdc(6,3) = mdc(3,6)$ e $3|6$, temos que $mdc(15,6) = mdc(6,3) = mdc(3,6) = 3$.

Nesse instante, vamos apresentar o Algoritmo de Euclides, que também é conhecido como Processo das Divisões Sucessivas. Esse método irá responder o questionamento feito no Comentário 1.1.26 sobre como calcular o $mdc(852, -458)$.

Consideremos a e b números inteiros ambos não simultaneamente nulos. Vamos calcular o $mdc(a,b)$ que, por sua vez, é igual ao $mdc(|a|,|b|)$ e desta forma podemos supor sem perder a generalidade que os inteiros a e b são positivos.

Iniciaremos o processo realizando a Divisão Euclidiana de a por b. Logo, existem os únicos números inteiros q_1 e r_1 tais que $a = bq_1 + r_1$, com $0 \leqslant r_1 < b$. Se $r_1 = 0$, então $b|a$ e, com isso, $mdc(a,b) = b$. Caso $r_1 \neq 0$, então pela Proposição 1.1.31 temos que $mdc(a,b) = mdc(b,r_1)$.

Repetindo o processo para b e r_1, existirão únicos números inteiros q_2 e r_2 de forma que $b = r_1q_2 + r_2$, com $0 \leqslant r_2 < r_1$. Se $r_2 = 0$, então $r_1|b$ e, assim, $mdc(a, b) = mdc(b, r_1) = r_1$. Por outro lado, se $r_2 \neq 0$, obtemos que $mdc(b, r_1) = mdc(r_1, r_2)$.

De mesmo modo, para r_1 e r_2, vão existir únicos q_3 e r_3 números inteiros tais que $r_1 = r_2q_3 + r_3$, com $0 \leqslant r_3 < r_2$. Se $r_3 = 0$, então $r_2|r_1$ e, a partir disto, obtemos que $mdc(a, b) = mdc(b, r_1) = mdc(r_1, r_2) = r_2$. Contudo, se $r_3 \neq 0$ vamos ter que $mdc(r_1, r_2) = mdc(r_2, r_3)$.

Prosseguindo com o mesmo raciocínio/pensamento, teremos $r_{k-1} = r_kq_{k+1} + r_{k+1}$, com $0 \leqslant r_{k+1} < r_k$ e $k \geqslant 2$. Atente que $r_1 > r_2 > r_3 > ... \geqslant 0$.

Afirmação: O inteiro $r_{k+1} = 0$.

De fato, consideremos o conjunto $X = \{r_1, r_2, ...\}$. Note que se todos os elementos desse conjunto não forem nulos, então temos que X seria um subconjunto não vazio de $\mathbb{Z}$ admitindo assim cotas inferiores (números negativos), mas não admitindo um menor elemento contrariando o Princípio do Menor Inteiro 1.1.11. Portanto, existe algum k inteiro positivo tal que $r_{k+1} = 0$.

Desta forma, $r_{k-1} = r_kq_{k+1}$, ou seja, $r_k|r_{k-1}$. Assim,

$$mdc(a, b) = mdc(b, r_1) = mdc(r_1, r_2) = mdc(r_2, r_3) = ... = mdc(r_{k-1}, r_k) = r_k$$

Finalmente, podemos calcular o máximo divisor comum entre quaisquer dois números inteiros não simultaneamente nulos.

Comentário 1.1.33. Esse processo das divisões sucessivas é outra forma de mostrar a existência do máximo divisor comum entre os números inteiros a e b, mas não nos fornece a existência da combinação linear que podemos expressar o $mdc(a, b)$ como é feito no Teorema de Bézout 1.1.27.

Exemplo 1.1.34. Vamos encontrar o $mdc(852, -458)$, que é igual ao $mdc(852, 458)$. Aplicando a Divisão Euclidiana de 852 por 458, existem únicos números inteiros 1 e 394 de maneira que $852 = 458 \cdot 1 + 394$ e, daí, $mdc(852, 458) = mdc(458, 394)$. Repetindo o processo para 458 e 394, temos que $458 = 394 \cdot 1 + 64$ e, assim, $mdc(458, 394) = mdc(394, 64)$. De mesmo modo, $394 = 64 \cdot 6 + 10$ donde $mdc(394, 64) = mdc(64, 10)$. Realizando mais uma vez a Divisão Euclidiana de 64 por 10, obtemos $64 = 10 \cdot 6 + 4$ e, então, $mdc(64, 10) = mdc(10, 4)$. Por fim, $10 = 4 \cdot 2 + 2$ implica que $mdc(10, 4) = mdc(4, 2) = mdc(2, 4)$ e, como $2|4$, $mdc(4, 2) = 2$. Portanto, $mdc(852, -458) = 2$.

Definição 1.1.35. Sejam $a, b \in \mathbb{Z}$ não simultaneamente nulos. Quando $mdc(a, b) = 1$, dizemos que a e b são primos entre si, ou coprimos, ou ainda, relativamente primos.

Teorema 1.1.36. Sejam a e b números inteiros não simultaneamente nulos. Diremos que a e b serão coprimos se, e somente se, existirem dois números inteiros x e y tais que $ax + by = 1$.

Demonstração. Seja $mdc(a, b) = 1$. Pelo Teorema 1.1.27, existem números inteiros x e y tais que $ax + by = mdc(a, b) = 1$. Por outro lado, suponhamos que existam números inteiros x e y de modo que $ax + by = 1$ e $mdc(a, b) = d$. Do fato do $mdc(a, b) = d$ segue que $d|a$ e $d|b$ donde tem-se, também, que $d|(ax + by) = 1$ (pela Proposição 1.1.8). Inclusive, $1|d$ e assim $d = \pm 1$. Como $d > 0$, só podemos ter que $d = 1$. □

Destacamos que o teorema acima caracteriza quando os números inteiros a e b serão coprimos. Inclusive, salientamos que a primeira implicação é apenas o Teorema de Bézout aplicado para o caso particular quando o máximo divisor comum de dois números inteiros é 1. Agora, vejamos dois corolários deste teorema para aplicação direta e que serão de grande utilidade mais adiante.

Corolário 1.1.37. Dados os números inteiros a e b, com $a \neq 0$ ou $b \neq 0$. Se $mdc(a, b) = d$, então $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Demonstração. Seja $mdc(a, b) = d$. Pelo Teorema 1.1.27, existem números inteiros x e y tais que $ax + by = d$. A partir disso, temos que $\frac{a}{d}x + \frac{b}{d}y = 1$ (repare que $\frac{a}{d}$ e $\frac{b}{d}$ são números inteiros, já que $d|a$ e $d|b$). Aplicando a recíproca do Teorema 1.1.36 para esta última igualdade, obtemos que $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. □

Corolário 1.1.38. Sejam a, b e c números inteiros, onde $b \neq 0$. Se $b|a$ e $mdc(a, c) = 1$, então $mdc(b, c) = 1$.

Demonstração. Se $b|a$, então temos que existe o número inteiro q de forma que $a = qb$. Além disso, $mdc(a, c) = 1$ donde segue do Teorema 1.1.36 que existem $x, y \in \mathbb{Z}$ tais que $ax + cy = 1$. Logo, $ax + cy = (qb)x + cy = b(qx) + cy = 1 \Rightarrow mdc(b, c) = 1$. □

Definição 1.1.39. Sejam os números inteiros a, b e c não todos nulos. O $mdc(a, b, c)$ é o maior inteiro positivo d que satisfaz as seguintes condições:

i) $d|a$, $d|b$ e $d|c$;

ii) Se existir $d_1 \in \mathbb{Z}$ tal que $d_1|a$, $d_1|b$ e $d_1|c$, então $d_1|d$.

Teorema 1.1.40. Sejam a, b e c números inteiros não todos nulos. Então,

$$mdc(a, b, c) = mdc(mdc(a, b), c).$$

Demonstração. Sejam $mdc(a,b,c) = d$ e $mdc(a,b) = d_1$. Note que $d_1|a$ e $d_1|b$ e, pelo Teorema 1.1.27, existem $x, y \in \mathbb{Z}$ tais que $ax + by = d_1$. Inclusive, observe que $d|a$ e $d|b$ e, com isso, $d|d_1$. Logo, d é um divisor comum de d_1 e c. Suponhamos agora que d_2 seja um divisor comum qualquer de d_1 e c, isto é, $d_2|a$, $d_2|b$ e $d_2|c$. Pela Definição 1.1.39, temos que $d_2|d$. Portanto, $mdc(a,b,c) = mdc(mdc(a,b),c) = d$. □

1.1.4 Mínimo Múltiplo Comum - MMC

Iremos, agora, analisar o conjunto de múltiplos de dois números inteiros ambos não nulos e saber se é possível que exista um menor elemento positivo que seja comum a esses números inteiros. Se existir esse elemento, vamos denominá-lo de *mínimo múltiplo comum* entre esses dois números inteiros.

Definição 1.1.41. Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$ e $b \neq 0$. O mínimo múltiplo comum entre os números inteiros a e b é o menor inteiro positivo m que satisfaz as seguintes condições:

i) $a|m$ e $b|m$;

ii) Se existir $m_1 \in \mathbb{Z}$ tal que $a|m_1$ e $b|m_1$, então $m|m_1$.

Em vez de ficarmos escrevendo "mínimo múltiplo comum entre os números inteiros a e b", iremos escrever $mmc(a,b)$ para indicar tal fato. A seguir, vejamos um exemplo.

Exemplo 1.1.42. Sejam os números inteiros -5 e 2. Listando o conjunto dos múltiplos de -5 e 2, que denotaremos por $M(-5)$ e $M(2)$ (respectivamente), obtemos $M(-5) = \{0, \pm5, \pm10, \pm15, \pm20, \pm25, ...\}$ e $M(2) = \{0, \pm2, \pm4, \pm6, \pm8, \pm10, ...\}$. Os múltiplos comuns entre -5 e 2 são 0, ±10, ±20, ±30, ... Diante disso, vemos que o menor múltiplo positivo e comum a esses números será o 10 e, portanto, $mmc(-5,2) = 10$ porque $(-5)|10$, $2|10$ e quaisquer um dos demais múltiplos comuns são divisíveis por 10.

Observação 1.1.43. O $mmc(0,0)$ não está definido, visto que o conjunto dos múltiplos de 0 possuirá um único elemento, ele próprio, e, pela definição de mínimo múltiplo comum, o $mmc(0,0)$ deve ser o menor elemento positivo - o que não existe.

Proposição 1.1.44. Sejam a e b números inteiros não nulos. Então:

i) $mmc(a,b)$ é único;

ii) $mmc(a,b) = mmc(b,a)$;

iii) $mmc(a,b) = mmc(|a|,|b|)$;

iv) $mmc(a,1) = |a|$;

v) se $a|b$, então $mmc(a,b) = |b|$.

Demonstração. Segue abaixo:

i) Suponhamos que $mmc(a,b) = m$ e $mmc(a,b) = m_1$, então $a|m$, $b|m$, $a|m_1$ e $b|m_1$. Pelo segundo item da Definição 1.1.41, $m|m_1$ assim como $m_1|m$. Portanto, segue que $m = m_1$.

ii) Seja $mmc(a,b) = m$ e $mmc(b,a) = m_1$, então temos que $a|m$, $b|m$, $a|m_1$ e $b|m_1$. Pelo segundo item da Definição 1.1.41, segue que $m|m_1$ e $m_1|m$. Logo, $m = m_1$.

iii) Seja $mmc(a,b) = m$. Assim, $a|m$ e $b|m$, ou seja, existem $q, r \in \mathbb{Z}$ tais que $m = qa$ e $m = rb$. Tomando o módulo de m temos que $m = |m| = |qa| = |q||a| \Rightarrow |a|\Big|m$ e $m = |m| = |rb| = |r||b| \Rightarrow |b|\Big|m$. Consideremos agora $m_1 \in \mathbb{Z}$ tal que $|a|\Big|m_1$ e $|b|\Big|m_1$, isto é, existem $k, l \in \mathbb{Z}$ de forma que $m_1 = k|a|$ e $m_1 = l|b|$. Note que $a|m_1$ porque se $a > 0$ temos $m_1 = ka$, mas se $a < 0$ obtemos $m_1 = (-k)a$. Analogamente mostra-se que $b|m_1$. Com isso, temos que $m|m_1$ e, portanto, $mmc(a,b) = mmc(|a|,|b|)$.

iv) Consideremos $mmc(a,1) = m$. Sabemos pelo item anterior que $mmc(a,1) = mmc(|a|,1)$ e assim basta mostrarmos para $a > 0$. Do fato de $mmc(a,1) = m$ temos que $a|m$ e $1|m$. Observe ainda que $a|a$ e $a|1$ mostrando que a é múltiplo comum de a e 1. Pelo segundo item da Definição 1.1.41, $m|a$, mas por outro lado temos que $a|m$. Portanto, $m = a$.

v) Suponhamos que $mmc(a,b) = m$. Podemos considerar sem perda de generalidade a e b maiores que zero porque $mmc(a,b) = mmc(|a|,|b|)$. Como $mmc(a,b) = m$, então $a|m$ e $b|m$. Repare que, por hipótese, $a|b$ e, além disso, $b|b$ evidenciando que b é um múltiplo comum de a e b. Pelo segundo item da Definição 1.1.41, $m|b$, mas por outro lado $b|m$. Portanto, $m = b$. □

Observação 1.1.45. Repare que a partir da propriedade (iii) da Proposição 1.1.44, podemos inferir que $mmc(a,b) = mmc(-a,-b) = mmc(-a,b) = mmc(a,-b) = mmc(|a|,|b|)$.

Teorema 1.1.46. Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$ e $b \neq 0$, então é válida a seguinte relação: $mdc(a,b) \cdot mmc(a,b) = |ab|$.

Demonstração. Suponhamos, sem perda de generalidade, a e b números inteiros positivos tais que $mdc(a,b) = d$ e $mmc(a,b) = m$. Note que $d|a$, $d|b$, $a|m$ e $b|m$, ou seja, $\frac{a}{d}$, $\frac{b}{d}$, $\frac{m}{a}$ e $\frac{m}{b}$ são números inteiros. Inclusive, $\frac{ab}{d}$ é um múltiplo comum de a e b e, assim, existe q número inteiro tal que $\frac{ab}{d} = mq$ uma vez que $mmc(a,b) = m$. Repare que $q > 0$, pois $m > 0$ e $\frac{ab}{d} > 0$. Da igualdade $\frac{ab}{d} = mq$, segue que $\frac{a}{d} = \frac{m}{b}q$ e $\frac{b}{d} = \frac{m}{a}q$, isto é, q é um divisor comum dos números inteiros $\frac{a}{d}$ e $\frac{b}{d}$. Contudo, $mdc(\frac{a}{d}, \frac{b}{d}) = 1$ o que implica $q = 1$, visto que $q|1$, $1|q$ e $q > 0$. Sendo assim, concluímos que $mdc(a,b) \cdot mmc(a,b) = ab$. □

Observação 1.1.47. O teorema acima nos permite encontrar o $mmc(a,b)$ a partir do $mdc(a,b)$ e vice-versa.

Corolário 1.1.48. Para quaisquer números inteiros a e b, $a \neq 0$ e $b \neq 0$. Então, $mmc(a, b) = |ab|$ se, e somente se, a e b são coprimos.

Demonstração. De fato, pelo Teorema 1.1.46 temos que $mdc(a, b) \cdot mmc(a, b) = |ab|$. Pela primeira implicação, o $mmc(a, b) = |ab|$ e, assim, $mdc(a, b) \cdot |ab| = |ab|$ donde segue que $mdc(a, b) = 1$. Reciprocamente, o $mdc(a, b) = 1$ e, a partir disto, $mmc(a, b) = |ab|$. □

Exemplo 1.1.49. Consideremos os números inteiros 852 e -458. Vamos encontrar o $mmc(852, -458)$. Pelo Teorema 1.1.46, temos que $mdc(852, -458) \cdot mmc(852, -458) = |852 \cdot (-458)|$, ou seja, $mdc(852, -458) \cdot mmc(852, -458) = 390.216$. Já sabemos, pelo Exemplo 1.1.34, que $mdc(852, -458) = 2$ e, assim, $2 \cdot mmc(852, -458) = 390.216$ donde segue que $mmc(852, -458) = 195.108$.

Definição 1.1.50. Sejam os números inteiros a, b e c não nulos. Definimos o $mmc(a, b, c)$ como o inteiro $m > 0$ tal que:

i) $a|m$, $b|m$ e $c|m$;

ii) Se existir $m_1 \in \mathbb{Z}$ tal que $a|m_1$, $b|m_1$ e $c|m_1$, então $m|m_1$.

Teorema 1.1.51. Sejam a, b e c números inteiros não nulos, então $mmc(a, b, c) = mmc(mmc(a, b), c)$.

Demonstração. Sejam $mmc(a, b, c) = m$ e $mmc(a, b) = m_1$. Note que $a|m_1$ e $b|m_1$ assim como $a|m$ e $b|m$. Logo, pelo item (ii) da Definição 1.1.41 ,temos que $m_1|m$, ou seja, m é múltiplo comum de m_1 e c. Suponhamos agora que m_2 seja um múltiplo comum qualquer de m_1 e c, isto é, $a|m_2$, $b|m_2$ e $c|m_2$. Pela Definição 1.1.50, temos que $m|m_2$. Portanto, $mmc(a, b, c) = mmc(mmc(a, b), c)$. □

1.2 Números Primos

Iremos dedicar essa seção para falar de uma categoria muito especial de números, os chamados números primos. Esses objetos de estudo são um mistério até os dias atuais porque não há algoritmo eficiente que nos forneça todos os números primos de maneira rápida e prática. Contudo, conhecemos alguns resultados que nos possibilitam compreendermos um pouco sobre esses números. Inclusive, a partir deles conseguimos estabelecer um teorema fundamental dos números inteiros intitulado Teorema Fundamental da Aritmética, que nos proporciona escrever qualquer número inteiro não nulo e diferente de 1 como um produto de fatores primos.

1.2.1 Números primos

Definição 1.2.1. Seja $p > 1$ um número inteiro. Dizemos que p é um número primo quando possuir exatamente quatro divisores.

Observação 1.2.2. Quando um número inteiro $a > 1$ possuir mais do que quatro divisores, então o chamamos de número composto. Em outras palavras, dizemos que um número inteiro $a > 1$ é composto quando ele não é primo.

Observação 1.2.3. O número 2 é o único número primo par. De fato, 2 é primo porque satisfaz a Definição 1.2.1 (seus únicos divisores são ± 1 e ± 2), e é o único primo par porque se a é um número par positivo e diferente de 2, então temos que ele terá pelo menos os seguintes divisores: ± 1, ± 2 e $\pm a$ contrariando assim a Definição 1.2.1.

Exemplo 1.2.4. O número 13 é primo, pois seus únicos divisores são ± 1 e ± 13. Por outro lado, 15 não é um número primo e sim composto uma vez que seus divisores são ± 1, ± 3, ± 5, ± 15.

A partir da Definição 1.2.1, seguem as seguintes afirmações abaixo:

i) Se p e q são números primos e $p|q$, então $p = q$;

De fato, se fosse $p \neq q$ e $p|q$, então o primo q teria os seguintes divisores ± 1, $\pm p$ e $\pm q$. Isso contradiz a hipótese de q ser primo.

ii) Sejam os números inteiros a e p, com p primo. Se $p \nmid a$, então $mdc(a, p) = 1$.

De fato, se $mdc(a, p) = d$, então $d|a$ e $d|p$. Do fato de $d|p$, temos que $d = \pm 1$ ou $d = \pm p$. Por hipótese, $p \nmid a$ donde temos que $d = \pm 1$ e, como $d > 0$, só podemos ter $d = 1$.

Vamos em busca de demonstrar o Teorema Fundamental da Aritmética, mas para isto veremos alguns resultados que se farão importantes para provar o teorema.

Proposição 1.2.5. Todo número composto $n > 1$ pode ser escrito como um produto de outros dois números inteiros a e b, com $1 < a < n$ e $1 < b < n$.

Demonstração. Seja o número inteiro $n > 1$ composto, então n possui mais do que os quatro divisores triviais (± 1 e $\pm n$). Logo, existem $a, b \in \mathbb{Z}$ tais que $1 < a < n$, $1 < b < n$ e $n = ab$. □

Proposição 1.2.6. Dados a, b e c números inteiros tais que a e b são coprimos. Se $a|bc$, então $a|c$.

Demonstração. Seja $mdc(a, b) = 1$, então pelo Teorema 1.1.36 existem x_o e y_o tais que $ax_o + by_o = 1$. Daí, multiplicando a igualdade pelo número inteiro c, obtemos $(ax_o)c + (by_o)c = c$ e, reescrevendo a igualdade, $(ac)x_o+(bc)y_o = c$. Pela hipótese de $a|bc$ temos que existe $k \in \mathbb{Z}$ de forma que $bc = ka$. Assim, $(ac)x_o + (ka)y_o = c$ e, por fim, $a(cx_o + ky_o) = c \Rightarrow a|c$. □

Proposição 1.2.7. Sejam a, b e p números inteiros, com p primo. Se $p|ab$, então $p|a$ ou $p|b$.

Demonstração. Se $p|a$ nada há para demonstrar. Entretanto, se $p \nmid a$, então temos que $mdc(a, p) = 1$. Daí, como $p|ab$ segue da Proposição 1.2.6 que $p|b$. □

Lema 1.2.8. Sejam $p, p_1, p_2, ...p_k$ números primos. Se $p|p_1p_2...p_k$, então $p = p_i$ para algum $i \in \{1, 2, ..., k\}$.

Demonstração. Para provar esse resultado, iremos utilizar indução sobre k.

Base de indução: Para $k = 1$ o resultado é satisfeito.

Hipótese de indução: Suponhamos que o lema seja satisfeito para k, ou seja, se $p|p_1p_1...p_k$, então $p = pi$ para algum $i \in \{1, 2, ..., k\}$.

Tese: Provaremos que para $k + 1$ é válido o lema. Se $p|p_1p_2...p_{k+1}$, então existe $q \in \mathbb{Z}$ tal que $p_1p_2...p_{k+1} = qp$. Note que podemos associar os elementos da seguinte forma $(p_1p_2...p_k)p_{k+1} = qp$, ou seja, $p|(p_1p_2...p_k)p_{k+1}$. Utilizando a Proposição 1.2.7, temos que $p|p_1p_2...p_k$ ou $p|p_{k+1}$. Se ocorrer o primeiro caso, a hipótese de indução nos garante a existência de $i \in \{1, 2, ..., k\}$ tal que $p = p_i$. Por outro lado, se ocorrer o fato de $p|p_{k+1}$ e, por p e p_{k+1} serem primos, temos $p = p_{k+1}$.

Portanto, o lema é satisfeito para todo $n \geqslant 1$. □

Finalmente vamos mostrar o Teorema Fundamental da Aritmética, que nos evidenciará a possibilidade de escrever qualquer número inteiro maior que 1 como produto de fatores primos.

Teorema 1.2.9 (Teorema Fundamental da Aritmética)**.** Seja $n > 1$ um número inteiro. Então existem $p_1, p_2, ..., p_k$ números primos (não necessariamente distintos) tais que $n = p_1p_2...p_k$ e esta fatoração é única independente da ordem de seus fatores.

Demonstração. Iremos dividir a prova em duas etapas: Existência e Unicidade.

Existência: Utilizaremos o Segundo Princípio de Indução sobre n.

• Base de indução: Para $n = 2$, é válido a existência de primos uma vez que 2 é primo e $n = 2$ coincide com a fatoração.

• Hipótese de indução: Suponhamos que dado o número inteiro u de forma que $2 \leqslant u < v$, então existirá $p_1, p_2, ...p_k$ tal que $u = p_1p_2...p_k$.

• Tese: Provaremos que o número inteiro v pode ser escrito como produto de fatores primos. Se v for um número primo, então basta escolher $p_1 = v$. Caso contrário, v será composto e, pela Proposição 1.2.5, vão existir $a, b \in \mathbb{Z}$ de forma que $1 < a < v$, $1 < b < v$ e $v = ab$. Pela hipótese de indução, vão existir números primos $x_1, x_2, ..., x_i$ e $y_1, y_2, ..., y_j$ tais que $a = x_1x_2...x_i$ e $b = y_1y_2...y_j$. Logo, $v = (x_1x_2...x_i)(y_1y_2...y_j)$.

Portanto, pelo Segundo Princípio da Indução, garantimos a existência do teorema.

Unicidade: Consideremos que n possa ser decomposto em fatores primos de duas formas, digamos que $n = p_1p_2...p_k = q_1q_2...q_l$. Além disso, suponhamos, sem perda de generalidade, que $l \geqslant k$. Diante de $p_1p_2...p_k = q_1q_2...q_l$, temos que $p_1|q_1q_2...q_l$ e, pelo Lema 1.2.8, existe algum $j \in \{1, 2, ..., l\}$ tal que $p_1 = q_j$. Logo, reordenando os índices de $q_j's$ se necessário, podemos supor $p_1 = q_1$. Assim, $p_2...p_k = q_2...q_l$. Repetindo o mesmo raciocínio k vezes, vamos obter que $p_j = q_j$ para todo $j = 1, 2, ..., k$. Resta provarmos que $k = l$. Sabemos que $1 = q_{k+1}...q_l$ e, a partir disto, $q_{k+1}|1$, o que é impossível uma vez que q_{k+1} é primo (o mesmo ocorre para $q_{k+2}, ..., q_l$). Portanto, $p_j = q_j$ para todo $j = 1, 2, ..., k$ e $k = l$. Isto prova que a decomposição é única. □

Corolário 1.2.10. Seja n um número inteiro maior do que 1. Então existem únicos números primos $p_1 < p_2 < ... < p_k$ e os números inteiros positivos $\alpha_1, \alpha_2, ..., \alpha_k$ tais que $n = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$.

Esse corolário segue do Teorema Fundamental da Aritmética (1.2.9), já que na fatoração pode haver números primos iguais e, nesse sentido, fazemos um agrupamento de fatores iguais.

Observação 1.2.11. Se n é um número inteiro menor do que -1 e queremos fatorar ele em números primos, basta fatorarmos $-n > 1$ em fatores primos e acrescentar o sinal de negativo na frente do primeiro fator primo, ou seja, se $-n = p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, então $n = -p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.

Exemplo 1.2.12. Observe que o número 352 pode ser decomposto em fatores primos da seguinte maneira $352 = 2^5 \cdot 11$, enquanto que 792 pode ser escrito como $792 = 2^3 \cdot 3^2 \cdot 11$. Se quiséssemos a fatoração primária de -352 e -792, basta colocarmos o sinal de negativo na frente do primeiro fator primo. Neste caso, teríamos $-352 = -2^5 \cdot 11$ e $-792 = -2^3 \cdot 3^2 \cdot 11$.

O Teorema Fundamental da Aritmética possui várias aplicações e, dentre elas, iremos apresentar uma que envolve o máximo divisor comum e o mínimo múltiplo comum de dois números inteiros.

Aplicação 1.2.13. Sejam $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ e $b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$. Então, $mdc(a,b) = p_1^{\gamma_1} p_2^{\gamma_2} ... p_k^{\gamma_k}$ e $mmc(a,b) = p_1^{\delta_1} p_2^{\delta_2} ... p_k^{\delta_k}$, onde $\gamma_i = min\{\alpha_i, \beta_i\}$ e $\delta_i = max\{\alpha_i, \beta_i\}$ para $i = 1, 2, ..., k$.

Demonstração. Vamos dividir a demonstração nas 2 partes abaixo:

(*1ª parte*) Mostraremos que o $mdc(a,b) = p_1^{\gamma_1} p_2^{\gamma_2} ... p_k^{\gamma_k}$, onde $\gamma_i = min\{\alpha_i, \beta_i\}$. É fácil perceber que $d|a$ e $d|b$, com $d = p_1^{\gamma_1} p_2^{\gamma_2} ... p_k^{\gamma_k}$ e $\gamma_i = min\{\alpha_i, \beta_i\}$. Resta-nos provar que dado qualquer outro divisor comum de a e b, então este divide d. Suponhamos que $n = \pm p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_k^{\epsilon_k}$ divida comumente a e b, então é claro que $\epsilon_i \leqslant \alpha_i$ e $\epsilon_i \leqslant \beta_i$; de modo que $\epsilon_i \leqslant \gamma_i$. Consequentemente, segue que $n|d$ e, portanto, $d = mdc(a,b)$.

(*2ª parte*) Mostraremos que o $mmc(a,b) = p_1^{\delta_1} p_2^{\delta_2} ... p_k^{\delta_k}$, onde $\delta_i = max\{\alpha_i, \beta_i\}$. É fácil ver que $a|m$ e $b|m$, com $m = p_1^{\delta_1} p_2^{\delta_2} ... p_k^{\delta_k}$ e $\delta_i = max\{\alpha_i, \beta_i\}$. Resta-nos provar que dado qualquer outro múltiplo comum de a e b, então m divide este. Suponhamos que $n = \pm p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_k^{\epsilon_k}$ seja múltiplo comum de a e b, então é claro que $\alpha_i \leqslant \epsilon_i$ e $\beta_i \leqslant \epsilon_i$; de modo que $\delta_i \leqslant \epsilon_i$. Consequentemente, segue que $m|n$ e, portanto, $mmc(a,b) = m$. □

Comentário 1.2.14. Essa aplicação nos traduz que o máximo divisor comum entre a e b serão as menores potências de primos que dividem a e b ao mesmo tempo enquanto que o mínimo múltiplo comum de a e b serão as maiores potências de primos que dividem a ou b.

Exemplo 1.2.15. Já sabemos, pelos Exemplos 1.1.34 e 1.1.49, que $mdc(852, 458) = 2$ e $mmc(852, 458) = 195.108$. Entretanto, se não soubéssemos disto, fazendo a decomposição primária de 852 e 458 temos que $852 = 2^2 \cdot 3 \cdot 71$ e $458 = 2 \cdot 229$. Logo, tomando as menores potências dos primos que dividem ambos os números simultaneamente temos 2 (que é justamente $mdc(852, 458)$) e as maiores potências dos primos que dividem ou 852 ou 458 tem-se $2^2 \cdot 3 \cdot 71 \cdot 229 = 195.108$ (que é justamente $mmc(852, 458)$).

Até o presente momento não discutimos a quantidade de números primos, ou seja, não mencionamos se o conjunto dos números primos é finito ou infinito. Nesse sentido, iremos, a seguir, enunciar e provar um teorema atribuído e demonstrado por Euclides. Esse resultado comprova definitivamente que existe uma infinidade de números primos.

Teorema 1.2.16 (Teorema de Euclides)**.** O conjunto P formado por números primos é infinito.

Demonstração. Suponhamos que o conjunto P formado por todos os números primos seja finito, ou seja, $P = \{p_1, p_2, ..., p_k\}$. Podemos supor ainda, sem perder a generalidade, que $p_1 < p_2 < \cdots < p_k$. Consideremos o número inteiro $a = p_1 p_2 ... p_k$. Tomemos, também, o número inteiro b sendo o sucessor de a, ou seja, $b = a + 1$. Assim, temos a igualdade $b = p_1 p_2 ... p_k + 1$ que, por sua vez, não pode ser um número primo porque $b > p_k$. Logo,

pelo Teorema Fundamental da Aritmética 1.2.9, existe algum primo $p_j \in P$ tal que $p_j|b$, isto é, existe $q \in \mathbb{Z}$ tal que $b = qp_j$. A partir disto, temos que $qp_j = p_1p_2...p_k + 1$ e, reorganizando essa igualdade, chegamos à $1 = p_j(q - p_1p_2...p_{j-1}p_{j+1}...p_k) \Rightarrow p_j|1$, o que é um absurdo uma vez que p_j é primo. Portanto, P é um conjunto infinito. □

Vamos, neste momento, mostrar um método de encontrar todos os números primos em um intervalo de 2 até um número inteiro positivo n qualquer. Este procedimento é chamado de *Crivo de Erastótenes* e, inclusive, é o método mais antigo, porém não tão eficiente para descobrirmos os números primos caso n seja um número muito grande.

Antes de descrevermos os procedimentos do método, vamos mostrar um lema concebido pelo próprio Erastótenes, que se fará de útil para a aplicação da técnica.

Lema 1.2.17 (Lema de Erastótenes)**.** Seja um número inteiro $n > 1$. Se n não é divisível por nenhum primo p tal que $p^2 \leqslant n$, então ele é primo.

Demonstração. Suponhamos que o número inteiro $n > 1$ não seja divisível por nenhum número inteiro p tal que $p^2 \leqslant n$. Se n for composto, segue que existe algum primo q que divide n. Tomemos o menor primo q e, assim, $n = qt$ para algum $t \in \mathbb{Z}$ de forma que $q \leqslant t$. Multiplicando a desigualdade por q, obtemos que $q^2 \leqslant qt = n$ (desigualdade não inverte porque como q é primo segue que $q > 0$) contradizendo a hipótese de não existir primo que divida n tal que $p^2 \leqslant n$. □

Estamos prontos para explicar o *Crivo de Erastótenes*. Esse procedimento consiste em listarmos os números inteiros positivos de 2 até n em uma tabela. Em seguida, iniciaremos pelo primeiro número da listagem, que é o 2. Como 2 é primo, "retiraremos" todos os múltiplos de 2, exceto o 2. Logo em seguida, passaremos ao próximo número não retirado da listagem, que será o 3. Como 3 é primo, iremos "retirar" todos os múltiplos de 3, exceto o 3. Feito isto, o próximo número não retirado da tabela será o 5 uma vez que o 4 é um múltiplo de 2 e foi retirado durante o primeiro passo do método. Diante do número 5, que é primo, repetiremos o processo de retirada dos múltiplos deste número, exceto o 5. Nesse sentido, utilizaremos esse artifício até o número primo p cujo quadrado não supere n, pois o primeiro valor não "retirado" da listagem é p^2.

Exemplo 1.2.18. Vamos encontrar todos os números primos entre 2 e 150. Para isto, vamos utilizar o *Crivo de Erastótenes*. Note que vamos realizar os processos de "retirar" os múltiplos até o primo 11 uma vez que $13^2 = 169$ superando nosso $n = 150$. Assim, os primos serão os números não riscados na tabela abaixo.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~
~~16~~	17	~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~	41	~~42~~	43	~~44~~	~~45~~
~~46~~	47	~~48~~	~~49~~	~~50~~	~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~	71	~~72~~	73	~~74~~	~~75~~
~~76~~	~~77~~	~~78~~	79	~~80~~	~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~	101	~~102~~	103	~~104~~	~~105~~
~~106~~	107	~~108~~	109	~~110~~	~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~	131	~~132~~	~~133~~	~~134~~	~~135~~
~~136~~	137	~~138~~	139	~~140~~	~~141~~	~~142~~	~~143~~	~~144~~	~~145~~	~~146~~	~~147~~	~~148~~	149	~~150~~

1.3 Equações Diofantinas

Para finalizarmos esse capítulo, vamos falar um pouco sobre as equações diofantinas. Essas equações levam este nome em homenagem ao matemático Diofanto, que dedicou sua vida estudando esses tipos de equações no universo dos números racionais e inteiros. Ressaltamos que a abordagem o qual utilizaremos neste trabalho são a respeito das equações diofantinas com soluções exclusivamente no conjunto dos números inteiros.

Diofanto foi um matemático grego (considerado "Pai da álgebra") que viveu por volta do século III d.C. e, assim como Euclides, não se conhece muito sobre sua vida. Entretanto, Diofanto nos legou uma obra chamada de *Aritmética*, que foi escrita também em 13 volumes como *Os Elementos* de Euclides, mas infelizmente só "sobreviveram" aos tempos atuais 6 ou 7 volumes (há divergências entre esse número). Além disso, esse é o mais antigo tratado que aborda a Álgebra uma vez que Diofanto utilizava o conceito algébrico para solucionar as equações sem ter uma linguagem geométrica diferindo-se dos seus antecessores. (HEFEZ, 2009) e (MOL, 2013).

O segundo volume do *Aritmética* possui 35 problemas e é o mais famoso porque em uma cópia deste livro (na edição francesa) e mais precisamente no problema 8, que trazia todas as soluções inteiras da equação $x^2 + y^2 = z^2$, possibilitou a um outro matemático, cerca de 1.300 anos depois de Diofanto, chamado Pierre de Fermat ($1601-1665$) a inspirar-se e construir o que ficara conhecido como o Último Teorema de Fermat. (HEFEZ, 2009), (MOL, 2013) e (SILVA, 2014).

Nas margens deste problema 8, Fermat escreveu as seguintes palavras: "Por outro lado, é impossível separar um cubo em dois cubos, ou uma biquadrada em duas biquadradas, ou, em geral, uma potência qualquer, exceto um quadrado em duas potências semelhantes. Eu descobri uma demonstração verdadeiramente maravilhosa disto, que todavia esta margem não é suficientemente grande para cabê-la."(há diferenciações sobre o que realmente Fermat escreveu entre escritores - aqui utilizamos tal qual encontramos

em (HEFEZ, 2009)). Esse teorema foi solucionado em 1995 por um matemático inglês chamado Andrew Wiles cuja demonstração utiliza técnicas avançadas de álgebra e, diante disso, acredita-se que Fermat se enganou ao afirmar que sabia/continha uma solução para o problema uma vez que naquela época a matemática estava acabando de conceber o cálculo diferencial integral. (HEFEZ, 2009), (MOL, 2013) e (SILVA, 2014).

1.3.1 Equações diofantinas lineares

Definição 1.3.1. Uma equação diofantina linear a duas incógnitas x e y é uma equação do tipo $ax + by = c$ no qual os coeficientes $a, b, c \in \mathbb{Z}$.

Exemplo 1.3.2. A equação $2x + 8y = 5$ é uma equação diofantina linear assim como a equação $3x - 5y = 12$. Contudo, as equações $\frac{1}{2}x + 2y = 5$ e $2x^2 - 3y = 5$ não são equações diofantinas lineares.

Dizemos que uma equação diofantina linear possui solução em $\mathbb{Z}$ se existirem os números inteiros x_o e y_o tais que a igualdade $ax_o + by_o = c$ seja verificada e, assim, o par ordenado (x_o, y_o) é chamado solução da equação. Diante disso, é natural nos questionarmos se toda equação diofantina linear possui solução e se a solução é única.

Consideremos a seguinte equação do Exemplo 1.3.2, $2x + 8y = 5$. Note que podemos reescreve-lá da seguinte forma $2x + 2(4y) = 5$ e, por fim, $2(x + 4y) = 5$. A partir da última igualdade vemos uma incoerência, já que 5 não é um número par e, para qualquer número inteiro da forma $x + 4y$, a expressão $2(x + 4y)$ sempre será um número par. Portanto, concluímos que nem toda equação diofantina possui solução.

Agora, considerando a equação $3x - 5y = 12$ (Exemplo 1.3.2), temos que $(4, 0)$ é solução da equação, pois a igualdade $3 \cdot 4 - 5 \cdot 0 = 12$ é verificada. Entretanto, os pares ordenados $(-1, -3)$, $(-6, -6)$ e $(9, 3)$ também são soluções uma vez que substituindo a primeira coordenada do par em x e a segunda em y a sentença é verificada. Portanto, a solução de uma equação diofantina linear não é única.

Nesse sentido, vamos em busca de um método para sabermos quando que uma equação diofantina possui soluções e como encontrar essas soluções.

Teorema 1.3.3. Uma equação diofantina linear $ax + by = c$ possui solução se, e somente se, $mdc(a, b)|c$.

Demonstração. Sejam $mdc(a, b) = d$ e (x_o, y_o) uma solução da equação diofantina linear $ax + by = c$. Observe que $d|a$ e $d|b$ e, pela Proposição 1.1.8, d divide qualquer combinação linear de a e b, ou seja, $d|(ax_o + by_o) = c$ uma vez que $ax_o + by_o = c$. Por outro lado, se $mdc(a, b) = d$ divide c, então existe $q \in \mathbb{Z}$ tal que $c = dq$. Do fato de $d = mdc(a, b)$, segue do Teorema 1.1.27 que existem $s, t \in \mathbb{Z}$ tais que $d = as + bt$. Substituindo essa última

igualdade em $c = dq$ temos que $c = a(sq) + b(tq)$ e, assim, tomando $x_o = sq$ e $y_o = tq$ obtemos que $c = ax_o + by_o$ donde segue que (x_o, y_o) é solução da equação diofantina linear $ax + by = c$. □

Corolário 1.3.4. Se $mdc(a, b) = 1$, então a equação diofantina linear $ax + by = c$ sempre tem solução para qualquer número inteiro c.

Demonstração. De fato, note que $mdc(a, b) = 1|c$ para qualquer número inteiro c (item (i) da Proposição 1.1.6). Portanto, segue do Teorema 1.3.3 que a equação $ax + by = c$ possui solução. □

Corolário 1.3.5. A equação diofantina linear $ax + by = 1$ possui solução se, e somente se, $mdc(a, b) = 1$.

Demonstração. Suponhamos que a equação $ax + by = 1$ possua solução, então, pelo Teorema 1.3.3, $mdc(a, b)\big|1$ e, assim, segue que $mdc(a, b) = 1$. Por outro lado, se $mdc(a, b) = 1$ segue do Corolário 1.3.4 que a equação $ax + by = 1$ possui solução. □

Vamos obter uma expressão que associa duas soluções da equação $ax + by = c$. Consideremos que (x_o, y_o) e (x_1, y_1) sejam soluções da equação $ax + by = c$. Então, $ax_o + by_o = c$ e $ax_1 + by_1 = c$. Disso, segue que $ax_o + by_o = ax_1 + by_1$ e, reescrevendo a expressão, temos $a(x_o - x_1) = b(y_1 - y_o)$. Dividindo essa última igualdade por $mdc(a, b)$, obtemos:

$$\frac{a}{mdc(a,b)}(x_o - x_1) = \frac{b}{mdc(a,b)}(y_1 - y_o).$$

Vamos denotar $\frac{a}{mdc(a,b)}$ e $\frac{b}{mdc(a,b)}$ por a' e b', respectivamente. Ou seja, a expressão passa a ser escrita por:

$$a'(x_o - x_1) = b'(y_1 - y_o). \tag{1.3}$$

Como $mdc(a', b') = 1$, segue da Proposição 1.2.6 que $a'|(y_1 - y_o)$ e $b'|(x_o - x_1)$, logo existem os números inteiros k e l tais que:

$$y_1 - y_o = a'k; \tag{1.4}$$

$$x_o - x_1 = b'l. \tag{1.5}$$

Substituindo as Equações (1.4) e (1.5) em (1.3), concluímos que:

$$\begin{aligned} a'b'l &= a'b'k \\ l &= k. \end{aligned}$$

Portanto, $x_1 = x_o - b'k$ e $y_1 = y_o + a'k$ para $k \in \mathbb{Z}$.

Proposição 1.3.6. Se a equação diofantina linear $ax + by = c$ possui solução (x_o, y_o), então a equação possui infinitas soluções e o conjunto de todas as soluções é

$$S = \left\{ \left(x_o - \frac{b}{d}t, y_o + \frac{a}{d}t \right);\ t \in \mathbb{Z} \right\},$$

onde $d = mdc(a, b)$.

Demonstração. Resta-nos mostrar que os elementos do conjunto S são soluções da equação $ax + by = c$ uma vez que a solução $(x_1, y_1) \in S$ por conta da relação que mostramos anteriormente. Consideremos o par ordenado $\left(x_o - \frac{b}{d}t, y_o + \frac{a}{d}t\right)$ com $t \in \mathbb{Z}$. Substituindo suas respectivas coordenadas na equação $ax + by = c$ temos:

$$\begin{aligned} a\left(x_o - \frac{b}{d}t\right) + b\left(y_o + \frac{a}{d}\right) &= ax_o - \frac{ab}{d}t + by_o + \frac{ab}{d}t \\ &= ax_o + by_o \\ &= c. \end{aligned}$$

Assim, concluímos a demonstração. □

Já sabemos como encontrar todas as soluções de uma equação diofantina linear sabendo apenas uma de suas soluções. Contudo, como descobrir uma de suas soluções para podermos aplicar a Proposição 1.3.6? Vejamos dois exemplos para determinar (x_o, y_o).

Exemplo 1.3.7. Seja a equação diofantina linear $2x - 4y = 12$. Primeiramente, devemos verificar se o $mdc(2, 4) = 2$ divide o 12. De fato, $2|12$, então, pelo Teorema 1.3.3, a referida equação possui solução. Logo após, vamos aplicar o Teorema 1.1.13 dividindo 4 por 2 e, assim, $4 = 2 \cdot 2 + 0$. Note que se multiplicarmos a igualdade por 3 e reescrevê-la de forma similar a equação, obtemos $12 = 2 \cdot 6 + 4 \cdot 0$. Portanto, uma solução dessa equação é $(6, 0)$. Aplicando a Proposição 1.3.6, todas as soluções desta equação são dadas pelo conjunto abaixo:

$$S = \left\{ \left(6 - \frac{4}{2}t, 0 + \frac{2}{2}t \right);\ t \in \mathbb{Z} \right\} = \{(6 - 2t, t);\ t \in \mathbb{Z}\}.$$

Exemplo 1.3.8. Consideremos a equação diofantina linear $3x + 5y = 13$. Observe que $mdc(3, 5)\big|13$ (pois $mdc(3, 5) = 1$) e, assim, a equação possui solução. Aplicando a Divisão Euclidiana de 5 por 3, temos que $5 = 3 \cdot 1 + 2$. Repetindo o processo para 3 e 2, obtemos $3 = 2 \cdot 1 + 1$. Vamos reescrever essas igualdades da seguinte forma:

$$2 = 5 + 3 \cdot (-1); \tag{1.6}$$

$$1 = 3 + 2 \cdot (-1). \tag{1.7}$$

Substituindo (1.6) em (1.7), temos:

$$1 = 3 \cdot 2 + 5 \cdot (-1).$$

Por fim, multiplicando a igualdade por 13, chegamos à $13 = 3 \cdot 26 + 5 \cdot (-13)$ donde se obtém $(26, -13)$ como solução da equação. Portanto, as demais soluções são dadas pelo conjunto abaixo:

$$S = \{(26 - 5t, -13 + 3t);\ t \in \mathbb{Z}\}.$$

De agora em diante, passaremos para nosso objeto de estudo que baseia-se em compreender a divisibilidade dos números inteiros por meio das congruências.

2 Aritmética Modular

Neste capítulo, iremos abordar a Aritmética Modular ou também chamada de Aritmética dos Restos, que é um sistema aritmético dos números inteiros. Esse sistema prioriza compreender as essências e propriedades dos restos da divisão entre dois números inteiros e, por este motivo, trouxemos o capítulo anterior. Cabe ressaltar que essa ideia de trabalhar com os restos de uma divisão está centrada nos conceitos de congruências e sistemas completos de resíduos os quais serão explicados no decorrer do trabalho.

Diante disto, dividimos o capítulo nas seguintes duas seções: **Congruências**, que abordaremos propriamente dito a relação de congruência entre dois números inteiros e os sistemas completos de resíduos; e **Atividade didática**, que descreveremos uma atividade que aplicamos com estudantes de um 6º ano do Ensino Fundamental, um 1º ano do Ensino Médio e uma turma de ingressantes no curso de Matemática Licenciatura no ano de 2020. Além disso, enfatizamos que o capítulo foi baseado nas literaturas de (DOMINGUES, 1991), (GOMES; SILVA, 2018), (HEFEZ, 2009) e (SANTOS, 2020).

2.1 Congruências

No dia-a-dia acabamos presenciando vários fenômenos cíclicos e, em muitas vezes, nem percebemos esses fatos ou não nos questionamos sobre eles. Alguns desses fenômenos que podemos citar são as horas de um relógio, os dias da semana e, até mesmo, as glaciações (períodos em que aproximadamente 10% da terra fica coberta de gelo dos pólos).

As situações que acabamos de mencionar, estão associadas com o conceito de congruências, que foi desenvolvido pelo matemático alemão Johann Carl Friederich Gauss ($1777 - 1855$) em seu livro intitulado *Disquisitiones Arithmeticae*, publicado em 1801 quando este tinha apenas 24 anos. (HEFEZ, 2009).

Em sua obra, Gauss reuniu resultados de outros matemáticos como, por exemplo, Leonhard Euler, Joseph-Louis Lagrange e Pierre de Fermat além de estruturar e resolver novos problemas envolvendo congruências. Convém salientar que tal livro aborda a Teoria dos Números (área da Matemática que procura estudar as propriedades dos números) e a Teoria Algébrica dos Números (ramo da Teoria dos Números que expande o conceito de número para número algébrico envolvendo polinômios). (HEFEZ, 2009) e (BOYER; MERZBACH, 2012).

2.1.1 Congruências

Definição 2.1.1. Consideremos m um número inteiro positivo. Dizemos que os números inteiros a e b são congruentes módulo m se os restos da Divisão Euclidiana de a e b por m são iguais. Neste caso, denotamos como $a \equiv b \ (mod\ m)$ (lê-se: a côngruo à b módulo m ou, simplesmente, a e b são congruentes módulo m).

Observação 2.1.2. Atente que podemos trabalhar apenas com $m > 1$, visto que todo número inteiro deixa resto 0 na divisão por 1 tornando assim a expressão $a \equiv b \ (mod\ 1)$ sempre verdadeira para qualquer $a, b \in \mathbb{Z}$. Isto não é interessante para a aritmética porque não nos evidência muitas informações.

Observação 2.1.3. Quando a relação $a \equiv b \ (mod\ m)$ é falsa, dizemos que a e b são incongruentes ou, simplesmente, que a e b não são congruentes módulo m denotando tal fato por $a \not\equiv b \ (mod\ m)$.

Exemplo 2.1.4. Sejam $m = 15$, $a = 28$ e $b = 73$. Repare que $28 \equiv 73 \ (mod\ 15)$ uma vez que, aplicando a Divisão Euclidiana de 28 e 73 por 15, obtemos $28 = 15 \cdot 1 + 13$ e $73 = 15 \cdot 4 + 13$ donde concluímos que os seus restos são iguais. Por outro lado, se tomarmos $b = 63$, temos que $28 \not\equiv 63 \ (mod\ 15)$, pois, realizando a Divisão Euclidiana de 63 por 15, tem-se $63 = 15 \cdot 4 + 3$ tornando visível que seus restos são diferentes.

O primeiro resultado envolvendo congruência, que veremos a seguir, é importante porque vai nos fornecer um dispositivo para sabermos se dois números inteiros são congruentes módulo m sem que necessitemos aplicar o Teorema 1.1.13 em cada um deles para analisarmos os seus restos na divisão por m. Nesse aspecto, caracterizamos tal resultado como um teorema.

Teorema 2.1.5. Sejam a, b e m números inteiros, com $m > 1$. Temos que $a \equiv b \ (mod\ m)$ se, e somente se, $m|(b - a)$.

Demonstração. Suponhamos que $a \equiv b \ (mod\ m)$, então, pelo Teorema 1.1.13, existem q, t e r números inteiros tais que $a = mq + r$ e $b = mt + r$, com $0 \leqslant r < |m| = m$. A partir disso, $b - a = m(t - q) \Rightarrow m|(b - a)$. Por outro lado, se $m|(b - a)$, então existe $q \in \mathbb{Z}$ tal que $b - a = mq$. Aplicando a Divisão Euclidiana de a e b por m, tem-se $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ tais que $a = mq_1 + r_1$ e $b = mq_2 + r_2$, com $0 \leqslant r_1 < m$ e $0 \leqslant r_2 < m$. Assim, $mq = m(q_2 - q_1) + r_2 - r_1$ e, reescrevendo a igualdade, obtém-se $m(q - q_2 + q_1) = r_2 - r_1$. Além disso, note que $-m < r_2 - r_1 < m$ donde segue que $r_2 - r_1 = 0$ (pois o único múltiplo de m nesse intervalo é 0). Portanto $r_1 = r_2$ concluindo que $a \equiv b \ (mod\ m)$. □

Proposição 2.1.6. Seja m um número inteiro maior que 1. Então temos que o conjunto $E = \{(a, b) \in \mathbb{Z}^2;\ a \equiv b \ (mod\ m)\}$ define uma relação de equivalência sobre $\mathbb{Z}$.

Demonstração. Para provarmos esta proposição, devemos mostrar que são satisfeitas as seguintes propriedades: Reflexiva, Simétrica e Transitiva.

Reflexiva: De fato, $a \equiv a \ (mod\ m)$ para todo $a \in \mathbb{Z}$, pois $m|0 = (a - a)$.

Simétrica: Se $a \equiv b \ (mod\ m)$, então $m|(b - a)$, isto é, existe $q \in \mathbb{Z}$ tal que $b - a = mq$. Observe que $a - b = m(-q) \Rightarrow m|(a - b) \Rightarrow b \equiv a \ (mod\ m)$.

Transitiva: Se $a \equiv b \ (mod\ m)$ e $b \equiv c \ (mod\ m)$, então temos que $m|(b - a)$ e $m|(c - b)$, ou seja, existem $q, t \in \mathbb{Z}$ tais que $b - a = mq$ e $c - b = mt$. Somando essas duas igualdades, obtemos $c - a = m(q + t) \Rightarrow m|(c - a) \Rightarrow a \equiv c \ (mod\ m)$.

Portanto, o conjunto E define uma relação de equivalência sobre $\mathbb{Z}$. □

Proposição 2.1.7. Sejam $a, b, c, d, m \in \mathbb{Z}$ com $m > 1$. Temos que:

i) Se $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, então $a + c \equiv b + d \ (mod\ m)$;

ii) Se $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, então $ac \equiv bd \ (mod\ m)$;

iii) $a + c \equiv b + c \ (mod\ m) \Leftrightarrow a \equiv b \ (mod\ m)$;

iv) $ac \equiv bc \ (mod\ m) \Leftrightarrow a \equiv b \ \left(mod\ \dfrac{m}{mdc(c, m)}\right)$.

Demonstração. Segue abaixo a prova dos itens.

i) Por hipótese, temos que $b - a = mq$ e $d - c = mk$ para algum $q, k \in \mathbb{Z}$. Somando as expressões, obtemos $(b + d) - (a + c) = m(q + k) \Rightarrow m\Big|[(b + d) - (a + c)]$. Portanto, $a + c \equiv b + d \ (mod\ m)$.

ii) Novamente, pela hipótese temos que $b - a = mq$ e $d - c = mk$ para algum $q, k \in \mathbb{Z}$. Observe que $bc - ac = m(qc)$ e $bd - bc = m(bk)$, ou seja, $ac \equiv bc \ (mod\ m)$ e $bc \equiv bd \ (mod\ m)$. Portanto, pela transitividade, $ac \equiv bd \ (mod\ m)$.

iii) De fato,

$$\begin{aligned} a + c \equiv b + c \ (mod\ m) &\Leftrightarrow m\Big|[(b + c) - (a + c)] \\ &\Leftrightarrow m|(b - a) \\ &\Leftrightarrow a \equiv b \ (mod\ m). \end{aligned}$$

iv) Seja $mdc(c, m) = d$, então $\frac{m}{d}$ e $\frac{c}{d}$ são números inteiros e, inclusive, coprimos. Daí,

$$\begin{aligned} ac \equiv bc \ (mod\ m) &\Leftrightarrow m|(bc - ac) \\ &\Leftrightarrow bc - ac = mq, q \in \mathbb{Z} \\ &\Leftrightarrow (b-a)\frac{c}{d} = \frac{m}{d}q, q \in \mathbb{Z} \\ &\Leftrightarrow \frac{m}{d}\Big|(b-a) \\ &\Leftrightarrow a \equiv b \ \left(mod\ \frac{m}{d}\right). \end{aligned}$$

□

Observação 2.1.8. Os itens (iii) e (iv) da proposição acima nos dizem que valem, respectivamente, a propriedade do cancelamento da adição e a propriedade do "cancelamento" da multiplicação para congruências.

Exemplo 2.1.9. Sejam a e b números inteiros tais que deixam resto 6 e 2 quando divididos por 7, respectivamente. Mostraremos qual será o resto da divisão de ab por 7. Note que $a \equiv 6 \ (mod\ 7)$ e $b \equiv 2 \ (mod\ 7)$, logo $ab \equiv 12 \ (mod\ 7)$. Por outro lado, $12 \equiv 5 \ (mod\ 7)$ e, pela transitividade da relação, $ab \equiv 5 \ (mod\ 7)$. Portanto, o resto da divisão de ab por 7 é 5.

Proposição 2.1.10. Sejam $a, b, m \in \mathbb{Z}$, com $m > 1$. Se $a \equiv b \ (mod\ m)$, então $a^n \equiv b^n \ (mod\ m)$, para todo $n \in \mathbb{N}$.

Demonstração. Basta aplicar $n - 1$ vezes o item (ii) da Proposição 2.1.7 para $c = a$ e $d = b$ uma vez que $a \equiv b \ (mod\ m)$. Assim, $a^n \equiv b^n \ (mod\ m)$, para todo $n \in \mathbb{N}$. □

Proposição 2.1.11. Sejam $a, b, p \in \mathbb{Z}$, com p primo. Então, $(a+b)^p \equiv a^p + b^p \ (mod\ p)$ e $(a-b)^p \equiv a^p - b^p \ (mod\ p)$.

Demonstração. Primeiro vamos recordar um conceito de Análise Combinatória (ramo da Matemática que estuda/analisa coleções finitas de objetos e procura realizar, em particular, contagem e combinação destes objetos, por exemplo).

O referido conceito será o de combinação, que nos diz o seguinte: Dado um conjunto X de n elementos distintos, vamos tomar um subconjunto de X com k elementos $(k \leqslant n)$ escolhidos entre os n. O Número de subconjuntos de X com k elementos é:

$$\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{n!}{k!(n-k)!}.$$

Além disso, faremos o uso do Binômio de Newton que nos diz que:

$$(x+y)^n = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) x^{n-k} \cdot y^k.$$

Isto pode ser provado via indução finita sobre n. Aqui não iremos realizar tal prova para não "fugirmos" mais do nosso assunto.

Note que pelo Binômio de Newton, podemos escrever:

$$\begin{aligned}(a+b)^p &= \sum_{k=0}^{p} \left(\begin{array}{c} p \\ k \end{array} \right) a^{p-k} \cdot b^k \\ &= a^p + b^p + \sum_{k=1}^{p-1} \left(\begin{array}{c} p \\ k \end{array} \right) a^{p-k} \cdot b^k.\end{aligned}$$

Assim, $(a+b)^p - (a^p + b^p) = \sum_{k=1}^{p-1} \left(\begin{array}{c} p \\ k \end{array} \right) a^{p-k} \cdot b^k$, onde $1 \leqslant k < p$.

Resta-nos provar que $\sum_{k=1}^{p-1} \left(\begin{array}{c} p \\ k \end{array} \right) a^{p-k} \cdot b^k$ é múltiplo de p. Para isto, é suficiente mostrarmos que $\left(\begin{array}{c} p \\ k \end{array} \right)$ é um múltiplo de p. De fato,

$$\left(\begin{array}{c} p \\ k \end{array} \right) = \frac{p!}{k!(p-k)!} = p \cdot \frac{(p-1)!}{k!(p-k)!} = p \cdot \frac{(p-1)(p-2)\cdots(p-k+1)\cancel{(p-k)!}}{k!\cancel{(p-k)!}}$$

$$= p \cdot \frac{(p-1)(p-2)\cdots(p-k+1)}{k!}.$$

Logo, $p \Big| \left[\left(\begin{array}{c} p \\ k \end{array} \right) \cdot k! \right]$. Do fato de p ser primo, temos que $p \Big| \left(\begin{array}{c} p \\ k \end{array} \right)$ ou $p|k!$. Além disso, $mdc(p,k) = 1$ para todo $1 \leqslant k < p$, pois, caso contrário, se $mdc(p,k) = d$ (com $d > 1$) para algum k (com $1 \leqslant k < p$), então $d|p$ e $d|k$. Como p é primo e seus únicos divisores positivos são 1 e p, logo $d = p$ (já que $d > 1$). Assim, $p|k$ (absurdo! porque $k < p$). Logo, $mdc(p,k) = 1$ para todo $1 \leqslant k < p$.

Afirmação: Se $mdc(a,b) = mdc(a,c) = 1$, então $mdc(a,bc) = 1$.

De fato, como $mdc(a,b) = mdc(a,c) = 1$, então temos pelo Teorema 1.1.36 que existem x, y, z, w números inteiros tais que $ax + by = 1$ e $az + cw = 1$. Se multiplicarmos esta última igualdade por b, então temos $a(bz)+(bc)w = b$. Substituindo $a(bz)+(bc)w = b$ em $ax+by = 1$, vamos ter $ax+a(bzy)+(bc)(wy) = 1$ se, e só se, $a(x+bzy)+(bc)(wy) = 1$. Portanto, pela reciproca do Teorema 1.1.36 segue que $mdc(a,bc) = 1$.

Desta forma, por esta afirmação acima, temos $mdc(p,k!) = 1$ (basta aplicarmos esta Afirmação acima $k-1$ vezes porque $mdc(p,k) = mdc(p,k-1) = 1$, para todo k número inteiro positivo menor do que p).

Então, $p \nmid k!$. Sendo assim,

$$p \Big| \left(\begin{array}{c} p \\ k \end{array} \right).$$

Logo, existe $t \in \mathbb{Z}$ tal que $\begin{pmatrix} p \\ k \end{pmatrix} = pt$.

Portanto,

$$(a+b)^p - (a^p + b^p) = \sum_{k=1}^{p-1} pt \cdot a^{p-k} \cdot b^k = p \cdot \sum_{k=1}^{p-1} t \cdot a^{p-k} \cdot b^k.$$

□

Proposição 2.1.12. Sejam $a, b \in \mathbb{Z}$ e $m, m_1, m_2, ..., m_k, n$ números inteiros maiores do que 1. Então, temos que:

i) Se $a \equiv b \ (mod\ m)$ e $n|m$, então $a \equiv b \ (mod\ n)$;

ii) $a \equiv b \ (mod\ m_i)$, para todo $i = 1, 2, ..., k$, se, e somente se, $a \equiv b \ (mod\ M)$, onde $M = mmc(m_1, m_2, ..., m_k)$;

iii) Se $a \equiv b \ (mod\ m)$, então $mdc(a, m) = mdc(b, m)$.

Demonstração. Segue abaixo a prova dos itens.

i) Por hipótese, $m|(b-a)$ e $n|m$, ou seja, existem números inteiros q, k tais que $b-a = mq$ e $m = nk$. Multiplicando esta última igualdade por q, temos $n(kq) = mq = b-a$. Portanto, $n|(b-a)$ donde segue que $a \equiv b \ (mod\ n)$.

ii) Suponhamos que $a \equiv b \ (mod\ m_i)$ para todo $i = 1, 2, ..., k$, então $b - a = m_i q$ com q inteiro. Observe que $mmc(m_1, m_2, ..., m_k) \Big| (b-a)$, pois $b-a$ é um múltiplo comum de m_i e, assim, $a \equiv b \ (mod\ mmc(m_1, m_2, ..., m_k))$. Por outro lado, se $a \equiv b \ (mod\ mmc(m_1, m_2, ..., m_k))$ e observando que $m_i \Big| mmc(m_1, m_2, ..., m_k)$ com $i = 1, 2, ..., k$, segue do item anterior que $a \equiv b \ (mod\ m_i)$.

iii) Seja $a \equiv b \ (mod\ m)$, então existe $q \in \mathbb{Z}$ tal que $b - a = mq$. Vamos mostrar que $mdc(a, m) = mdc(b, m)$. De fato, note que:

$$d = mdc(b, m) = mdc(b + (a - a), m) = mdc((b - a) + a, m) = mdc(mq + a, m).$$

Segue da Proposição 1.1.31 que $mdc(mq + a, m) = mdc(a, m)$. Isto conclui a demonstração. □

Iremos demonstrar agora os critérios de divisibilidade de 2 até 10. É claro que esses critérios já poderiam ter sido demonstrados no capítulo anterior, porém a notação de congruência torna mais elegante o modo de dispor os números durante a prova destes resultados.

Teorema 2.1.13. Todo número inteiro n é divisível por 2 se, e somente se, o algarismo das unidades de n for $0, 2, 4, 6$ ou 8.

Demonstração. Observe que $10 \equiv 0\ (mod\ 2)$. Pela Proposição 2.1.10, temos:

$$\begin{aligned} 10^2 &\equiv 0\ (mod\ 2) \\ 10^3 &\equiv 0\ (mod\ 2) \\ &\vdots \\ 10^i &\equiv 0\ (mod\ 2),\ \text{para todo } i \in \mathbb{N}^* \\ &\vdots \end{aligned}$$

Diante disso, atente que $10^i = 2T_i$, para todo $i \in \mathbb{N}^*$ e T_i um número inteiro. Assim, tem-se que $10^i a_i = 2T_i a_i$ para $a_i \in \mathbb{Z}$, ou seja, um múltiplo de 2 quando multiplicado por um número inteiro ainda continua sendo divisível por 2.

Suponhamos que n seja um múltiplo de 2, então $n \equiv 0\ (mod\ 2)$. Vamos escrever n em sua representação posicional de base 10, isto é, $n = 10^k a_k + 10^{k-1} a_{k-1} + ... + 10a_1 + a_o$, com $a_j \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, para todo $j = 1, 2, ..., k$. Logo,

$$10^k a_k + 10^{k-1} a_{k-1} + ... + 10a_1 + a_o \equiv 0\ (mod\ 2) \quad \Rightarrow \quad 2T + a_o \equiv 0\ (mod\ 2),$$

onde $T = T_k a_k + T_{k-1} a_{k-1} + \cdots + T_2 a_2 + T_1 a_1$ e cada $T_j \in \mathbb{Z}$.

Dê $2T + a_o \equiv 0\ (mod\ 2)$, segue $a_o \equiv 0\ (mod\ 2)$. Portanto, $a_o = 0, 2, 4, 6$ ou 8 por ser o algarismo das unidades e este estar no intervalo $0 \leqslant a_o \leqslant 9$.

Por outro lado, se $a_o = 0, 2, 4, 6$ ou 8, então $a_o \equiv 0\ (mod\ 2)$. Além disso, se escrevermos $n = 10^k a_k + 10^{k-1} a_{k-1} + ... + 10a_1 + a_o$, então temos um número divisível por 2 uma vez que todas as parcelar $10^k a_k + 10^{k-1} a_{k-1} + ... + 10a_1 + a_o$ são múltiplas de 2 e, assim, $n \equiv 0\ (mod\ 2)$. □

Exemplo 2.1.14. Observe que o número -564 é divisível por 2, pois o algarismo das unidades é 4. A título de curiosidade, $-564 = 2 \cdot (-282)$.

Teorema 2.1.15. Todo número inteiro n é divisível por 3 se, e somente se, a soma de seus algarismos é divisíveis por 3.

Demonstração. Observe que $10 \equiv 1\ (mod\ 3)$. Pela Proposição 2.1.10, temos:

$$\begin{aligned} 10^2 &\equiv 1\ (mod\ 3) \\ 10^3 &\equiv 1\ (mod\ 3) \\ &\vdots \\ 10^i &\equiv 1\ (mod\ 3),\ \text{para todo } i \in \mathbb{N}^* \\ &\vdots \end{aligned}$$

Diante disso, atente que $10^i = 3T_i + 1$, para todo $i \in \mathbb{N}^*$ e T_i um número inteiro. Assim, tem-se $10^i a_i = 3T_i a_i + a_i$, para $a_i \in \mathbb{Z}$.

Sendo $n \in \mathbb{Z}$ tal que $n \equiv 0\ (mod\ 3)$ e o escrevendo no sistema posicional de base 10, temos que $n = 10^k a_k + 10^{k-1}a_{k-1} + ... + 10a_1 + a_o$, com $a_j \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ para todo $j = 1, 2, ..., k$. Logo, $10^k a_k + 10^{k-1}a_{k-1} + ... + 10a_1 + a_o \equiv 0\ (mod\ 3)$ se, e somente se, $3T + a_k + a_{k-1} + ... + a_1 + a_o \equiv 0\ (mod\ 3)$, onde $T = T_k a_k + T_{k-1}a_{k-1} + \cdots + T_2 a_2 + T_1 a_1$ e cada $T_j \in \mathbb{Z}$ para todo $j = 1, 2, ..., k$. Por fim, $a_k + a_{k-1} + ... + a_1 + a_o \equiv 0\ (mod\ 3)$.

Agora, se $a_k + a_{k-1} + ... + a_1 + a_o \equiv 0\ (mod\ 3)$ é evidente que n será múltiplo de 3, pois $n = 10^k a_k + 10^{k-1}a_{k-1} + ... + 10a_1 + a_o$ implica em $n = 3T + a_k + a_{k-1} + ... + a_1 + a_o$, para $T = T_k a_k + T_{k-1}a_{k-1} + \cdots + T_2 a_2 + T_1 a_1$ e cada $T_j \in \mathbb{Z}$. Desta última igualdade, extraí-se $n = 3T + 3Q = 3(T + Q)$, com $Q = a_k + a_{k-1} + \cdots + a_2 + a_1$. Portanto, segue o resultado. □

Exemplo 2.1.16. O número 5.235 é divisível por 3, pois $5 + 2 + 3 + 5 = 15$ e $3|15$. A título de curiosidade, $5.235 = 3 \cdot 1.745$.

Teorema 2.1.17. Todo número inteiro é divisível por 4 se, e somente se, o número formado pelos seus dois últimos algarismos é múltiplo de 4.

Demonstração. Note que $10^2 \equiv 0\ (mod\ 4)$ e $10 \equiv 2\ (mod\ 4)$. Assim, pelo item (ii) da Proposição 2.1.7, temos $10^3 \equiv 0\ (mod\ 4)$ e, repetindo esse processo sempre com a nova congruência que vamos obtendo, teremos:

$$\begin{aligned} 10^4 &\equiv 0\ (mod\ 4) \\ 10^5 &\equiv 0\ (mod\ 4) \\ &\vdots \\ 10^i &\equiv 0\ (mod\ 4),\ \text{para todo } i \in \mathbb{N}^* - \{1\} \\ &\vdots \end{aligned}$$

Diante disso, atente que $10^i = 4T_i$, para todo $i \in \mathbb{N}^* - \{1\}$ e T_i um número inteiro. Assim, tem-se que $10^i a_i = 4T_i a_i$, para $a_i \in \mathbb{Z}$.

Sendo $n \in \mathbb{Z}$ tal que $n \equiv 0\ (mod\ 4)$ e o escrevendo no sistema posicional de base 10, temos que $n = 10^k a_k + 10^{k-1}a_{k-1} + ... + 10a_1 + a_o$, para $a_j \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ para todo $j = 1, 2, ..., k$. Então,

$$10^k a_k + 10^{k-1}a_{k-1} + ... + 10a_1 + a_o \equiv 0\ (mod\ 4) \ \Rightarrow\ 4T + 10a_1 + a_o \equiv 0\ (mod\ 4),$$

onde $T = T_k a_k + T_{k-1}a_{k-1} + \cdots + T_3 a_3 + T_2 a_2$ e cada $T_j \in \mathbb{Z}$. Isto nos leva à

$$10a_1 + a_o \equiv 0\ (mod\ 4).$$

Por outro lado, se $10a_1 + a_o \equiv 0\ (mod\ 4)$, então temos

$$\begin{aligned} n = 10^k a_k + 10^{k-1}a_{k-1} + ... + 10a_1 + a_o \ &\Rightarrow\ n = 4T + 10a_1 + a_o \\ &\Rightarrow\ n = 4T + 4Q = 4(T+Q), \end{aligned}$$

onde $T = T_k a_k + T_{k-1}a_{k-1} + \cdots + T_3 a_3 + T_2 a_2$ e $4Q = 10a_1 + a_o$. □

Exemplo 2.1.18. O número -44.324 é divisível por 4, pois o número formado pelos dois últimos algarismos de -44.324 é divisível por 4, isto é, $4|24$. A título de curiosidade, $-44.324 = 4 \cdot (-11.081)$.

Teorema 2.1.19. Todo número inteiro n é divisível por 5 se, e somente se, o último algarismo de n for 0 ou 5.

Demonstração. Observe que $10 \equiv 0\ (mod\ 5)$. Pela Proposição 2.1.10 temos:

$$\begin{aligned} 10^2 &\equiv 0\ (mod\ 5) \\ 10^3 &\equiv 0\ (mod\ 5) \\ &\vdots \\ 10^i &\equiv 0\ (mod\ 5),\ \text{para todo } i \in \mathbb{N}^* \\ &\vdots \end{aligned}$$

Diante disso, atente que $10^i = 5T_i$, para todo $i \in \mathbb{N}^*$ e T_i um número inteiro. Assim, tem-se que $10^i a_i = 5T_i a_i$, para $a_i \in \mathbb{Z}$.

Sendo $n \in \mathbb{Z}$ tal que $n \equiv 0\ (mod\ 5)$ e o escrevendo no sistema posicional de base 10, temos $n = 10^k a_k + 10^{k-1}a_{k-1} + ... + 10a_1 + a_o$, com $a_j \in \{0,1,2,3,4,5,6,7,8,9\}$ para todo $j = 1, 2, ..., k$. Então,

$$10^k a_k + 10^{k-1}a_{k-1} + ... + 10a_1 + a_o \equiv 0\ (mod\ 5) \ \Rightarrow\ 5T + a_o \equiv 0\ (mod\ 5),$$

onde $T = T_k a_k + T_{k-1}a_{k-1} + ... + T_2 a_2 + T_1 a_1$ e cada $T_j \in \mathbb{Z}$.

Dê $5T + a_o \equiv 0\ (mod\ 5)$, obtém-se $a_o \equiv 0\ (mod\ 5)$, ou seja, a_o é um múltiplo de 5 e, por este ser o algarismo das unidades de n, só podemos ter que $a_o = 0$ ou $a_o = 5$. Por outro lado, se a_o se múltiplo de 5, é imediato que n será divisível por 5. □

Exemplo 2.1.20. Repare que 570.565 é divisível por 5, já que o algarismo da unidade é 5. Sendo assim, $570.565 = 5 \cdot 114.113$.

Teorema 2.1.21. Todo número inteiro n é divisível por 6 se, e somente se, n é múltiplo de 2 e 3 simultaneamente.

Demonstração. Consideremos $n \equiv 0\ (mod\ 6)$. Note que $2|6$ e, pelo item (i) da Proposição 2.1.12, $n \equiv 0\ (mod\ 2)$. Entretanto, também sabemos que $3|6$ e, pela mesma proposição,

$n \equiv 0\ (mod\ 3)$. Portanto, n é divisível por 2 e 3 simultaneamente. Por outro lado, se $n \equiv 0\ (mod\ 2)$ e $n \equiv 0\ (mod\ 3)$, então, pelo item (ii) da Proposição 2.1.12, temos que $n \equiv 0\ (mod\ mmc(2,3))$, ou seja, $n \equiv 0\ (mod\ 6)$. □

Exemplo 2.1.22. O número 3.123.792 é divisível por 6, pois 3.123.792 é divisível por 2 (já que o algarismo da unidade é 2) e por 3 (já que a soma de seus algarismos é 27 e 3|27) simultaneamente. Assim, $3.123.792 = 6 \cdot 520.632$.

Teorema 2.1.23. Todo número inteiro n é divisível por 7 se, e somente se, a diferença entre o dobro do algarismo das unidades de n com o número formado pelos algarismos remanescentes, exceto pela unidade, é múltiplo de 7.

Demonstração. Seja $n \equiv 0\ (mod\ 7)$. Escrevendo n na representação posicional na base 10, temos que $n = 10^k a_k + 10^{k-1}a_{k-1} + ... + 10a_1 + a_o$, logo

$$10^k a_k + 10^{k-1}a_{k-1} + ... + 10a_1 + a_o \equiv 0\ (mod\ 7).$$

Vamos escrever $a_o = 21a_o - 20a_o$ e, com isso,

$$10^k a_k + 10^{k-1}a_{k-1} + ... + 10a_1 + 21a_o - 20a_o \equiv 0\ (mod\ 7).$$

Observe que $21 \equiv 0\ (mod\ 7)$, daí

$$10^k a_k + 10^{k-1}a_{k-1} + ... + 10a_1 - 20a_o \equiv 0\ (mod\ 7).$$

A partir disso, temos:

$$10[(10^{k-1}a_k + 10^{k-2}a_{k-1} + ... + a_1) - 2a_o] \equiv 0\ (mod\ 7).$$

Como o $mdc(10,7) = 1$, segue da Proposição 1.2.6 que

$$(10^{k-1}a_k + 10^{k-2}a_{k-1} + ... + a_1) - 2a_o \equiv 0\ (mod\ 7).$$

Por outro lado, se $(10^{k-1}a_k + 10^{k-2}a_{k-1} + ... + a_1) - 2a_o \equiv 0\ (mod\ 7)$, então multiplicando por 10 temos

$$10^k a_k + 10^{k-1}a_{k-1} + ... + 10a_1 - 20a_o \equiv 0\ (mod\ 7).$$

Somando $21a_o$, obtém-se

$$10^k a_k + 10^{k-1}a_{k-1} + ... + 10a_1 - 20a_o + 21a_o \equiv 21a_o \equiv 0\ (mod\ 7).$$

Disso segue que $n = 10^k a_k + 10^{k-1}a_{k-1} + ... + 10a_1 + a_o \equiv 0\ (mod\ 7)$. □

Exemplo 2.1.24. O número 2.576 é divisível por 7. De fato, pelo Teorema 2.1.23, temos que $2 \cdot 6 - 257 = 12 - 257 = -245$ e, reaplicando o Teorema 2.1.23 para $|-245| = 245$, teremos $2 \cdot 5 - 24 = -14$. Aqui vê-se que $7|(-14)$ e, então, $7|245$ (em particular, $7|(-245)$). Como $7|(-245)$, segue que $2.576 = 7 \cdot 368$.

Teorema 2.1.25. Todo número inteiro n é divisível por 8 se, e somente se, o número formado pelos últimos três algarismos de n for múltiplo de 8.

Demonstração. Observe que $10^3 \equiv 0\ (mod\ 8)$ e $10 \equiv 2\ (mod\ 8)$. Assim, pelo item (ii) da Proposição 2.1.10, temos $10^4 \equiv 0\ (mod\ 8)$ e, repetindo esse processo sempre com a nova congruência que vamos obtendo, teremos:

$$\begin{aligned} 10^5 &\equiv 0\ (mod\ 8) \\ 10^6 &\equiv 0\ (mod\ 8) \\ &\vdots \\ 10^i &\equiv 0\ (mod\ 8),\ \text{para todo } i \in \mathbb{N}^* - \{1,2\} \\ &\vdots \end{aligned}$$

Diante disso, atente que $10^i = 8T_i$, para todo $i \geqslant 3$ e T_i um número inteiro. Assim, tem-se $10^i a_i = 8T_i a_i$, para $a_i \in \mathbb{Z}$, ou seja, um múltiplo de 8 quando multiplicado por um número inteiro ainda continua sendo divisível por 8.

Considerando n um número inteiro múltiplo de 8, então $n \equiv 0\ (mod\ 8)$. Vamos escrever n em sua representação posicional de base 10, isto é, $n = 10^k a_k + 10^{k-1}a_{k-1} + ... + 10a_1 + a_o$, com $a_j \in \{0,1,2,3,4,5,6,7,8,9\}$ para todo $j = 1, 2, ..., k$. Logo,

$$\begin{aligned} 10^k a_k + 10^{k-1}a_{k-1} + ... + 10a_1 + a_o \equiv 0\ (mod\ 8) &\Rightarrow 8T + 10^2 a_2 + 10a_1 + a_o \equiv 0\ (mod\ 8) \\ &\Rightarrow 10^2 a_2 + 10a_1 + a_o \equiv 0\ (mod\ 8), \end{aligned}$$

onde $T = T_k a_k + T_{k-1}a_{k-1} + \cdots + T_4 a_4 + T_3 a_3$ e cada $T_j \in \mathbb{Z}$.

Por outro lado, se $10^2 a_2 + 10a_1 + a_o \equiv 0\ (mod\ 8)$, então é imediato que $n = 10^k a_k + 10^{k-1}a_{k-1} + ... + 10a_1 + a_o$ será um múltiplo de 8 uma vez que $n = 8T + 10^2 a_2 + 10a_1 + a_o = 8T + 8Q = 8(T + Q)$, com $T = T_k a_k + T_{k-1}a_{k-1} + \cdots + T_4 a_4 + T_3 a_3$, cada T_j inteiro e $8Q = 10^2 a_2 + 10a_1 + a_o$. □

Exemplo 2.1.26. Observe que 520.256 é divisível por 8, pois o número formado pelos três últimos algarismos de 520.256 é múltiplo de 8, ou seja, $256 = 32 \cdot 8$. Portanto, pelo Teorema 2.1.25, $8|520.256$, a saber $520.256 = 8 \cdot 65.032$.

Teorema 2.1.27. Todo número inteiro n é divisível por 9 se, e somente se, a soma de seus algarismos é múltiplo de 9.

Demonstração. Observe que $10 \equiv 1\ (mod\ 9)$. Pela Proposição 2.1.10, temos:

$$\begin{aligned} 10^2 &\equiv 1\ (mod\ 9) \\ 10^3 &\equiv 1\ (mod\ 9) \\ &\vdots \\ 10^i &\equiv 1\ (mod\ 9),\ \text{para todo } i \in \mathbb{N}^* \\ &\vdots \end{aligned}$$

Diante disso, atente que $10^i = 9T_i + 1$, para todo $i \geqslant 1$ e T_i um número inteiro. Assim, tem-se que $10^i a_i = 9T_i a_i + a_i$ para $a_i \in \mathbb{Z}$.

Sendo $n \in \mathbb{Z}$ tal que $n \equiv 0\ (mod\ 9)$ e o escrevendo no sistema posicional de base 10, temos que $n = 10^k a_k + 10^{k-1}a_{k-1} + ... + 10a_1 + a_o$, com $a_j \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ para todo $j = 1, 2, ..., k$. Logo, $10^k a_k + 10^{k-1}a_{k-1} + ... + 10a_1 + a_o \equiv 0\ (mod\ 9)$ se, e somente se, $9T + a_k + a_{k-1} + ... + a_1 + a_o \equiv 0\ (mod\ 9)$, com $T = T_k a_k + T_{k-1}a_{k-1} + \cdots + T_2 a_2 + T_1 a_1$ e cada $T_j \in \mathbb{Z}$. Por fim, $a_k + a_{k-1} + ... + a_1 + a_o \equiv 0\ (mod\ 9)$.

Agora, se $a_k + a_{k-1} + ... + a_1 + a_o \equiv 0\ (mod\ 9)$ é evidente que n será múltiplo de 9, pois:

$$\begin{aligned} n = 10^k a_k + 10^{k-1}a_{k-1} + ... + 10a_1 + a_o &\Rightarrow n = 9T + a_k + a_{k-1} + ... + a_1 + a_o \\ &\Rightarrow n = 9T + 9Q \\ &\Rightarrow n = 9(T + Q), \end{aligned}$$

onde $T = T_k a_k + T_{k-1}a_{k-1} + \cdots + T_2 a_2 + T_1 a_1$; cada $T_j \in \mathbb{Z}$, com $j = 1, 2, 3, ..., k$; e $9Q = a_k + a_{k-1} + \cdots + a_1 + a_o$ .Portanto, segue o resultado. □

Exemplo 2.1.28. O número 5.672.358 é divisível por 9 uma vez que a soma dos algarismos de 5.672.358 é $5 + 6 + 7 + 2 + 3 + 5 + 8 = 36$ e $9|36$. Portanto, $5.672.358 = 9 \cdot 630.262$.

Teorema 2.1.29. Todo número inteiro n é divisível por 10 se, e somente se, n é múltiplo de 2 e 5 simultaneamente.

Demonstração. Suponhamos que $n \equiv 0\ (mod\ 10)$. Repare que $2|10$ assim como $5|10$, então, pelo item (i) da Proposição 2.1.12, temos $n \equiv 0\ (mod\ 2)$ e $n \equiv 0\ (mod\ 5)$. Portanto, n é divisível por 2 e 5 simultaneamente. Por outro lado, se $n \equiv 0\ (mod\ 2)$ e $n \equiv 0\ (mod\ 5)$, então, pelo item (ii) da Proposição 2.1.10, segue que $n \equiv 0\ (mod\ mmc(2, 5))$, ou seja, $n \equiv 0\ (mod\ 10)$. □

Exemplo 2.1.30. O número 658.265.154.250 é divisível por 10, pois 658.265.154.250 é divisível por 2 e 5 simultaneamente (uma vez que o algarismo da unidade é 0). Assim, $658.265.154.250 = 10 \cdot 65.826.515.425$.

Comentário 2.1.31. O critério de divisibilidade por 10 pode ser reformulado como: Todo número inteiro é divisível por 10 se, e somente se, o algarismo das unidades deste número inteiro é 0. Isso é verificado facilmente, pois dado o número inteiro n divisível por 10 então este é divisível por 2 e 5 simultaneamente. Como n é divisível por 2 temos que n é par enquanto que n divisível por 5 tem o algarismo das unidades sendo 0 ou 5. Se o algarismo das unidades de n fosse 5, então este não poderia ser divisível por 2 assim como se o algarismo das unidades fosse $2, 4, 6$ ou 8 não seria múltiplo de 5. Portanto, só podemos ter que o algarismo das unidades é 0. Por outro lado, se 0 é o algarismo das unidades do inteiro n, então este é divisível por 2 e 5 simultaneamente e, assim, n é divisível por 10 (pois na fatoração primária de n estarão presentes os números primos 2 e 5).

2.1.2 Sistema Completo de Resíduos

Iremos a partir de agora, compreender os conjuntos conhecidos como Sistemas Completos de Resíduos bem como apresentar alguns dos seus resultados mais importantes.

Observação 2.1.32. Sejam $a, r, m \in \mathbb{Z}$, com $m > 1$ e r é o resto da divisão de a por m. Então $a \equiv r \ (mod\ m)$, com $0 \leqslant r < m$. De fato, como r é o resto da divisão de a por m, então temos que $a = mq + r$, para algum $q \in \mathbb{Z}$ além de $0 \leqslant r < m$. Reescrevendo a última expressão, tem-se $a - r = mq \Rightarrow m|(a - r) \Rightarrow a \equiv r \ (mod\ m)$, com $0 \leqslant r < m$. A recíproca também é válida.

Desta observação acima temos que a é congruente módulo m a um dos números inteiros do conjunto $\{0, 1, 2, ..., m - 1\}$. Sendo assim, dizer que a é congruente ao seu resto na divisão por m é, simplesmente, encontrar o número inteiro positivo r no conjunto $\{0, 1, 2, ..., m - 1\}$ que torne a expressão $a \equiv r \ (mod\ m)$ válida. Inclusive, repare que $r_i \not\equiv r_j \ (mod\ m)$ com $r_i, r_j \in \{0, 1, 2, ..., , m - 1\}$ para $i \neq j$, pois, caso contrário, teríamos que $r_j - r_i = mq$ para algum $q \in \mathbb{Z}$ onde $-m < r_j - r_i < m$, concluindo que $r_i = r_j$. Este é um exemplo de um sistema completo de resíduos módulo m, que definiremos a partir de agora.

Definição 2.1.33. Sejam m um número inteiro maior que 1. Chamamos de sistema completo de resíduos módulo m todo conjunto $\{r_1, r_2, ..., r_m\}$ se $r_i \not\equiv r_j \ (mod\ m)$ sempre que $i \neq j$.

Exemplo 2.1.34. Um sistema completo de resíduos módulo 7 é, por exemplo, o conjunto $\{21, 22, 23, 24, 25, 26, 27\}$ ou $\{7, 8, 9, 10, 11, 12, 13\}$. Entretanto, $\{3, 6, 7, 8, 9, 10, 11\}$ não é um sistema completo de resíduos módulo 7, pois $10 \equiv 3 \ (mod\ 7)$.

Proposição 2.1.35. Sejam o número inteiro $m > 1$ e $A = \{r_1, r_2, ..., r_m\}$ é um sistema completo de resíduos módulo m. Se a é um número inteiro, existe exatamente um r_i em A de forma que $a \equiv r_i \ (mod\ m)$.

Demonstração. Pela Observação 2.1.32, $a \equiv r \ (mod\ m)$, onde r é o resto da divisão de a por m. Assim, $r \in \{0, 1, 2, ..., m-1\}$. Por outro lado, $A = \{r_1, r_2, ..., r_m\}$ satisfaz a seguinte relação $r_i \not\equiv r_j \ (mod\ m)$ se $i \neq j$ e, portanto, realizando a divisão de $r_1, r_2, ..., r_m$ por m, obtemos m restos distintos dois a dois. A partir disso, para algum $r_i \in A$, tem-se que $r_i = mq_i + r$ com $0 \leqslant r < m$ e $q_i \in \mathbb{Z}$. Logo, $r \equiv r_i \ (mod\ m)$ e, pela transitividade, obtermos $a \equiv r_i \ (mod\ m)$. □

Proposição 2.1.36. Sejam $a, k, m \in \mathbb{Z}$, com $m > 1$ e $mdc(m, k) = 1$. Se $\{a_1, a_2, ..., a_m\}$ é um sistema completo de resíduos módulo m, então temos que $\{a+ka_1, a+ka_2, ..., a+ka_m\}$ também será um sistema completo de resíduos módulo m.

Demonstração. Para mostrarmos esse resultado, basta considerarmos dois elementos distintos do conjunto $\{a + ka_1, a + ka_2, ..., a + ka_m\}$ e provar que eles não são congruentes. De fato, se $a + ka_i \equiv a + ka_j \ (mod\ m)$ com $i \neq j$ e $i, j = 1, 2, ..., m$, temos que:

$$a + ka_i \equiv a + ka_j \ (mod\ m) \quad \Leftrightarrow \quad ka_i \equiv ka_j \ (mod\ m).$$

Como $mdc(m, k) = 1$, segue da Proposição 2.1.7 item (iv) que $a_i \equiv a_j \ (mod\ m)$. Contudo, isto é um absurdo porque $a_i \not\equiv a_j \ (mod\ m)$, pois o conjunto $\{a_1, , a_2, ..., a_m\}$ é um sistema completo de resíduos módulo m. Portanto, segue o resultado. □

2.2 Atividade Didática

Nesta seção, relataremos o processo de construção, planejamento e aplicação de uma atividade didática organizada e executada por nós. Esta prática pedagógica foi realizada no Ensino Básico - em duas escolas - e no Ensino Superior - em uma universidade - no município de Rio Grande.

A ideia surgiu após discutirmos amplamente sobre o assunto de divisibilidade e a enorme dificuldade que a grande maioria dos estudantes possuem em relação a essa temática. Refletindo sobre isto, acordamos da necessidade de concebermos uma prática pedagógica que despertasse o interesse dos discentes e que ao mesmo tempo fosse significativa para eles.

Nessa perspectiva, concordamos que trabalhar com situações-problemas, que "[...] são problemas de aplicação que retratam situações reais do dia-a-dia e que exigem o uso da Matemática para serem resolvidos."(DANTE, 2003), seria uma ótima maneira de entusiasmar os alunos, pois quando operamos com contextos reais viabilizamos que seja

enxergado pelos estudantes a aplicabilidade da matemática sobre aquele assunto tornando o aprendizado significativo. Além disso, situações-problemas proporcionam o desenvolvimento do raciocínio lógico porque estimulam o pensar em estratégias para resolver a problemática.

Assim sendo, buscamos "[...] estabelecer, por meio de investigações, critérios de divisibilidade [...]"(BRASIL, 2018) envolvendo o conceito de congruência sem apresentar a notação da relação, mas sim conceito de soma, subtração, multiplicação e divisão entre dois números inteiros. Inclusive, frisamos a importância de entendermos esse conceito com notações mais simples, pois quando for inserido a notação formal, no Ensino Superior, será mais fácil de assimilar e significar esse conteúdo.

Na sequência, descreveremos: a **metodologia**, em que abordaremos os locais de aplicação, o público alvo e os materiais necessários; os **objetivos**, no qual listamos as finalidades pretendidas com a proposta; a **aplicação**, onde relataremos propriamente dito a execução da tarefa; e **algumas considerações**, em que discorreremos sobre as características da atividade.

2.2.1 Metodologia

A atividade didática foi desenvolvida com uma turma de 6º ano do Ensino Fundamental na E. M. E. F. Bento Gonçalves, um 1º ano do Ensino Médio na E. E. E. M. Lília Neves e com uma turma de ingressantes no curso de Matemática Licenciatura do 1º semestre de 2020 na Universidade Federal do Rio Grande. Cabe destacarmos que a turma do 6º ano possuía 15 estudantes enquanto haviam 18 e 50 alunos no 1º ano do Ensino Médio e no Ensino Superior, respectivamente. Também mencionamos que no Ensino Fundamental foi aplicado no ano de 2019 e nas demais foi no ano de 2020 por questão de disponibilidade das instituições.

A proposta requiriu a formulação das problemáticas, que neste caso foram três situações-problemas envolvendo noções de tempo (contidas no Anexo A). Inclusive, foi impresso calendários dos anos de 2019 à 2024 porque foi um material suporte para auxiliar os alunos no desenvolvimento da prática pedagógica. Relatamos ainda a construção de quatro questionamentos de opinião para que os alunos nos retornassem sobre o que eles acharam da atividade (contidos no Anexo B, bem como os calendários).

2.2.2 Objetivos

Nossos objetivos com a prática foram: Perceber se os estudantes conseguem formular estratégias para solucionar os problemas propostos; verificar se os discentes identificam elementos cruciais para auxiliá-los na solução; analisar se os alunos compartilham e/ou comparam suas ideias com os demais; estabelecer conexões com o conteúdo de divisi-

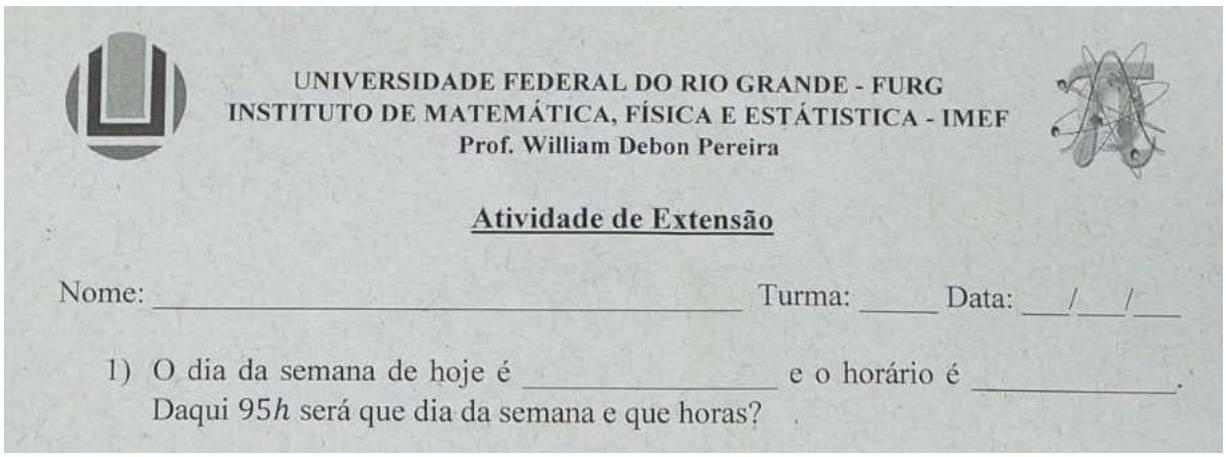
bilidade; e, conforme sugere a BNCC (BRASIL, 2018), aprimorar as habilidades com operações básicas; relembrar a Divisão Euclidiana e desenvolver o raciocínio lógico, investigativo e a capacidade de produzir argumentos lógicos através dos saberes matemáticos aprendidos.

2.2.3 Aplicação

Nos dias 12 de novembro de 2019, 30 de janeiro e 11 de março de 2020, fomos até as instituições de ensino E. M. E. F. Bento Gonçalves, E. E. E. M. Lília Neves e Universidade Federal do Rio Grande, respectivamente para desenvolver uma atividade didática com os estudantes das turmas de um 6º ano do Ensino Fundamental, um 1º ano do Ensino Médio e os ingressantes do curso de Matemática Licenciatura. Destacamos que a proposta foi a mesma para os três níveis de Ensino e teve como propósito verificar as compreensões deles a respeito do conceito de divisibilidade. Inclusive, o relato foi feito de maneira unificada enfatizando pontos de diferenças entre estes níveis de Ensino.

Ao chegarmos à sala de aula, nos apresentamos para os estudantes como acadêmicos do curso de Matemática Licenciatura da Universidade Federal do Rio Grande. Além disso, explicamos que iríamos aplicar uma atividade com o intuito de analisar a forma com que eles relacionavam os problemas diante dos princípios de divisibilidade intrínsecos à proposta. Convém acentuar que fomos extremamente bem recebidos pelos estudantes e que todos participaram da aplicação da atividade.

Em seguida, solicitamos que os discentes formassem grupos de no máximo 4 integrantes para iniciarmos a prática pedagógica. Logo após eles formarem seus grupos, entregamos o primeiro problema para cada um dos estudantes e pedimos para que colocassem algumas informações nas lacunas que haviam no problema, já que o mesmo era versátil, conforme nos mostra a Figura 1.


UNIVERSIDADE FEDERAL DO RIO GRANDE - FURG
INSTITUTO DE MATEMÁTICA, FÍSICA E ESTÁTISTICA - IMEF
Prof. William Debon Pereira

Atividade de Extensão

Nome: _____ Turma: _____ Data: ___/___/___

1) O dia da semana de hoje é _____ e o horário é _____.
Daqui $95h$ será que dia da semana e que horas?

Figura 1 – Primeiro problema.

A tarefa inicial se resumia em prever o dia da semana e o horário que seria após

passadas 95 horas em relação ao dia da semana e horário que foi preenchido nas lacunas pelos estudantes. A princípio, foi um estudo introdutório para que eles pudessem ter ideias para as próximas situações, bem como relembrarem operações básicas de matemática como soma, subtração, multiplicação e/ou divisão.

Posteriormente, esclarecemos que esse primeiro problema seria solucionado em conjunto para que eles compreendessem melhor a proposta. Entretanto, antes de iniciarmos a resolução da questão, perguntamos se algum deles tinha alguma ideia de como proceder para encontrar a solução, pois deste modo estávamos estimulando que eles pensassem e discutissem sobre meios de chegar a resposta sem depender do professor.

Na turma do 6º ano, após alguns segundos de silêncio, o único a nos responder foi uma menina que concluiu que se um dia possuía 24 horas, era possível somar de 24 em 24 horas até alcançar às 95 horas do problema. Contudo, ela não chegou a completar seu raciocínio, posto que chegaríamos à 96 horas e, ao ser questionada sobre o que fazer com o excedente, ela não soube responder. Solicitamos que ela desenvolvesse sua lógica e pensasse um pouco mais sobre aquele pequeno detalhe, porém não obteve sucesso.

No Ensino Médio, alguns estudantes já sabiam a resposta porque seguiram seu raciocínio mentalmente. Quando perguntamos o modo como eles resolveram, rapidamente mencionaram que foram somando de 24 em 24 horas até encontrar 96 horas (4 dias) e assim retiraram 1 hora das 96 encontrada, donde perceberam que se passariam então 3 dias mais 23 horas.

Por fim, os alunos do curso de Matemática Licenciatura surpreenderam, pois vários estudantes propuseram diversas ideias/estratégias para solucionar o problema inicial. Uma delas foi a mesma dita pelos discentes do Ensino Básico enquanto outras envolviam equações do primeiro grau e tentativa e erro.

Nesse momento, depois das ideias de cada um dos níveis de Ensino, requisitamos que eles resolvessem a questão por meio do pensamento que haviam mencionado. Embora os estudantes do Ensino Básico não tenham seguido suas próprias estratégias e sim nossa resolução (exceto por um estudante do Médio), o Ensino Superior prosseguiu satisfatoriamente com seus planejamentos para a solução. Não sabemos exatamente o porquê do 6º e do 1º ano desistirem das suas próprias ideias, mas conjecturamos que possa ter havido insegurança e medo de errar, como também não ter maturidade com esse tipo de abordagem devido a forma como o professor possivelmente desenvolveu o conteúdo.

É comum que os estudantes priorizem a resposta do docente ao invés de seus próprios métodos para compreender a questão. Isto se deve ao fato da insegurança e falta de convicção em seus pensamentos para com a problemática porque pensam que o professor possui todo o conhecimento e que aquele modo é o único jeito de chegar a resposta, o que nem sempre é verdade. Outro ponto pode ser o modo como o professor

desenvolveu os conteúdos, pois onde prioriza-se o roteiro e não a liberdade de raciocinar sobre os problemas atinge diretamente na aprendizagem das crianças e jovens.

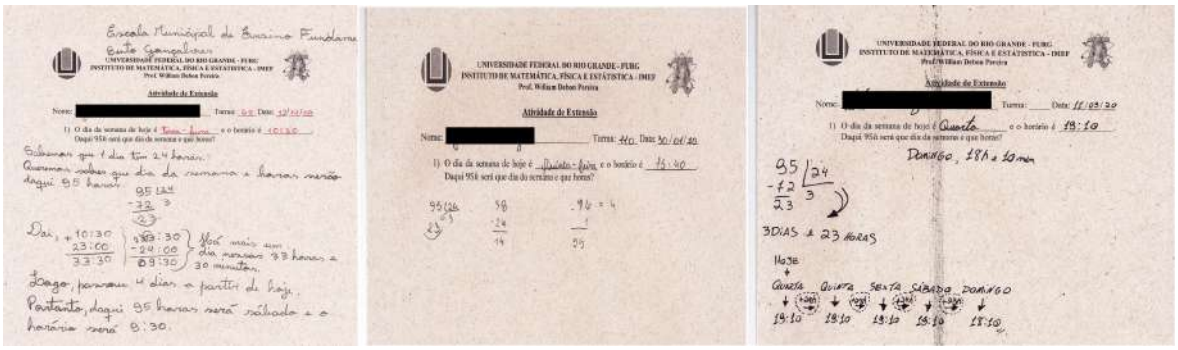


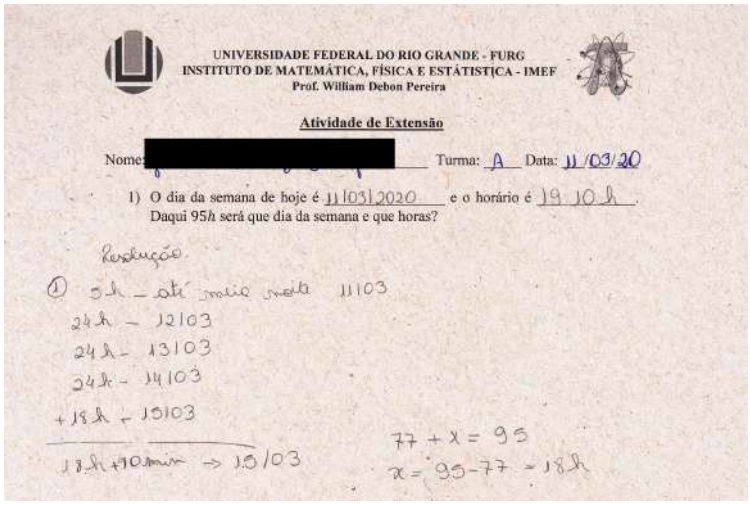
Figura 2 – Resolução do 1º problema por um estudante do Ensino Fundamental, Médio e Superior da esquerda para a direita.

Observamos que ao analisar o modo como foi efetuada a tarefa inicial (Figura 2), pode-se perceber que o Ensino Fundamental literalmente transcreveu as informações tal qual colocamos no quadro diferente do Ensino Médio, que apenas realizaram os cálculos e suprimiram todo texto explicativo. Em contrapartida, o Ensino Superior mostrou-se ainda mais maduro em relação a isto e procederam de forma independente justificando cada passo executado. Isto nos evidência que conforme avançam de nível escolar, os discentes ganham autonomia de saber o que é relevante para eles apesar de que tais verbetes (texto explicativo) auxiliam a relembrar os métodos feitos.

A imagem central, na Figura 2, merece minuciosamente um pouco mais de relevância porque é a resolução do único aluno do Ensino Médio que aplicou sua ideia para concluir o problema (cálculo da subtração de 96 por 1). Percebe-se que ele abstraiu todo o contexto em apenas uma operação, isto é, ele descreve o entendimento que possui referente à $96 \equiv 0 \ (mod\ 24)$ e $95 \equiv 23 \ (mod\ 24)$ (claro que não nesta notação) quando escreve $96 = 4$ (96 horas equivale à 4 dias) e conclui, em fala, que se passariam na verdade 3 dias mais 23 horas. Esta forma de raciocinar revela os conhecimentos sobre divisibilidade que o discente possui mesmo não tendo feito uso do cálculo de divisão.

Outra resposta digna de destaque é a do licenciando em Matemática (na Figura 2), pois além de ter relação direta com as mesmas congruências mencionadas anteriormente, é usado um raciocínio distinto do utilizado pelo estudante do Ensino Médio já que nesta é executada a divisão. Da mesma forma, acrescentamos a solução de outro aluno do Ensino Superior, como vemos na Figura 3 (abaixo), no qual é desenvolvido um método similar ao do primeiro licenciando exceto pelo cálculo de divisão que aqui é subentendido pelo agrupamento que fora realizado.

Repare que essas três formas (a do Ensino Médio e as duas do Ensino Superior) de concluir a proposta inicial nos mostram que não há um único caminho para se seguir


UNIVERSIDADE FEDERAL DO RIO GRANDE - FURG
INSTITUTO DE MATEMÁTICA, FÍSICA E ESTATÍSTICA - IMEF
Prof. William Debon Pereira

Atividade de Extensão

Nome: [redacted] Turma: A Data: 11/03/20

1) O dia da semana de hoje é 11/03/2020 e o horário é 19:10 h.
Daqui 95h será que dia da semana e que horas?

Resolução.

① 5h – até meia noite 11/03
24h – 12/03
24h – 13/03
24h – 14/03
+18h – 15/03
18h+10min → 15/03

77 + x = 95
x = 95 – 77 = 18h

Figura 3 – Solução do 1º problema de um aluno do Ensino Superior

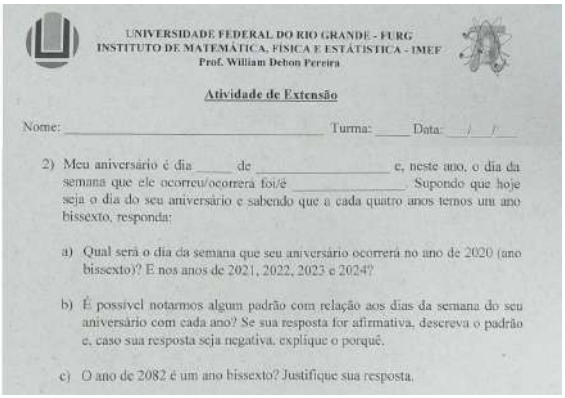
e que todos convergem para o conceito de divisibilidade. É interessante pontuar que, por mais que eles não entendam as congruências ali inseridas, eles possuem os conhecimentos sobre divisibilidade seja por meio do raciocínio mental, operação de divisão ou realizando agrupamento. São através desses mecanismos que demonstram o quanto eles sabem de divisibilidade, mas que acabam procurando subterfúgios para não recaírem na utilização das contas de dividir. Acredita-se que isto ocorre por causa da enorme dificuldade em realizar tal operação, pois deve haver uma carência na explicação desse cálculo na base.

Enquanto resolvíamos a primeira questão, sempre fomos questionando-os sobre o que fazer em seguida e também significando cada um dos resultados obtidos para que ajudasse no pensamento matemático deles. A partir disso, notamos que eles tinham conhecimentos pontuais e que iriam auxiliá-los na solução do problema como, por exemplo, eles sabiam que um dia possuía 24 horas (sem essa informação, não seria possível resolver o problema).

Depois disso, recolhemos o primeiro problema e entregamos o segundo juntamente com os calendários de 2019 à 2024, além de pedirmos para que eles preenchessem as lacunas da tarefa com as informações cabíveis. O segundo problema consistia numa situação envolvendo o dia de aniversário de cada estudante e haviam três itens a serem respondidos, conforme a Figura 4.

O primeiro item consistia em fazer as previsões do dia da semana que ocorreria novamente o aniversário deles nos anos de 2020 à 2024, enquanto o segundo tratava da relação entre os dias da semana com o dia da semana dos seus aniversários a cada ano. Por fim, o terceiro tópico abordava uma questão para verificar se determinado ano era ou não bissexto, explicando seu raciocínio.

Nessa segunda parte da proposta, explicamos que iríamos apenas acompanhá-los sanando as possíveis dúvidas uma vez que não queríamos que eles ficassem dependentes de



UNIVERSIDADE FEDERAL DO RIO GRANDE - FURG
INSTITUTO DE MATEMÁTICA, FÍSICA E ESTATÍSTICA - IMEF
Prof. William Debon Pereira

Atividade de Extensão

Nome: _____ Turma: ____ Data: __/__/__

2) Meu aniversário é dia ____ de _____ e, neste ano, o dia da semana que ele ocorreu/ocorrerá foi/é _____. Supondo que hoje seja o dia do seu aniversário e sabendo que a cada quatro anos temos um ano bissexto, responda:

a) Qual será o dia da semana que seu aniversário ocorrerá no ano de 2020 (ano bissexto)? E nos anos de 2021, 2022, 2023 e 2024?

b) É possível notarmos algum padrão com relação aos dias da semana do seu aniversário com cada ano? Se sua resposta for afirmativa, descreva o padrão e, caso sua resposta seja negativa, explique o porquê.

c) O ano de 2082 é um ano bissexto? Justifique sua resposta.

Figura 4 – Segundo problema.

nós para solucionar o problema. Inclusive, ressaltamos a importância de escreverem seus pensamentos para organizarem as ideias/estratégias para o desenvolvimento da segunda etapa.

Em todas as turmas, ao caminharmos pela sala de aula alguns minutos após termos entregado a situação-problema, observamos que vários alunos estavam parados sem um plano de ação para realizar a atividade ou não sabiam como proceder. Sendo assim, procuramos auxiliá-los, inicialmente, perguntando coisas como o número de dias que possuía um ano e as semanas para ver se surgia alguma noção de como se resolvia o problema. Embora eles soubessem responder nossos questionamentos, eles não conseguiram enxergar como que aquelas informações os ajudariam a solucionar à questão.

A partir disso, tivemos que auxiliá-los no primeiro item utilizando nossos dados (nossa data de nascimento) e fazendo a previsão apenas para o ano de 2020, pois eles deveriam realizar os demais. Ressaltamos que ao longo da nossa explanação sobre o exercício, procuramos instigá-los a terem seus próprios métodos por meio de indagações como: O que obtemos se realizarmos uma divisão entre o número de dias do ano pelo número de dias que há em uma semana? Em que isso pode nos ajudar? O que significa o resto dessa divisão?

Infelizmente, os estudantes do 6º ano continuaram, num primeiro momento, sem perceber a conexão entre as informações até nós reexplicarmos e fazermos o exercício para o ano de 2021. Por outro lado, os alunos do Ensino Médio assim como os do Ensino Superior conseguiram compreender a nossa resolução de forma mais rápida, além de realizarem com maestria o item inicial. Desta maneira, todos conseguiram finalizar a tarefa através da nossa solução, ou seja, adaptaram nossa resposta para encaixar no contexto deles.

É notório que, na Figura 5 (acima), todos executaram com perfeição o algoritmo da divisão mostrando que eles tem noções sobre $365 \equiv 1 \ (mod\ 7)$ e $366 \equiv 2 \ (mod\ 7)$, ou melhor, perceberam e associaram que tais números não são divisíveis por 7. A maior

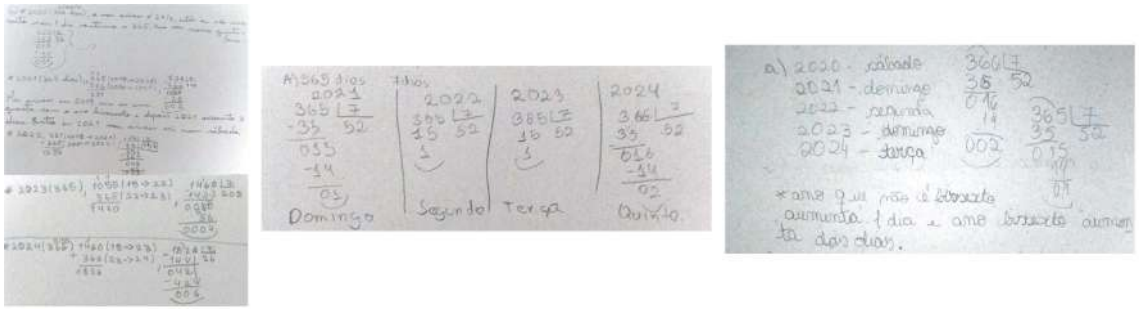


Figura 5 – Resolução do item (a) do segundo problema por um aluno do Ensino Fundamental, Médio e Superior da esquerda para a direita.

dificuldade deles foi começar, pois não conseguiram estabelecer um plano para por em prática. Pensamos que tal adversidade possa ter ocorrido por causa de não haver esse costume de pensar para depois executar e sim já sair aplicando fórmulas para achar a solução, posto que algumas escolas são ensinados desta forma, apenas aplicação de algoritmos.

Na maioria das escolas, são alguns professores que criam atividades didáticas para que os alunos sejam desafiados a solucionar através do pensar, pois a maioria acaba se acomodando. Contudo, faz-se necessário incentivar o raciocínio para que os discentes saibam lidar com outras situações e signifiquem os conteúdos aprendidos no seu cotidiano.

Em relação ao segundo item, alguns já tinham o conhecimento do padrão que estava ocorrendo, isto é, sabiam que quando o ano era convencional o dia da semana que aconteceria seu próximo aniversário era 1 dia após o dia da semana do ano anterior e quando era bissexto eram 2 dias. Salientamos que não houve problemas em nenhum dos níveis de Ensino em responder a pergunta embora muitos não tenham justificado o porquê de tal ocorrência de forma significativa.

O último item envolvia a questão de divisibilidade por 4 e alguns estudantes conseguiram responder utilizando esta ideia enquanto outros utilizaram da informação que 2020 era bissexto donde foram somando de 4 em 4 anos até alcançar o ano proposto para finalizar a atividade. Assim como o anterior, não houve nenhuma dificuldade ou dúvida por parte dos discentes. Na Figura 6 (abaixo), pode-se ver a resolução de um aluno do Ensino Fundamental, Médio e Superior.

A resposta do estudante do Ensino Fundamental, na Figura 6, ganha destaque porque, além de concluir o item (c) com a menção do critério de divisibilidade por 4, mostra a sua criatividade em realizar associações históricas para encaixar-se no contexto de sua lógica. Embora, toda sua associação sobre o ano 4 d.C. ter iniciado os anos bissextos não estar correta, pois é sabido que este teve seu inicio em 48 a.C com a implementação do Calendário Juliano.

Atente também que a imagem da direita, na Figura 6, merece um destaque maior,

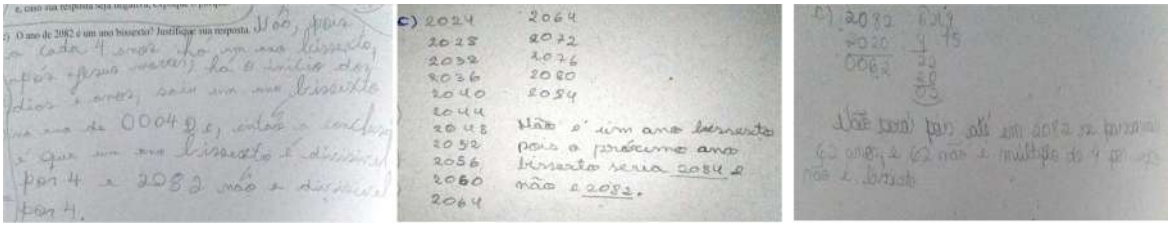


Figura 6 – Resolução do item (c) do segundo problema por um aluno do Ensino Fundamental, Médio e Superior da esquerda para a direita.

pois o estudante percebeu que $2082 \not\equiv 2020 \ (mod\ 4)$ por meio das operações básicas que fez ($2082-2020 = 0062$ e $62 = 4\cdot 15+2$) sem entrar, novamente, em detalhes de congruência. Inclusive, observou que anos bissextos são múltiplos de 4 quando este escreve "Não será, pois até 2082 se passarão 62 anos, e 62 não é múltiplo de 4 por isto não é bissexto.". Por todos esses aspectos listados na sua resposta, entende-se a sua compreensão sobre divisibilidade através de seu raciocínio e percepção de saber encontrar a quantidade de anos para se chegar a 2082 por meio de 2020 e, ainda, de realizar a divisão por 4, já que anos bissextos tem sua ocorrência de 4 em 4 anos.

A terceira situação-problema (Anexo A) não foi possível de ser executada porque não havia tempo suficiente para tal. Então, para finalizar solicitamos que os discentes respondessem as seguintes quatro questões dissertativas sobre a atividade (sendo a última questão aplicada apenas para os ingressantes no curso de Matemática Licenciatura):

i) O que você achou da atividade? Justifique.

ii) O que você compreende a partir das discussões envolvidas durante a atividade? Explique.

iii) Alguma sugestão para aperfeiçoar a atividade?

iv) Que conteúdos matemáticos estão por trás da resolução dessa atividade?

Os alunos do 6º ano do Ensino Fundamental foram os únicos estudantes que não responderam os questionamentos, pois já havia tocado o sinal para eles irem embora. Contudo, solicitamos para que eles respondessem as perguntas em casa e entregassem para a docente deles na próxima aula de matemática para que então ela pudesse nos entregar, mas a professora regente disse que eles não fizeram.

Referente ao primeiro questionamento, percebemos que a proposta pedagógica foi bem recebida pelos alunos do Ensino Médio e Ensino Superior porque eles, na grande maioria, responderam que acharam a atividade interessante e atrativa, pois envolvia bastante o raciocínio e lógica para a sua execução. Ademais, disseram que esse tipo de atividade os estimula a refletirem sobre coisas que nunca haviam parado para pensar antes, como o porquê de tais fenômenos ocorrerem. Isto pode ser observado na Figura 7 (abaixo).

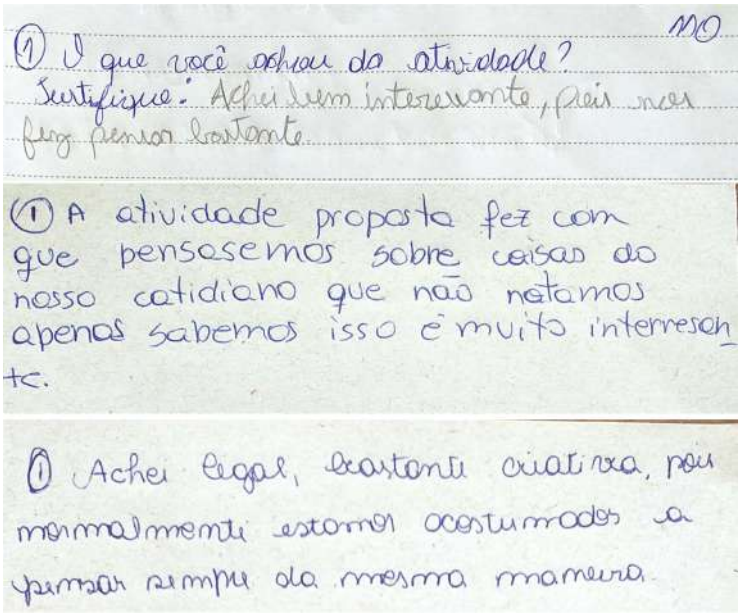


Figura 7 – Resposta da primeira questão de um aluno do Ensino Médio e de dois do Ensino Superior de cima para baixo.

Isso evidência que propostas pedagógicas envolvidas com o fazer pensar tornam-se mais cativantes para alunos, pois o ensino deixa de ser mecanizado para algo aplicado em suas vidas. E ainda, possibilita associações cognitivas entre o que está sendo aprendido com suas vivências cotidianas propiciando um melhor reconhecimento daqueles conceitos.

A respeito da segunda pergunta, acabou ocorrendo um equívoco no Ensino Médio porque, por um descuido, acabamos escrevendo na lousa a seguinte pergunta: "Achou válido atividades como as desenvolvidas em aula? Por quê?". Embora não consigamos realizar uma comparação entre o Ensino Médio e o Ensino Superior por conta desta falha, tal questionamento não deixa de ser relevante para o trabalho uma vez que nos outorga enxergar se a proposta é pertinente.

Desta forma, o Ensino Médio achou válido, em sua totalidade, aplicar atividades como esta porque, além de tornar a aula mais atrativa e dinâmica, faz desenvolver o raciocínio lógico - já mencionado na primeira pergunta. Inclusive, ressaltaram que com esta tarefa eles aprimoram seus conhecimentos, isto é, aprendem mais sobre outras coisas. Isto pode ser observado na Figura 8 (abaixo) nas imagens da direita.

No Ensino Superior, verificamos que eles compreenderam as diferentes formas de resolver os problemas como também a reflexão como instrumento para justificar suas soluções. É importante oportunizar que os alunos conheçam outros métodos de resolução e saibam explicar com clareza a lógica imersa em suas estratégias porque isto fará com que estabeleçam associações entre os seus cálculos e pensamentos para que eles signifiquem. Isto pode ser observado na Figura 8 (abaixo) nas imagens da esquerda.

Ainda sobre a Figura 8, realçamos a imagem da direita-baixo a respeito da ar-

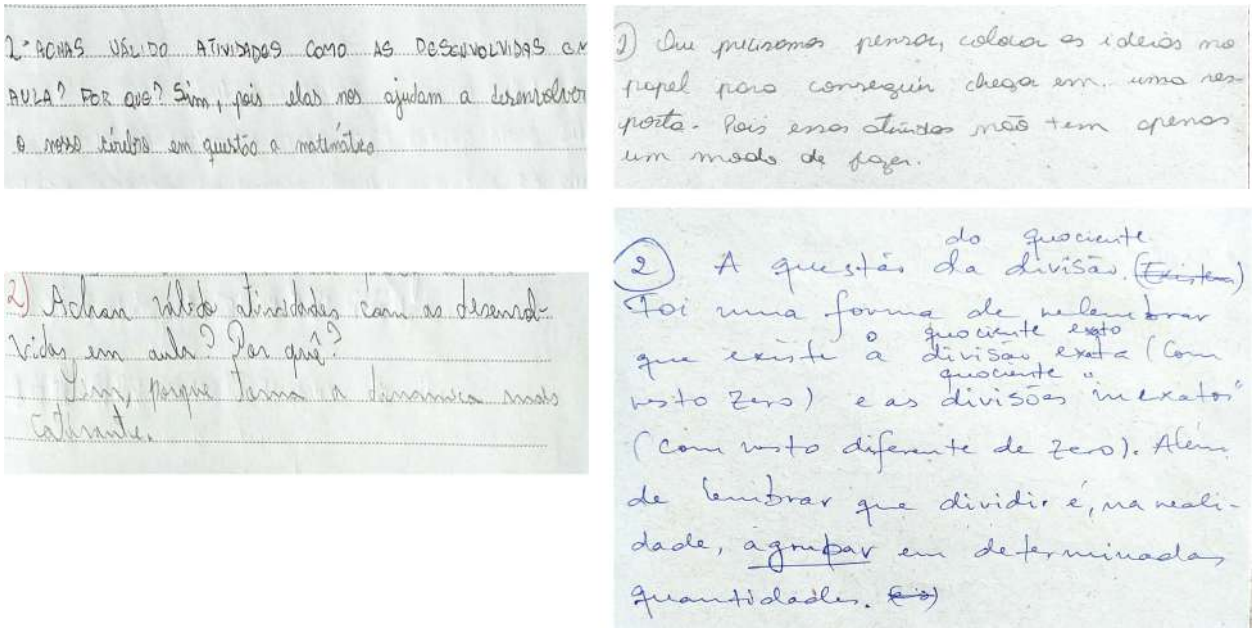


Figura 8 – Resposta da segunda questão de dois alunos do Ensino Médio (esquerda) e do Ensino Superior (direita).

gumentação, pois retrata diretamente ao conteúdo de divisibilidade que a tarefa exigia. Nesta resposta, fica claro que o objetivo sobre estabelecer conexões com a divisibilidade dos números inteiros foi cumprido/atingido quando este escreve que compreende "A questão da divisão/do quociente. Foi uma forma de relembrar que existe a divisão exata/o quociente exato (com resto zero) e as divisões/quociente "inexatos" (com restos diferente de zero). Além de lembrar que dividir é, na realidade, agrupar em determinadas quantidades.".

No questionamento sobre sugestões para melhorar a atividade (terceira pergunta), a maioria dos discentes ficou satisfeita com a maneira que se encontra a proposta. Já outros sugeriram que o aplicador explique as demais formas de chegar aos resultados e trabalhe com outras temáticas para chamar ainda mais a atenção dos alunos.

Por fim, a quarta indagação relativa aos conteúdos matemáticos que são identificados na tarefa, os ingressantes do curso de Matemática Licenciatura foram os únicos a responderem porque esta questão foi elaborada justamente para eles visando um olhar deles como docentes. Suas respostas foram desde raciocínio lógico e operações básica a identificação de padrões.

Todas essas respostas tornam significante a prática porque mostra seu potencial de ensino, posto que revela que o aprender matemática não é apenas realizar cálculos e sim interpretá-los de forma expressiva e construtiva através do raciocínio lógico, conforme sugere a BNCC (BRASIL, 2018). Cabe, então, ao professor desenvolver e/ou proporcionar estes meios para difundir o conhecimento através de atividades que instiguem os alunos e torne-os seres investigativos, pois eles aprendem quando estão em contato com a práxis.

2.2.4 Algumas considerações

A forma como foi planejada e desenvolvida a atividade concede ao professor saber se as turmas conseguiram entender o conceito de divisibilidade imbricado na proposta. Além disso, é propiciado a interação entre os discentes para poderem realizar trocas de ideias sobre como proceder com os problemas uma vez que é oportunizado a formação de grupos quanto o diálogo.

Propostas didáticas, como a relatada, são interessantes porque trabalham a Matemática de outra perspectiva - aquela do pensar, planejar e executar o plano - e isto permite associar os conhecimentos intrínsecos à atividade. Ademais, despertam curiosidade e fascínio nos discentes em sua realização porque viabiliza um olhar mais crítico sobre a forma como é ensinado nas escolas.

Realizando um comparativo entre as turmas, pôde-se notar que no Ensino Superior os alunos estavam mais motivados em participar da proposta pedagógica enquanto que no Ensino Básico não mostraram-se tão entusiasmados. Acreditamos que tal desmotivação tenha se dado por conta da maturidade, a falta de interesse deles, déficit nos conteúdos básicos que a tarefa exigia ou até mesmo a ausência de atividades desse gênero. Todos esses apontamentos influenciam no progresso da tarefa porque revela que o aluno não está bem ou precisa de um reforço para reaver a carência dos conteúdos necessários.

Sabemos que em algumas escolas, a maioria dos professores não desenvolvem práticas que requerem que os alunos pensem, pois vemos que os exercícios são todos mecanizados e não exigem muito além de aplicação de algum algoritmo. Claro que, compreender o emprego da fórmula é importante, mas faz-se necessário estimular o raciocínio porque acaba formando indivíduos capacitados para interpretar situações adversas em seu dia a dia.

Assim sendo, percebemos que estimular o raciocínio lógico por meio de investigações e o pensar em argumentos que validem suas ideias através dos conhecimentos matemáticos é uma forma de potencializar o Ensino de Matemática. Salientamos que isto não faltou na proposta, já que a mesma utilizou desses tópicos para atingir seus objetivos de forma satisfatória.

No que tangencia o conteúdo de divisibilidade, percebemos que todos eles possuem conhecimentos a cerca desta temática, porém a maior dificuldade que tiveram foi referente a como começar a resolver porque, como mencionado anteriormente, pode ser que algumas escolas não fomentem o suficiente práticas desse gênero. Embora essa adversidade tenha surgido, conseguimos esclarecer e encorajar-los a terem suas próprias ideias diante de diversos questionamentos.

Em virtude de todos esses fatos mencionados, podemos concluir que a atividade possui potencial para a aplicação desde que o professor esteja auxiliando a turma. Inclu-

sive, é preciso que os estudantes estejam motivados em participar das tarefas porque isso refletirá no desempenho deles durante a execução da proposta.

3 Congruências Lineares

O presente capítulo destina-se introduzir a noção de congruências lineares, que são equações envolvendo o conceito de congruência. Este princípio matemático é muito mais interessante do que trabalharmos apenas com congruências entre dois números inteiros porque, a partir dele, podemos modelar diversos problemas aritméticos (um exemplo de problema poderá ser visto na primeira seção deste capítulo).

Também abordaremos alguns teoremas de suma importância para a Teoria dos Números e que, por sua vez, possuem conexões com as referidas congruências lineares. Dentre eles, podemos citar o Teorema de Euler, que evidencia uma premissa interessante relacionando uma potência de um número inteiro com o seu resto na divisão por um outro inteiro positivo coprimo a este; e o Teorema de Wilson, que nos fornece um argumento matemático curioso a cerca dos misteriosos números primos.

Para uma melhor compreensão desses fundamentos, fragmentamos o capítulo em duas seções. A primeira - Equações de Congruências Lineares - trará a definição de congruências lineares assim como resultados que nos permitem saber quando é admitido solução e métodos de resolução destes objetos matemáticos. A segunda, Alguns Teoremas Clássicos da Aritmética, como o nome já sugere, apresentará alguns dos teoremas mais relevantes para o desenvolvimento da Aritmética. Ressaltamos ainda que para realizarmos essas discussões sobre as congruências lineares, utilizamos as seguintes obras literárias: (DOMINGUES, 1991), (GOMES; SILVA, 2018), (HEFEZ, 2009) e (SANTOS, 2020).

3.1 Equações de Congruências Lineares

Consideremos o seguinte problema: O dobro de um número inteiro, que está entre 8 e 28 (excluindo-se ambos), deixa resto 3 na divisão por 5. Que número é este?

Para resolvermos este problema, poderíamos testar um por um os números pares de 9 até 27 e ir verificando quem deixa resto 3 na divisão por 5; concluindo assim que o número procurado será a metade deste número encontrado. Contudo, solucionar problemas desse modo nem sempre será fácil, pois o intervalo poderia ser maior e/ou ter mais de uma resposta para o problema. Diante disso, reescrevendo a questão em linguagem matemática envolvendo o conceito de congruência, obtém-se a equação $2x \equiv 3 \ (mod \ 5)$ e, a esta, nomeamos de congruência linear ou equação de congruência linear.

São equações desse tipo que serão o tema central desta seção. A partir delas, investigaremos e compreenderemos quando haverá solução e até mesmo métodos de solucioná-las. Enquanto não possuímos muitas informações sobre esse conceito, iremos deixar para

resolver este problema ao longo da subseção a seguir.

3.1.1 Equações de Congruências Lineares

Definição 3.1.1. Toda equação da forma $ax \equiv b \ (mod\ m)$, onde a, b e m são números inteiros tais que $a \neq 0$ e $m > 1$, são chamadas de congruências lineares ou equações de congruências lineares.

Exemplo 3.1.2. A equação $2x \equiv 4 \ (mod\ 9)$ é uma equação de congruência linear assim como $2x \equiv 3 \ (mod\ 2)$. Contudo, as expressões $x^2 \equiv 1 \ (mod\ 2)$ e $6xy \equiv 0 \ (mod\ 12)$ não são equações de congruências lineares.

Vamos mostrar agora o primeiro resultado sobre essa temática. Este, no que lhe diz respeito, é crucial para começarmos a conhecer os mecanismos para solucionar tais congruências lineares.

Proposição 3.1.3. Sejam $a, b, m \in \mathbb{Z}$, com $m > 1$. A congruência linear $ax \equiv b \ (mod\ m)$ possui solução se, e somente se, $mdc(a, m) \Big| b$.

Demonstração. Consideremos x_o uma solução da congruência linear $ax \equiv b \ (mod\ m)$, ou seja, $ax_o \equiv b \ (mod\ m)$. Diante disso, sabemos que $m|(ax_o - b)$, isto é, existe um número inteiro y_o tal que $ax_o - b = my_o$. Organizando esta igualdade, obtemos $ax_o - my_o = b$. Note que esta última sentença matemática é uma equação diofantina linear em que sua solução é o par ordenado (x_o, y_o). A partir disto, pelo Teorema 1.3.3, o $mdc(a, m) \Big| b$ uma vez que a equação diofantina admite solução. Por outro lado, se $mdc(a, m) \Big| b$, então, pelo Teorema 1.3.3, a equação diofantina linear $ax + my = b$ possui solução, digamos que seja o par ordenado (x_o, y_o). Neste sentido, $ax_o + my_o = b$ e, reordenando esta igualdade, temos que $ax_o - b = m(-y_o) \Leftrightarrow m|(ax_o - b) \Leftrightarrow ax_o \equiv b \ (mod\ m)$. □

Comentário 3.1.4. Esta Proposição 3.1.3 não nos diz como encontrar a solução de uma determinada congruência linear, mas evidencia, em sua demonstração, uma relação entre as congruências lineares e as equações diofantinas lineares. Repare nas seguintes equivalências:

$$ax \equiv b \ (mod\ m) \Leftrightarrow m|(ax - b) \Leftrightarrow \exists y \in \mathbb{Z}, ax - b = my \Leftrightarrow ax - my = b.$$

Portanto, podemos afirmar que encontrar a solução de uma congruência linear é solucionar a equação diofantina linear a ela associada.

Diante disso, podemos retornar ao problema inicial desta seção para resolvê-lo. Retomamos a equação de congruência linear $2x \equiv 3 \ (mod\ 5)$, que possui solução uma vez que $mdc(2, 5) = 1$ e $1|3$, pela Proposição 3.1.3.

Note que $2x \equiv 3\ (mod\ 5)$ é equivalente à equação diofantina linear $2x - 5y = 3$, para $y \in \mathbb{Z}$. Ao realizar o método discutido no Capítulo 1 Seção 1.3, descobre-se que a solução de $2x - 5y = 3$ é o par ordenado $(5t - 6, 2t - 3)$, para algum $t \in \mathbb{Z}$. Além disso, sabemos que $8 < 2x < 28$, ou seja, $4 < x < 14$. Substituindo x por $5t - 6$ nesta última desigualdade, ficamos com $4 < 5t - 6 < 14$. Resolvendo essa sentença matemática, obtemos que $2 < t < 4$. Por fim, note que o único valor de t que satisfaz a questão é $t = 3$, onde obtém-se $x = 9$. Portanto, o número inteiro cujo dobro, que está no intervalo $(8, 28)$, deixa resto 3 na divisão por 5 é o número 9.

Observação 3.1.5. Atente que se $x' \equiv x_o\ (mod\ m)$, com $x', x_o \in \mathbb{Z}$, e x_o é solução da congruência $ax \equiv b\ (mod\ m)$, então x' também será solução da referida congruência linear. De fato, basta multiplicar por a a congruência $x' \equiv x_o\ (mod\ m)$ fazendo com que tenhamos $ax' \equiv ax_o \equiv b\ (mod\ m)$.

Teorema 3.1.6. Sejam $a, b, m \in \mathbb{Z}$, com $m > 1$ e $mdc(a, m)\big|b$. Se x_o é solução da congruência $ax \equiv b\ (mod\ m)$, então o conjunto

$$S = \left\{x_o,\ x_o + \frac{m}{d},\ x_o + 2\frac{m}{d},\ ...,\ x_o + (d-1)\frac{m}{d}\right\},$$

onde $d = mdc(a, m)$, forma um sistema completo de soluções incongruentes duas a duas da congruência.

Demonstração. Repare que toda solução x' da congruência $ax \equiv b\ (mod\ m)$ satisfaz $ax' \equiv ax_o\ (mod\ m)$, conforme visto na Observação 3.1.5. Sendo assim, aplicando o item (iv) da Proposição 2.1.7, obtemos que $x' \equiv x_o\ \left(mod\ \frac{m}{d}\right)$ e, com isto, existe o número inteiro k tal que

$$x' - x_o = k\frac{m}{d}.$$

Realizando a Divisão Euclidiana de k por d, temos a existência de únicos q, r números inteiros tais que $k = dq + r$ com $0 \leqslant r < d$ e, portanto,

$$x' - x_o = mq + r\frac{m}{d} \Leftrightarrow x' - \left(x_o + r\frac{m}{d}\right) = mq,$$

ou seja, $x' \equiv x_o + r\frac{m}{d}\ (mod\ m)$ para $r \in \{0, 1, 2, ..., d-1\}$. Por outro lado, os números $x_o + r\frac{m}{d}$, com $0 \leqslant r < d$, são soluções da congruência $ax \equiv b\ (mod\ m)$, pois

$$a\left(x_o + r\frac{m}{d}\right) = ax_o + r\frac{a}{d}m \equiv ax_o \equiv b\ (mod\ m).$$

Resta-nos provar que esses números são dois a dois incongruentes módulo m. Com efeito, para $i, j \in \{0, 1, 2, ..., d-1\}$,

$$x_o + i\frac{m}{d} \equiv x_o + j\frac{m}{d}\ (mod\ m) \Leftrightarrow i\frac{m}{d} \equiv j\frac{m}{d}\ (mod\ m).$$

Como $0 \leqslant i, j < d$, então $0 \leqslant i\frac{m}{d}, j\frac{m}{d} < m$. Além disso, temos que

$$i\frac{m}{d} - j\frac{m}{d} = mk,\ k \in \mathbb{Z},$$

donde segue que $i\frac{m}{d} = j\frac{m}{d}$ (pois o único múltiplo de m no intervalo $-m < i\frac{m}{d} - j\frac{m}{d} < m$ é o 0) e, por conseguinte, $i = j$. □

Exemplo 3.1.7. Seja a congruência $3x \equiv 3\ (mod\ 6)$. Note que $x = 1$ é solução desta congruência. Para encontrarmos os outros dois resultados incongruentes à 1, já que $mdc(3, 6) = 3$, basta fazermos:

$$1 + \frac{6}{mdc(3,6)} = 1 + \frac{6}{3} = 3 \ \text{ e } \ 1 + 2 \cdot \frac{6}{mdc(3,6)} = 1 + 2 \cdot \frac{6}{3} = 5.$$

Logo, obtemos as soluções 1, 3 e 5 da congruência $3x \equiv 3\ (mod\ 6)$ que são incongruentes entre si.

Corolário 3.1.8. Seja $mdc(a, m) = 1$, então a congruência $ax \equiv b\ (mod\ m)$ possui uma única solução.

Demonstração. Com efeito, a congruência linear $ax \equiv b\ (mod\ m)$ possui solução uma vez que $mdc(a, m) = 1$ e $1|b$. Digamos que x_o seja a solução desta congruência, logo $ax_o \equiv b\ (mod\ m)$. Se houver outras soluções da congruência, estes serão:

$$x_o,\ x_o + m,\ x_o + 2m, ...,\ x_o + nm, ...$$

Note que essas soluções são congruentes duas à duas, pois, dados k_1 e k_2 números inteiros quaisquer, temos:

$$\begin{aligned} x_o + k_1m \equiv x_o + k_2m\ (mod\ m) &\Leftrightarrow k_1m \equiv k_2m\ (mod\ m) \\ &\Leftrightarrow k_1m \equiv k_2m \equiv 0\ (mod\ m). \end{aligned}$$

Portanto, segue que x_o é a única solução. □

Observação 3.1.9. A congruência $ax \equiv 1\ (mod\ m)$ possui solução se, e somente se, $mdc(a, m) = 1$. Isso é imediato da Proposição 3.1.3. Além disso, esta congruência linear admite uma única solução, conforme o Corolário 3.1.8, a qual chamamos de inverso multiplicativo módulo m.

Corolário 3.1.10. Sejam $m > 1$ um número inteiro e R um conjunto de resíduos módulo m. Se $b \in \mathbb{Z}$, então a congruência $rx \equiv b\ (mod\ m)$ possui uma única solução em R para todo $r \in R$.

Demonstração. A congruência $rx \equiv b\ (mod\ m)$ possui uma única solução módulo m porque $mdc(r, m) = 1$ (uma vez que $r \in R$) e $1|b$. Qualquer solução $x_o \in \mathbb{Z}$ é tal que $mdc(x_o, m) = 1$ e, com efeito, tem um único correspondente módulo m em R. □

Proposição 3.1.11. Toda congruência linear $ax \equiv b \ (mod \ m)$ que possui solução é equivalente a uma congruência do tipo $x \equiv c \ (mod \ n)$.

Demonstração. Seja x_o uma solução da congruência $ax \equiv b \ (mod \ m)$. Então, sabemos que $mdc(a,m)\Big|b$ e, a partir disto, considerando $d = mdc(a,m)$ temos que:

$$\frac{a}{d}x \equiv \frac{b}{d} \ \left(mod \ \frac{m}{d}\right).$$

Vamos denotar $\frac{a}{d} = a'$, $\frac{b}{d} = b'$ e $\frac{m}{d} = n$. Assim ficamos com a seguinte expressão,

$$a'x \equiv b' \ (mod \ n).$$

Observe que $mdc(a', n) = 1$ (pois segue do Corolário 1.1.37). Sendo assim,

$$x \equiv a'^{-1}b' \ (mod \ n) \Leftrightarrow x \equiv c \ (mod \ n),$$

onde $c = a'^{-1}b'$ e a'^{-1} é o inverso multiplicativo de a' módulo n. Isto, portanto, finaliza a demonstração. □

Exemplo 3.1.12. Seja a congruência linear $2x \equiv 4 \ (mod \ 6)$. É claro que tal equação possui solução, pois $mdc(2,6) = 2$ e $2|4$. Se dividirmos a referida congruência linear pelo $mdc(2,6) = 2$, obtemos uma outra equação, a saber $x \equiv 2 \ (mod \ 3)$, equivalente a principal.

Exemplo 3.1.13. Consideremos a congruência $2x \equiv 5 \ (mod \ 15)$. Observe que $mdc(2,15) = 1$ e $1|5$, logo esta congruência admite uma única solução módulo 15. Diante disso, pelo item (ii) da Proposição 2.1.12, a solução desta congruência é solução simultânea das seguintes congruências: $2x \equiv 5 \equiv 2 \ (mod \ 3)$ e $2x \equiv 5 \equiv 0 \ (mod \ 5)$. Não é difícil ver que, por inspeção, $x = 10$ é solução destas duas últimas expressões. Portanto, todas as soluções são da forma $x = 10 + 15t$ para algum t inteiro.

Exibiremos a partir deste ponto uma pequena passagem sobre congruências lineares do tipo $ax \equiv y \ (mod \ m)$ em que x, y são as incógnitas. Vamos mostrar que existe relação entre as soluções da referida congruência com a seguinte equação diofantina linear de duas incógnitas $ax - y = mb$.

Observe que a congruência linear $ax \equiv y \ (mod \ m)$ é equivalente a equação diofantina linear de três incógnitas $ax - y - mz = 0$. Fixando um valor inteiro qualquer b para a incógnita z, reduzimos a equação diofantina linear em uma outra à duas incógnitas, a saber $ax - y = mb$, que possui solução uma vez que $mdc(a, -1) = 1$ e $1|mb$. Diante disso, resolvendo tal equação obtemos a solução (x_o, y_o) e, por sua vez, tal resultado é solução da congruência $ax \equiv y \ (mod \ m)$.

O próximo resultado irá garantir que existem soluções não triviais com valores absolutos e pequenos para a congruência com duas incógnitas.

Teorema 3.1.14. Considere o número inteiro $m > 1$ não sendo um quadrado e outro número inteiro a cujo $mdc(a, m) = 1$. A congruência $ax \equiv y \ (mod\ m)$ possui solução $(x_o, y_o) \in \mathbb{Z}^2$ de forma que $0 < |x_o| < \sqrt{m}$ e $0 < |y_o| < \sqrt{m}$.

Demonstração. Seja $k \in \mathbb{Z}$ tal que $k - 1 < \sqrt{m} < k$. Observe que existe tal k porque m não é um quadrado. Consideremos o seguinte conjunto

$$A = \{(u, v) \in \mathbb{Z}^2;\ 0 \leqslant u < k\ \wedge\ 0 \leqslant t < k\}.$$

Atente que a quantidade de elementos deste conjunto será k^2, que é maior do que m porque $(k-1)^2 < (\sqrt{m})^2 = m < k^2$. A partir disso, como o número de inteiros não congruentes entre si módulo m é no máximo m e temos k^2 pares ordenados $(u, v) \in A$ que escritos da forma $au - v$ nos fornecem k^2 números inteiros, então temos que existem $(u_k, v_k) \in A$ com $k = 1, 2$, diferentes, de modo que:

$$au_1 - v_1 \equiv au_2 - v_2 \ (mod\ m) \Leftrightarrow a(u_1 - u_2) \equiv v_2 - v_1 \ (mod\ m).$$

Diante disso, se tivermos $u_1 = u_2$, então $m|(v_2 - v_1)$, que só pode acontecer quando $v_1 = v_2$. Por outro lado, se tivermos $v_1 = v_2$, então $m|(u_1 - u_2)$ (pois $mdc(a, m) = 1$) e isto só ocorre quando $u_1 = u_2$. Como sabemos que $(u_1, v_1) \neq (u_2, v_2)$, segue que a diferença entre as respectivas entradas é diferente de 0, isto é, $x_o = u_1 - u_2 \neq 0$ e $y_o = v_1 - v_2 \neq 0$. Inclusive, temos que $|x_o| = |u_1 - u_2| \leqslant k - 1 < \sqrt{m}$ e $|y_o| = |v_1 - v_2| \leqslant k - 1 < \sqrt{m}$ (pois $-k < u_1 - u_2 < k$ e $-k < v_2 - v_1 < k$). Portanto, (x_o, y_o) é solução da congruência $ax \equiv y \ (mod\ m)$. □

Exemplo 3.1.15. Consideremos a equação $2x \equiv y \ (mod\ 5)$. Repare que $2 < \sqrt{5} < 3$ e, realizando um comparativo com a demonstração do Teorema 3.1.14, temos $k = 3$. Logo, o conjunto $A = \{(u, v) \in \mathbb{Z}^2;\ 0 \leqslant u < 3\ \wedge\ 0 \leqslant t < 3\}$ possui 9 elementos. Como o número de inteiros incongruentes dois a dois módulo 5 é no máximo 5, vão existir, por exemplo, os pares ordenados distintos $(0, 1)$ e $(2, 0)$ de forma que $2 \cdot 0 - 1 \equiv 2 \cdot 2 - 0 \ (mod\ 5)$. Reorganizando, obtemos $2(0 - 2) \equiv 1 - 0 \ (mod\ 5)$. Portanto, $(-2, 1)$ é solução da congruência linear de duas incógnitas $2x \equiv y \ (mod\ 5)$ cujo módulo de suas entradas são menores que $\sqrt{5}$.

3.2 Alguns Teoremas Clássicos da Aritmética

Iremos realizar, nesta seção, uma discussão de três teoremas importantes para o desenvolvimento da Teoreia dos Números. Estes são: Teorema de Euler, Teorema de Wilson e Teorema Chinês dos Restos.

Cada um desses teoremas possuem suas peculiaridades e nos fornecem fortes relações entre os números inteiros envolvendo o conceito de congruências. Inclusive, é a partir deles que conseguimos facilitar cálculos extensos para chegar a solução de determinados problemas.

3.2.1 Teorema de Euler

Leonhard Paul Euler (1707-1783) foi um matemático suíço que nasceu em Basiléia. Ele foi o mais prolífico dos demais matemáticos de sua época, pois produziu diversos trabalhos e resultados em quase todas as áreas da Matemática bem como na Física. (BOYER; MERZBACH, 2012), (HEFEZ, 2009) e (MOL, 2013).

Seu pai, Paul Euler, era um ministro protestante naquela época e, através dele, Leonhard foi influenciado a estudar Teologia - estudo crítico dos Deuses. Entretanto, Johann Bernoulli (1667-1748) - outro matemático suíço nascido em Basiléia e orientador de Leonhard Euler - convenceu Paul Euler a deixar seu filho estudar Matemática, obtendo sucesso. (BOYER; MERZBACH, 2012).

Nos últimos anos de sua vida, período em que mais produziu trabalhos, Euler passou quase totalmente cego, pois com o passar dos anos sua visão com o olho direito foi ficando debilitada e também desenvolveu catarata no olho esquerdo. Sua morte ocorreu no dia 18 de setembro de 1783, quando ele tinha 76 anos de idade enquanto tomava chá na companhia de seu neto. (BOYER; MERZBACH, 2012), (HEFEZ, 2009) e (MOL, 2013).

No que tangencia os trabalhos de Leonhard Euler na Matemática, podemos ressaltar a relação entre os poliedros convexos, a identidade de Euler e a reta de Euler. Particularizando no ramo da Aritmética e Teoria dos Números, Leonhard Euler desenvolveu uma função - chamada função phi de Euler - que nos proporciona conhecer a quantidade de números coprimos ao número natural não nulo m. A partir desta função que ele estabeleceu o teorema que leva seu nome, o qual iremos apresentar e demonstrar.

Definição 3.2.1. Chamamos de *sistema reduzido de resíduos (ou restos) módulo* m o conjunto de números inteiros $R = \{r_1, r_2, ..., r_k\}$ tais que são cumpridas tais propriedades:

i) $mdc(r_i, m) = 1$, para todo $i = 1, 2, ...k$;

ii) $r_i \not\equiv r_j \ (mod\ m)$ se $i \neq j$;

iii) Para cada $n \in \mathbb{Z}$ tal que $mdc(n, m) = 1$, existe i tal que $n \equiv r_i \ (mod\ m)$.

Observação 3.2.2. É possível obtermos um sistema reduzido de resíduos módulo m a partir de um sistema completo qualquer de resíduos também módulo m. Para isto, basta eliminar os elementos do sistema completo que não são coprimos com m.

Exemplo 3.2.3. Seja $Q = \{0, 1, 2, 3, 4, 5, 6, 7\}$ o sistema completo de resíduos módulo 8. Se retirarmos deste conjunto os elementos $0, 2, 4$ e 6, obtemos um sistema reduzido de resíduos módulo 8, o qual denotamos por $R = \{1, 3, 5, 7\}$.

Proposição 3.2.4. Dados dois sistemas reduzidos de resíduos módulo m, então ambos tem o mesmo número de elementos.

Demonstração. Consideremos $R = \{r_1, r_2, ...r_k\}$ e $S = \{s_1, s_2, ..., s_l\}$ dois sistemas reduzidos de resíduos módulo m. Dado $s_i \in S$, com $1 \leqslant i \leqslant l$, temos que $mdc(s_i, m) = 1$. Além disso, do fato de R ser um sistema reduzido de resíduos módulo m, existe um único j, com $1 \leqslant j \leqslant k$, tal que $s_i \equiv r_j \ (mod\ m)$. Isto acaba definindo uma função α entre esses sistemas. Por outro lado, existe uma função β de S em R do mesmo modo. Suponhamos que $\beta(s_i) = r_t$, com $1 \leqslant t \leqslant k$, então $s_i \equiv r_t \ (mod\ m)$. Disto conclui-se que $r_j \equiv r_t \ (mod\ m)$ (pois $s_i \equiv r_j \ (mod\ m)$). Isto só ocorre se $j = t$. Logo, veja que β é a função inversa de α e, assim, α é bijetiva. Portanto, R e S possuem o mesmo número de elementos. □

Vamos agora designar por $\phi(m)$ o número de elementos de um sistema reduzido de resíduos módulo m, com $m > 1$. A função ϕ, quando aplicada em m, faz corresponder à um número natural entre 1 e $m - 1$ representando a quantidade de números que são primos entre si com m. Além disso, ponhamos $\phi(1) = 1$. Isto nos define uma função $\phi : \mathbb{N}^* \to \mathbb{N}^*$ chamada de Função ϕ de Euler.

Definição 3.2.5 (Função ϕ de Euler)**.** Seja o número natural $m \geqslant 1$. Representaremos por $\phi(m)$ a quantidade de números naturais não nulos menores que ou iguais a $m-1$ que são coprimos com m.

Observação 3.2.6. Atente que a função ϕ, quando aplicada no número natural $m \geqslant 1$, nos fornece exatamente a quantidade de elementos que possui o conjunto abaixo.

$$A = \{a \in \mathbb{N}^*;\ a < m\ \wedge\ mdc(a, m) = 1\}.$$

Exemplo 3.2.7. Consideremos $m = 2$ e encontraremos $\phi(2)$. Para isto, basta reparar que o conjunto $A = \{a \in \mathbb{N}^*;\ a < 2\ \wedge\ mdc(a, 2) = 1\ \} = \{1\}$. Portanto, $\phi(2) = 1$.

Exemplo 3.2.8. Seja $m = 3$. Vamos encontrar $\phi(3)$ e, para isto, repare que o conjunto $A = \{a \in \mathbb{N}^*;\ a < 3\ \wedge\ mdc(a, 3) = 1\ \} = \{1, 2\}$. Portanto, $\phi(3) = 2$.

Exemplo 3.2.9. Consideremos $m = 4$ e encontraremos $\phi(4)$. Para isto, note que o conjunto $A = \{a \in \mathbb{N}^*;\ a < 4\ \wedge\ mdc(a, 4) = 1\ \} = \{1, 3\}$. Portanto, $\phi(4) = 2$.

Exemplo 3.2.10. Se $m = 5$, temos $A = \{a \in \mathbb{N}^*;\ a < 5\ \wedge\ mdc(a, 5) = 1\ \} = \{1, 2, 3, 4\}$. Portanto, $\phi(5) = 4$.

Exemplo 3.2.11. Seja $m = 6$. Vamos encontrar $\phi(6)$ e, para isto, basta observar que o conjunto $A = \{a \in \mathbb{N}^*;\ a < 6\ \wedge\ mdc(a, 6) = 1\ \} = \{1, 5\}$. Portanto, $\phi(6) = 2$.

Observando os cinco exemplos anteriores, podemos perceber que há uma relação entre os números primos com a Função ϕ de Euler. Isto é o que veremos na proposição a seguir.

Proposição 3.2.12. Seja o número natural $m \geqslant 2$. Então $\phi(m) = m - 1$ se, e somente se, m é um número primo.

Demonstração. Suponhamos que $\phi(m) = m-1$. Nesse sentido, há $m-1$ números naturais que são coprimos com m, com esses números entre 0 e m. Consideremos o conjunto $X = \{1, 2, ..., m-1\}$. Para mostrarmos que m é um número primo, basta provarmos que o conjunto X forma um sistema reduzido de resíduos módulo m. É imediato que $mdc(a, m) = 1$ para todo $a \in X$ e que $a_i \not\equiv a_j \ (mod\ m)$ se $i \neq j$. Agora, para cada número inteiro n tal que $mdc(n, m) = 1$, temos que, pela Divisão Euclidiana, existem únicos números inteiros q, r tais que $n = mq + r$, com $r \in X$. Disso, concluí-se que $n \equiv r \ (mod\ m)$. Logo, X é um sistema reduzido de resíduos módulo m e, por conseguinte, m é primo. Por outro lado, se m é um número primo, então os primeiros $m - 1$ números naturais menores do que m serão coprimos com m, pois os únicos divisores positivos de m são 1 e m; e, a respeito dos demais números entre 0 e m, não entrará m no conjunto dos seus divisores porque m é o maior deles, não podendo dividi-los. Logo, sobra o único número natural que os divide comumente, o número 1. Portanto, $\phi(m) = m - 1$. □

No decorrer desta subseção, vamos encontrar um algoritmo para calcular a $\phi(m)$ para qualquer número inteiro $m \geqslant 2$.

Proposição 3.2.13. Seja o número natural não nulo n. Então, se $d \in \mathbb{N}^*$,

$$\sum_{d|n} \phi(d) = n.$$

Demonstração. Seja o conjunto dos n primeiros números naturais não nulos, $I_n = \{1, 2, ..., n\}$, e $d \in \mathbb{N}^*$ tal que $d|n$. Definiremos o conjunto $I_d = \{k \in I_n;\ mdc(k, n) = d\}$. Observe que dado outro número natural c tal que $c|n$ e $c \neq d$, então teremos que $I_d \cap I_c = \emptyset$. Assim, a união de todos os conjuntos I_d será exatamente I_n. Portanto,

$$n = \#I_n = \sum_{d|n} \#I_d.$$

Por outro lado, os elementos de I_d são múltiplos de d da forma dk, com $mdc\left(k, \frac{n}{d}\right) = 1$ e $k \leqslant \frac{n}{d}$. Portanto, $\#I_d = \phi\left(\frac{n}{d}\right)$. Repare que quando d varia todos os divisores de n, a razão entre n por d também varia por todos os divisores de n e, assim,

$$n = \sum_{d|n} \#I_d = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d).$$

□

Exemplo 3.2.14. Seja o número natural 18. Note que os divisores positivos de 18 são os elementos do conjunto $D(18) = \{1, 2, 3, 6, 9, 18\}$, então

$$\sum_{d|18} \phi(d) \quad = \quad \phi(1) + \phi(2) + \phi(3) + \phi(6) + \phi(9) + \phi(18) = 18.$$

Proposição 3.2.15. Dados o conjunto $R = \{r_1, r_2, ..., r_{\phi(m)}\}$ um sistema reduzido de resíduos módulo m e $a \in \mathbb{Z}$ cujo $mdc(a, m) = 1$. Então, o conjunto $R' = \{ar_1, ar_2, ..., ar_{\phi(m)}\}$ é um sistema reduzido de resíduos módulo m.

Demonstração. Seja $ar_i \in R'$, com $1 \leqslant i \leqslant \phi(m)$. Primeiramente, vamos mostrar que $mdc(ar_i, m) = 1$. De fato, se $mdc(ar_i, m) = d$, então $d|ar_i$ e $d|m$. Assim, existem $q, t \in \mathbb{Z}$ tais que $ar_i = dq$ e $m = dt$. Observe que

$$\begin{aligned}(ar_i)t = (dq)t &\Leftrightarrow (ar_i)t = (dt)q \\ &\Leftrightarrow (ar_i)t = mq.\end{aligned}$$

Ou seja, $m|(ar_i)t$. Como $mdc(a, m) = 1$, então $m|r_it$. Contudo, temos que $mdc(r_i, m) = 1$ (pois R é um sistema reduzido de resíduos módulo m), logo $m|t$. Desta forma, $m = dt = d(mk)$, para $k \in \mathbb{Z}$. A partir disto, obtemos $1 = dk \Leftrightarrow d = k = 1$. Mostraremos agora que dados dois elementos de R', estes serão congruentes só se forem iguais. Sejam ar_i e ar_j em R', com $i, j \in \{1, 2, ..., \phi(m)\}$, então

$$ar_i \equiv ar_j \ (mod\ m) \Leftrightarrow r_i \equiv r_j \ (mod\ m).$$

Do fato de R ser um sistema reduzido de resíduos módulo m, temos $i = j$. Por último, suponhamos n um número inteiro tal que $mdc(n, m) = 1$. Repare que a congruência linear $ax \equiv 1 \ (mod\ m)$ admite solução (pois $mdc(a, m) = 1|1$), digamos o número inteiro x_o. Logo, $ax_o \equiv 1 \ (mod\ m)$. Disto segue que, para $y_o \in \mathbb{Z}$, $ax_o - my_o = 1$ e como $mdc(n, m) = 1$, pelo Teorema 1.1.36, vão existir $s, t \in \mathbb{Z}$ tais que $ns + mt = 1$ se, e somente se, $(nx_o)s + m(x_ot) = x_o$. Substituindo esta última igualdade em $ax_o - my_o = 1$, obtém-se $(nx_o)(as) + m(ax_ot - y_o) = 1$ e, pelo Teorema 1.1.36, segue $mdc(nx_o, m) = 1$. Logo, vai existir i, para algum $i \in \{1, 2, ..., \phi(m)\}$, tal que $nx_o \equiv r_i \ (mod\ m)$ (pois R é um sistema reduzido de resíduos módulo m). Sendo assim, atente que:

$$n \equiv (ax_o)n \equiv a(x_on) \equiv ar_i \ (mod\ m).$$

Portanto, $R' = \{ar_1, ar_2, ..., ar_{\phi(m)}\}$ é um sistema reduzido de resíduos módulo m. □

Teorema 3.2.16 (Teorema de Euler)**.** Sejam $m, a \in \mathbb{Z}$ com $m > 1$ e $mdc(a, m) = 1$. Então, temos que $a^{\phi(m)} \equiv 1 \ (mod\ m)$.

Demonstração. Consideremos $R = \{r_1, r_2, ..., r_{\phi(m)}\}$ um sistema reduzido de resíduos módulo m, então, pela Proposição 3.2.15, $R' = \{ar_1, ar_2, ..., ar_{\phi(m)}\}$ é um sistema reduzido de resíduos módulo m. Logo,

$$\begin{aligned}ar_1ar_2...ar_{\phi(m)} \equiv r_1r_2...r_{\phi(m)} \ (mod\ m) &\Leftrightarrow a^{\phi(m)}r_1r_2...r_{\phi(m)} \equiv r_1r_2...r_{\phi(m)} \ (mod\ m) \\ &\Leftrightarrow a^{\phi(m)} \equiv 1 \ (mod\ m),\end{aligned}$$

uma vez que $mdc(r_i, m) = 1$, para todo $1 \leqslant i \leqslant \phi(m)$, e assim $mdc(\prod r_i, m) = 1$. Isto finaliza a demonstração. □

Exemplo 3.2.17. Consideremos os números inteiros 2 e 3. Repare que $mdc(2,3) = 1$ e assim, pelo Teorema 3.2.16, $2^{\phi(3)} \equiv 1 \ (mod\ 3)$. Sabemos que $\phi(3) = 2$ (pelo Exemplo 3.2.8), donde conclui-se que $4 \equiv 1 \ (mod\ 3)$.

Corolário 3.2.18 (Pequeno Teorema de Fermat)**.** Sejam $a \in \mathbb{Z}$ e p um número primo tais que $mdc(a,p) = 1$. Tem-se que $a^{p-1} \equiv 1 \ (mod\ p)$.

Demonstração. Basta notar que como p é um número primo, $\phi(p) = p - 1$. Assim, aplicando o Teorema 3.2.16, temos que $a^{p-1} \equiv 1 \ (mod\ p)$. □

Afirmação 3.2.19. Sejam $a, m, r \in \mathbb{N}$, onde $m > 1$, $r \neq 0$ e $mdc(m,r) = 1$. A sequência $a, a+r, a+2r, ..., a+(n-1)r$ não possui dois termos que deixem o mesmo resto na divisão por m.

Demonstração. Suponhamos que, para k_1 e k_2 distintos e pertencentes à $\{0, 1, 2, ..., n-1\}$, os termos $a+k_1r$ e $a+k_2r$ deixem restos iguais a l na divisão por m. Logo, $a+k_1r = mq_1+l$ e $a+k_2r = mq_2+l$, onde $q_1, q_2 \in \mathbb{N}$. Subtraindo essas duas igualdades membro à membro, obtemos $(k_1 - k_2)r = m(q_1 - q_2)$. Repare que $m|[(k_1 - k_2)r]$, mas como $mdc(m,r) = 1$ segue que $k_1 \equiv k_2 \ (mod\ m)$, o que só é possível se $k_1 = k_2$. □

Proposição 3.2.20. Sejam m e n números naturais tais que $mdc(m,n) = 1$. Então $\phi(mn) = \phi(m)\phi(n)$.

Demonstração. Para o caso em que $m = n = 1$ é imediato, já que $\phi(mn) = 1 = 1 \cdot 1 = \phi(m)\phi(n)$. Já o caso em que $n = 1$ temos as seguintes igualdades,

$$\begin{aligned} \phi(m \cdot 1) &= \phi(m) \\ &= \phi(m) \cdot 1 \\ &= \phi(m)\phi(n). \end{aligned}$$

Analogamente, prova-se para o caso em que $m = 1$. Resta-nos provar o caso em que $m > 1$ e $n > 1$. Para isto, consideremos a seguinte tabela abaixo em que dispomos os números naturais de 1 a mn.

$$\begin{array}{ccccccc} 1 & 2 & ... & k & ... & n \\ n+1 & n+2 & ... & n+k & ... & 2n \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ (m-1)n+1 & (m-1)n+2 & ... & (m-1)n+k & ... & mn \end{array}$$

Note que, pela Proposição 1.1.31, $mdc(qn+k, n) = mdc(n,k)$ e, assim, os números naturais da k-ésima coluna são coprimos com n se, e somente se, k é um número coprimo com n. Logo, o número de naturais da primeira linha que são coprimos com n é $\phi(n)$, ou

seja, existem $\phi(n)$ colunas cujos números são primos entre si com n. Por outro lado, para cada $k \in \{1, 2, ..., n\}$, consideremos a seguinte sequência:

$$k, k+n, k+2n, ..., k+(m-1)n.$$

Pela Afirmação 3.2.19, tal sequência não possuirá dois termos distintos cujo resto da divisão por m seja igual. Sendo assim, teremos m restos distintos (que, quando reunidos, formam o conjunto $\{0, 1, 2, ..., m-1\}$). Além disso, tem-se $mdc(qn+k, m) = mdc(m, r)$, onde $r \in \{0, 1, 2, ..., m-1\}$ é o resto da divisão de um termo por m. Disto, temos que o número de naturais que são coprimos com m é igual ao número de restos obtidos pela divisão de seus termos por m e que sejam coprimos com m, que, por sua vez, é igual a $\phi(m)$. Logo, em cada uma das $\phi(n)$ colunas (que possuem os números naturais coprimos com n) há exatamente $\phi(m)$ números naturais primos entre si com m. Portanto, $\phi(mn) = \phi(m)\phi(n)$. □

Exemplo 3.2.21. Consideremos 235 e encontraremos $\phi(235)$. Atente que $235 = 5 \cdot 47$ e, ainda, $mdc(5, 47) = 1$. Sendo assim, $\phi(235) = \phi(5)\phi(47)$. Como 5 e 47 são números primos, sabemos que $\phi(5) = 4$ e $\phi(47) = 46$. Portanto, $\phi(235) = 4 \cdot 46 = 184$.

Para o próximo resultado, precisamos compreender uma definição.

Definição 3.2.22. Um número inteiro é dito livre de quadrados quando a sua fatoração primária conter apenas números primos distintos.

Exemplo 3.2.23. Os números inteiros 12 e 375 não são livre de quadrados, pois $12 = 2^2 \cdot 3$ (possui 2 fatores 2) e $375 = 3 \cdot 5^3$ (possui 3 fatores 5). Já o número inteiro 6 é livre de quadrados porque $6 = 2 \cdot 3$ (não possui fatores primos iguais).

Corolário 3.2.24. Seja $m \in \mathbb{Z}$ livre de quadrados, com $m > 1$. Então, para todo número inteiro a e natural k, tem-se que $a^{k\phi(m)+1} \equiv a \ (mod\ m)$.

Demonstração. Como m é um número inteiro livre de quadrados, então podemos escrever $m = p_1 p_2 ... p_r$, onde $p_1, p_2, ..., p_r$ são números primos distintos. Daí,

$$\begin{aligned} \phi(m) &= \phi(p_1 p_2 ... p_r) \\ &= \phi(p_1)\phi(p_2)...\phi(p_r) \\ &= (p_1 - 1)(p_2 - 1)...(p_r - 1). \end{aligned}$$

Daí, pondo $k_i = k(p_1 - 1)(p_2 - 1)...(p_i - 1)(p_{i+1} - 1)...(p_r - 1)$, com $1 \leqslant i \leqslant r$, temos, para todo número inteiro a, número natural k e i, que:

$$a^{k\phi(m)+1} \equiv a^{k_i(p_i-1)+1} \equiv \left(a^{(p_i-1)}\right)^{k_i} a \equiv a \ (mod\ p_i),$$

onde na última congruência foi utilizado o Pequeno Teorema de Fermat 3.2.18. Como o mínimo múltiplo comum entre p_1, p_2, ..., p_r é igual à $p_1 p_2 ... p_r = m$ (pois todos são primos distintos), segue do item (ii) da Proposição 2.1.12 que $a^{k\phi(m)+1} \equiv a \ (mod\ m)$. □

Afirmação 3.2.25. Sejam n um número inteiro, k um número natural e p um número primo. Então $mdc(n, p^k) = 1$ se, e somente se, p não divide n.

Demonstração. Se $mdc(n, p^k) = 1$, então, pelo Teorema 1.1.36, existem $x, y \in \mathbb{Z}$ tais que $nx + p^k y = 1$. Logo, $p(p^{k-1}y) = 1 - nx$, ou seja, $nx \equiv 1 \ (mod\ p)$. Sendo assim, $p \nmid nx$, donde segue que $p \nmid n$ e $p \nmid x$. Por outro lado, se $p \nmid n$, então nenhuma outra potência de p irá dividir n. Sendo assim, o único divisor comum de n e p^k será 1. Portanto, $mdc(n, p^k) = 1$. □

Proposição 3.2.26. Dados p um número primo e um número natural k, então temos que $\phi(p^k) = p^k - p^{k-1}$.

Demonstração. Observe que existem exatamente p^{k-1} números naturais de 1 à p^k que são divisíveis por p, a saber $p, 2p, ..., (p^{k-1})p$. Diante disso, retirando esses elementos, obtermos um subconjunto de $\{1, 2, ..., p^k\}$ que contém precisamente $p^k - p^{k-1}$ elementos que, por sua vez, serão coprimos com p^k pela Afirmação 3.2.25. Portanto, $\phi(p^k) = p^k - p^{k-1}$. □

Iremos agora mostrar o algoritmo para calcular a $\phi(m)$ para qualquer $m \geqslant 2$.

Teorema 3.2.27. Considere o número natural $m > 1$ e seja $m = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ a decomposição primária de m. Então,

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_k}\right).$$

Demonstração. Para provarmos esse teorema, utilizaremos indução sobre k.

Base de indução: Para $k = 1$ é imediato uma vez que $\phi(m) = \phi(p_1^{\alpha_1})$ e, pela Proposição 3.2.26, temos que $\phi(p_1^{\alpha_1}) = p_1^{\alpha_1} - p_1^{\alpha_1 - 1}$ donde segue que $\phi(m) = m\left(1 - \frac{1}{p_1}\right)$.

Hipótese de indução: Suponhamos que o teorema seja satisfeito para todo número natural menor ou igual que k.

Tese: Provaremos a veracidade do teorema para o sucessor de k, ou seja, para $k+1$. Seja o número inteiro $m > 1$ cujo sua fatoração primária seja $m = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k} p_{k+1}^{\alpha_{k+1}}$. Daí,

$$\phi(m) = \phi(p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k} p_{k+1}^{\alpha_{k+1}}) \quad = \quad \phi(p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k})\phi(p_{k+1}^{\alpha_{k+1}})$$

Note que $\phi(p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}) = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_k}\right)$ e também temos que $\phi(p_{k+1}^{\alpha_{k+1}}) = p_{k+1}^{\alpha_{k+1}} - p_{k+1}^{\alpha_{k+1}-1} = p_{k+1}^{\alpha_{k+1}}\left(1 - \frac{1}{p_{k+1}}\right)$. Logo

$$\begin{aligned}\phi(m) &= p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k} p_{k+1}^{\alpha_{k+1}}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_k}\right)\left(1 - \frac{1}{p_{k+1}}\right) \\ &= m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_k}\right)\left(1 - \frac{1}{p_{k+1}}\right)\end{aligned}$$

Portanto, o teorema é válido para todo $k \in \mathbb{N}$. □

Exemplo 3.2.28. Seja o número inteiro 504. Fatorando-o, obtemos $504 = 2^3 \cdot 3^2 \cdot 7$. Assim, $\phi(504) = 504\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{7}\right) = 144$.

3.2.2 Teorema de Wilson

John Wilson (1741-1793) foi um professor de matemática e juiz britânico nascido na Inglaterra. Ficou conhecido por um teorema que é atribuído a ele, mas que foi publicado primeiramente pelo seu professor de matemática Edward Waring (1736-1798). Nem Wilson e muito menos Waring conseguiram provar tal resultado, porém Joshep-Louis Lagrange (1736-1813), que foi um matemático francês (embora atualmente o local de seu nascimento pertença a Itália), foi o primeiro a demonstrar a recíproca do resultado. (CAMPOS; AVILA, 2015).

O Teorema de Wilsom é um grande resultado para a matemática porque é mais um teste de primalidade, isto é, fornece condições para sabermos se um determinado número inteiro positivo é ou não primo. Embora seus cálculos sejam extensos por envolver a noção de fatorial (dizemos que o fatorial de um número inteiro positivo n, denotado por $n!$, é o produto nos n primeiros números inteiros positivos não nulos), é uma técnica que merece reconhecimento por, justamente, trazer os números primos para a discussão.

Antes de enunciarmos e provarmos o Teorema de Wilson, iremos demonstrar uma afirmação que se fará útil para concluirmos a veracidade do resultado atribuído a John Wilson.

Afirmação 3.2.29. Seja p um número primo. O número inteiro a é o seu próprio inverso módulo p se, e somente se, $a \equiv 1 \ (mod\ p)$ ou $a \equiv -1 \ (mod\ p)$.

Demonstração. Seja $a \in \mathbb{Z}$. Se este for seu próprio inverso módulo p, então $a^2 \equiv 1 \ (mod\, p)$. Desta congruência, obtemos a expressão $a^2 - 1 = pk$, para algum $k \in \mathbb{Z}$. Atente que $a^2 - 1 = (a-1)(a+1) = pk$, ou seja, $p|[(a-1)(a+1)]$. Como p é primo, decorre da Proposição 1.2.7 que $p|(a-1)$ ou $p|(a+1)$. Logo, $a \equiv 1 \ (mod\ p)$ ou $a \equiv -1 \ (mod\ p)$. Em contrapartida, se $a \equiv 1 \ (mod\ p)$ ou $a \equiv -1 \ (mod\ p)$, temos que $p|(a-1)$ ou $p|(a+1)$, isto é, $p|(a^2 - 1)$. Portanto, $a^2 \equiv 1 \ (mod\ p)$. □

Teorema 3.2.30 (Teorema de Wilson)**.** O número inteiro $p > 1$ é primo se, e somente se $(p-1)! \equiv -1 \ (mod\ p)$.

Demonstração. Suponhamos que p seja primo. Podemos supor que $p \geqslant 5$, pois para $p = 2$ e $p = 3$ é satisfeito o resultado uma vez que $(2-1)! = 1 \equiv -1 \ (mod\ 2)$ e $(3-1)! = 2 \equiv -1 \ (mod\ 3)$. Consideremos a seguinte congruência linear $ax \equiv 1 \ (mod\ p)$, onde $a \in \{1, 2, ..., p-1\}$. Diante disso, a e p são coprimos, ou seja, $mdc(a, p) = 1$. Pela Observação 3.1.9 e Corolário 3.1.8, segue que a congruência linear admite uma única

solução. Digamos que b seja solução da referida congruência, com $1 \leqslant b \leqslant p-1$. Então, $ab \equiv 1\ (mod\ p)$. Logo, a e b são inversos módulo p e, pela Afirmação 3.2.29, $a = b$ se, e somente se, $a = 1$ ou $a = p-1$. Já, referente aos demais números, $2, 3, ..., p-2$, podemos agrupá-los em $\frac{p-3}{2}$ pares (a, b) de forma que satisfaçam $ab \equiv 1\ (mod\ p)$. Multiplicando todas essas congruências, temos que

$$2 \cdot 3 \cdot ... \cdot (p-2) \equiv 1\ (mod\ p) \Leftrightarrow 2 \cdot 3 \cdot ... \cdot (p-2) \cdot (p-1) \equiv p-1\ (mod\ p).$$

Repare que $p-1 \equiv -1\ (mod\ p)$ e, por transitividade, temos que $(p-1)! \equiv -1\ (mod\ p)$. Reciprocamente, se $(p-1)! \equiv -1\ (mod\ p)$, então temos que p é primo porque, caso contrário, p seria composto e teria um divisor d, com $1 < d < p$. Assim, $d \leqslant p-1$ donde segue que d será um dos fatores de $(p-1)!$ e, portanto, $d \big| (p-1)!$. Contudo, pela hipótese, p é divisor de $(p-1)!+1$ e o mesmo ocorre para d, o que só seria viável se d fosse divisor de 1 (isto é $d = 1$) o que não é o caso uma vez que $d > 1$. Portanto p é primo. □

Exemplo 3.2.31. Consideremos $p = 5$, então $(5-1)! = 4! = 24$. Disto, note que $4! + 1 = 25$ é divisível por 5 porque $5 \cdot 5 = 25$. Portanto, 5 é primo.

Exemplo 3.2.32. Seja $p = 13$, então $(13-1)! = 12! = 479.001.600$. A partir daí, observe que $12! + 1 = 479.001.601$. Realizando a divisão deste número por 13, temos que $12! + 1 = 13 \cdot 36.846.277$. Portanto, 13 é primo.

3.2.3 Teorema Chinês dos Restos

O Teorema Chinês dos Restos teve origem nos problemas formulados pelos matemáticos chineses por volta de 287 d.C. com o objetivo de solucionar questões envolvendo a astronomia e os movimentos periódicos do corpos celestes. Destacamos ainda que os gregos também desenvolveram tal método simultaneamente com os chineses.

Teorema 3.2.33 (Teorema Chinês dos Restos)**.** Se $mdc(m_i, m_j) = 1$ para todo par m_i e m_j, com $i \neq j$, então o sistema $x \equiv c_i\ (mod\ m_i)$, com $i = 1, 2, ..., k$, possui uma única solução módulo $M = m_1 m_2 ... m_k$. As soluções são:

$$x_o = M_1 y_1 c_1 + ... + M_k y_k c_k + tM,$$

onde $t \in \mathbb{Z}$, $M_i = \frac{M}{m_i}$ e y_i é solução de $M_i y \equiv 1\ (mod\ m_i)$.

Demonstração. Observe que $m_i | M_j$, se $i \neq j$, e $M_i y_i \equiv 1\ (mod\ m_i)$. Inclusive, atente que $M_i y_i c_i \equiv c_i\ (mod\ m_i)$ (basta multiplicar por c_i a congruência $M_i y_i \equiv 1\ (mod\ m_i)$). Diante disso,

$$x_o = M_1 y_1 c_1 + ... + M_k y_k c_k + tM \equiv M_1 y_1 c_1 + ... + M_k y_k c_k \equiv M_i y_i c_i \equiv c_i\ (mod\ m_i).$$

Contudo, se x'_o é outra solução do sistema, então

$$x_o \equiv x'_o \ (mod\ m_i), \forall i = 1, 2, ..., k.$$

Como $mdc(m_i, m_j) = 1$, para $i \neq j$, segue que $mmc(m_1, m_2, ..., m_k) = m_1 m_2 ... m_k = M$ e, portanto, pelo item (ii) da Proposição 2.1.12, temos que $x_o \equiv x'_o \ (mod\ M)$. □

Exemplo 3.2.34. Vamos resolver um problema proposto por um matemático chinês chamado Sun-Tsu. A questão é assim enunciada: *Um número deixa resto* 2, 3 *e* 2 *quando dividido por* 3, 5 *e* 7, *respectivamente. Que número é este?* Reescrevendo em linguagem matemática envolvendo congruências lineares, temos:

$$\begin{aligned} x &\equiv 2 \ (mod\ 3) \\ x &\equiv 3 \ (mod\ 5) \\ x &\equiv 2 \ (mod\ 7). \end{aligned}$$

Repare que $M = 3 \cdot 5 \cdot 7 = 105$ e assim $M_1 = 35$, $M_2 = 21$ e $M_3 = 15$. Resolvendo separadamente as equações de congruências lineares $35y \equiv 1 \ (mod\ 3)$, $21y \equiv 1 \ (mod\ 5)$ e $15y \equiv 1 \ (mod\ 7)$ obtemos as respectivas soluções $y_1 = 2$, $y_2 = 1$ e $y_3 = 1$. Portanto, uma solução módulo 105:

$$x_o = M_1 y_1 c_1 + M_2 y_2 c_2 + M_3 y_3 c_3 = 233.$$

Observe que $233 \equiv 23 \ (mod\ 105)$ e, disto, segue que 23 é a solução do problema de Sun-Tsu. As demais soluções serão dadas pela expressão $23 + 105t$, com $t \in \mathbb{Z}$.

Proposição 3.2.35. Seja o sistema de congruências $x \equiv c_i \ (mod\, m_i)$, com $i \in \{1, 2\}$. Este sistema possui solução se, e somente se, $c_i \equiv c_j \ (mod\ M)$, com $i \neq j$ e $M = mdc(m_i, m_j)$. Ademais, dado uma solução a do sistema, então um número b também será solução se, e somente se, $a \equiv b \ (mod\ N)$, com $N = mmc(m_i, m_j)$.

Demonstração. Consideremos o sistema de congruências $x \equiv c_i \ (mod\ m_i)$, com $i \in \{1, 2\}$. Logo, existe $y_i \in \mathbb{Z}$ tal que $m_i y_i = c_i - x$. Repare que $m_i y_i - m_j y_j$, com $i \neq j$, obtém-se:

$$m_i y_i - m_j y_j = (c_i - x) - (c_j - x) = c_i - c_j.$$

Se observarmos, chegamos a uma equação diofantina linear $m_i y_i - m_j y_j = c_i - c_j$ que admite solução se, e somente se, $mdc(m_i, m_j) = M$ divide $c_i - c_j$. Portanto, temos a relação $c_i \equiv c_j \ (mod\ M)$. Para mostrarmos a segunda afirmação, consideremos a uma solução do sistema, isto é, $a \equiv c_i \ (mod\ m_i)$ para $i \in \{1, 2\}$. Mas se b é outra solução do sistema, temos que $b \equiv c_i \ (mod\ m_i)$ e disso segue que $a \equiv b \ (mod\ m_i)$. Pelo item (ii) da Proposição 2.1.12, concluímos que $a \equiv b \ (mod\ N)$, onde $N = mmc(m_i, m_j)$ com $i \neq j$. Reciprocamente, se $a \equiv b \ (mod\ N)$, então $a \equiv b \equiv c_i \ (mod\ m_i)$ já que a é solução do sistema. □

Exemplo 3.2.36. Consideremos o seguinte sistema de congruências lineares:

$$\begin{aligned} x &\equiv 11 \ (mod\ 15) \\ x &\equiv 10 \ (mod\ 13). \end{aligned}$$

Repare que $10 \equiv 11 \ (mod\ 1)$, logo, pela Proposição 3.2.35, tal sistema admite solução.

As soluções das congruências $13y \equiv 1 \ (mod\ 15)$ e $15y \equiv 1 \ (mod\ 13)$, separadamente calculadas, são iguais à 7. Logo, a solução módulo 195 é dada por:

$$x_o = 15 \cdot 7 \cdot 10 + 13 \cdot 7 \cdot 11 = 1050 + 1001 = 2051 \equiv 101 \ (mod\ 195).$$

Portanto, $x = 101$ é uma solução do sistema. As demais serão fornecidas por $101 + 195t$, para $t \in \mathbb{Z}$.

4 Congruências Quadráticas

Neste último capítulo, discutiremos a cerca das congruências quadráticas da forma $x^2 \equiv a \ (mod\, p)$, onde $a, p \in \mathbb{Z}$ com p número primo tal que $p \nmid a$. Diante destas estruturas, podemos pensar em três questionamentos básicos para iniciarmos nossos estudos - (1º) Tais congruências sempre possuem solução?; (2º) Como identificar quais admitem e quais não admitem solução?; e (3º) Como encontrar suas soluções? Para elucidarmos estes questionamentos, realizamos um estudo minucioso sobre o tema através das seguintes literaturas: (DOMINGUES, 1991), (GOMES; SILVA, 2018) e (SANTOS, 2020).

4.1 Congruências quadráticas

Sejam $p > 2$ um número primo e $a_1, a_2, a_3 \in \mathbb{Z}$, onde a_1 não é múltiplo de p. Chamamos de congruência quadrática toda equação da forma $a_1y^2+a_2y+a_3 \equiv 0 \ (mod\, p)$.

Estamos interessados em encontrar soluções para $a_1y^2 + a_2y + a_3 \equiv 0 \ (mod\ p)$. Então, vamos manipular tal congruência (completar quadrado).

$$\begin{aligned} a_1y^2 + a_2y + a_3 \equiv 0 \ (mod\ p) &\Leftrightarrow 4a_1^2y^2 + 4a_1a_2y + 4a_1a_3 \equiv 0 \ (mod\ p) \\ &\Leftrightarrow 4a_1^2y^2 + 4a_1a_2y + a_2^2 - a_2^2 + 4a_1a_3 \equiv 0 \ (mod\ p) \\ &\Leftrightarrow (2a_1y + a_2)^2 - a_2^2 + 4a_1a_3 \equiv 0 \ (mod\ p) \\ &\Leftrightarrow (2a_1y + a_2)^2 \equiv a_2^2 - 4a_1a_3 \ (mod\ p) \\ &\Leftrightarrow x^2 \equiv a \ (mod\ p), \end{aligned}$$

onde $x = 2a_1y + a_2$ e $a = a_2^2 - 4a_1a_3$.

Logo, se solucionarmos a equação de congruência $x^2 \equiv a \ (mod\ p)$, então basta encontrarmos a solução da congruência linear $x_o \equiv 2a_1y + a_2 \ (mod\ p)$ (onde x_o é um número inteiro tal que $x_o^2 \equiv a \ (mod\, p)$) que obteremos a solução da congruência quadrática $a_1y^2 + a_2y + a_3 \equiv 0 \ (mod\ p)$.

4.1.1 Congruências quadráticas $x^2 \equiv a \ (mod\ p)$

Definição 4.1.1. Sejam a e p números inteiros tais que p é primo e $mdc(a, p) = 1$. Diremos que a é um *resíduo quadrático módulo p* se a congruência $x^2 \equiv a \ (mod\, p)$ admitir solução. Caso contrário, diremos que a não é um resíduo quadrático módulo p, ou melhor, a é um resíduo não-quadrático módulo p.

Exemplo 4.1.2. Observe que 12 é um resíduo quadrático módulo 13, pois a equação $x^2 \equiv 12 \ (mod\ 13)$ tem, por exemplo, $x = 5$ como solução. Em contrapartida, 5 é

um resíduo não-quadrático módulo 13 porque não há nenhum valor de x para que a congruência $x^2 \equiv 5 \ (mod\ 13)$ seja satisfeita, conforme veremos no Exemplo 4.1.13.

Observação 4.1.3. Atente que 1 sempre será um resíduo quadrático módulo p, já que $x = 1$ e $x = p - 1$ satisfazem a equação $x^2 \equiv 1 \ (mod\ p)$.

Observação 4.1.4. A congruência quadrática $x^2 \equiv a \ (mod\ 2)$ sempre admite solução. De fato, basta notar que se a é par, então $x = 0$ é uma solução enquanto que se a for ímpar, $x = 1$ será solução.

Diante desta última observação, podemos analisar apenas as congruências quadráticas $x^2 \equiv a \ (mod\ p)$ em que p é um número primo ímpar.

A Definição 4.1.1 e o Exemplo 4.1.2 já respondem o primeiro dos três questionamentos que nos fizemos no início deste capítulo. Nem toda congruência quadrática da forma $x^2 \equiv a \ (mod\ p)$ admite solução. Seguiremos então para solucionar as outras duas perguntas.

O primeiro resultado sobre congruências quadráticas da forma $x^2 \equiv a \ (mod\ p)$ acaba nos fornecendo a quantidade de soluções incongruentes. Segue abaixo seu enunciado e demonstração.

Teorema 4.1.5. Seja p um número primo ímpar tal que p não divida o número inteiro a. A congruência $x^2 \equiv a \ (mod\ p)$, caso tenha solução, tem duas, e somente duas, soluções incongruentes módulo p.

Demonstração. Se a congruência $x^2 \equiv a \ (mod\ p)$ admite solução x_o, então é claro que $-x_o$ também é solução porque $(-x_o)^2 = x_o^2$. Agora queremos provar que x_o e $-x_o$ são incongruentes módulo p. Para isto, vamos supor, por absurdo, que $x_o \equiv -x_o \ (mod\ p)$. A partir disto, obtemos que $2x_o \equiv 0 \ (mod\ p)$ e, como p é ímpar e $p \nmid x_o$, concluímos que $2x_o \not\equiv 0 \ (mod\ p)$. Disto segue que $x_o \not\equiv -x_o \ (mod\ p)$. Falta mostrarmos que existem apenas duas soluções incongruentes. Sendo assim, consideremos y uma solução da congruência $x^2 \equiv a \ (mod\ p)$, então $y^2 \equiv a \ (mod\ p)$. Assim, pelo item (i) da Proposição 2.1.7, decorre que $y^2 - x_o^2 \equiv 0 \ (mod\ p)$ (pois $p|(x_o^2 - a)$). Com isso, segue que $p|(y^2 - x_o^2)$, isto é, $p|[(y + x_o)(y - x_o)]$. Como p é um número primo, resulta da Proposição 1.2.7 que $y \equiv x_o \ (mod\ p)$ ou $y \equiv -x_o \ (mod\ p)$. □

Agora vamos considerar p um número primo ímpar e $x \in R = \{1, 2, ..., p - 1\}$. Definiremos ainda o seguinte conjunto:

$$S = \{(x, p - x) \in \mathbb{Z}^2; x^2 \equiv (p - x)^2 \ (mod\ p)\}.$$

É fato que $S \neq \emptyset$, pois basta notar que $-k \equiv p - k \ (mod\ p)$, com $k \in R$, e aplicar a Proposição 2.1.10 para $n = 2$. Logo, o par $(k, p - k) \in S$. Além do mais, notamos haver

$p-1$ elementos no conjunto S porque p é um número primo ímpar fixo e x varia em R. Atente ainda que o par $(p-k,k) \in S$, já que $k^2 \equiv (p-k)^2 \ (mod\ p) \Leftrightarrow (p-k)^2 \equiv k^2 \ (mod\, p)$. Isto acarreta que há pares de elementos em S o qual nos fornecem congruências iguais, a saber $(k, p-k)$ e $(p-k, k)$. Se retirarmos os pares que nos proporcionam congruências iguais, teremos um conjunto S' com metade dos elementos de S, ou seja, S' tem exatamente $\frac{p-1}{2}$ pares da forma $(x, p-x)$ tais que $x^2 \equiv (p-x)^2 \ (mod\ p)$. Ora, se S' tem tal quantidade de elementos, é porque $x \in R' = \{1, 2, ..., \frac{p-1}{2}\}$. Portanto, há $\frac{p-1}{2}$ elementos em R que são resíduos quadráticos módulo p e $\frac{p-1}{2}$ que são resíduos não-quadráticos módulo p.

Esse raciocínio demonstra o seguinte teorema abaixo.

Teorema 4.1.6. Seja p um número inteiro maior do que 2 e primo. Dentre os elementos do conjunto $R = \{1, 2, ..., p-1\}$, existem $\frac{p-1}{2}$ resíduos quadráticos e $\frac{p-1}{2}$ que não são.

O Teorema 4.1.6 nos traduz que a quantidade de resíduos quadráticos e não-quadráticos dentro de $R = \{1, 2, ..., p-1\}$ são iguais à $\frac{p-1}{2}$.

Exemplo 4.1.7. Consideremos $p = 7$ e $R = \{1, 2, 3, 4, 5, 6\}$. Perceba que $x^2 \equiv 1 \ (mod\ 7)$, $x^2 \equiv 2 \ (mod\ 7)$ e $x^2 \equiv 4 \ (mod\ 7)$ possuem solução igual à 1, -3 e 5, respectivamente. Então, pelo Teorema 4.1.6, tem-se a insolubilidade de $x^2 \equiv 3 \ (mod\ 7)$, $x^2 \equiv 5 \ (mod\ 7)$ e $x^2 \equiv 6 \ (mod\ 7)$.

A próxima proposição é interessante, pois nos caracteriza quando uma congruência da forma $x^2 \equiv 1 \ (mod\ p)$ terá ou não solução e, inclusive, nos fornece a sua solução.

Proposição 4.1.8. Seja p um número inteiro primo ímpar. A congruência $x^2 \equiv -1 \ (mod\, p)$ tem solução se, e somente se, $p \equiv 1 \ (mod\ 4)$.

Demonstração. Segue abaixo a prova deste resultado.

($\Longrightarrow$) Consideremos x_o solução da congruência $x^2 \equiv -1 \ (mod\ p)$, ou melhor dizendo, $x_o^2 \equiv -1 \ (mod\ p)$. Aplicando a Proposição 2.1.10 para $n = \frac{p-1}{2}$, obtemos:

$$(x_o^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \ (mod\ p),$$

e, por conta do Corolário 3.2.18, temos:

$$(x_o^2)^{\frac{p-1}{2}} = x_o^{p-1} \equiv 1 \ (mod\ p).$$

Logo, segue que $(-1)^{\frac{p-1}{2}} \equiv 1 \ (mod\, p)$. Ora, $(-1)^{\frac{p-1}{2}} = \pm 1$ e $-1 \not\equiv 1 \ (mod\, p)$, acarretando $(-1)^{\frac{p-1}{2}} = 1$. Consequentemente, $\frac{p-1}{2}$ é par, ou seja, é da forma $2k$, com $k \in \mathbb{N}$. Assim, $p - 1 = 4k$ e, portanto, $p \equiv 1 \ (mod\ 4)$.

($\Longleftarrow$) Consideremos p um primo ímpar e $p \equiv 1\ (mod\ 4)$. Pelo Teorema de Wilson 3.2.30, temos $(p-1)! \equiv -1\ (mod\ p)$. Reescrevendo, obtém-se:

$$1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-2) \cdot (p-1) \equiv -1\ (mod\ p).$$

Já sabemos que $-k \equiv (p-k)\ (mod\ p)$, para todo $k \in \{1, 2, ..., \frac{p-1}{2}\}$. Logo,

$$\begin{aligned} 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \cdots (-2) \cdot (-1) &\equiv -1\ (mod\ p) \\ (-1)^{\frac{p-1}{2}} \cdot \left[\left(\frac{p-1}{2}\right)!\right]^2 &\equiv -1\ (mod\ p). \end{aligned}$$

Como $p = 4k+1$ (pois $p \equiv 1\ (mod\ 4)$), com $k \in \mathbb{N}$, resulta em $\frac{p-1}{2}$ ser par. Portanto,

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1\ (mod\ p).$$

□

Observação 4.1.9. O número $\left(\frac{p-1}{2}\right)!$ é solução para toda congruência $x^2 \equiv -1\ (mod\ p)$, para algum número primo p ímpar tal que $p \equiv 1\ (mod\ 4)$.

Exemplo 4.1.10. Seja o número primo 29. Repare que $29 \equiv 1\ (mod\ 4)$, logo $x^2 \equiv -1\ (mod\ 29)$ admite solução. Uma das soluções é $\left(\frac{29-1}{2}\right)! = 14!$. Observe que:

$$14! = \underline{14 \cdot 13 \cdot 12 \cdot 11 \cdot 10} \cdot \underline{9 \cdot 8 \cdot 7 \cdot 6 \cdot 5} \cdot \underline{4 \cdot 3 \cdot 2} \equiv \underline{4} \cdot \underline{11} \cdot \underline{24} \equiv 12\ (mod\ 29).$$

Já a próxima solução incongruente será dada por $29 - 12 = 17$.

Um resultado estabelecido por Euler e importantíssimo para a Teoria de Congruências Quadráticas da forma $x^2 \equiv a\ (mod\ p)$ é o conhecido como Lema de Euler. Esta afirmação nos garante uma técnica para sabermos quando $x^2 \equiv a\ (mod\ p)$ terá solução para qualquer número a inteiro coprimo com p. Abaixo seguem o enunciado e a prova deste significante resultado.

Lema 4.1.11 (Lema de Euler)**.** Sejam p um número primo ímpar e a um número inteiro não divisível por p. Então:

i) $a^{\frac{p-1}{2}} \equiv \pm 1\ (mod\ p)$;

ii) $a^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$ se, e somente se, $x^2 \equiv a\ (mod\ p)$ tem solução.

Demonstração. Segue abaixo a prova dos respectivos itens.

i) Atente que, pelo Corolário 3.2.18,

$$\begin{aligned} \left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} &\equiv 1\ (mod\ p) \\ \left(a^{\frac{p-1}{2}}\right)^2 - 1 &\equiv 0\ (mod\ p) \\ \left(a^{\frac{p-1}{2}} + 1\right)\left(a^{\frac{p-1}{2}} - 1\right) &\equiv 0\ (mod\ p). \end{aligned}$$

Portanto, $p \Big| \left(a^{\frac{p-1}{2}} + 1\right)$ ou $p \Big| \left(a^{\frac{p-1}{2}} - 1\right)$, isto é,

$$a^{\frac{p-1}{2}} \equiv -1 \ (mod\ p) \text{ ou } a^{\frac{p-1}{2}} \equiv 1 \ (mod\ p).$$

ii) Suponhamos, por absurdo, que $x^2 \equiv a \ (mod\ p)$ não admita solução. A partir da Proposição 3.1.3 e do Corolário 3.1.8, decorre que a equação de congruência linear $bx \equiv a \ (mod\ p)$, com $b \in \{1, 2, ..., p-1\}$, possui exatamente uma única solução $c \in \{1, 2, ..., p-1\}$, pois $mdc(b, p) = 1$. Como a é um resíduo não-quadrático módulo p, é claro que $b \neq c$ (caso $b = c$, a equação $x^2 \equiv a \ (mod\ p)$ admite $x = b$ como solução - contrariando nossa hipótese). Vamos reescrever o conjunto $\{1, 2, ..., p-1\}$ como:

$$\{1, 2, ..., p-1\} = \left\{b_1, c_1, b_2, c_2, ..., b_{\frac{p-1}{2}}, c_{\frac{p-1}{2}}\right\},$$

tal que $b_i c_i \equiv a \ (mod\ p)$, para todo $i \in \left\{1, 2, ..., \frac{p-1}{2}\right\}$. Pelo Teorema de Wilson 3.2.30, obtemos:

$$\begin{aligned} -1 &\equiv (p-1)! = (p-1) \cdot (p-2) \cdots 2 \cdot 1 \ (mod\ p) \\ -1 &\equiv (b_{\frac{p-1}{2}} c_{\frac{p-1}{2}}) \cdot (b_{\frac{p-3}{2}} c_{\frac{p-3}{2}}) \cdots (b_2 c_2) \cdot (b_1 c_1) \ (mod\ p) \\ -1 &\equiv a \cdot a \cdots a = a^{\frac{p-1}{2}} \ (mod\ p). \end{aligned}$$

Reciprocamente, se a equação $x^2 \equiv a \ (mod\ p)$ admite solução, então existe $x_o \in \mathbb{Z}$ tal que $p \nmid x_o$ e $x_o^2 \equiv a \ (mod\ p)$. Assim,

$$a^{\frac{p-1}{2}} \equiv x_o^{p-1} \equiv 1 \ (mod\ p),$$

onde usamos a Proposição 2.1.10, para $\frac{p-1}{2}$, e o Pequeno Teorema de Fermat 3.2.18. □

Comentário 4.1.12. A partir do Lema de Euler 4.1.11, segue imediatamente que a condição necessária e suficiente para que a congruência quadrática $x^2 \equiv a \ (mod\ p)$ não admita solução é $a^{\frac{p-1}{2}} \equiv -1 \ (mod\ p)$.

O Lema de Euler 4.1.11 acabou respondendo definitivamente nosso segundo questionamento feito no início deste capítulo (Como identificar se $x^2 \equiv a \ (mod\ p)$ admite ou não solução?). Resta-nos verificar maneiras de encontrar uma solução. Antes disto, vamos ver alguns exemplos da aplicabilidade do referido lema.

Exemplo 4.1.13. A congruência quadrática $x^2 \equiv 5 \ (mod\ 13)$ não admite solução. De fato, observe que $\frac{13-1}{2} = 6$ e, assim,

$$5^6 = (5^2)^3 \equiv 12^3 \equiv (-1)^3 \equiv -1 \ (mod\ 13).$$

Portanto, pelo Comentário 4.1.12, $x^2 \equiv 5 \ (mod\ 13)$ não possui solução.

Exemplo 4.1.14. Considere a congruência quadrática $x^2 \equiv 8\ (mod\ 17)$. Verificaremos se tal congruência possui ou não solução. Repare que $\frac{17-1}{2} = 8$ e, assim,

$$8^8 = \underline{8^2 \cdot 8^2} \cdot \underline{8^2 \cdot 8^2} \equiv \underline{13^2} \cdot \underline{13^2} \equiv \underline{16} \cdot \underline{16} \equiv \underline{(-1)} \cdot \underline{(-1)} = 1\ (mod\ 17).$$

Portanto, pelo Lema de Euler 4.1.11, a congruência $x^2 \equiv 8\ (mod\ 17)$ admite solução. Por inspeção, descobre-se que $x = 5$ é uma solução e, então, $17 - 5 = 12$ é a outra solução incongruente.

Exemplo 4.1.15. Analisaremos se a congruência $x^2 \equiv 4\ (mod\ 7)$ admite solução. Note que $\frac{7-1}{2} = 3$ e, daí,

$$4^3 = 64 \equiv 1\ (mod\ 7).$$

Por conseguinte, segue do Lema de Euler 4.1.11 que a congruência admite solução, a saber $x = 2$ e $x = 7 - 2 = 5$.

Exemplo 4.1.16. Consideremos a congruência $x^2 \equiv 5\ (mod\ 17)$. Iremos verificar a existência ou inexistência de solução. Repare que $\frac{17-1}{2} = 8$ e, assim,

$$5^8 = \underline{5^2 \cdot 5^2} \cdot \underline{5^2 \cdot 5^2} \equiv \underline{8^2} \cdot \underline{8^2} \equiv 13^2 \equiv 16 \equiv -1\ (mod\ 17).$$

Portanto, pelo Comentário 4.1.12, a congruência $x^2 \equiv 8\ (mod\ 17)$ não admite solução.

Exemplo 4.1.17. Verificaremos se há solução para a congruência $x^2 \equiv 2\ (mod\ 5)$. Observe que $\frac{5-1}{2} = 2$ e com isso,

$$2^2 = 4 \equiv -1\ (mod\ 5).$$

Dessa forma, $x^2 \equiv 2\ (mod\ 5)$ não admite solução.

4.1.2 Símbolo de Legendre

Adrien Marie Legendre (1752-1833) foi um matemático que nasceu na França. Dentre todas as suas contribuições matemáticas, ele mais admirava aqueles trabalhos referentes a Integrais Elípticas e Teoria dos Números. (BOYER; MERZBACH, 2012).

Nesta subseção, abordaremos um dos trabalhos realizados por Legendre no ramo da Teoria dos Números, mais especificamente, o Símbolo de Legendre. Este importante conceito matemático nos fornece informações valiosas sobre a existência ou inexistência de soluções para congruêncais quadráticas do tipo $x^2 \equiv a\ (mod\ p)$, com p um número primo ímpar, por meio de resultados práticos e uma notação mais simples e sofisticada.

Definição 4.1.18. Sejam a e p números inteiros, com p primo ímpar e a não divisível por p. Definimos o *Símbolo de Legendre* por:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } a \text{ é um resíduo quadrático módulo } p \\ -1, & \text{se } a \text{ não é um resíduo quadrático módulo } p \end{cases}.$$

Exemplo 4.1.19. Nos Exemplos 4.1.14 e 4.1.15, vimos que 8 e 4 são resíduos quadráticos módulo 17 e 7, respectivamente. Assim, temos que:

$$\left(\frac{8}{17}\right) = \left(\frac{4}{7}\right) = 1.$$

Exemplo 4.1.20. Nos Exemplos 4.1.16 e 4.1.17, vimos que 5 e 2 não são resíduos quadráticos módulo 17 e 5. Sendo assim, temos que:

$$\left(\frac{5}{17}\right) = \left(\frac{2}{5}\right) = -1.$$

Observação 4.1.21. O Símbolo de Legendre é uma função. Ela está definida como:

$$\begin{aligned} f : (\mathbb{Z} - p\mathbb{Z}) \times P' &\rightarrow \{-1, 1\} \\ (a, p) &\mapsto \left(\frac{a}{p}\right), \end{aligned}$$

onde $p\mathbb{Z}$ e P' são os conjuntos dos múltiplos de p e dos números primos ímpares, respectivamente.

Teorema 4.1.22 (Critério de Euler)**.** Sejam p um número primo ímpar e a um número inteiro não divisível por p. Então,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (mod\ p).$$

Demonstração. Imediato do Lema de Euler 4.1.11. □

Comentário 4.1.23. O Critério de Euler 4.1.22 nos traduz que a condição necessária e suficiente para que a seja um resíduo quadrático módulo p é $\left(\frac{a}{p}\right) = 1$. Inclusive, temos que se $\left(\frac{a}{p}\right) = -1$, então a é um resíduo não-quadrático módulo p e vice-versa.

Proposição 4.1.24. Sejam a, b, p números inteiros, com p primo ímpar e a, b não divisíveis por p. Então:

i) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$;

ii) $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{se } p \equiv 1 \ (mod\ 4) \\ -1, & \text{se } p \equiv 3 \ (mod\ 4) \end{cases}$;

iii) Se $a \equiv b \ (mod\ p)$, então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

iv) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$;

v) $\left(\frac{a^2}{p}\right) = 1$.

Demonstração. Segue abaixo as demonstração de cada item.

i) Pelo Critério de Euler 4.1.22, $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}\ (mod\ p)$. Repare que $\left(\frac{-1}{p}\right) = \pm 1$ e $(-1)^{\frac{p-1}{2}} = \pm 1$. Como p é um primo ímpar, não é possível que $1 \equiv -1\ (mod\ p)$ e assim tem-se igualdade $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

ii) Pelo fato de p ser um número primo ímpar, então temos duas possibilidades de escrevê-lo quando dividido por 4; a saber $p = 4k_1 + 1$ ou $p = 4k_2 + 3$, para algum $k_1, k_2 \in \mathbb{Z}$. No primeiro caso, tem-se $p \equiv 1\ (mod\ 4)$ e, pela Proposição 4.1.8, $x^2 \equiv -1\ (mod\ p)$ admite solução. Logo, $\left(\frac{-1}{p}\right) = 1$. No segundo caso, tem-se $p \equiv 3\ (mod\ 4)$, ou melhor, $p - 1 \equiv 2\ (mod\ 4)$. Então, existe $y \in \mathbb{Z}$ tal que $p - 1 = 2(2y + 1)$. Sendo assim, $\frac{p-1}{2} = 2y + 1$, ou seja, é um número ímpar. Logo, $(-1)^{\frac{p-1}{2}} = -1 = \left(\frac{-1}{p}\right)$.

iii) Se $a \equiv b\ (mod\ p)$, então, pela Proposição 2.1.10, $a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}}\ (mod\ p)$. Pelo Critério de Euler 4.1.22, decorre $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ (mod\ p)$ e $\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}}\ (mod\ p)$, ou seja, $\left(\frac{a}{p}\right) \equiv \left(\frac{b}{p}\right)\ (mod\ p)$. Como $\left(\frac{a}{p}\right) = \pm 1$, $\left(\frac{b}{p}\right) = \pm 1$ e p é primo ímpar; implica na igualdade $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

iv) Basta observar, pelo Critério de Euler 4.1.22, que:

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)\ (mod\ p).$$

Como $\left(\frac{ab}{p}\right) = \pm 1$, $\left(\frac{a}{p}\right) = \pm 1$, $\left(\frac{b}{p}\right) = \pm 1$ e p é primo ímpar, tem-se a igualdade

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

v) Basta reparar que $x^2 \equiv a^2\ (mod\ p)$ sempre admite $x = a$ como solução, logo $\left(\frac{a^2}{p}\right) = 1$. □

Comentário 4.1.25. Se a é um número inteiro não divisível pelo número primo ímpar p e sua fatoração primária é $a = \pm 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, com $p_1, p_2, ..., p_k$ números primos ímpares distintos e $\alpha_0, \alpha_1, \alpha_2, ..., \alpha_k$ números naturais. Então, decorre do item (iv) da Proposição 4.1.24 que:

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right) \cdot \left(\frac{2}{p}\right)^{\alpha_0} \cdot \left(\frac{p_1}{p}\right)^{\alpha_1} \cdot \left(\frac{p_2}{p}\right)^{\alpha_2} \cdots \left(\frac{p_k}{p}\right)^{\alpha_k}.$$

Podemos eliminar, caso haja, todos os expoentes pares (pois todos serão iguais a 1 por conta do item (v) da Proposição 4.1.24). Logo, para conhecer $\left(\frac{a}{p}\right)$, basta conhecer $\left(\frac{\pm 1}{p}\right)$ e, para os termos cujo o expoente não é par, $\left(\frac{2}{p}\right)$ e $\left(\frac{p_i}{p}\right)$, para todo p_i número primo ímpar diferente de p, onde $i \in \{1, 2, ..., k\}$.

Já conhecemos $\left(\frac{\pm 1}{p}\right)$. Vamos, a partir de agora, buscar resultados que nos forneçam informações sobre $\left(\frac{2}{p}\right)$ e $\left(\frac{q}{p}\right)$ para todo q primo ímpar diferente de p.

Mostraremos duas afirmações que se farão necessárias para começarmos a entender o Símbolo de Legendre $\left(\frac{2}{p}\right)$.

Afirmação 4.1.26. Sejam p um número primo ímpar e k um número natural. Então,

i) Se k é par, então $k \equiv k(-1)^k (mod\ p)$;

ii) Se k é ímpar, então $p - k \equiv k(-1)^k\ (mod\ p)$;

Demonstração. Segue abaixo a demonstração de cada um dos itens.

i) Veja que $k - k$ é um múltiplo de p. Além disso, $k - k(-1)^k$ continua sendo múltiplo de p uma vez que $(-1)^k = 1$ por k ser par. Portanto, segue que $k \equiv k(-1)^k\ (mod\ p)$.

ii) Veja que $(p - k) + k$ é um múltiplo de p. Além disso, $(p - k) - k(-1)^k$ continua sendo múltiplo de p uma vez que $(-1)^k = -1$ por k ser ímpar. Portanto, segue que $p - k \equiv k(-1)^k\ (mod\ p)$. □

Afirmação 4.1.27. Seja p um número primo ímpar. Então:

i) Se $p \equiv 1\ (mod\ 8)$ ou $p \equiv 7\ (mod\ 8)$, então $\frac{p^2-1}{8}$ é par;

ii) Se $p \equiv 3\ (mod\ 8)$ ou $p \equiv 5\ (mod\ 8)$, então $\frac{p^2-1}{8}$ é ímpar.

Demonstração. Segue abaixo a demonstração dos respectivos itens.

i) Basta reparar que $p = 8k_1 + 1$ ou $p = 8k_2 + 7$, para algum $k_1, k_2 \in \mathbb{Z}$. Além disso,

$$\frac{p^2 - 1}{8} = \frac{(p+1)(p-1)}{8}.$$

(1º caso) Quando $p = 8k_1 + 1$, tem-se:

$$\frac{(p+1)(p-1)}{8} = \frac{(8k_1 + 2)(8k_1)}{8} = 2k_1(4k_1 + 1).$$

(2º caso) Quando $p = 8k_2 + 7$, tem-se:

$$\begin{aligned} \frac{(p+1)(p-1)}{8} &= \frac{(8k_2 + 8)(8k_2 + 6)}{8} \\ &= (k_2 + 1)(8k_2 + 6) \\ &= 2(k_2 + 1)(4k_2 + 3). \end{aligned}$$

Portanto, $\frac{p^2-1}{8}$ é par.

ii) Basta reparar que $p = 8k_1 + 3$ ou $p = 8k_2 + 5$, para algum $k_1, k_2 \in \mathbb{Z}$. Além disso,

$$\frac{p^2-1}{8} = \frac{(p+1)(p-1)}{8}.$$

(1º caso) Quando $p = 8k_1 + 3$, tem-se:

$$\begin{aligned}\frac{(p+1)(p-1)}{8} &= \frac{(8k_1+4)(8k_1+2)}{8} \\ &= \frac{64k_1^2+48k_1+8}{8} \\ &= 8k_1^2+6k_1+1 = 2(4k_1^2+3k_1)+1.\end{aligned}$$

(2º caso) Quando $p = 8k_2 + 5$, tem-se:

$$\begin{aligned}\frac{(p+1)(p-1)}{8} &= \frac{(8k_2+6)(8k_2+4)}{8} \\ &= \frac{64k_2^2+80k_2+24}{8} \\ &= 8k_2^2+10k_2+3 = 2(4k_2+5k_2+1)+1.\end{aligned}$$

Portanto, $\frac{p^2-1}{8}$ é ímpar. □

Agora podemos provar um resultado que mostra quando 2 é ou não um resíduo quadrático módulo p, com p um número primo ímpar.

Teorema 4.1.28. Para p um número primo ímpar, temos:

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{se } p \equiv 1 \ (mod\ 8) \text{ ou } p \equiv 7 \ (mod\ 8) \\ -1, & \text{se } p \equiv 3 \ (mod\ 8) \text{ ou } p \equiv 5 \ (mod\ 8) \end{cases}.$$

Demonstração. Pelo Critério de Euler 4.1.22, temos $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \ (mod\ p)$. Consideremos as seguintes $\frac{p-1}{2}$ congruências abaixo (que existem por conta da Afirmação 4.1.26).

$$\begin{aligned} p-1 &\equiv 1(-1)^1 \ (mod\ p) && (4.1)\\ 2 &\equiv 2(-1)^2 \ (mod\ p) && (4.2)\\ p-3 &\equiv 3(-1)^3 \ (mod\ p) && (4.3)\\ 4 &\equiv 4(-4)^4 \ (mod\ p) && (4.4)\\ &\vdots \\ k &\equiv \frac{p-1}{2}(-1)^{\frac{p-1}{2}} \ (mod\ p). && (4.5)\end{aligned}$$

Se $\frac{p-1}{2}$ é par, então podemos reescrever a última congruência da lista acima como:

$$k = \frac{p-1}{2} \equiv \frac{p-1}{2}(-1)^{\frac{p-1}{2}} \ (mod\ p).$$

Caso contrário, se $\frac{p-1}{2}$ é ímpar, então

$$k = p - \frac{p-1}{2} \equiv \frac{p-1}{2}(-1)^{\frac{p-1}{2}} \ (mod\ p).$$

Observe que o lado esquerdo das Congruências de (4.1) até (4.5) são todos pares. Se multiplicarmos essas $\frac{p-1}{2}$ congruências membro a membro, teremos:

$$2 \cdot 4 \cdots (p-3) \cdot (p-1) \equiv (-1)^{1+2+3+\cdots+\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \ (mod\ p). \tag{4.6}$$

Afirmação X: O produto dos primeiros $\frac{p-1}{2}$ números naturais pares não nulos, onde p é primo ímpar, é igual à $2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$.

De fato, basta observar que $2 \cdot 4 \cdots (p-3) \cdot (p-1) = 2 \cdot 4 \cdots 2\left(\frac{p-3}{2}\right) \cdot 2\left(\frac{p-1}{2}\right)$. Portanto,

$$2 \cdot 4 \cdots 2\left(\frac{p-3}{2}\right) \cdot 2\left(\frac{p-1}{2}\right) = 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!.$$

Afirmação Y: A soma dos $\frac{p-1}{2}$ primeiros números naturais não nulos, onde p é primo ímpar, é igual à $\frac{p^2-1}{8}$.

De fato, basta observar que:

$$\begin{aligned}
1 + 2 + \cdots + \frac{p-3}{2} + \frac{p-1}{2} &= \frac{\overbrace{2 + 4 + \cdots + (p-3) + (p-1)}^{\frac{p-1}{2} \text{ elementos.}}}{2} \\
&= \frac{\overbrace{(p+1) + (p+1) + \cdots + (p+1) + (p+1)}^{\frac{p-1}{4} \text{ elementos.}}}{2} \\
&= \frac{\frac{(p-1)}{4}(p+1)}{2} \\
&= \frac{(p-1)(p+1)}{8} = \frac{p^2-1}{8}.
\end{aligned}$$

Pelas afirmações X e Y, a Congruência (4.6) fica escrita como:

$$2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{p^2-1}{8}} \left(\frac{p-1}{2}\right)! \ (mod\ p).$$

Como $mdc\left(\left(\frac{p-1}{2}\right)!, p\right) = 1$, segue pelo item (iv) da Proposição 2.1.7 que

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \ (mod\ p).$$

Assim, pela transitividade das congruência, tem-se que

$$\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}} \ (mod\ p).$$

Como ambos os membros desta congruência assumem valores 1 ou -1 e sabemos que $1 \not\equiv -1 \ (mod\ p)$ (pois p primo ímpar), decorre a igualdade abaixo.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

A partir daí, do item (i) da Afirmação 4.1.27, temos que $\frac{p^2-1}{8}$ é par quando ocorre de $p \equiv 1 \ (mod\ 8)$ ou $p \equiv 7 \ (mod\ 8)$. Do item (ii) da Afirmação 4.1.27, temos que $\frac{p^2-1}{8}$ é ímpar quando ocorre de $p \equiv 3 \ (mod\ 8)$ ou $p \equiv 5 \ (mod\ 8)$. Portanto,

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{se } p \equiv 1 \ (mod\ 8) \text{ ou } p \equiv 7 \ (mod\ 8) \\ -1, & \text{se } p \equiv 3 \ (mod\ 8) \text{ ou } p \equiv \ 5 \ (mod\ 8) \end{cases}.$$

□

Exemplo 4.1.29. Vamos verificar se 2 é um resíduo quadrático módulo 41. Repare que $41 \equiv 1 \ (mod\ 8)$ e, então, pelo Teorema 4.1.28, $\left(\frac{2}{41}\right) = 1$. Consequentemente, 2 é um resíduo quadrático módulo 41.

Exemplo 4.1.30. Verificaremos se $x^2 \equiv 2 \ (mod\ 101)$ admite solução. Atente que $101 \equiv 5 \ (mod\ 8)$ e, então, pelo Teorema 4.1.28, $\left(\frac{2}{101}\right) = -1$. Consequentemente, 2 é um resíduo não-quadrático módulo 101.

4.2 Lei da Reciprocidade Quadrática Gaussiana

Iremos agora em busca de compreender o Símbolo de Legendre $\left(\frac{q}{p}\right)$, para q e p números primos ímpares distintos. Ressaltamos que o resultado principal que nos fornecerá o método de calcular tal Símbolo de Legendre é chamado Lei da Reciprocidade Quadrática de Gauss.

Existem muitas demonstrações para essa lei e só 8 são de autoria do próprio Gauss. Mencionamos também que tal relação já era de conhecimento dos matemáticos Euler e Legendre. (SANTOS, 2020).

Lema 4.2.1 (Lema de Gauss)**.** Sejam p um número primo ímpar e a um número inteiro não divisível por p. Consideremos os menores resíduos positivos dos números inteiros

$$a, 2a, 3a, ..., \frac{p-1}{2}a.$$

Se l for o número destes resíduos que são maiores do que $\frac{p}{2}$, então,

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

Demonstração. Como $p \nmid a$, segue que nenhum múltiplo da forma ia, com $1 \leqslant i \leqslant p-1$, será divisível por p. De fato, se ia fosse divisível por p, então existiria um número inteiro q tal que $ia = qp$. Além disso, $mdc(i,p) = 1$ porque i não é múltiplo de p (pois $0 < i < p$). Logo, pela Proposição 2.1.7, $p|a$ contrariando nossa hipótese.

A partir disso, aplicando a Divisão Euclidiana 1.1.13 de cada um dos elementos do conjunto $A = \left\{a, 2a, ..., \frac{p-1}{2}a\right\}$ por p, existiram $q_j, r_j \in \mathbb{Z}$ tais que:

$$ja = pq_j + r_j, \text{com } 1 \leqslant r_j \leqslant p-1 \text{ e } j \in \left\{1, 2, ..., \frac{p-1}{2}\right\}.$$

Então o conjunto dos restos destas divisões será $R = \{r_1, r_2, ..., r_{\frac{p-1}{2}}\}$. Tomamos $m_1, m_2, ..., m_k$, números de R que são menores do que $\frac{p}{2}$, e $n_1, n_2, ..., n_l$, números de R maiores do que $\frac{p}{2}$; onde $k + l = \frac{p-1}{2}$. Estes números existem! De fato, basta observar que $1 \leqslant r_j < \frac{p}{2}$ ou $\frac{p}{2} < r_j \leqslant p-1$ (pois $1 \leqslant r_j \leqslant p-1$). Assim, obtém-se $R = \{r_1, r_2, ..., r_{\frac{p-1}{2}}\} = \{m_1, m_2, ..., m_k, n_1, n_2, ..., n_l\}$.

Consideremos, a partir de agora, o seguinte conjunto:

$$S = \{m_1, m_2, ..., m_k, p-n_1, p-n_2, ..., p-n_l\}.$$

Temos $1 \leqslant m_u$ (porque isto ocorre com os $r_j's$) e $p - n_t < \frac{p}{2}$ (pois $n_t > \frac{p}{2}$), com $u \in \{1, 2, ..., k\}$ e $t \in \{1, 2, ..., l\}$. Como os $r_j's$ são todos distintos, temos que $m_u's$ também o são, assim como os números $p - n_t$.

Afirmação: $m_u \neq p - n_t$, para todo $u \in \{1, 2, ..., k\}$ e $t \in \{1, 2, ..., l\}$.

Suponhamos por absurdo que $m_u = p - n_t$. Assim, $m_u + n_t = p$ e ainda, pela Observação 2.1.32, existem $j_1, j_2 \in \left\{1, 2, ..., \frac{p-1}{2}\right\}$ tais que $j_1 a \equiv m_u \ (mod\ p)$ e $j_2 a \equiv n_t \ (mod\ p)$. Donde decorre a congruência abaixo:

$$p = m_u + n_t \equiv (j_1 + j_2)a \ (mod\ p), \text{com } 1 \leqslant j_1 + j_2 \leqslant p-1,$$

o que é um absurdo!

Diante disto, concluímos $S = \left\{1, 2, ..., \frac{p-1}{2}\right\}$ e,

$$\begin{aligned} \left(\frac{p-1}{2}\right)! &= m_1 m_2 \cdots m_k (p-n_1)(p-n_2)\cdots(p-n_l) \\ &\equiv m_1 m_2 \cdots m_k n_1 n_2 \cdots n_l (-1)^l \ (mod\ p), \end{aligned}$$

pois $p - n_t \equiv -n_t \ (mod\ p)$. Além do mais, $m_1 m_2 \cdots m_k n_1 n_2 \cdots n_l = r_1 r_2 \cdots r_{\frac{p-1}{2}}$. Donde segue,

$$\begin{aligned} m_1 m_2 \cdots m_k n_1 n_2 \cdots n_l (-1)^l &\equiv r_1 r_2 \cdots r_{\frac{p-1}{2}} (-1)^l \ (mod\ p) \\ &\equiv a \cdot 2a \cdots \frac{p-1}{2}a \cdot (-1)^l = \left(\frac{p-1}{2}\right)! \cdot a^{\frac{p-1}{2}} \cdot (-1)^l \ (mod\ p). \end{aligned}$$

Portanto,

$$\left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! \cdot a^{\frac{p-1}{2}} \cdot (-1)^l \ (mod\ p).$$

Repare que $mdc\left(\left(\frac{p-1}{2}\right)!, p\right) = 1$ e, consequentemente,

$$\begin{aligned} 1 \equiv a^{\frac{p-1}{2}} \cdot (-1)^l \ (mod\ p) &\Leftrightarrow a^{\frac{p-1}{2}} \equiv a^{p-1} \cdot (-1)^l \ (mod\ p) \\ &\Leftrightarrow a^{\frac{p-1}{2}} \equiv \underline{a^{p-1}} \cdot (-1)^l \equiv \underline{1} \cdot (-1)^l \ (mod\ p), \end{aligned}$$

onde está sublinhado foi utilizado o Pequeno Teorema de Fermat 3.2.18.

Por fim, pelo Critério de Euler 4.1.22, possuímos a seguinte congruência,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (mod\ p).$$

Pela transitividade da relação de congruência, decorre

$$\left(\frac{a}{p}\right) \equiv (-1)^l \ (mod\ p).$$

Como p é um número primo ímpar, $\left(\frac{a}{p}\right) = \pm 1$ e $(-1)^l = \pm 1$; obtém-se que $\left(\frac{a}{p}\right) = (-1)^l$. □

Exemplo 4.2.2. Consideremos o número primo 7 e o número inteiro 18. É claro que $7 \nmid 18$. Além disso, sejam 18, $2 \cdot 18$ e $3 \cdot 18$. Note que

$$\begin{aligned} 18 &= 7 \cdot 2 + 4; \\ 2 \cdot 18 &= 7 \cdot 5 + 1; \\ 3 \cdot 18 &= 7 \cdot 7 + 5. \end{aligned}$$

Temos dois restos, e apenas dois, que são maiores do que $\frac{7}{2}$. Portanto, pelo Lema de Gauss 4.2.1,

$$\left(\frac{18}{7}\right) = (-1)^2 = 1.$$

Sendo assim, a congruência $x^2 \equiv 18 \equiv 4 \ (mod\ 7)$ admite solução.

Agora iremos definir um conceito importante para podermos demonstrar o próximo lema e a própria Lei da Reciprocidade Quadrática Gaussiana.

Definição 4.2.3. O "maior inteiro" é uma função que associa a cada número real x ao maior número inteiro menor do que ou igual à x. Denotamos por $\lfloor x \rfloor$.

Observação 4.2.4. A função do "maior inteiro" é chamada de função chão ou função piso.

Exemplo 4.2.5. O maior inteiro menor do que ou igual à 7 é $\lfloor 7 \rfloor = 7$.

Exemplo 4.2.6. O maior inteiro menor do que ou igual à $\frac{3}{2}$ é $\left\lfloor \frac{3}{2} \right\rfloor = 1$.

Exemplo 4.2.7. O maior inteiro menor do que ou igual à $-\pi$ é $\lfloor -\pi \rfloor = -4$.

Exemplo 4.2.8. O maior inteiro menor do que ou igual à $-\sqrt{5}$ é $\left\lfloor -\sqrt{5} \right\rfloor = -3$.

Lema 4.2.9. Se a e p são números inteiros ímpares, com p primo e a não-divisível por p, então,

$$\left(\frac{a}{p}\right) = (-1)^M,$$

onde $M = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor$.

Demonstração. Aplicando a Divisão Euclidiana 1.1.13 de cada um dos elementos do conjunto $A = \left\{a, 2a, ..., \frac{p-1}{2}a\right\}$ por p, existiram $q_j, r_j \in \mathbb{Z}$ tais que:

$$ja = pq_j + r_j, \text{com } 0 < r_j < p \text{ e } j \in \left\{1, 2, ..., \frac{p-1}{2}\right\}. \tag{4.7}$$

Dividindo a igualdade e a desigualdade por p, tem-se

$$\frac{ja}{p} = q_j + \frac{r_j}{p}, \text{com } 0 < \frac{r_j}{p} < 1 \text{ e } j \in \left\{1, 2, ..., \frac{p-1}{2}\right\}.$$

Repare que $\left\lfloor \frac{ja}{p} \right\rfloor = q_j$. Assim, podemos reescrever as Equações (4.7) como:

$$ja = p\left\lfloor \frac{ja}{p} \right\rfloor + r_j, \text{com } 0 < r_j < p \text{ e } j \in \left\{1, 2, ..., \frac{p-1}{2}\right\}. \tag{4.8}$$

Por outro lado, pelo Lema de Gauss 4.2.1, $\left(\frac{a}{p}\right) = (-1)^l$, onde l é o número de resíduos maiores do que $\frac{p}{2}$. Mostraremos que $\left(\frac{a}{p}\right) = (-1)^l = (-1)^M$, mas, para isto, devemos provar que $l \equiv M \ (mod\ 2)$, isto é, l e M possuem a mesma paridade (ambos são pares ou ambos são ímpares).

Somando as Equações de (4.8),obtemos

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor p + \sum_{j=1}^{\frac{p-1}{2}} r_j,$$

que equivale à

$$a\sum_{j=1}^{\frac{p-1}{2}} j = p\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor + \sum_{u=1}^{k} m_u + \sum_{t=1}^{l} n_t, \tag{4.9}$$

pois, como vimos na demonstração do Lema de Gauss 4.2.1, $R = \{r_1, r_2, ..., r_{\frac{p-1}{2}}\} = \{m_1, m_2, ..., m_k, n_1, n_2, ..., n_l\}$, onde $m_1, m_2, ..., m_k$ e $n_1, n_2, ..., n_l$ são os resíduos módulo p menores e maiores do que $\frac{p}{2}$, respectivamente.

A partir da Igualdade (4.9),

$$\begin{aligned} a\sum_{j=1}^{\frac{p-1}{2}} j &= p\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor + \sum_{u=1}^{k} m_u + \sum_{t=1}^{l}(p - n_t + 2n_t - p) \\ &= p\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor + \sum_{u=1}^{k} m_u + \sum_{t=1}^{l}(p - n_t) + 2\sum_{t=1}^{l} n_t - p\sum_{t=1}^{l} 1 \\ &= p\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor + \sum_{u=1}^{k} m_u + \sum_{t=1}^{l}(p - n_t) + 2\sum_{t=1}^{l} n_t - lp. \end{aligned} \tag{4.10}$$

Também vimos na demonstração do Lema de Gauss 4.2.1 que $S = \{m_1, m_2, ..., m_k, p - n_1, p - n_2, ..., p - n_l\} = \left\{1, 2, ..., \frac{p-1}{2}\right\}$. Logo, a Igualdade (4.10) fica

$$a\sum_{j=1}^{\frac{p-1}{2}} j = p\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor + \sum_{j=1}^{\frac{p-1}{2}} j + 2\sum_{t=1}^{l} n_t - lp.$$

Logo,

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = p\left[\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor - l\right] + 2\sum_{t=1}^{l} n_t.$$

Atente que $a - 1$ é par (pois a é ímpar) e p é ímpar, o que podemos concluir

$$\begin{aligned} 0 &\equiv (a-1)\sum_{j=1}^{\frac{p-1}{2}} j \ (mod\ 2) \\ &\equiv p\left[\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor - l\right] + 2\sum_{t=1}^{l} n_t \ (mod\ 2) \\ &\equiv p\left[\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor - l\right] \ (mod\ 2). \end{aligned} \tag{4.11}$$

Como $mdc(p, 2) = 1$ e $0 = p \cdot 0$, podemos eliminar p da Igualdade (4.11), isto é,

$$0 \equiv \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor - l \ (mod\ 2).$$

donde

$$l \equiv M \ (mod\ 2).$$

Isto conclui a demonstração! □

Finalmente estamos prontos para enunciar e demonstrar a Lei da Reciprocidade Quadrática Gaussiana.

A prova que forneceremos aqui é devido ao matemático Eisenstein (1823-1852) e nela há elementos geométricos que facilitam nossa compreensão. (SANTOS, 2020).

Teorema 4.2.10 (Lei da Reciprocidade Quadrática Gaussiana)**.** Sejam q e p números inteiros primos distintos. Então vale que

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Demonstração. Consideremos o retângulo $ABCD$ determinado pelos vértices $A(0,0)$, $B\left(\frac{p}{2},0\right)$, $C\left(\frac{p}{2},\frac{q}{2}\right)$ e $D\left(0,\frac{q}{2}\right)$, conforme na Figura 9.

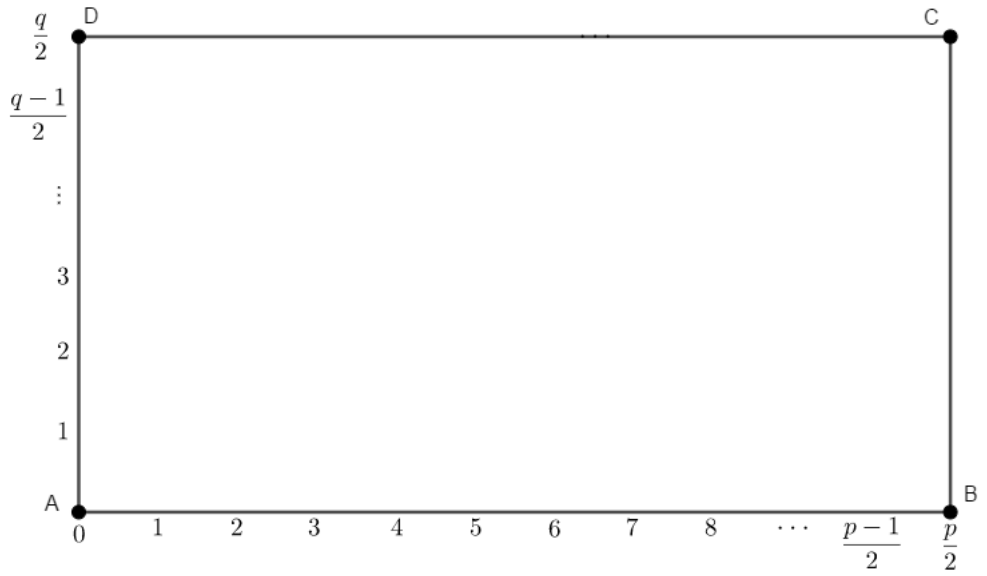


Figura 9 – Retângulo de comprimento $\frac{p}{2}$ e largura $\frac{q}{2}$.

Marcamos agora os pontos internos a este retângulo que pertencem ao produto cartesiano $X \times Y$, onde $X = \left\{1, 2, ..., \frac{p-1}{2}\right\}$ e $Y = \left\{1, 2, ..., \frac{q-1}{2}\right\}$, como visto na Figura 10. É claro que a quantidade de elementos internos a este retângulo é igual à:

$$\frac{p-1}{2} \cdot \frac{q-1}{2}. \tag{4.12}$$

A partir de agora, consideremos a equação da reta que passa pelos pontos A e C (diagonal do retângulo $ABDC$), a saber $y = \frac{q}{p}x$, de acordo com a Figura 11.

Repare que $mdc\,(p, i) = 1$, para todo $i \in X$. Logo, a reta $y = \frac{q}{p}x$ não conterá se quer um ponto de $X \times Y$.

A reta $y = \frac{q}{p}x$ intersectará as retas $x = k$ (retas paralelas aos lados AD e BC do retângulo), nos pontos $\left(k, \frac{q}{p}k\right)$, onde $k \in X$.

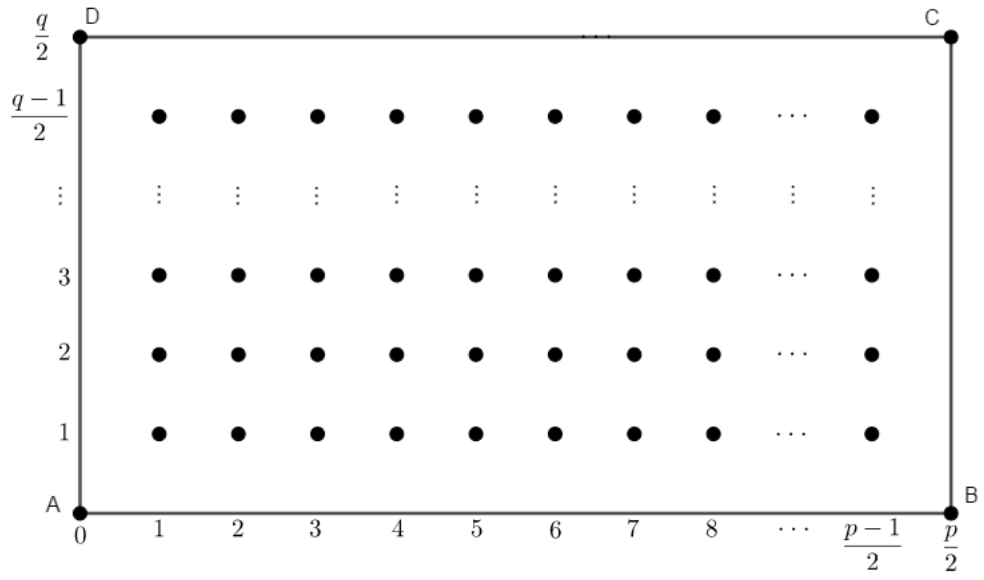


Figura 10 – Retângulo $ABCD$ com os pontos internos.

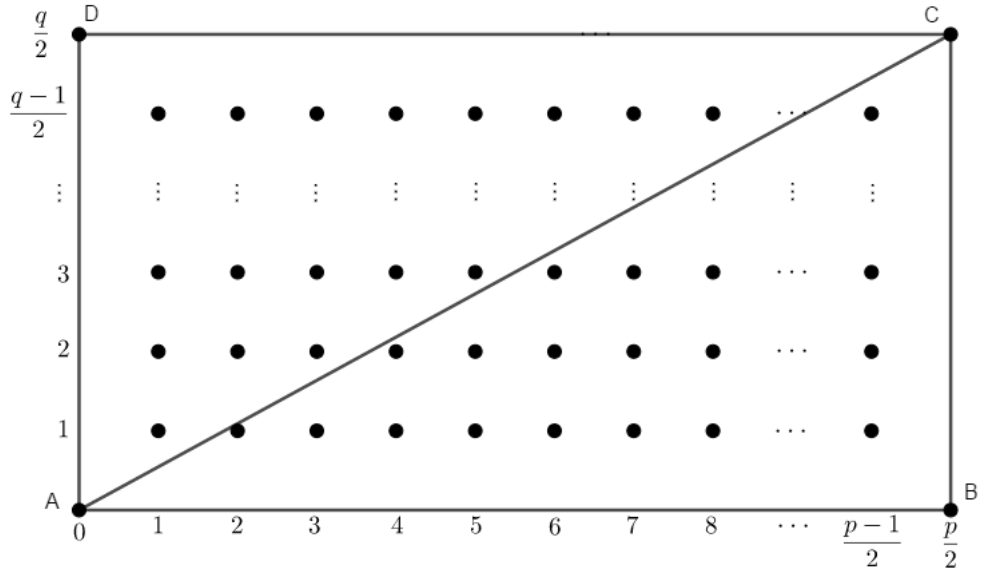


Figura 11 – Retângulo $ABCD$ com sua diagonal.

Como $\frac{q}{p}k$ não é um inteiro, temos que $\left\lfloor \frac{q}{p}k \right\rfloor$ será a quantidade de pontos internos ao retângulo que pertencem a reta $x = k$ e estão acima do segmento AB e abaixo da reta y.

Logo, o número de pontos internos ao triângulo ABC será igual à:

$$M = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{qk}{p} \right\rfloor. \tag{4.13}$$

De forma análoga, considerando as interseção entre $y = \frac{q}{p}x$ e as retas $y = l$, onde

$l \in Y$, obteremos que a quantidade de pontos internos ao triângulo ACD é igual à:

$$N = \sum_{l=1}^{\frac{q-1}{2}} \left\lfloor \frac{ql}{p} \right\rfloor. \tag{4.14}$$

Sendo assim, das Igualdades (4.12), (4.13) e (4.14), segue

$$M + N = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Aplicando o Lema 4.2.9, temos:

$$\left(\frac{p}{q}\right) = (-1)^M \quad \text{e} \quad \left(\frac{q}{p}\right) = (-1)^N.$$

Donde obtém-se:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^M(-1)^N = (-1)^{M+N} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

□

Observação 4.2.11. Repare nas seguintes equivalências:

$$\begin{aligned}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} &\Leftrightarrow \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)^2 = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)\\ &\Leftrightarrow \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right).\end{aligned}$$

Exemplo 4.2.12. Vamos calcular o Símbolo de Legendre $\left(\frac{680}{71}\right)$. Observe que a fatoração primária de 680 é igual à $2^3 \cdot 5 \cdot 17$. Assim,

$$\left(\frac{680}{71}\right) = \left(\frac{2^3 \cdot 5 \cdot 17}{71}\right) = \left(\frac{2}{71}\right)^3\left(\frac{5}{71}\right)\left(\frac{17}{71}\right).$$

Atente que $71 \equiv 7 \ (mod\ 8)$, então, pela Proposição 4.1.28, $\left(\frac{2}{71}\right) = 1$. Precisamos encontrar $\left(\frac{5}{71}\right)$ e $\left(\frac{17}{71}\right)$. Para isto, utilizamos a Lei da Reciprocidade Quadrática de Gauss.

$$\begin{aligned}\left(\frac{5}{71}\right) &= (-1)^{\frac{5-1}{2}\frac{71-1}{2}}\left(\frac{71}{5}\right)\\ &= (-1)^{70}\left(\frac{1}{5}\right)\\ &= 1 \cdot 1 = 1,\end{aligned}$$

já,

$$\begin{aligned}\left(\frac{17}{71}\right) &= (-1)^{\frac{17-1}{2}\frac{71-1}{2}}\left(\frac{71}{17}\right)\\ &= (-1)^{280}\left(\frac{3}{17}\right)\\ &= 1 \cdot (-1)^{\frac{3-1}{2}\frac{17-1}{2}}\left(\frac{17}{3}\right)\\ &= (-1)^8\left(\frac{2}{3}\right)\\ &= -1,\end{aligned}$$

pois $3 \equiv 3 \ (mod\ 8)$ e, pelo Teorema 4.1.28, $\left(\frac{2}{3}\right) = -1$.

Portanto,

$$\left(\frac{680}{71}\right) = \left(\frac{2}{71}\right)^3 \left(\frac{5}{71}\right)\left(\frac{17}{71}\right) = 1^3 \cdot 1 \cdot (-1) = -1.$$

Sendo assim, a congruência $x^2 \equiv 680 \ (mod\ 71)$ não admite solução.

Exemplo 4.2.13. Calcularemos o Símbolo de Legendre $\left(\frac{-280}{17}\right)$. Repare que a fatoração primária de $-280 = -1 \cdot 2^3 \cdot 5 \cdot 7$. Logo,

$$\left(\frac{-280}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{2}{17}\right)^3 \left(\frac{5}{17}\right)\left(\frac{7}{17}\right).$$

Atente que $17 \equiv 1 \ (mod\ 4)$. Assim, pelo item (ii) da Proposição 4.1.24, $\left(\frac{-1}{17}\right) = 1$. Além disso, $17 \equiv 1 \ (mod\ 8)$ donde segue, pela Proposição 4.1.28, que $\left(\frac{2}{17}\right) = 1$. Resta-nos encontrar $\left(\frac{5}{17}\right)$ e $\left(\frac{7}{17}\right)$. Para isto, utilizaremos a Lei da Reciprocidade Quadrática.

$$\begin{aligned}\left(\frac{5}{17}\right) &= (-1)^{\frac{5-1}{2}\frac{17-1}{2}}\left(\frac{17}{5}\right)\\ &= (-1)^{16}\left(\frac{2}{5}\right)\\ &= 1 \cdot (-1) = -1,\end{aligned}$$

já que $5 \equiv -3 \ (mod\ 8)$ e, pela Proposição 4.1.28, $\left(\frac{2}{5}\right) = -1$. Agora,

$$\begin{aligned}\left(\frac{7}{17}\right) &= (-1)^{\frac{7-1}{2}\frac{17-1}{2}}\left(\frac{17}{7}\right)\\ &= (-1)^{24}\left(\frac{3}{7}\right)\\ &= 1 \cdot (-1)^{\frac{3-1}{2}\frac{7-1}{2}}\left(\frac{7}{3}\right)\\ &= (-1)^3\left(\frac{1}{3}\right)\\ &= (-1) \cdot 1 = -1.\end{aligned}$$

Logo,

$$\left(\frac{-280}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{2}{17}\right)^3 \left(\frac{5}{17}\right)\left(\frac{7}{17}\right) = 1 \cdot (1)^3 \cdot (-1) \cdot (-1) = 1.$$

Portanto, a congruência $x^2 \equiv -280 \ (mod\ 17)$ admite solução, a saber $x_1 = 4$ e $x_2 = p - x_1 = 17 - 4 = 13$.

5 Conclusão

Após todo o estudo realizado neste trabalho, entende-se que a noção de congruência é substancialmente imprescindível para a Teoria dos Números, já que nos possibilita inferirmos propriedades para o conjunto $\mathbb{Z}$ dos números inteiros. Ademais, proporciona sabermos/discutirmos sobre os fenômenos cíclicos que nos rodeiam, pois estão conectados com o referido conceito.

Um outro ponto debatido no corpo deste trabalho é a respeito da atividade didática (Capítulo 2), que envolveu o conceito de congruência aplicado a situações problemas de fenômenos cíclicos. Esta atividade proporcionou, desde sua estruturação até a aplicação, um enriquecimento de como ser professor, bem como, tornar-se crítico com os problemas aplicados em sala de aula. Também permitiu/favoreceu o pensamento matemático de ideias mais complexas (neste caso, congruências) para serem trabalhadas no Ensino Básico por meio de ferramentas mais simples (operações básicas).

No âmbito das congruências lineares, desenvolvido no Capítulo 3, foi possível modelar problemas aritméticos envolvendo os restos das divisões dos números inteiros e compreender certas propriedades destes números. Inclusive, pudemos vislumbrar o Teorema de Wilson, que nos garantiu um teste de primalidade diante da caracterização dos números primos. Isto desenvolveu conhecimentos grandiosos porque expandiu nossos pensamentos algébricos.

Por fim, mas não menos importante, discorreu-se sobre congruências de grau 2 ou também chamadas de congruências quadráticas (Capítulo 4). Neste espaço, estabelecemos os principais resultados em relação as soluções deste objeto matemático além de sermos capazes de entender as ideias fundamentais que culminaram no resultado principal - Lei da Reciprocidade Quadrática Gaussiana. Esta lei nos permitiu discutir a solução de qualquer congruência quadrática da forma $x^2 \equiv a \ (mod\ p)$, com p um número primo e a um número inteiro não divisível por p.

A partir de todo esse aprendizado sobre as congruências e suas propriedades naturais e elementares, podemos dizer que atingimos nossas metas de adquirir mais conhecimento matemático. A propósito, diante deste aprendizado, podemos futuramente estudar classes residuais - que permitem definir outras aritméticas dentro do conjunto dos números inteiros e é a base de todo o cálculo computacional atual.

Referências

BERTONE, A. M. A. *Introdução à Teoria dos Números*. [S.l.]: Uberlândia, MG: UFU, 2014. Citado na página 21.

BOYER, C. B.; MERZBACH, U. C. *História da Matemática*. 3ª. ed. [S.l.]: São Paulo: Edgar Blücher, 2012. Tradução de Helena Castro. ISBN 978-85-212-0641-5. Citado 3 vezes nas páginas 38, 70 e 86.

BRASIL. *Base Nacional Comum Curricular (BNCC)*. [S.l.]: Brasília: MEC/CONSED/UNDIME, 2018. Citado 3 vezes nas páginas 52, 53 e 61.

CAMPOS, W.; AVILA, J. A. J. *Um critério de primalidade baseado no Teorema de Wilson*. [S.l.]: TCC (Mestrado em Matemática) – Universidade Federal de São João del-Rei; PROFMAT – Mestrado Profissional em Matemática em Rede Nacional, 2015. Citado na página 77.

DANTE, L. R. *Didática da Resolução de problemas de matemática. 1ª a 5ª série. Para estudantes do curso Magistério e professores do 1º grau.* 12ª ed.. ed. [S.l.]: São Paulo: Ática, 2003. Citado na página 51.

DOMINGUES, H. H. *Fundamentos de Aritmética*. [S.l.]: São Paulo: Atual Editora, 1991. ISBN 85-7056-342-6. Citado 5 vezes nas páginas 11, 13, 38, 64 e 81.

GOMES, O. R.; SILVA, J. C. *Estruturas Algébricas para Licenciatura: Elementos de Aritmética Superior*. 1ª. ed. [S.l.]: São Paulo: Edgar Blücher, 2018. v. 2. ISBN 978-85-212-1146-4. Citado 5 vezes nas páginas 11, 13, 38, 64 e 81.

HEFEZ, A. *Aritmética*. [S.l.]: Rio de Janeiro: SBM, 2009. ISBN 978-85-8337-105-2. Citado 9 vezes nas páginas 11, 13, 16, 17, 33, 34, 38, 64 e 70.

LUCHETTA, V. O. J. *Euclides e os "Elementos"*. [S.l.]: A Matemática Interativa na Internet, 2008. Disponível em: <https://www.ime.usp.br/∼leo/imatica/historia/euclides.html>. Acesso em: 18 dez. 2019. Citado na página 16.

MACHADO, M. *Étienne Bézout*. [S.l.]: ZTFNews.org, 2013. Disponível em: <https://ztfnews.eus/2013/09/27/etienne-bezout/>. Acesso em: 19 dez. 2020. Citado na página 20.

MOL, R. S. *Introdução à História da Matemática*. [S.l.]: Belo Horizonte: CAED-UFMG, 2013. ISBN 978-85-64724-26-6. Citado 3 vezes nas páginas 33, 34 e 70.

SANTOS, J. P. d. O. *Introdução à Teoria dos Números*. 3ª. ed. [S.l.]: Rio de Janeiro: IMPA, 2020. ISBN 978-85-244-0496-2. Citado 7 vezes nas páginas 11, 13, 38, 64, 81, 92 e 97.

SILVA, B. S. *O Último Teorema de Fermat para n=3*. [S.l.]: TCC (Mestrado em Matemática) – Universidade Federal do Estado do Rio de Janeiro; Centro de Ciências Exatas e Tecnologia; PROFMAT – Mestrado Profissional em Matemática em Rede Nacional, 2014. CDU 536.21. Citado 2 vezes nas páginas 33 e 34.

Anexos

ANEXO A – Situações-problemas

UNIVERSIDADE FEDERAL DO RIO GRANDE - FURG
INSTITUTO DE MATEMÁTICA, FÍSICA E ESTÁTISTICA - IMEF
Prof. William Debon Pereira

Atividade de Extensão

Nome: _____ Turma: _____ Data: ___/___/___

1) O dia da semana de hoje é _____ e o horário é _____. Daqui $95h$ será que dia da semana e que horas?

UNIVERSIDADE FEDERAL DO RIO GRANDE - FURG
INSTITUTO DE MATEMÁTICA, FÍSICA E ESTÁTISTICA - IMEF
Prof. William Debon Pereira

Atividade de Extensão

Nome: _____ Turma: _____ Data: ___/___/___

2) Meu aniversário é dia _____ de _____ e, neste ano, o dia da semana que ele ocorreu/ocorrerá foi/é _____. Supondo que hoje seja o dia do seu aniversário e sabendo que a cada quatro anos temos um ano bissexto, responda:

   a) Qual será o dia da semana que seu aniversário ocorrerá no ano de 2020 (ano bissexto)? E nos anos de 2021, 2022, 2023 e 2024?

   b) É possível notarmos algum padrão com relação aos dias da semana do seu aniversário com cada ano? Se sua resposta for afirmativa, descreva o padrão e, caso sua resposta seja negativa, explique o porquê.

   c) O ano de 2082 é um ano bissexto? Justifique sua resposta.

UNIVERSIDADE FEDERAL DO RIO GRANDE - FURG
INSTITUTO DE MATEMÁTICA, FÍSICA E ESTÁTISTICA - IMEF
Prof. William Debon Pereira

Atividade de Extensão

Nome: _____ Turma: _____ Data: ___/___/___

3) O cometa Halley é um corpo celeste sem luz própria, que é visível a olho nu da terra a cada 74 ~ 79 anos. Supondo que ele esteja passando pela terra regularmente a cada 75 anos e sabendo que sua última aparição foi no ano de 1986, responda:

   a) Esse cometa pode retornar no ano de 2062? Por quê?

   b) Qual é sua idade no ano de reaparição desse cometa logo após sua última aparição?

   c) Agora, analisando o ano de 2361. É possível que o cometa apareça nesse ano? Por quê?

   d) Qual é o ano que o cometa Halley pode ser visto novamente a partir do ano de 2446?

ANEXO B – Questionário e Calendários

Abaixo encontram-se as 4 questões aplicadas com os estudantes após o término da Atividade Didática.

i) O que você achou da atividade? Justifique.

ii) O que você compreende a partir das discussões envolvidas durante a atividade? Explique.

iii) Alguma sugestão para aperfeiçoar a atividade?

iv) Que conteúdos matemáticos estão por trás da resolução dessa atividade?

Observação: O quarto questionamento foi aplicado apenas para os ingressantes do curso de Matemática Licenciatura.

Nas próximas páginas estarão os calendários dos anos de 2019 à 2024 que foram utilizados como suporte para a realização da segunda situação-problema.

Janeiro 2019

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
1		1	2	3	4	5	6
2	7	8	9	10	11	12	13
3	14	15	16	17	18	19	20
4	21	22	23	24	25	26	27
5	28	29	30	31			

Fevereiro 2019

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
5					1	2	3
6	4	5	6	7	8	9	10
7	11	12	13	14	15	16	17
8	18	19	20	21	22	23	24
9	25	26	27	28			

Março 2019

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
9					1	2	3
10	4	5	6	7	8	9	10
11	11	12	13	14	15	16	17
12	18	19	20	21	22	23	24
13	25	26	27	28	29	30	31

Abril 2019

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
14	1	2	3	4	5	6	7
15	8	9	10	11	12	13	14
16	15	16	17	18	19	20	21
17	22	23	24	25	26	27	28
18	29	30					

Maio 2019

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
18			1	2	3	4	5
19	6	7	8	9	10	11	12
20	13	14	15	16	17	18	19
21	20	21	22	23	24	25	26
22	27	28	29	30	31		

Junho 2019

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
22						1	2
23	3	4	5	6	7	8	9
24	10	11	12	13	14	15	16
25	17	18	19	20	21	22	23
26	24	25	26	27	28	29	30

Julho 2019

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
27	1	2	3	4	5	6	7
28	8	9	10	11	12	13	14
29	15	16	17	18	19	20	21
30	22	23	24	25	26	27	28
31	29	30	31				

Agosto 2019

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
31				1	2	3	4
32	5	6	7	8	9	10	11
33	12	13	14	15	16	17	18
34	19	20	21	22	23	24	25
35	26	27	28	29	30	31	

Setembro 2019

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
35							1
36	2	3	4	5	6	7	8
37	9	10	11	12	13	14	15
38	16	17	18	19	20	21	22
39	23	24	25	26	27	28	29
40	30						

Outubro 2019

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
40		1	2	3	4	5	6
41	7	8	9	10	11	12	13
42	14	15	16	17	18	19	20
43	21	22	23	24	25	26	27
44	28	29	30	31			

Novembro 2019

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
44					1	2	3
45	4	5	6	7	8	9	10
46	11	12	13	14	15	16	17
47	18	19	20	21	22	23	24
48	25	26	27	28	29	30	

Dezembro 2019

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
48							1
49	2	3	4	5	6	7	8
50	9	10	11	12	13	14	15
51	16	17	18	19	20	21	22
52	23	24	25	26	27	28	29
1	30	31					

2019

Calendario 365 .com.br

Janeiro 2020

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
1			1	2	3	4	5
2	6	7	8	9	10	11	12
3	13	14	15	16	17	18	19
4	20	21	22	23	24	25	26
5	27	28	29	30	31		

Fevereiro 2020

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
5						1	2
6	3	4	5	6	7	8	9
7	10	11	12	13	14	15	16
8	17	18	19	20	21	22	23
9	24	25	26	27	28	29	

Março 2020

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
9							1
10	2	3	4	5	6	7	8
11	9	10	11	12	13	14	15
12	16	17	18	19	20	21	22
13	23	24	25	26	27	28	29
14	30	31					

Abril 2020

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
14			1	2	3	4	5
15	6	7	8	9	10	11	12
16	13	14	15	16	17	18	19
17	20	21	22	23	24	25	26
18	27	28	29	30			

Maio 2020

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
18					1	2	3
19	4	5	6	7	8	9	10
20	11	12	13	14	15	16	17
21	18	19	20	21	22	23	24
22	25	26	27	28	29	30	31

Junho 2020

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
23	1	2	3	4	5	6	7
24	8	9	10	11	12	13	14
25	15	16	17	18	19	20	21
26	22	23	24	25	26	27	28
27	29	30					

Julho 2020

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
27			1	2	3	4	5
28	6	7	8	9	10	11	12
29	13	14	15	16	17	18	19
30	20	21	22	23	24	25	26
31	27	28	29	30	31		

Agosto 2020

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
31						1	2
32	3	4	5	6	7	8	9
33	10	11	12	13	14	15	16
34	17	18	19	20	21	22	23
35	24	25	26	27	28	29	30
36	31						

Setembro 2020

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
36		1	2	3	4	5	6
37	7	8	9	10	11	12	13
38	14	15	16	17	18	19	20
39	21	22	23	24	25	26	27
40	28	29	30				

Outubro 2020

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
40				1	2	3	4
41	5	6	7	8	9	10	11
42	12	13	14	15	16	17	18
43	19	20	21	22	23	24	25
44	26	27	28	29	30	31	

Novembro 2020

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
44							1
45	2	3	4	5	6	7	8
46	9	10	11	12	13	14	15
47	16	17	18	19	20	21	22
48	23	24	25	26	27	28	29
49	30						

Dezembro 2020

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
49		1	2	3	4	5	6
50	7	8	9	10	11	12	13
51	14	15	16	17	18	19	20
52	21	22	23	24	25	26	27
53	28	29	30	31			

2020

Calendario 365 .com.br

Janeiro 2021

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
53					1	2	3
1	4	5	6	7	8	9	10
2	11	12	13	14	15	16	17
3	18	19	20	21	22	23	24
4	25	26	27	28	29	30	31

Fevereiro 2021

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
5	1	2	3	4	5	6	7
6	8	9	10	11	12	13	14
7	15	16	17	18	19	20	21
8	22	23	24	25	26	27	28

Março 2021

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
9	1	2	3	4	5	6	7
10	8	9	10	11	12	13	14
11	15	16	17	18	19	20	21
12	22	23	24	25	26	27	28
13	29	30	31				

Abril 2021

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
13				1	2	3	4
14	5	6	7	8	9	10	11
15	12	13	14	15	16	17	18
16	19	20	21	22	23	24	25
17	26	27	28	29	30		

Maio 2021

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
17						1	2
18	3	4	5	6	7	8	9
19	10	11	12	13	14	15	16
20	17	18	19	20	21	22	23
21	24	25	26	27	28	29	30
22	31						

Junho 2021

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
22		1	2	3	4	5	6
23	7	8	9	10	11	12	13
24	14	15	16	17	18	19	20
25	21	22	23	24	25	26	27
26	28	29	30				

Julho 2021

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
26				1	2	3	4
27	5	6	7	8	9	10	11
28	12	13	14	15	16	17	18
29	19	20	21	22	23	24	25
30	26	27	28	29	30	31	

Agosto 2021

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
30							1
31	2	3	4	5	6	7	8
32	9	10	11	12	13	14	15
33	16	17	18	19	20	21	22
34	23	24	25	26	27	28	29
35	30	31					

Setembro 2021

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
35			1	2	3	4	5
36	6	7	8	9	10	11	12
37	13	14	15	16	17	18	19
38	20	21	22	23	24	25	26
39	27	28	29	30			

Outubro 2021

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
39					1	2	3
40	4	5	6	7	8	9	10
41	11	12	13	14	15	16	17
42	18	19	20	21	22	23	24
43	25	26	27	28	29	30	31

Novembro 2021

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
44	1	2	3	4	5	6	7
45	8	9	10	11	12	13	14
46	15	16	17	18	19	20	21
47	22	23	24	25	26	27	28
48	29	30					

Dezembro 2021

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
48			1	2	3	4	5
49	6	7	8	9	10	11	12
50	13	14	15	16	17	18	19
51	20	21	22	23	24	25	26
52	27	28	29	30	31		

2021

Calendario 365 .com.br

Janeiro 2022

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
52						1	2
1	3	4	5	6	7	8	9
2	10	11	12	13	14	15	16
3	17	18	19	20	21	22	23
4	24	25	26	27	28	29	30
5	31						

Fevereiro 2022

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
5		1	2	3	4	5	6
6	7	8	9	10	11	12	13
7	14	15	16	17	18	19	20
8	21	22	23	24	25	26	27
9	28						

Março 2022

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
9		1	2	3	4	5	6
10	7	8	9	10	11	12	13
11	14	15	16	17	18	19	20
12	21	22	23	24	25	26	27
13	28	29	30	31			

Abril 2022

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
13					1	2	3
14	4	5	6	7	8	9	10
15	11	12	13	14	15	16	17
16	18	19	20	21	22	23	24
17	25	26	27	28	29	30	

Maio 2022

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
17							1
18	2	3	4	5	6	7	8
19	9	10	11	12	13	14	15
20	16	17	18	19	20	21	22
21	23	24	25	26	27	28	29
22	30	31					

Junho 2022

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
22			1	2	3	4	5
23	6	7	8	9	10	11	12
24	13	14	15	16	17	18	19
25	20	21	22	23	24	25	26
26	27	28	29	30			

Julho 2022

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
26					1	2	3
27	4	5	6	7	8	9	10
28	11	12	13	14	15	16	17
29	18	19	20	21	22	23	24
30	25	26	27	28	29	30	31

Agosto 2022

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
31	1	2	3	4	5	6	7
32	8	9	10	11	12	13	14
33	15	16	17	18	19	20	21
34	22	23	24	25	26	27	28
35	29	30	31				

Setembro 2022

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
35				1	2	3	4
36	5	6	7	8	9	10	11
37	12	13	14	15	16	17	18
38	19	20	21	22	23	24	25
39	26	27	28	29	30		

Outubro 2022

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
39						1	2
40	3	4	5	6	7	8	9
41	10	11	12	13	14	15	16
42	17	18	19	20	21	22	23
43	24	25	26	27	28	29	30
44	31						

Novembro 2022

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
44		1	2	3	4	5	6
45	7	8	9	10	11	12	13
46	14	15	16	17	18	19	20
47	21	22	23	24	25	26	27
48	28	29	30				

Dezembro 2022

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
48				1	2	3	4
49	5	6	7	8	9	10	11
50	12	13	14	15	16	17	18
51	19	20	21	22	23	24	25
52	26	27	28	29	30	31	

2022

Calendario 365 .com.br

Janeiro 2023

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
52							1
1	2	3	4	5	6	7	8
2	9	10	11	12	13	14	15
3	16	17	18	19	20	21	22
4	23	24	25	26	27	28	29
5	30	31					

Fevereiro 2023

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
5			1	2	3	4	5
6	6	7	8	9	10	11	12
7	13	14	15	16	17	18	19
8	20	21	22	23	24	25	26
9	27	28					

Março 2023

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
9			1	2	3	4	5
10	6	7	8	9	10	11	12
11	13	14	15	16	17	18	19
12	20	21	22	23	24	25	26
13	27	28	29	30	31		

Abril 2023

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
13						1	2
14	3	4	5	6	7	8	9
15	10	11	12	13	14	15	16
16	17	18	19	20	21	22	23
17	24	25	26	27	28	29	30

Maio 2023

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
18	1	2	3	4	5	6	7
19	8	9	10	11	12	13	14
20	15	16	17	18	19	20	21
21	22	23	24	25	26	27	28
22	29	30	31				

Junho 2023

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
22				1	2	3	4
23	5	6	7	8	9	10	11
24	12	13	14	15	16	17	18
25	19	20	21	22	23	24	25
26	26	27	28	29	30		

Julho 2023

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
26						1	2
27	3	4	5	6	7	8	9
28	10	11	12	13	14	15	16
29	17	18	19	20	21	22	23
30	24	25	26	27	28	29	30
31	31						

Agosto 2023

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
31		1	2	3	4	5	6
32	7	8	9	10	11	12	13
33	14	15	16	17	18	19	20
34	21	22	23	24	25	26	27
35	28	29	30	31			

Setembro 2023

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
35					1	2	3
36	4	5	6	7	8	9	10
37	11	12	13	14	15	16	17
38	18	19	20	21	22	23	24
39	25	26	27	28	29	30	

Outubro 2023

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
39							1
40	2	3	4	5	6	7	8
41	9	10	11	12	13	14	15
42	16	17	18	19	20	21	22
43	23	24	25	26	27	28	29
44	30	31					

Novembro 2023

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
44			1	2	3	4	5
45	6	7	8	9	10	11	12
46	13	14	15	16	17	18	19
47	20	21	22	23	24	25	26
48	27	28	29	30			

Dezembro 2023

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
48					1	2	3
49	4	5	6	7	8	9	10
50	11	12	13	14	15	16	17
51	18	19	20	21	22	23	24
52	25	26	27	28	29	30	31

2023

Calendario 365 .com.br

Janeiro 2024

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
1	1	2	3	4	5	6	7
2	8	9	10	11	12	13	14
3	15	16	17	18	19	20	21
4	22	23	24	25	26	27	28
5	29	30	31				

Fevereiro 2024

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
5				1	2	3	4
6	5	6	7	8	9	10	11
7	12	13	14	15	16	17	18
8	19	20	21	22	23	24	25
9	26	27	28	29			

Março 2024

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
9					1	2	3
10	4	5	6	7	8	9	10
11	11	12	13	14	15	16	17
12	18	19	20	21	22	23	24
13	25	26	27	28	29	30	31

Abril 2024

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
14	1	2	3	4	5	6	7
15	8	9	10	11	12	13	14
16	15	16	17	18	19	20	21
17	22	23	24	25	26	27	28
18	29	30					

Maio 2024

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
18			1	2	3	4	5
19	6	7	8	9	10	11	12
20	13	14	15	16	17	18	19
21	20	21	22	23	24	25	26
22	27	28	29	30	31		

Junho 2024

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
22						1	2
23	3	4	5	6	7	8	9
24	10	11	12	13	14	15	16
25	17	18	19	20	21	22	23
26	24	25	26	27	28	29	30

Julho 2024

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
27	1	2	3	4	5	6	7
28	8	9	10	11	12	13	14
29	15	16	17	18	19	20	21
30	22	23	24	25	26	27	28
31	29	30	31				

Agosto 2024

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
31				1	2	3	4
32	5	6	7	8	9	10	11
33	12	13	14	15	16	17	18
34	19	20	21	22	23	24	25
35	26	27	28	29	30	31	

Setembro 2024

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
35							1
36	2	3	4	5	6	7	8
37	9	10	11	12	13	14	15
38	16	17	18	19	20	21	22
39	23	24	25	26	27	28	29
40	30						

Outubro 2024

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
40		1	2	3	4	5	6
41	7	8	9	10	11	12	13
42	14	15	16	17	18	19	20
43	21	22	23	24	25	26	27
44	28	29	30	31			

Novembro 2024

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
44					1	2	3
45	4	5	6	7	8	9	10
46	11	12	13	14	15	16	17
47	18	19	20	21	22	23	24
48	25	26	27	28	29	30	

Dezembro 2024

	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
48							1
49	2	3	4	5	6	7	8
50	9	10	11	12	13	14	15
51	16	17	18	19	20	21	22
52	23	24	25	26	27	28	29
1	30	31					

2024

Calendario 365 .com.br