UNIVERSIDADE FEDERAL DO PARÁ

PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

OSÉAS GUIMARÃES FERREIRA NETO

APLICAÇÕES DE DIVISIBILIDADE E CONGRUÊNCIA MODULAR: DO ENSINO BÁSICO AO SUPERIOR

Bragança – Pará
2021

OSÉAS GUIMARÃES FERREIRA NETO

APLICAÇÕES DE DIVISIBILIDADE E CONGRUÊNCIA MODULAR: DO ENSINO BÁSICO AO SUPERIOR

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT da Universidade Federal do Pará como requisito parcial para obtenção do grau de Mestre em Matemática.

Linha de Pesquisa: Teoria dos Números.

Orientadora: Profª. Drª. Marly dos Anjos Nunes

Bragança – Pará
2021

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD
Sistema de Bibliotecas da Universidade Federal do Pará
Gerada automaticamente pelo módulo Ficat, mediante os dados fornecidos pelo(a) autor(a)

G963a Guimarães, Oséas Guimarães Ferreira Neto.
Aplicações de divisibilidade e congruência modular: do ensino básico ao superior / Oséas Guimarães Ferreira Neto Guimarães. — 2021.
96 f. : il. color.

Orientador(a): Profª. Dra. Marly dos Anjos Nunes Anjos
Coorientador(a): Prof. Dr. Edson Jorge de Matos
Dissertação (Mestrado) - Universidade Federal do Pará, Campus Universitário de Bragança, Programa de Mestrado Profissional em Ensino da Matemática, Bragança, 2021.

1. Critérios de Divisibilidade. 2. Congruência. 3. Aplicações. I. Título.

CDD 512.72

OSÉAS GUIMARÃES FERREIRA NETO

APLICAÇÕES DE DIVISIBILIDADE E CONGRUÊNCIA MODULAR: DO ENSINO BÁSICO AO SUPERIOR

Dissertação submetida ao corpo docente do Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, campus de Bragança da Universidade Federal do Pará, como requisito parcial para obtenção do título de Mestre em Matemática, na área de concentração Teoria dos Números.

DATA DA AVALIAÇÃO: 15 / 12 / 2021

CONCEITO: _____

BANCA EXAMINADORA

_____

Profª. Drª. Marly dos Anjos Nunes
Membro interno – UFPA

_____

Prof. Dr. Edson Jorge de Matos
Membro interno– UFPA

_____

Profª. Drª. Edilene Farias Rozal
Membro interno – UFPA

_____

Profª. Drª. Andréia Gomes Pinheiro
Membro externo – IFPA

Bragança – Pará
2021

Dedico este trabalho primeiramente a Deus, razão de toda minha vida; a minha família, em especial a minha amada esposa, minha mãe, meu pai, e aos meus dois amados filhos.

“Se você é capaz de se indignar diante de uma injustiça no mundo, então somos companheiros.”

(Che Guevara)

AGRADECIMENTOS

Primeiramente a Deus, pois graças a Ele estou chegando ao fim de mais uma jornada e realizando um sonho de obter o título de Mestre.

Aos meus pais, Ronaldo de Lima Guimarães Ferreira e Olizete da Silva Ferreira, por todo carinho, apoio, por sempre me incentivarem (em especial nos estudos), e por sempre fazerem tudo que podiam para dar a melhor criação possível a mim e a minha irmã; vocês sempre serão meus exemplos.

À minha amada Esposa, Kelly da Silva e Silva, por todo o apoio e dedicação que me deu durante os momentos difíceis ao longo do curso e por suportar com paciência os momentos de ausência durante os finais de semana de estudo em Bragança.

Aos meus filhos, Daniela da Silva Guimarães e Manuel da Silva Guimarães, pelo amor e alegrias depositadas nos momentos de angústia, pressão e por também suportarem com a paciente ternura da infância os momentos de ausência durante os finais de semana de estudos.

À minha irmã Lidiane de Lima Guimarães Ferreira por todo incentivo e apoio.

Agradeço a todos os meus familiares por sempre acreditarem em mim e me incentivarem durante todas as empreitadas da vida acadêmica.

À Profª. Drª. Marly dos Anjos Nunes, por aceitar a tarefa de me orientar durante a realização desse trabalho.

Aos professores Dr. Edson Jorge Matos, Drª. Edilene Farias Rozal e Drª. Andréia Gomes Pinheiro, por aceitarem participar da banca examinadora.

A todos os servidores da UFPA, campus Bragança, em especial a todos os professores vinculados ao PROFMAT por suas contribuições ao longo do curso.

Aos meus colegas de turma Gil Medeiros, Luís Jorge, Pablo Gatinho, Edvaldo Queiroz, Fabrício, Emerson, Júlio César, Mauro e Elane por todas as aflições, risadas e momentos de estudo compartilhados ao longo do curso.

Aos meus amigos, Felipe Ferreira, Marcos Pinheiro, Paulo Elison, Janilton de Souza, Alexandre Ataíde, Elielson Cardoso, Mesaque Pinheiro, Emídio dos Santos e Ronaldo Gurjão [*in memoriam*], pelo apoio aos estudos e descontração durante os momentos mais difíceis que vivemos na pandemia.

A todos aqueles que foram meus professores durante meus anos de estudante na Educação Básica e na Graduação em Matemática.

A todos que contribuíram de forma direta ou indireta para realização desse trabalho.

RESUMO

Esta dissertação apresenta aplicações que serão resolvidas usando os critérios de divisibilidade e congruência modular, partindo das dificuldades encontradas nos alunos do ano final do ensino médio nos conteúdos do eixo Números do ensino fundamental II. Nosso objetivo ao explorar essas aplicações destacando as relações entre os critérios de divisibilidade e a congruência modular é o de solucionar essas dificuldades ainda no ensino fundamental, especificamente no 6º e 7º anos, dentro dos parâmetros da Base Nacional Comum Curricular (BNCC), além de oferecer uma fonte de pesquisa para professores do ensino básico e que possa ser usada também no ensino superior. Usando uma pesquisa bibliográfica iniciamos nossa pesquisa com a fundamentação teórica acerca do conjunto dos números inteiros e definimos divisão euclidiana explorando os principais critérios de divisibilidade, evidenciando o seu uso nas equações diofantinas e a sua relação com a congruência modular. Obtendo como resultado oito aplicações que foram tratadas usando as duas linguagens de maneira que possibilite a criação de alternativas didáticas que relacionem os conteúdos aritméticos e algébricos nos dois ciclos de ensino. As aplicações sugeridas convergem para uma abordagem que relaciona os conteúdos de divisibilidade e congruência modular em situações práticas que reforçam as necessidades de uma atenção a esses assuntos para a formação matemática.

Palavras-chave: Critérios de Divisibilidade, Congruência, Aplicações.

ABSTRACT

This dissertation presents applications that will be solved using the divisibility and modular congruence criteria, starting from the difficulties encountered by students in the final year of high school in the contents of the Numbers axis of elementary school II. Our objective in exploring these applications, highlighting the relationships between the divisibility criteria and modular congruence, is to solve these difficulties even in elementary education, specifically in the 6th and 7th years, within the parameters of the Common National Curriculum Base (BNCC), in addition to provide a source of research for elementary school teachers that can also be used in higher education. Using a bibliographical research, we started our research with the theoretical foundation about the set of whole numbers and we defined Euclidean division exploring the main divisibility criteria, showing its use in Diophantine equations and its relationship with modular congruence. Obtaining as a result eight applications that were treated using both languages in a way that allows the creation of didactic alternatives that relate the arithmetic and algebraic contents in the two teaching cycles. The suggested applications converge to an approach that relates the contents of divisibility and modular congruence in practical situations that reinforce the need for attention to these issues for mathematical training.

Keywords: Divisibility Criteria, Congruence, Applications.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SÍMBOLOS

$\mathbb{N}$	Conjunto dos números naturais.
$\mathbb{Z}$	Conjunto dos números inteiros.
$\mathbb{Q}$	Conjunto dos números racionais.
$\mathbb{R}$	Conjunto dos números reais.
$\Longrightarrow$	Implicação.
$\Leftrightarrow$	Equivalente.
$=$	Igual.
$\neq$	Diferente.
$>$	Maior.
$<$	Menor.
$\geq$	Maior ou igual.
$\leq$	Menor ou igual.
$\in$	Pertence.
$\notin$	Não pertence.
$\equiv$	Congruente.
$\not\equiv$	Não congruente.
$\subset$	Está contido.
$\not\subset$	Não está contido.
$\cup$	União.
$\cap$	Intersecção.
$\mid$	Divide.
$\nmid$	Não divide.
$\setminus$	Diferença de conjuntos.
$\forall$	Para todo.
$\therefore$	Portanto.
$\emptyset$	Conjunto vazio.
$\sum$	Somatório.
■	Indica o fim de uma demonstração.

SUMÁRIO

Capítulo 1

Introdução

No livro "*Sapiens: uma breve história da humanidade"*, Yuval Harari descreve com riqueza de detalhes as três grandes revoluções que moldaram o curso da história humana no planeta. A primeira foi a Revolução Cognitiva, seguidas pela Revolução Agrícola e a Revolução Científica. Cada uma delas têm aspectos próprios, mas há uma intersecção que nos chama bastante atenção nessas revoluções: a presença da Matemática. Do homem primitivo ao moderno e conectado, houve um grande percurso, e nessa caminhada a transformação pela qual a Matemática com seus símbolos e números passou é uma marca da nossa evolução, enquanto seres pensantes.

Nessa longa evolução, alguns povos tiveram importantes contribuições matemáticas, entre eles podemos destacar os Egípcios e os Gregos como os pioneiros da Matemática no que hoje chamamos de Geometria e Aritmética. Os Egípcios com os seus trabalhos de engenharia e agrimensura tinham a Matemática como uma arte auxiliar, já os Gregos atribuíram um caráter científico a ela, decorrência de uma atitude filosófica e especulativa da vida. Embora a Matemática seja uma construção coletiva, cabe ressaltar a importância de alguns estudiosos da área. O primeiro é Tales de Mileto (640 – 546 a.C), que segundo os historiadores introduziu o estudo da Matemática na Grécia, fruto de um aprendizado com os sacerdotes egípcios. Em seguida podemos destacar Pitágoras de Samos (580? – 500? a.C), famoso pelo teorema que leva o seu nome, foi ele quem difundiu a Matemática pela Grécia e suas colônias, com o auxílio dos seus discípulos da escola pitagórica. Juntos eles dotaram a Aritmética como um fundamento lógico e filosófico.

Outro importante nome é o de Euclides de Alexandria, pois coube a ele reunir e sistematizar a maior parte do conhecimento matemático da época. Sem muitas criações próprias, aparentemente seu maior mérito foi o de estabelecer um padrão rigoroso de apresentação dos conhecimentos matemáticos, algo que ainda não tinha ocorrido. A obra Os Elementos de Euclides foi amplamente aceita e consagrada, tornando-se um instrumento de consulta recorrente, isso explica o fato de ser considerado o segundo livro mais lido ao longo dos tempos. Dividida em treze livros dos quais os dez primeiros são destinados a geometria, e os três últimos ao estudo da Aritmética. Nestes encontramos a teoria dos números naturais, o conceito de divisibilidade, números primos, números perfeitos, MDC (máximo divisor comum), MMC (mínimo múltiplo comum), além, é claro, da famosa divisão com resto de um natural, que é chamada até hoje de divisão euclidiana, estabelecendo assim o algoritmo mais eficiente na determinação do máximo divisor entre dois números inteiros.

Após os trabalhos de Euclides, a Aritmética teve uma pausa de cerca de cinco séculos, voltando a ter um destaque nos trabalhos de Diofanto de Alexandria, por volta de 250 d.C. Sua obra também foi escrita em treze volumes, dos quais apenas sete chegaram até nós, neles Diofanto faz uma abordagem totalmente algébrica, tornando-se o pioneiro neste sentido, pois, até então, a Aritmética sempre era apresentada com uma linguagem e interpretação geométrica. Diofanto rompeu essa tradição, visto que sua abordagem algébrica visava encontrar soluções em números racionais e inteiros de equações algébricas com uma ou mais variáveis. Seus trabalhos inspiraram outros grandes nomes como o matemático francês Pierre de Fermat (1601 – 1665) e o suíço Leonhard Euler (1707 – 1783), sendo este o responsável por introduzir a ideia de congruência modular em um natural, teoria essa desenvolvida posteriormente por Carl Friedrich Gauss (1777 – 1855), na famosa obra "*Disquisitiones Arithmeticae"*, publicada em 1801.

A necessidade de utilização de métodos de contagem é, sem dúvida, a coluna central por trás da Aritmética, sistematizada em axiomas e teoremas ao longo dos séculos, hoje essa importante teoria é usada em larga escala nos algoritmos do universo digital da informática, com ênfase a Criptografia, e pode ser subdividida em quatro grandes campos de atuação, dependendo dos métodos adotados na abordagem das questões que são investigadas, são elas: Teoria Elementar, Teoria Analítica dos Números, Teoria Algébrica e Teoria Geométrica.

Neste trabalho iremos adotar a Teoria Elementar dos números, com ênfase aos processos de divisibilidade e de congruência modular, uma vez que são esses os conhecimentos apresentados aos alunos no início do ciclo fundamental II, 6º e 7º anos, eles irão servir de base para as outras áreas e séries subsequentes da matemática, isto é, esses conhecimentos compõem a matemática necessária e indispensável para qualquer cidadão.

Ao longo de quinze anos trabalhando com pré-vestibular, sempre encontrei muitos alunos com grandes dificuldades nos processos de divisão e na transposição da linguagem verbal para a simbólica exigida em exames como o Enem. Esses entraves me incomodavam, pois me questionava, como um aluno que vai realizar o vestibular não sabe executar uma divisão com resto, fazer uma simplificação, organizar uma equação de duas variáveis ou diferenciar um MMC de um MDC? Com o tempo criei estratégias metodológicas para atenuar esses problemas, promovendo oficinas de matemática básica, onde revisava os conteúdos do ensino fundamental II, com ênfase nos conteúdos de 6º e 7º anos.

Em 2019 entrei para o quadro de professores da rede pública do Estado do Pará, foi nesse momento que tive o meu primeiro contato com o ciclo do fundamental II, permitindo assim observar e vivenciar os problemas encontrados no ensino médio e nas turmas de pré-vestibular. No mesmo ano, passei para o mestrado PROFMAT, outra experiência transformadora na minha vida, pois era a

oportunidade de verificar se aqueles problemas que enfrentávamos com os alunos no ciclo básico poderiam proporcionar alternativas no ensino superior.

Diante de tais experiências foi natural então nos perguntarmos:

De que forma é possível minimizar as dificuldades de divisibilidade e de transposição de linguagens no Ensino Médio ainda no fundamental com o uso de aplicações dos critérios de divisibilidade e de congruência modular?

É possível fazer uma relação através dessas aplicações entre os critérios de divisibilidade e congruência modular no ensino superior?

A experiência que estava tendo como docente do ciclo básico e discente na pós-graduação se tornou uma oportunidade para entender, refletir e preparar alternativas que viessem de encontro a essa problemática. Nesse momento percebemos que os critérios de divisibilidade eram a peça central nesse procedimento, pois além de dinamizar a divisão, também possibilitava a resolução de equações diofantinas, oferecendo um entendimento prático e contextualizado das congruências modulares.

Nosso objetivo geral é a apresentação de algumas aplicações de divisibilidade e congruência que possam ser usadas no ensino básico e superior, oferecendo aos professores destes ciclos uma fonte de pesquisa para a elaboração e produção de aulas que proporcionem uma base mais sólida dos fundamentos da matemática elementar no ciclo básico além de promover uma análise dos critérios de divisibilidade através da congruência modular no ensino superior. Os nossos objetivos específicos são:

- Capacitar o aluno a utilizar os critérios de divisibilidades, em especial dos números primos ($p \leq 13$);
- Apresentar a notação de congruência modular, com ênfase as propriedades operatórias e as generalizações;
- Estabelecer e relacionar os critérios de divisibilidade com congruência modular apresentando aplicações que possam ser resolvidas com o uso das duas técnicas.

Estruturalmente, este trabalho está organizado em 5 (cinco) capítulos, contados a partir da introdução (capítulo 1) até as considerações finais (capítulo 5). No capítulo 2 iremos abordar o conjunto dos números inteiros, a divisão dos inteiros, números primos, os critérios de divisibilidade dos números primos e compostos que sejam formados por ($p \leq 13$), divisão euclidiana, o MDC e o MMC e equações diofantinas. No capítulo 3 será feita a definição da congruência modular, com suas propriedades básicas e operatórias, o pequeno Teorema de Fermat, o Teorema de Euler e o Teorema Chinês dos restos. Por fim, no capítulo 4 vamos apresentar algumas aplicações com o uso da divisibilidade e da congruência modular.

As aplicações que serão apresentadas neste trabalho, além de explorar os critérios de divisibilidade e as propriedades da congruência modular, oferece uma conexão entre eles, possibilitando

ao aluno determinar os restos das divisões com potências de expoentes muito grandes, bem como, a resolução de equações diofantinas apenas com o uso dos critérios de divisibilidade. Esses conceitos e métodos são explorados em outras dissertações direcionadas ao PROFMAT, o que de certa forma entra em consonância com este trabalho, porém elas, em sua imensa maioria, têm uma abordagem direcionada ao ensino médio e a preparação para olimpíadas, enquanto este trabalho tem um direcionamento ao 6º e 7º anos do ensino fundamental e as disciplinas de Aritmética e Teoria dos Números no ensino superior, afim de promover a relação entre divisibilidade e congruência modular.

Capítulo 2

Os Parâmetros Curriculares Nacionais (PCN) agrupam os conteúdos de Matemática para o Ensino Fundamental em quatro grandes temas: números e operações, espaços e formas, grandezas e medidas, além do tratamento da informação. O conjunto dos números inteiros se insere na temática números e operações, sendo isto justificado nos PCN pelo fato de

> Além das situações do cotidiano os números negativos também surgiram no interior da Matemática na resolução de equações algébricas. No entanto, sua aceitação seguiu de uma longa e demorada trajetória. Só no século XIX os negativos foram interpretados como uma ampliação dos naturais e incorporam as leis da Aritmética. Passaram então a integrar a hierarquia dos sistemas numéricos como números inteiros. (BRASIL, 1998, p.97)

Dessa forma, o conjunto de conhecimentos e habilidades operatórias que devem ser agregados acerca dos números inteiros pelos alunos, segundo os PCN, deve ser construído por intermédio do seu contato com o conjunto numérico, que ocorrerá naturalmente durante o processo de resolução de problemas. Isso ocorre na medida em que a aprendizagem se sedimenta, por conferirmos aos inteiros características de objetos próprios de estudo, valorizando assim suas inter-relações, suas propriedades e sua constituição histórica.

O conjunto dos inteiros $\mathbb{Z}$ (abreviatura do termo alemão zahlen, cujo significado é número ou algarismo) tem na sua própria construção teórica sucessivos momentos de preconceito e descrédito por parte da comunidade científica, quanto a sua aceitação, logo necessitou superar diversos limites conceituais de noções cotidianas e empíricas. Quando Lima (1982), nos diz que "Incluir ou não o número 0 no conjunto $\mathbb{N}$ dos números naturais é uma questão de preferência pessoal ou, mais objetivamente, de conveniência", e entendemos que a problemática sobre a visualização dos negativos como números verdadeiros, e a respeito da associação do significado do "menos" (que pode indicar subtração ou simétrico de um número inteiro), isso precisa ser muito bem enfatizado, porque geralmente os discentes necessitam de uma atenção maior nesse momento, portanto a chegada dos números negativos, por vezes, gera muitas dúvidas.

Faz-se necessário então uma apresentação criteriosa e sequencial da estrutura dos $\mathbb{Z}$, sendo assim, neste capítulo expomos o conjunto dos inteiros, com suas propriedades usando o Princípio da Boa ordenação, incluímos também a divisibilidade, os números primos com o Teorema Fundamental da Aritmética, a divisão euclidiana, as definições de múltiplos e divisores, os critérios de divisibilidade, o uso do Máximo Divisor Comum (MDC), do Mínimo Múltiplo Comum (MMC) e finalizamos o capítulo mostrando as equações diofantinas.

2.1. Conjunto dos Inteiros

O nosso ponto de partida será o de admitir que o leitor esteja familiarizado com o conjunto dos números inteiros

$$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\},$$

juntamente com as operações de adição $(a, b) \mapsto a + b$ e de multiplicação $(a, b) \mapsto a \cdot b$.

Em $\mathbb{Z}$ há um subconjunto que se destaca, sendo ele chamado de conjunto dos números naturais e representado na notação

$$\mathbb{N} = \{1, 2, 3, 4, 5, \cdots\}.$$

Utilizando o conjunto dos números naturais, podemos também particionar o conjunto dos inteiros em três subconjuntos

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-\mathbb{N}\},$$

onde $(-\mathbb{N})$ é o conjunto dos simétricos dos elementos de $\mathbb{N}$.

Na subseção a seguir faremos uma abordagem essencialmente axiomática, partindo de uma lista de propriedades básicas dos números inteiros e das duas operações para obter as demais propriedades.

2.1.1. A Adição e a Multiplicação

As operações de adição e de multiplicação em $\mathbb{Z}$ possuem as seguintes propriedades:

1) *A adição e a multiplicação são bem definidas:*

Para todos $a, b, a', b' \in \mathbb{Z}$, se $a = a'$ e $b = b'$, então $a + b = a' + b'$ e $a \cdot b = a' \cdot b'$.

Essa propriedade é a que permite somar um dado número inteiro a ambos os lados de uma igualdade, ou multiplicar ambos os lados por um mesmo número.

2) *A adição e a multiplicação são comutativas:*

Para todos $a, b \in \mathbb{Z}, a + b = b + a$ e $a \cdot b = b \cdot a$.

3) *A adição e a multiplicação são associativas:*

Para todos $a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$ e $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

4) *A adição e a multiplicação possuem elementos neutros:*

Para todo $a \in \mathbb{Z}$, $a + 0 = a$ e $a \cdot 1 = a$.

5) *A adição possui elementos simétricos:*

Para todo $a \in \mathbb{Z}$, existe $b(= -a)$ tal que $a + b = 0$.

6) *A multiplicação é distributiva com relação a adição:*

Para todos $a, b, c \in \mathbb{Z}$, tem-se $a \cdot (b + c) = a \cdot b + a \cdot c$.

Vejamos duas proposições que são consequências desses axiomas.

Proposição 1. Para todo $a \in \mathbb{Z}$, temos $a.0 = 0$.

Demonstração.

Escrevemos $0 = 0 + 0$ e aplicamos o princípio multiplicativo seguido a propriedade distributiva, assim

$$a \cdot 0 = a(0 + 0) = a \cdot 0 + a \cdot 0$$

Somando $-(a \cdot 0)$ aos membros extremos da igualdade, pelas Propriedades 5, 3, 2 e 4, obtemos:

$$0 = -(a \cdot 0) + a \cdot 0 = -(a \cdot 0) + (a \cdot 0 + a \cdot 0)$$

$$0 = (-(a \cdot 0) + a \cdot 0) + a \cdot 0 = 0 + a \cdot 0$$

$$0 = a \cdot 0$$ ■

Proposição 2. A adição é compatível e cancelativa com respeito à igualdade:

$$\forall\, a, b, c \in \mathbb{Z}, a = b \Leftrightarrow a + c = b + c$$

Demonstração.

Da hipótese $a = b$ e desde que $c = c$, pelo fato de a adição ser bem definida, da propriedade 1, obtemos, $a + c = b + c$.

Suponha agora que $a + c = b + c$. Somando $(-c)$ a ambos os lados, obtemos o desejado. ■

2.1.2. Ordenação dos Inteiros

Antes de caracterizar os inteiros, isto é, mostrar a propriedade que somente seja admitida nesse conjunto, faremos a ordenação desses números, sendo assim admitiremos mais dois axiomas.

7) *Fechamento de* $\mathbb{N}$.

O conjunto $\mathbb{N}$ é fechado para adição e para a multiplicação, ou seja, para todos $a, b \in \mathbb{N}$, tem-se que $a + b \in \mathbb{N}$ e $a \cdot b \in \mathbb{N}$.

8) *Tricotomia.*

Dados $a, b \in \mathbb{Z}$, uma, e apenas uma, das seguintes possibilidades é verificada:

$$i)\ a = b; \qquad ii)\ b - a \in \mathbb{N} \qquad iii) -(b - a) = a - b \in \mathbb{N}$$

Diremos que a é menor do que b, simbolizado por $a < b$, toda vez que a propriedade (ii) acima for verificada.

Com essa definição, temos que a propriedade (iii) acima equivale a afirmar que $b < a$. Assim, a tricotomia nos diz que, dados $a, b \in \mathbb{Z}$, uma, e somente uma, das seguintes condições é verificada:

$$i)\ a = b \qquad ii)\ a < b \qquad iii)\ b < a$$

Usaremos a notação $b > a$, que se lê b é maior do que a, para representar $a < b$.

Como $a - 0 = a$, decorre das definições que $a > 0$ se, e somente se, $a \in \mathbb{N}$. Portanto,

$$\{x \in \mathbb{Z}; x > 0\} = \mathbb{N} \quad \text{e} \quad \{x \in \mathbb{Z}; x < 0\} = -\mathbb{N}$$

Daí decorre que $a > 0$ se, e somente se, $-a < 0$.

Proposição 3. A relação "menor do que" é transitiva:

$$\forall\, a, b, c \in \mathbb{Z}, a < b \; e \; b < c \Rightarrow a < c$$

Demonstração.

Supondo $a < b$ e $b < c$, temos que $b - a \in \mathbb{N}$ e $c - b \in \mathbb{N}$. Como $\mathbb{N}$ é aditivamente fechado, temos que, $c - a = (b - a) + (c - b) \in \mathbb{N}$, logo $a < c$. ■

Proposição 4. A adição é compatível e cancelativa com respeito à relação "menor do que":

$$\forall\, a, b, c \in \mathbb{Z}, a < b \iff a + c < b + c$$

Demonstração.

Suponha que $a < b$. Logo, $b - a \in \mathbb{N}$. Portanto, $(b + c) - (a + c) = b - a \in \mathbb{N}$, o que implica que $a + c < b + c$.

Reciprocamente, suponha que $a + c < b + c$. Pela primeira parte da proposição, podemos usar o princípio aditivo para somar $(-c)$ a ambos os lados da desigualdade, o que nos conduz ao resultado que desejamos provar. ■

Proposição 5. A multiplicação por elementos de $\mathbb{N}$ é compatível e cancelativa com respeito à relação "menor do que":

$$\forall\, a, b \in \mathbb{Z}, \forall c \in \mathbb{N}, a < b \iff ac < bc$$

Demonstração.

Suponha que $a < b$. Logo, $b - a \in \mathbb{N}$. Assim, se $c \in \mathbb{N}$, pelo fato de $\mathbb{N}$ ser multiplicativamente fechado, temos, $bc - ac = (b - a)c \in \mathbb{N}$, logo,$ac < bc$.

Reciprocamente, suponha que $ac < bc$, com $c \in \mathbb{N}$. Pela tricotomia, temos três possibilidades a analisar:

(i) $a = b$. Isso acarretaria $ac = bc$, o que é falso.

(ii) $b < a$. Isso acarretaria, pela primeira parte da demonstração, que $bc < ac$, o que também é falso.

(iii) $a < b$. Esta é a única possibilidade válida. ■

Proposição 6. A multiplicação é compatível e cancelativa com respeito à igualdade:

$$\forall\, a, b \in \mathbb{Z}, \forall\, c \in \mathbb{Z} \setminus \{0\}, a = b \iff ac = bc$$

Demonstração.

A implicação $a = b \Rightarrow ac = bc$ vale também quando $c = 0$ e decorre imediatamente do fato de a multiplicação ser bem definida pela propriedade 1. Suponha agora que $ac = bc$. Temos duas possibilidades:

(i) Caso $c > 0$. Se $a < b$, pela proposição 5, temos que $ac < bc$, o que é um absurdo. Se $b < a$, pelo mesmo argumento acima, $bc < ac$, o que é um absurdo. Portanto, a única alternativa válida é $a = b$.

(ii) Caso $-c > 0$. A argumentação segue a mesma linha usada no caso (i) acima para $c > 0$, levando em conta que $d < e$ se, e somente se, $-d > -e$. ■

Segue-se daí que $\mathbb{Z}$ é um *domínio de integridade*, isto é, se a e b são inteiros tais que $ab = 0$, então $a = 0$ ou $b = 0$. De fato, se $a \neq 0$, então $ab = 0 = 0a$. Pelo cancelamento de $a \neq 0$, segue-se que $b = 0$.

Essa propriedade admite a seguinte formulação contrapositiva:

Para todos $a, b \in \mathbb{Z} \setminus \{0\}$*, tem-se que* $ab \neq 0$.

Observe que a relação $(<)$ não é uma relação de ordem, pois não é reflexiva. Podemos no entanto, por meio dela, obter uma relação de ordem, como descrevemos a seguir.

Diremos que a é menor ou igual do que b, ou que b é maior ou igual do que a, escrevendo $a \leq b$ ou $b \geq a$, se $a < b$ ou $a = b$.

Note que $a \leq b$ se, e somente se, $b - a \in \mathbb{N} \cup \{0\}$. Veja que a relação $(<)$ não satisfaz uma relação de ordem, pois não admite ser reflexiva, porém a relação $(\leq)$, satisfaz as seguintes propriedades:

1) É *reflexiva*: $\forall\ a\ \in \mathbb{Z}, a \leq a$.

2) É *antissimétrica*: $\forall\ a, b\ \in \mathbb{Z}, a \leq b$ e $b \leq a\ \Rightarrow a = b$.

3) É *transitiva*: $\forall\ a, b, c\ \in \mathbb{Z}, a \leq b$ e $b \leq c\ \Rightarrow a \leq c$.

Agora definiremos a importante noção de valor absoluto.

Seja $a \in \mathbb{Z}$, definimos $|\ .\ |: \mathbb{Z} \to \mathbb{Z}_+$

$$|a| = \begin{cases} a, & se\ a \geq 0 \\ -a, & se\ a < 0 \end{cases}$$

Observe que para todo $a \in \mathbb{Z}$, tem-se que $|a| \geq 0$ e $|a| = 0$ se, e somente se, $a = 0$.

O número inteiro $|a|$ é chamado de *módulo* ou *valor absoluto* de a.

Proposição 7. Para $a, b\ \in \mathbb{Z}$ e $r \in \mathbb{N}$, temos

$i)\ |ab| = |a||b|;$

$ii)\ |a| \leq r\ se, e\ somente\ se, -r \leq a \leq r;$

$iii)\ -|a| \leq a \leq |a|;$

$iv)\ a\ desigualdade\ triangular$

$$\big||a| - |b|\big| \leq |a \pm b| \leq |a| + |b|$$

Demonstração.

$i)$ Vamos realizar essa demonstração de acordo com os sinais de a e b.

$a = 0 \Rightarrow a.b = 0$ e $|a| = 0 \Rightarrow |a.b| = 0$ e $|a|.|b| = 0 \Rightarrow |a.b| = |a|.|b|$.

$b = 0 \Rightarrow a.b = 0$ e $|b| = 0 \Rightarrow |a.b| = 0$ e $|a|.|b| = 0 \Rightarrow |a.b| = |a|.|b|$.

$a > 0$ e $b > 0 \Rightarrow a.b > 0$ e $|a| = a$ e $|b| = b \Rightarrow |a.b| = a.b = |a|.|b|$.

$a > 0$ e $b < 0 \Rightarrow a.b < 0$ e $|a| = a$ e $|b| = -b \Rightarrow |a.b| = -a.b = a.(-b) = |a|.|b|$.

$a < 0$ e $b > 0 \Rightarrow a.b < 0$ e $|a| = -a$ e $|b| = b \Rightarrow |a.b| = -a.b = (-a).b = |a|.|b|$.

$a < 0$ e $b < 0 \Rightarrow a.b > 0$ e $|a| = -a$ e $|b| = -b \Rightarrow |a.b| = a.b = (-a).(-b) = |a|.|b|$.

Em todos os casos observamos que sempre $|a.b| = |a|.|b|$.

$ii)$ Caso $a \geq 0$:

$$|a| \leq r \Leftrightarrow -r \leq a = |a| \leq r$$

Caso $a < 0$:

$$|a| \leq r \Leftrightarrow -r \leq -a = |a| \leq r \Leftrightarrow -r \leq a \leq r$$

$iii)$ Segue do item anterior, pondo $r = |a|$.

$iv)$ Temos, pelo item $iii)$, que

$$-(|a| + |b|) \leq a \pm b \leq |a| + |b|.$$

Pelo item $ii)$ segue-se que $|a \pm b| \leq |a| + |b|$.

Por outro lado,

$$|a| = |a \pm b \mp b| \leq |a \pm b| + |b|,$$

daí $|a| - |b| \leq |a \pm b|$.

Analogamente, $|b| - |a| \leq |a \pm b|$, ou seja, $-|a \pm b| \leq |a| - |b|$,

Portanto,

$$-|a \pm b| \leq |a| - |b| \leq |a \pm b|,$$

o que por $ii)$ implica que $|a| - |b| \leq |a \pm b|$. ■

2.1.3. Princípio da Boa Ordenação

Até o momento todas as propriedades acima mencionadas e provadas em $\mathbb{Z}$ são satisfeitas no conjunto dos racionais $(\mathbb{Q})$ e dos reais $(\mathbb{R})$. No entanto, há uma propriedade adicional que somente os inteiros possuem, chamado de *Princípio da Boa Ordenação*.

Antes de enunciarmos mais este axioma, definimos conjunto limitado inferiormente e menor elemento do conjunto.

Seja S um subconjunto de $\mathbb{Z}$, *limitado inferiormente*, se existir $c \in \mathbb{Z}$ tal que $c \leq x$, $\forall\, x \in S$. Diremos que $a \in S$ é um menor elemento de S se $a \leq x, \forall\, x \in S$.

Note que um menor elemento de S, se existir, é único, pois se a e a' são menores elementos de S, temos $a \leq a'$ e $a' \leq a$, o que acarreta $a = a'$.

Por exemplo, $\mathbb{Z}$ e $-\mathbb{N}$ não são limitados inferiormente, nem possuem um menor elemento. Por outro lado, $\mathbb{N}$ é limitado inferiormente e possui 1 como menor elemento.

A propriedade que veremos a seguir merece destaque, pois além de diferenciar os números inteiros dos racionais e dos reais, configura o único axioma que faltava para caracterizar por completo os números inteiros, assim qualquer propriedade dos números inteiros pode ser deduzida por meio desses nove axiomas.

9) *Princípio da Boa Ordenação*

Se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente então S possui um menor elemento.

Em particular, como qualquer subconjunto de $\mathbb{N}$ é limitado inferiormente (por 1), temos que todo subconjunto não vazio de $\mathbb{N}$ possui um menor elemento.

O conjunto dos $\mathbb{Z}$ tem algumas propriedades que podem ser demonstradas com o uso do Princípio da Boa Ordenação (Propriedade 9).

Vale ressaltar que uma das mais importantes consequências do Princípio da Boa Ordenação é o Princípio da Indução Matemática, que na prática se encaixa na axiomática de Peano como o axioma 4, (Teorema 1).

Teorema 1. (Princípio da Indução Matemática) Sejam S um subconjunto de $\mathbb{Z}$ e $a \in \mathbb{Z}$ tais que

$i)\ a \in S$.

$ii)\ S$ é fechado com respeito à operação de "somar 1" a seus elementos, ou seja,

$$\forall\, n, n \in S\ \Rightarrow n + 1\ \in S.$$

Então, $\{x \in \mathbb{Z}; x \geq a\} \subset S$.

Demonstração.

Seja S' um subconjunto de $\mathbb{Z}$, tal que $S' = \{x \in \mathbb{Z}; x \geq a\}$.

Agora suponhamos por absurdo que $S' \not\subset S$, logo $S' \backslash S \neq 0$. Como esse conjunto é limitado inferiormente (por a), existe um menor elemento c em $S' \backslash S$. Pelo fato de $c \in S'$ e $c \notin S$, temos que $c > a$. Portanto, $c - 1 \in S'$ e $c - 1 \in S$. Pela hipótese sobre S, temos que $c = (c - 1) + 1 \in S$, como $c \in S'$, obtemos uma contradição com o fato de $c \in S' \backslash S$. ■

Segue-se, do Princípio de Indução Matemática, um importante instrumento para provar teoremas:

Teorema 2. (Prova por Indução Matemática) Seja $a \in \mathbb{Z}$ e seja $p(n)$ uma sentença aberta em n. Suponha que

(i) $p(a)$ é verdadeiro;

(ii) $\forall\, n \geq a, p(n) \Rightarrow p(n+1)$ é verdadeiro.

Então, $p(n)$ é verdadeiro para todo $n \geq a$.

Demonstração.

Seja $\mathcal{V} = \{n \in \mathbb{Z}; p(n)$ é $verdadeira\}$, ou seja, $\mathcal{V}$ é o subconjunto dos elementos de $\mathbb{Z}$ para os quais $p(n)$ é verdadeira.

Como por (i) $a \in \mathcal{V}$ e por (ii)

$$\forall n, n \in \mathcal{V} \implies n+1 \in \mathcal{V},$$

segue-se do Princípio de Indução Matemática que $\{x \in \mathbb{Z}; x \geq a\} \subset \mathcal{V}$. ■

Exemplo 1.

Mostre por indução que a expressão abaixo é válida para soma dos n primeiros números naturais.

$$S_n = \frac{\mathrm{n(n+1)}}{2}$$

Solução.

Provaremos por indução em "n". Considere $n = 1$, assim temos que

$i)$ $P(1)$: $S_1 = 1 = \frac{1(1+1)}{2}$. Assim $P(1)$ é verdadeiro.

$ii)$ Por hipótese de indução em n, supomos verdadeira

$$P(n)\colon S_n = \frac{\mathrm{n(n+1)}}{2}$$

Mostraremos que será verdadeiro para $P(n+1)$, isto é,

$$P(n+1)\colon S_{n+1} = \frac{\mathrm{(n+1)(n+2)}}{2}$$

Para isso vamos somar $n+1$ a ambos os membros de $P(n)$.

$$S_{n+1} = S_n + n + 1 = \frac{\mathrm{n(n+1)}}{2} + n + 1$$

$$S_{n+1} = \frac{\mathrm{n(n+1)} + 2\mathrm{(n+1)}}{2} = \frac{\mathrm{(n+1)(n+2)}}{2},$$

logo $p(n+1)$ é verdadeira portanto, $p(n) = S_n$ é válida para todo $n \in \mathbb{N}$.

2.2. Divisão dos Inteiros

A operação de divisão apresenta, no contexto matemático, aspectos mais complicados do que a adição, a subtração e a multiplicação, tanto do ponto de vista operacional quanto conceitual. E como a divisão entre dois inteiros nem sempre é possível, faz-se necessário expressar essa possibilidade através da relação de divisibilidade.

Quando não existir uma relação de divisibilidade entre dois inteiros, notamos que, ainda é possível efetuar uma "divisão com resto pequeno", chamada de divisão euclidiana (item 2.4). O fato de sempre ser possível efetuar tal divisão é responsável por várias propriedades dos inteiros que iremos explorar agora.

2.2.1. Divisibilidade

Definição 1. Dados dois números naturais a e b com $a \neq 0$, diremos que a divide b, escrevendo $a \mid b$, quando existir um $c \in \mathbb{Z}$ tal que $b = a.c$. Neste caso, diremos também que a é um divisor ou um fator de b, ou ainda, que b é um múltiplo de a.

A notação $a \mid b$ diz que b é um múltiplo de a e não uma operação matemática em $\mathbb{Z}$.

A negação dessa notação será $a \nmid b$ e diremos que b não é um múltiplo de a, ou seja, não existe um $c \in \mathbb{Z}$ tal que $b = a.c$.

Proposição 8. Sejam $a, b, c \in \mathbb{Z}$. Tem-se que:

$i)$ $1 \mid a$, $a \mid a$ e $a \mid 0$.

$ii)$ $0 \mid a \Leftrightarrow a = 0$.

$iii)$ a divide b se, e somente se, $|a|$ divide $|b|$.

$iv)$ se $a \mid b$ e $b \mid c$, então $a \mid c$.

Demonstração.

(i) Isto decorre das igualdades $a = a \cdot 1$, $a = 1 \cdot a$ e $0 = 0 \cdot a$.

(ii) Suponhamos que $0 \mid a$; logo existe $c \in \mathbb{Z}$ tal que $a = c \cdot 0$. Pela proposição 1 conclui-se que $a = 0$. Para a recíproca basta observar que $0 \mid 0$,

(iii)

$(\Rightarrow)$ $a \mid b \Rightarrow b = a.q \Rightarrow |b| = |a|.|q|,\ |q| \in \mathbb{Z} \Rightarrow |a| \mid |b|$

$(\Leftarrow)$ $|a| \mid |b| \Rightarrow |b| = |a|.|q|$, com 4 casos:

1) $b > 0$ e $a > 0 \Rightarrow b = a.q \Rightarrow a \mid b$

2) $b > 0$ e $a < 0 \Rightarrow b = (-a).q \Rightarrow a|b$

3) $b < 0$ e $a > 0 \Rightarrow -b = a.q \Rightarrow a|b$

4) $b < 0$ e $a < 0 \Rightarrow -b = (-a).q \Rightarrow a|b$

(iv) $a|b$ e $b|c$ implica que existem $f, g \in \mathbb{Z}$, tais que $b = fa$ e $c = gb$. Substituindo o valor de b da primeira equação na outra, obtemos

$$c = gb = g(fa) = (gf)a$$

o que nos mostra que $a|c$. ■

Os itens (i) e (ii) da proposição acima nos dizem que todo número inteiro a é divisível por ± 1 e por $\pm a$.

Note também que (i) inclui o caso $0|0$ e, portanto, todo número inteiro divide 0. Assim, 0 tem infinitos divisores.

Suponha que $a|b$ e que $a \neq 0$. Seja $c \in \mathbb{Z}$ tal que $b = ca$. O número inteiro c, univocamente determinado, é chamado de quociente de b por a e denotado por $c = \frac{b}{a}$.

Exemplo 2.

$$\frac{0}{1} = \frac{0}{2} = 0,\ \frac{6}{1} = 6,\ \frac{6}{2} = 3,\ \frac{6}{-3} = -2,\ \frac{6}{3} = 2,\ \frac{6}{6} = 1$$

Uma observação importante é que $\frac{b}{a}$ só está definido quando $a \neq 0$ e $a|b$.

Proposição 9. Se $a, b, c, d \in \mathbb{Z}$, então $a|b$ e $c|d \Rightarrow ac|bd$

Demonstração.

Se $a|b$ e $c|d$, então $\exists\ f, g \in \mathbb{Z}, b = fa$ e $d = gc$. Portanto, $bd = (fg)(ac)$, logo $ac|bd$. ■

Em particular, se $a|b$, então $ac|bc$, para todo $c \in \mathbb{Z}$.

Proposição 10. Sejam $a, b, c \in \mathbb{Z}$, tais que $a|(b \pm c)$. Então, $a|b \Leftrightarrow a|c$.

Demonstração.

Suponhamos que $a|(b + c)$. Logo, existe $f \in \mathbb{Z}$ tal que $b + c = fa$.

Agora, se $a|b$, temos que existe $g \in \mathbb{Z}$ tal que $b = ga$. Juntando as duas igualdades acima, vamos ter $ga + c = fa$, donde segue-se que $c = (f - g)a$, logo $a|c$.

Por outro lado, se $a|(b - c)$ e $a|b$, pelo caso anterior, temos que $a|-c$, o que implica que $a|c$. ■

Proposição 11. Se $a, b, c \in \mathbb{Z}$ são tais que $a|b$ e $a|c$, então para todo $x, y \in \mathbb{Z}$

$$a|(xb + yc)$$

Demonstração.

Desde que $a|b$ e $a|c$ existem $f, g \in \mathbb{Z}$ tais que $b = fa$ e $c = ga$. Logo,

$$xb + yc = x(fa) + y(ga) = (xf + yg)a$$

o que prova o resultado. ■

Proposição 12. Dados $a, b \in \mathbb{Z}$, onde $b \neq 0$, temos que $a|b \Longrightarrow |a| \leq |b|$.

Demonstração.

De fato, se $a|c$, existe $c \in \mathbb{Z}$ tal que $b = ca$. Tomando módulos, temos que $|b| = |c||a|$. Com $b \neq 0$, temos que $c \neq 0$, logo $1 \leq |c|$ e, consequentemente, $|a| \leq |a||c| = |b|$. ■

Em particular, se $a \in \mathbb{Z}$ e $a|1$, então $0 < |a| \leq 1$, logo $|a| = 1$ e, portanto, $a = \pm 1$.

Como, para $b \neq 0$, temos que todo divisor a de b é tal que $|a| \leq |b|$, segue-se, nesse caso, que b tem um número finito de divisores que estão no intervalo $-|b| \leq a \leq |b|$.

Observe que a relação de divisibilidade em $\mathbb{N} \cup \{0\}$ é uma relação de ordem, pois ela é reflexiva (Proposição 8 (i)), transitiva (Proposição 8 (ii)) e também é antissimétrica (Proposição 12).

Devemos observar, portanto, que a relação de divisibilidade não é uma relação de ordem em $\mathbb{Z}$, pois, apesar de ainda ser reflexiva e transitiva, ela não é antissimétrica. De fato, $\pm 2 | \pm 2$, mas $2 \neq -2$.

As próximas três proposições são de grande importância, uma vez que as mesmas serão utilizadas nas congruências, que será abordada no capítulo 3.

Proposição 13. Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a - b$ divide $a^n - b^n$.

Demonstração.

Vamos provar essa proposição com o uso da indução sobre n.

Observe que a afirmação é verdadeira para $n = 1$, pois $a - b$ divide $a^1 - b^1 = a - b$.

Suponhamos, agora, que $a - b | a^n - b^n$. Escrevamos

$$a^{n+1} - b^{n+1} = aa^n - \boldsymbol{ba^n} + \boldsymbol{ba^n} - bb^n = (a-b)a^n + b(a^n - b^n)$$

Como $a - b | a - b$ e, por hipótese, $a - b | a^n - b^n$, decorre das igualdades acima e da Proposição 11, que $a - b | a^{n+1} - b^{n+1}$, estabelecendo, assim, o resultado para todo $n \in \mathbb{N}$. ■

A proposição acima tem uma aplicação muito interessante que é o fato de que todo número da forma $10^n - 1$, onde n é natural, seja divisível por 9. Para verificarmos isso, basta fazer $a = 10$ e $b = 1$, obtendo que $a - b = 9$ divide $a^n - b^n = 10^n - 1$.

Proposição 14. Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N} \cup \{0\}$. Temos que $a + b$ divide $a^{2n+1} + b^{2n+1}$.

Demonstração.

Vamos provar essa proposição com o uso da indução sobre n.

A afirmação é verdadeira para $n = 0$, pois $a + b$ divide $a^1 + b^1 = a + b$.

Suponhamos, agora, que $a + b | a^{2n+1} + b^{2n+1}$. Escrevamos

$$a^{2(n+1)+1} + b^{2(n+1)+1} = a^2 a^{2n+1} - \boldsymbol{b^2 a^{2n+1}} + \boldsymbol{b^2 a^{2n+1}} + b^2 b^{2n+1}$$

$$a^{2(n+1)+1} + b^{2(n+1)+1} = (a^2 - b^2)a^{2n+1} + b^2(a^{2n+1} + b^{2n+1})$$

Como $a+b$ divide $a^2-b^2=(a+b)(a-b)$ e, por hipótese, $a+b|a^{2n+1}+b^{2n+1}$, decorre das igualdades acima e da Proposição 11, que $a+b|a^{2(n+1)+1}+b^{2(n+1)+1}$, estabelecendo, assim, o resultado para todo $n \in \mathbb{N}$. ■

Proposição 15. Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a+b$ divide $a^{2n}-b^{2n}$.

Demonstração.

Novamente usaremos indução sobre n.

A afirmação é verdadeira para $n=1$, pois $a+b$ divide $a^2-b^2=(a+b)(a-b)$.

Suponhamos, agora, que $a+b|a^{2n}-b^{2n}$. Escrevamos

$$a^{2(n+1)}-b^{2(n+1)}=a^2a^{2n}-\boldsymbol{b^2a^{2n}+b^2a^{2n}}-b^2b^{2n}=(a^2-b^2)a^{2n}+b^2(a^{2n}-b^{2n}).$$

Como $a+b|a^2-b^2$ e, por hipótese, $a+b|a^{2n}-b^{2n}$, decorre das igualdades acima e da Proposição 11 que $a+b|a^{2(n+1)}-b^{2(n+1)}$, o que estabelece, desse modo, o resultado para todo $n \in \mathbb{N}$. ■

2.3. Números Primos

Nesse item, vamos iniciar o estudo dos números primos. Este é sem dúvida um dos conceitos mais importantes de toda a Matemática, uma vez que esses números desempenham um papel fundamental e a eles estão associados diversos problemas cujas soluções ajudaram a construir a Matemática que temos hoje.

Do ponto de vista da estrutura multiplicativa dos naturais, os números primos são os mais simples e ao mesmo tempo são suficientes para gerar todos os números naturais, logo, todos os números inteiros não nulos, conforme veremos a seguir no *Teorema Fundamental da Aritmética*.

2.3.1. Teorema Fundamental da Aritmética

Definição 2. Um número natural maior do que 1 que só possui como divisores positivos 1 e ele próprio é chamado de *número primo*.

Um número maior do que 1 e que não é primo será dito *composto*.

Portanto, se um número natural $n>1$ é composto, existirá um divisor natural n_1 de n tal que $1<n_1<n$. Logo, existirá um número natural n_2 tal que

$$n=n_1n_2, \text{ com } 1<n_1<n \text{ e } 1<n_2<n.$$

Assim, os números 2, 3, 5, 7, 11 e 13 são números primos, enquanto 4, 6, 8, 9, 10 e 12 são números compostos.

Teorema 3. (Teorema Fundamental da Aritmética) Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.

Demonstração.

Usaremos o Princípio da Indução. Se $n = 2$, o resultado é obviamente verificado.

Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale para n.

Se o número n é primo, nada temos a demonstrar. Suponhamos, então, que n seja composto. Logo, existem números naturais n_1 e $n_2$tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, \cdots, p_r$ e $q_1, \cdots, q_s$, tais que,

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

Portanto, $n = p_1 \cdots p_r q_1 \cdots q_s$.

Agora, vamos provar a unicidade da escrita.

Suponha que tenhamos $n = p_1 \cdots p_r = q_1 \cdots q_s$, onde os p_i e os q_j são números primos. Como $p_1 | q_1 \cdots q_s$, temos que $p_1 = q_j$ para algum j, que, após reordenamento de $q_1 \cdots q_s$, podemos supor que seja q_1. Portanto,

$$p_2 \cdots p_r = q_2 \cdots q_s.$$

Como $p_2 \cdots p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares.

■

Teorema 4. Dado um número inteiro $n \neq 0, 1, -1$, existem primos $p_1 < \cdots < p_r$ e $\alpha_1, \cdots, \alpha_r \in \mathbb{N}$, univocamente determinados, tais que

$$n = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}. \quad (2.1)$$

Isso se faz necessário, pois quando estivermos lidando com a decomposição em fatores primos de dois, ou mais números naturais, usaremos o recurso de acrescentar fatores da forma $p^0 (= 1)$, onde p é um número primo qualquer. Assim, dados $n, m \in \mathbb{N}$ com $n > 1$ e $m > 1$ quaisquer, podemos escrever

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \text{ e } m = p_1^{\beta_1} \cdots p_r^{\beta_r},$$

usando o mesmo conjunto de primos $p_1, \cdots, p_r$, desde que permitamos que os expoentes $\alpha_1, \cdots, \alpha_r$, $\beta_1, \cdots, \beta_s$, variem em $\mathbb{N} \cup \{0\}$ e não apenas em $\mathbb{N}$.

Dessa forma, os números $2^3 \cdot 3^2 \cdot 7 \cdot 11$ e $2 \cdot 5^2 \cdot 13$ podem ser escritos da seguinte forma, respectivamente, $2^3 \cdot 3^2 \cdot 5^0 \cdot 7 \cdot 11. 13^0$ e $2 \cdot 3^0 \cdot 5^2 \cdot 7^0 \cdot 11^0 \cdot 13$.

Note que um número natural $n > 1$, escrito na forma $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, como visto no teorema acima, será um quadrado perfeito, ou seja, se o número n pode ser escrito na forma $n = a^2$ se, e somente se, cada expoente α_i for par.

Quando escrevemos um número composto n de forma fatorada, isto é, em função de números primos $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, dizemos que n está na forma canônica.

Proposição 16. Seja $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ um número natural escrito na forma acima. Se n' é um divisor positivo de n, então

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

onde $0 \leq \beta_i \leq \alpha_i$, para $i = 1, \cdots, r$

Demonstração.

Seja n' um divisor positivo de n e seja p^{β} a potência de um primo p que figura na decomposição de n' em fatores primos. Como $p^{\beta} | n$, segue que p^{β} divide algum $p_i^{\alpha_i}$, por ser primo com os demais $p_j^{\alpha_j}$, e, consequentemente, $p = p_i$ e $0 \leq \beta \leq \alpha_i$. ■

Teorema 5. A quantidade de divisores de um número natural $\mathbb{N}$, $d(n)$, é dado pelo produto de todos os sucessivos expoentes de seus fatores primos.

Demonstração.

Seja n um número composto escrito da forma $n = p_1^{\alpha} \times p_2^{\beta} \times p_3^{\gamma} \times \cdots$, então:

$d(p_1^{\alpha}) = \{p_1^0,\ p_1^1, p_1^2, \cdots, p_1^{\alpha}\}$, ou seja, $(\alpha + 1)$ divisores; (linha 1)

$d\left(p_2^{\beta}\right) = \left\{p_2^0,\ p_2^1, p_2^2, \cdots, p_2^{\beta}\right\}$, ou seja, $(\beta + 1)$ divisores; (linha 2)

$d\left(p_3^{\gamma}\right) = \left\{p_3^0,\ p_3^1, p_3^2, \cdots, p_3^{\gamma}\right\}$, ou seja, $(\gamma + 1)$ divisores; (linha 3)

Multiplicando-se agora os $(\alpha + 1)$ divisores da linha 1 pelos $(\beta + 1)$ divisores da linha 2 e, em seguida, os $[(\alpha + 1) \times (\beta + 1)]$ divisores anteriores pelos $(\gamma + 1)$ divisores da linha 3 e, assim, sucessivamente, obtemos a quantidade $d(n)$ de divisores de $\mathbb{N}$, ou seja:

$$d(n) = (\alpha + 1) \times (\beta + 1) \times (\gamma + 1) \times \cdots \quad (2.2)$$

■

Exemplo 3. Determine a quantidade de divisores positivos de 360.

Solução.

Iniciamos escrevendo o número 360, na sua forma canônica, ou seja, $360 = 2^3 \times 3^2 \times 5^1$, em seguida, verificamos os expoentes dos fatores primos $(\alpha = 3, \beta = 2, \gamma = 1)$, assim usamos esses valores em (2.2).

$$d(360) = (3 + 1) \times (2 + 1) \times (1 + 1) = 4 \times 3 \times 2 = 24$$

Logo, 360 possui 24 divisores positivos.

A quantidade de divisores de um número, pode ser usada também para saber se aquele valor em análise é ou não um quadrado perfeito, ou seja, se o número n pode ser escrito na forma $n = a^2$, onde n, $a \in \mathbb{N}$. Nesse caso, devemos observar a paridade do valor encontrado, se $d(n)$ for um número ímpar, então ele é um quadrado perfeito, sendo par, não.

Exemplo 4. Determine se os números 144 e 180 são quadrados perfeitos.

Solução.

Escrevendo os números na forma canônica, temos: $144 = 2^4 \times 3^2$ e $180 = 2^2 \times 3^2 \times 5^1$,

$$d(144) = (4+1) \times (2+1) = 15$$

$$d(180) = (2+1) \times (2+1) \times (1+1) = 18$$

Como $d(144)$ é ímpar, então 144 é um quadrado perfeito, enquanto $d(180)$ é par, logo 180 não é um quadrado perfeito.

A fatoração de números naturais em primos revela toda a estrutura multiplicativa desses números, permitindo, entre muitas outras coisas, determinar facilmente o MDC e o MMC de um conjunto qualquer de números, como veremos nos itens 2.6 e 2.7, respectivamente.

2.3.2. Distribuição dos Números Primos

Notamos até aqui o quão importante são os números primos para a Matemática, mas sempre nos questionamos com uma pergunta clássica: “Quantos números primos existem?”. Essa pergunta foi respondida em um teorema enunciado e demonstrado por Euclides no Livro IX dos *Elementos*. Utilizaremos a mesma prova dada por Euclides, que usou pela primeira vez segundo os registros uma demonstração por redução ao absurdo em matemática. Essa prova é considerada uma das pérolas da matemática.

Teorema 6. Existem infinitos números primos.

Demonstração.

Suponha que exista apenas um número finito de números primos $p_1, \cdots, p_r$. Considere o número natural

$$n = p_1 p_2 \cdots p_r + 1$$

Pelo Teorema 6, o número n possui um fator primo p que, portanto, deve ser um dos $p_1, \cdots, p_r$ e, consequentemente, divide o produto $p_1 p_2 \cdots p_r$. Mas isto implica que p divide 1, o que é absurdo. ■

Agora que sabemos que existem infinitos números primos, como podemos obter uma lista contendo os números primos até uma dada ordem. Um dos métodos mais usados é chamado de *Crivo de Erastóstenes,* tal procedimento é devido ao matemático Erastóstenes, que viveu por volta de 230 a.C.

Esse dispositivo prático permite determinar todos os números primos até a ordem que se deseja, porém ele não é muito eficiente para ordens muito elevadas. Como nosso estudo é direcionado ao ensino básico (6º e 7º anos), o Crivo de Erastóstenes atende as nossas necessidades.

Vamos então elaborar a tabela de todos os números primos inferiores a 200. Nessa construção, devemos empregar o procedimento ensinado por Erastóstenes, cuja regra é a seguinte:

Escrevem-se todos os números naturais, a partir de 2, até o número considerado;

- A partir de 2, exclusive, cancelam-se todos os múltiplos de 2;
- A partir de 3, exclusive, cancelam-se todos os múltiplos de 3;
- A partir de 5, exclusive, cancelam-se todos os múltiplos de 5;
- A partir de 7, 11 e 13, exclusive, cancelam-se todos os múltiplos de 7, 11 e 13 respectivamente;

Não é necessário prosseguir com este procedimento até chegar a 200, para isso vamos usar um resultado devido ao próprio Erastóstenes.

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

Demonstração.

Suponhamos, por absurdo, que n não seja divisível por nenhum número primo p tal que $p^2 \leq n$ e que não seja primo. Seja q o menor número primo que divide n; então, $n = qn_1$, com $q \leq n_1$. Segue daí que $q^2 \leq qn_1 = n$. Logo, n é divisível por um número primo q tal que $q^2 \leq n$, absurdo. ■

Tabela 01 – Crivo de Erastótenes menores que 200

Números primos menores que 200									
1	**2**	**3**	4	**5**	6	**7**	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	**97**	98	99	100
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
151	152	153	154	155	156	**157**	158	159	160
161	162	**163**	164	165	166	**167**	168	169	170
171	172	**173**	174	175	176	177	178	**179**	180
181	182	183	184	185	186	187	188	189	190
191	192	**193**	194	195	196	**197**	198	**199**	200

Fonte: O próprio Autor

Portanto, na nossa tabela 01 de números de 1 a 200, seguimos até alcançarmos o primo 13, pois o próximo primo é 17, cujo quadrado supera 200, ou seja, $17^2 > 200$.

Observe que o Lema 1 também nos fornece um teste de primalidade, pois, para verificar se um dado número n é primo, basta verificar que não é divisível por nenhum primo p que não supere $\sqrt{n}$. Outra importante questão que se coloca é de como os números primos se distribuem dentro dos números naturais. Em particular, qual pode ser a distância entre dois primos consecutivos?

Na tabela 1, nota-se que há vários pares de números primos que diferem de duas unidades. Esses são: $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(41,43)$, $(59,61)$, $(71,73)$, $(101,103)$, $(107,109)$, $(137,139)$, $(149,151)$, $(191,193)$, $(197,199)$. Os números primos com essa propriedade são chamados de *primos gêmeos*. Até o presente momento, ainda não se sabe se existem infinitos pares de primos gêmeos. Por outro lado, em contraste com esses pares de primos consecutivos muito próximos, existem primos consecutivos arbitrariamente afastados. Portanto, não há nenhum padrão que descreva o quanto dois primos consecutivos estão longe um do outro.

2.4. Divisão Euclidiana

Mesmo quando um número inteiro b ≠ 0 não divide o número inteiro a, Euclides, nos seus *Elementos*, utiliza, sem enuncia-lo explicitamente, o fato de que é sempre possível efetuar a divisão de a por b, com resto. Esse resultado, cuja demonstração faremos abaixo, não só é um importante instrumento na obra de Euclides, como também é um resultado central da teoria.

Teorema 7. (Divisão Euclidiana) Sejam a e b dois números inteiros, com $b \neq 0$. Existem dois únicos números inteiros q e r tais que

$$a = bq + r, \text{ com } 0 \leq r < |b| \qquad (2.3)$$

Demonstração.

Considere o conjunto

$$S = \{x = a - by; y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$$

Existência: Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$, então existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$, logo $a - nb > 0$, o que mostra que S é não vazio. O conjunto S é limitado inferiormente por 0, logo, pelo Princípio da Boa Ordenação, temos que S possui um menor elemento r. Suponhamos então que $r = a - bq$. Sabemos que $r \geq 0$. Vamos mostrar que $r < |b|$. Suponhamos por absurdo que $r \geq |b|$.

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

Unicidade: Suponha que $a = bq + r = bq' + r'$, onde $q, q', r, r' \in \mathbb{Z}$, $0 \leq r < |b|$ e $0 \leq r' < |b|$, Assim, temos que $-|b| < -r \leq r' - r \leq r' < |b|$. Logo, $|r' - r| < |b|$. Por outro lado, $b(q - q') = r' - r$, o que implica que

$$|b||q - q'| = |r' - r| < |b|,$$

o que só é possível se $q = q'$ e consequentemente, $r = r'$. ■

Os números que q e r que aparecem no teorema acima são chamados respectivamente de ***quociente*** e de ***resto*** da divisão de a por b. Assim, da divisão euclidiana, temos que o resto da divisão de a por b é zero se, e somente se, b divide a. Quando o resto da divisão for zero ($r = 0$), dizemos que a divisão é exata.

Exemplo 5. O quociente e o resto da divisão de 17 por 3 são $q = 5$ e $r = 2$. O quociente e o resto da divisão de -17 por 3 são $q = -6$ e $r = 1$.

Dado um número natural a, a unicidade do quociente e do resto na divisão euclidiana por b nos permite definir duas importantes funções que descrevermos a seguir.

A primeira delas denotamos por $q_b(a)$ o quociente da divisão do número a por b, definimos a função quociente por b como segue:

$$q_b: \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$a \longmapsto q_b(a)$$

Corolário 1. Dados dois inteiros a e b com $b > 0$, existe um único número inteiro $n(= q_b(a))$ tal que

$$nb \leq a < (n + 1)b$$

Demonstração.

Pela divisão euclidiana, temos que existem q e $r \in \mathbb{Z}$ com $0 \leq r < b$, univocamente determinados, tais que $a = bq + r$. Para concluir, basta tomar $n = q$. ■

Esse corolário foi a justificativa usada por Euclides, sem demonstração, para um inteiro $a > 0$ possa ser dividido. O inteiro $q_b(a)$ pode também ser interpretado como o maior inteiro menor ou igual do que o número racional $\frac{a}{b}$.

De fato, pois pelo corolário 1, temos que, se r é o resto da divisão de a por b, então

$$q_b(a)b \leq a = q_b(a)b + r < (q_b(a) + 1)b,$$
$$q_b(a) \leq \frac{a}{b} < q_b(a) + 1$$

Assim, o inteiro $q_b(a)$ será denotado pelo símbolo $\left[\frac{a}{b}\right]$ e será chamado de parte inteira do número racional $\frac{a}{b}$.

A segunda função importante determinada pela divisão euclidiana é a função resto, definida por:

$$r_b: \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$a \longmapsto r_b(a)$$

onde $r_b(a)$ é o resto da divisão de a por b.

Exemplo 6. Dado um número inteiro $n \in \mathbb{Z}$ qualquer, temos duas possibilidades:

$i)$ o resto da divisão de n por 2 é 0, ou seja, existe $q \in \mathbb{N}$ tal que $n = 2q$;

$ii)$ o resto da divisão de n por 2 é 1, ou seja, existe $q \in \mathbb{N}$ tal que $n = 2q + 1$.

Portanto, os números inteiros dividem-se em duas classes, a dos números na forma $2q$ para algum $q \in \mathbb{Z}$, chamados de *números pares*, e a dos números da forma $2q + 1$, chamados de números ímpares. Essa classificação já havia sido feita por Pitágoras para os números naturais, isto é, os naturais também podem ser pares ou ímpares.

Apesar de parecer um aspecto simples, a paridade de um número inteiro será importante na determinação da paridade da soma e do produto de dois números a partir da paridade dos números envolvidos na operação.

2.5. Critérios de Divisibilidade

O currículo escolar do ensino fundamental já contempla os critérios de divisibilidade, uma vez que eles serão utilizados em outras áreas da matemática, como Geometria e Álgebra. Na prática esse conjunto de regras a serem memorizadas e aplicadas de maneira direta, só é útil quando for mais simples que a própria divisão. Esse é um dos motivos que fazem os alunos sempre lembrarem dos critérios de divisibilidade do 2, 3, 5 e 10 por exemplo e quase nunca dos critérios do 7, 11 e 13. No entanto, o aluno que desenvolve a habilidade de usar com frequência as regras de divisibilidade, em especial na resolução de problemas, tem como consequência imediata (a) memorização dos critérios e (b) velocidade de resolução. Esse segundo ponto se mostrará muito necessário quando o aluno for prestar algum exame, como as provas Olímpicas ou o Enem por exemplo, pois neles o tempo será um fator a ser considerado no desempenho do exame. Ainda nesse sentido, usamos muito os critérios de divisibilidade para simplificar resultados, pois é comum nos exames seletivos as repostas serem dadas na forma de frações irredutíveis, ou seja, frações que não podem ser simplificadas.

De modo geral, podemos definir de forma direta que os critérios de divisibilidade são as regras que nos permitem, sem efetuar a divisão, saber se um dado número é, ou não, divisível por outro. Veremos também que, a partir da determinação dos restos, poderemos verificar tais critérios. Antes, porém, vamos precisar definir os conceitos de múltiplos e divisores de um número inteiro.

2.5.1. Múltiplos e Divisores de um Inteiro

Sejam a e b dois números naturais. Diz-se que a divide b, se existir um número inteiro k, tal que $b = a.k$. Podemos encontrar também outras terminologias que satisfazem essa definição, tais como: a é divisor de b, que b é divisível por a ou ainda que b é múltiplo de a.

a) Múltiplo de um Inteiro

Definição 3. Múltiplo é cada um dos produtos que se obtém, multiplicando-se o número N por outro inteiro qualquer:

Representamos o conjunto dos múltiplos de um número inteiro N por: Múlt. N; $M(N)$ ou ainda $\dot{N}$, essa última notação é devida a K. F. Gauss. Como $N = \{0,\ \pm1,\ \pm2,\ \pm3,\ \cdots\}$, teremos para um múltiplo de N os números:

$\{N \times 0, N \times (\pm1), N \times (\pm2), N \times (\pm3), \cdots\}$, isto é, $\dot{N} = \{0, \pm N, \pm 2N, \pm 3N, \cdots\}$

Exemplo 7. Determinar os múltiplos inteiros de 3.

$3 \times 0 = 0, 3 \times (\pm1) = \pm3, 3 \times (\pm2) = \pm6, \cdots$. Portanto $\dot{3} = \{0, \pm3, \pm6, \pm9, \cdots\}$

b) Múltiplos Comuns.

São números que pertencem simultaneamente ao conjunto dos múltiplos de dois ou mais números dados.

Representamos o conjunto dos múltiplos comuns de dois ou mais números inteiros por M_C.

Exemplo 8. Determinar os múltiplos inteiros comuns de 3 e 4.

$$\dot{3} = \{0, \pm3, \pm6, \pm9, \pm\mathbf{12}, \pm15, \pm18, \pm21, \pm\mathbf{24}, \pm27, \pm30, \pm33, \pm\mathbf{36}, \pm39, \cdots\}$$

$$\dot{4} = \{0, \pm4, \pm8, \pm\mathbf{12}, \pm16, \pm20, \pm\mathbf{24}, \pm28, \pm32, \pm\mathbf{36}, \pm40, \cdots\}$$

Assim, com a intersecção dos conjuntos de múltiplos acima, teremos:

$$M_C(3,4) = \{0, \pm12, \pm24, \pm36, \cdots\}.$$

c) Divisor de um Inteiro

Definição 4. São números que dividem exatamente um número inteiro dado.

Representamos o conjunto dos divisores de um número inteiro qualquer N por $D_{(N)}$.

Exemplo 9. Determinar todo os divisores inteiros exatos de 20.

O ±1 é divisor de 20, pois, $20 \div (\pm1) = \pm20 \Rightarrow$ resto zero.

O ±2 é divisor de 20, pois, $20 \div (\pm2) = \pm10 \Rightarrow$ resto zero.

O ±4 é divisor de 20, pois, $20 \div (\pm4) = \pm5 \Rightarrow$ resto zero.

O ±5 é divisor de 20, pois, $20 \div (\pm5) = \pm4 \Rightarrow$ resto zero.

O ±10 é divisor de 20, pois, $20 \div (\pm10) = \pm2 \Rightarrow$ resto zero.

O ± 20 é divisor de 20, pois, $20 \div (\pm 20) = \pm 1 \Rightarrow$ resto zero.

Portanto, temos $D_{(20)} = \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20\}$.

d) Divisores Comuns

São os números que dividem simultaneamente dois ou mais números dados.

O conjunto dos divisores comuns de dois ou mais números inteiros será denotado por $D_{(C)}$.

Exemplo 10. Determinar os divisores inteiros exatos comuns de 18 e 30.

$$D_{(18)} = \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18\}$$

$$D_{(30)} = \{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30\}$$

Assim, com a intersecção dos conjuntos de divisores acima, teremos:

$$D_{(C)}(18, 30) = \{\pm 1, \pm 2, \pm 3, \pm 6\}.$$

Teorema 9. (Teorema Fundamental da Divisibilidade) Se um número d divide uma de duas parcelas a e b de uma adição, a soma S e a outra parcela apresentará o mesmo resto em relação a esse divisor.

Demonstração.

Se d é o divisor de a, então, $a = \dot{d}$;

$$\frac{\mathrm{b}}{\mathrm{d}} = q_1 + r \ \rightarrow b = d.q_1 + r \ \therefore b = \dot{d} + r \qquad (*)$$

Se $a + b = S \rightarrow \dot{d} + \dot{d} + r = S \ \rightarrow S = \dot{d} + r \qquad (**)$

De $(*)$ e $(**)$, podemos observar que o resto é o mesmo, ou seja, S e b deixam o mesmo resto quando divididos por d. ■

Teorema 10. Se vários números $a, b, c, \cdots$ forem divididos por um mesmo divisor d, a soma S desses números e a soma dos restos $r_1 + r_2 + r_3 + \cdots$, ou seja, S_r, obtidos dessas divisões por esse divisor, apresentará o mesmo resto em relação ao mesmo divisor.

Demonstração.

$$\frac{\mathrm{a}}{\mathrm{d}} = q_1 + r_1 \rightarrow a = d.q_1 + r_1 \therefore a = \dot{d} + r_1$$

$$\frac{\mathrm{b}}{\mathrm{d}} = q_2 + r_2 \rightarrow b = d.q_2 + r_2 \therefore b = \dot{d} + r_2$$

$$\frac{\mathrm{c}}{\mathrm{d}} = q_3 + r_3 \rightarrow c = d.q_3 + r_3 \therefore c = \dot{d} + r_3$$

$$\vdots$$

Somando as igualdades anteriores, membro a membro, teremos:

$$a + b + c + \cdots = (\dot{d} + r_1) + (\dot{d} + r_2) + (\dot{d} + r_3) + \cdots \text{ ou}$$

$$a + b + c + \cdots = \underbrace{\dot{d} + \dot{d} + \dot{d} + \cdots}_{\dot{d}} + \underbrace{r_1 + r_2 + r_3 + \cdots}_{S_r} \text{ ou ainda,}$$

$$S = \dot{d} + S_r \qquad (2.4)$$

Dividindo-se os dois membros por d e aplicando o Teorema Fundamental da Divisibilidade (Teorema 9), podemos afirmar que tanto a soma S como a soma dos restos S_r deixam o mesmo resto quando divididos por d. ■

Teorema 11. Dividindo-se vários números $a, b, c, \cdots$ pelo mesmo divisor d, o produto P desses números e o produto dos restos P_r, dessas divisões por esse divisor, apresentará o mesmo resto em relação ao mesmo divisor.

Demonstração.

Tomemos, inicialmente, os números a e b e para o divisor o número d.

$$\begin{array}{r|l} a & d \\ r_1 & q_1 \end{array} \ldots (1) \qquad \begin{array}{r|l} b & d \\ r_2 & q_2 \end{array} \ldots (2)$$

De (1) e (2), podemos escrever que:

$$a = d.q_1 + r_1 \therefore a = \dot{d} + r_1 \quad (3)$$

$$b = d.q_2 + r_2 \therefore b = \dot{d} + r_2 \quad (4)$$

Multiplicando-se (3) e (4), membro a membro, teremos:

$$a \times b = \left(\dot{d} + r_1\right) \times \left(\dot{d} + r_2\right) = \dot{d} \times \dot{d} + \dot{d} \times r_1 + \dot{d} \times r_2 + r_1 \times r_2$$

$$a \times b = \dot{d} + r_1 \times r_2$$

Se tomarmos três fatores e fizermos um desenvolvimento análogo ao anterior concluiremos que:

$$a \times b \times c = \dot{d} + r_1 \times r_2 \times r_3$$

Assim, para n fatores, isto é, $a \times b \times c \times \cdots$, teremos

$$\underbrace{a \times b \times c \times \cdots}_{P} = \dot{d} + \underbrace{r_1 \times r_2 \times r_3 \times \cdots}_{P_r} \quad (5)$$

$$P = \dot{d} + P_r \qquad (2.5)$$

Dividindo-se os dois membros de (5) por d e aplicando o Teorema Fundamental da Divisibilidade (Teorema 9), podemos afirmar que tanto o produto P como o produto dos restos P_r deixam o mesmo resto quando divididos por d. ■

Teorema 12. Dividindo-se n números iguais $a, a, a, \cdots$ pelo mesmo divisor d, a potência gerada por a^n e a gerada por r^n, onde r seja o resto da divisão do fator a por d, apresentará o mesmo resto em relação a esse divisor.

Demonstração.

Tomemos, inicialmente, o número a para o divisor o número d.

$$\begin{array}{r|l} a & d \\ r_1 & q_1 \end{array} \ldots (1) \qquad \begin{array}{r|l} b & d \\ r_2 & q_2 \end{array} \ldots (2)$$

De (1) e (2), podemos escrever que:

$$a = d.q_1 + r_1 \therefore a = \dot{d} + r_1 \quad (3)$$

$$b = d.q_2 + r_2 \therefore b = \dot{d} + r_2 \quad (4)$$

Multiplicando-se (3) e (4), membro a membro, teremos:

$$a \times b = (\dot{d} + r_1) \times (\dot{d} + r_2) = \dot{d} \times \dot{d} + \dot{d} \times r_1 + \dot{d} \times r_2 + r_1 \times r_2$$

$$a \times b = \dot{d} + r_1 \times r_2$$

Se tomarmos três fatores e fizermos um desenvolvimento análogo ao anterior concluiremos que:

$$a \times b \times c = \dot{d} + r_1 \times r_2 \times r_3$$

Fazendo $a = b = c = \cdots = a$ e $r_1 = r_2 = r_3 = \cdots = r$

Assim, para n fatores, isto é, $a \times a \times a \times \cdots$, teremos

$$\underbrace{a \times a \times a \times \cdots}_{a^n} = \dot{d} + \underbrace{r \times r \times r \times \cdots}_{r^n} \quad (5)$$

$$a^n = \dot{d} + r^n \qquad (2.6)$$

Dividindo-se os dois membros de (5) por d e aplicando o Teorema Fundamental da Divisibilidade (Teorema 9), podemos afirmar que a potência gerada por a^n bem como a potência dos restos r^n deixam o mesmo resto quando divididos por d. ■

Os últimos quatro teoremas apresentados (9, 10, 11 e 12) serão as bases de sustentação para demonstramos os critérios de divisibilidade. A escolha desse formato se justifica pelo fato de os livros didáticos usados no ciclo básico apresentarem apenas a divisão euclidiana, sem o uso de congruências, no entanto, ele por si só é suficiente para ratificar os critérios que iremos apresentar além de pavimentar o caminho que será usado nas congruências do capítulo seguinte deste trabalho.

2.5.2. Principais Critérios

Na apresentação dos critérios de divisibilidade iremos agrupar os divisores em quatro grupos, sendo os dois primeiros grupos, formados por divisores que têm características em comum, o terceiro grupo apenas por números primos e o último grupo é formado por divisores de números compostos formados pelo produto dos números presentes nos grupos anteriores.

- Grupo A (2^n, 5^n e 10^n), para todo $n \geq 1$.
- Grupo B (3 e 9)
- Grupo C (7, 11 e 13)
- Grupo D (6, 15, 21, 33, 35, 55, 65, 77 e ⋯)

A) Divisibilidade por 2^n, 5^n ou 10^n.

Teorema 13. Um número é divisível por 2^n, 5^n ou 10^n, quando os n últimos algarismos da direita formarem um número divisível por 2^n, 5^n ou 10^n.

Demonstração.

Considere

$$N = abc\cdots stu \qquad (2.7)$$

um número composto por m algarismos.

Vamos então analisar agora (2.7) com $1, 2, 3, \cdots, n$ algarismos, em uma adição da forma:

$$N = 10^{n-1} \times a + (bc\cdots stu)$$

Para $n = 1$, isto é, N com um algarismo, temos: $N = a \Longrightarrow N = 10^{1-1} \times a$

Para $n = 2$, isto é, N com um algarismo, temos

$$N = ab \Longrightarrow N = 10^{2-1} \times a + b \text{ ou ainda } N = \dot{10} \times a + b$$

Para $n = 3$, isto é, N com um algarismo, temos

$$N = abc \Longrightarrow N = 10^{3-1} \times a + bc \text{ ou ainda } N = \dot{10} \times a + bc$$

$$\vdots$$

Para $N = \underbrace{abc\cdots stu}_{n\ alg.} \Longrightarrow N = \left[\dot{10}\right]^{n-1} \times a + \underbrace{bc\cdots stu}_{n-1\ alg.}\cdots \quad (1)$

Como $10 = 2 \times 5 \Longrightarrow 10 = \dot{2}$ e $10 = \dot{5}$, deduz-se que:

$\left[\dot{10}\right]^{n-1} = \left[\dot{2}\right]^{n-1}$ e $\left[\dot{10}\right]^{n-1} = \left[\dot{5}\right]^{n-1}$, então, podemos escrever:

$$N = \left[\dot{2}\right]^{n-1} \times a + \underbrace{bc\cdots stu}_{n-1\ alg.}\cdots \quad (2) \text{ ou } N = \left[\dot{5}\right]^{n-1} \times a + \underbrace{bc\cdots stu}_{n-1\ alg.}\cdots \quad (3)$$

Aplicando o Teorema Fundamental da Divisibilidade (teorema 9) em (1), (2) e (3), temos que

- Um número é divisível por 2^1 ou por 5^1, isto é, por 2 ou por 5, quando o último algarismo da direita for um número divisível por 2 ou por 5;
- Um número é divisível por 2^2 ou por 5^2, isto é, por 4 ou por 25, quando os dois últimos algarismos da direita formarem um número divisível por 4 ou por 25;
- Um número é divisível por 2^3 ou por 5^3, isto é, por 8 ou por 125, quando os três últimos algarismos da direita formarem um número divisível por 8 ou por 125, $\cdots$ e assim por diante;
- Um número é divisível por $10^1, 10^2, 10^3, \cdots$, quando terminar em um zero, dois zeros, três zeros, ... e assim por diante. ■

Exemplo 11. Verificar se o número 7.692.315.148 é divisível por 2, por 4 e por 8, caso não seja, determinar o seu resto.

1º) Por 2. $\begin{array}{r|l} 8 & 2 \\ 0 & 4 \end{array}$ 2º) Por 4. $\begin{array}{r|l} 48 & 4 \\ 0 & 12 \end{array}$ 3º) Por 8. $\begin{array}{r|l} 148 & 8 \\ 4 & 18 \end{array}$

Após efetuarmos as divisões usando os critérios do teorema 13, podemos afirmar que o número dado é divisível por 2, é divisível por 4, mas não é divisível por 8 e, nessa divisão, o resto é igual a 4.

Exemplo 12. Verificar se o número 7.692.315.850 é divisível por 5, por 25 e por 125, caso não seja, determinar o seu resto.

1º) Por 5. $\begin{array}{r|l} 0 & 5 \\ 0 & 0 \end{array}$ 2º) Por 25. $\begin{array}{r|l} 50 & 25 \\ 0 & 2 \end{array}$ 3º) Por 125. $\begin{array}{r|l} 850 & 125 \\ 100 & 6 \end{array}$

Após efetuarmos as divisões usado os critérios do teorema 13, podemos afirmar que o número dado é divisível por 5, é divisível por 25, mas não é divisível por 125 e, nessa divisão, o resto é igual a 100.

Exemplo 13. Verificar se o número 92.315.600 é divisível por 10, por 100 e por 1.000, caso não seja, determinar o seu resto.

O número dado é divisível por 10, pois o último algarismo da direita é o zero;

O número dado é divisível por 100, pois os últimos algarismos da direita são iguais a zero;

O número dado não é divisível por 1.000, pois os três últimos algarismos da direita não são iguais a zero, e o resto é igual a 600.

B) Divisibilidade por 9 ou 3.

Teorema 14. Um número é divisível por 9 ou por 3, quando a soma de seus algarismos for um número divisível por 9 ou por 3.

Demonstração.

Sabemos que: $10^1 = 10 = 9 + 1 \Longrightarrow 10^1 = \dot{9} + 1$

$$10^2 = 100 = 99 + 1 \Longrightarrow 10^2 = \dot{9} + 1$$

$$10^3 = 1000 = 999 + 1 \Longrightarrow 10^3 = \dot{9} + 1$$

$$\vdots$$

$$10^n = 1\underbrace{000\cdots0}_{n\ zero(s)} = 99\cdots9 + 1 \Longrightarrow 10^n = \dot{9} + 1$$

Isto é, qualquer potência de 10 é igual a um múltiplo de 9 mais 1.

Seja (2.7) um número com n algarismos. Explicitando esse número na forma polinômica, teremos

$$N = a \times 10^{n-1} + b \times 10^{n-2} + c \times 10^{n-3} + \cdots + s \times 10^2 + t \times 10^1 + u \times 10^0$$

$$N = a \times (\dot{9} + 1) + b \times (\dot{9} + 1) + c \times (\dot{9} + 1) + \cdots + s \times (\dot{9} + 1) + t \times (\dot{9} + 1) + u$$

Desenvolvendo e ordenando convenientemente, teremos

$$N = \underbrace{a \times \dot{9} + b \times \dot{9} + c \times \dot{9} + \cdots + s \times \dot{9} + t \times \dot{9}}_{múltiplo\ de\ 9} + \underbrace{a + b + c + \cdots + s + t + u}_{Soma\ dos\ algarismos}$$

$$N = \dot{9} + (a + b + c + \cdots + s + t + u) \quad (4)$$

Dividindo os dois membros de (4) por 9 e aplicando o Teorema Fundamental da Divisibilidade (teorema 9), teremos que, N só será divisível por 9 se a soma dos seus algarismos for um múltiplo de 9. Como todo múltiplo de 9 também é múltiplo de 3, então podemos escrever que, N só será divisível por 3 se a soma dos seus algarismos também for um múltiplo de 3. ■

Exemplo 14. Verificar se o número $N = 72.843.621.312$ é divisível por 3 e, em seguida, por 9.

$$S_{alg.} = 7 + 2 + 8 + 4 + 3 + 6 + 2 + 1 + 3 + 1 + 2 = 39$$

1º) Por 3. $\begin{array}{r|l} 39 & 3 \\ 0 & 13 \end{array}$ 2º) Por 9. $\begin{array}{r|l} 39 & 9 \\ 3 & 4 \end{array}$

O número N dado é divisível por 3, mas não é divisível por 9.

C_1) Divisibilidade por 7.

Apesar do número 7 ter vários critérios de divisibilidade, vamos usar o mais recente deles. Em 2019, um garoto nigeriano de 12 anos, radicado na Inglaterra, chamado de Chika Ofili, foi agraciado com o prêmio TruLittle Hero Awards, que reconhece as notáveis realizações de crianças e jovens de até 17 anos no Reino Unido. Apesar do método em si já constar na literatura especializada, conforme [2], isso em nada diminui o mérito de Chika, pois o mesmo deu visibilidade a uma maneira mais simples de verificar se um número é ou não divisível por 7.

Teorema 15. Um número é divisível por 7, se o quíntuplo do seu algarismo da unidade somado com o número formado pelos outros algarismos for divisível por 7.

Demonstração.

Seja (2.7) um número com n algarismos e que seja divisível por 7, isto é, $N = abc \cdots stu = 7k$, com $k \in \mathbb{Z}$. Explicitando esse número na forma polinômica, teremos:

$$N = a \times 10^{n-1} + b \times 10^{n-2} + c \times 10^{n-3} + \cdots + s \times 10^2 + t \times 10^1 + u \times 10^0 = 7k$$

$$N = a \times 10^{n-1} + b \times 10^{n-2} + c \times 10^{n-3} + \cdots + s \times 10^2 + t \times 10^1 + u = 7k$$

Somando $49u$ nos dois membros da expressão acima, teremos:

$$N = a \times 10^{n-1} + b \times 10^{n-2} + c \times 10^{n-3} + \cdots + s \times 10^2 + t \times 10^1 + 50u = 7k + 49u$$

Percebemos que N é formado pela soma de vários múltiplos de 10, logo podemos tirar o 10 em evidência.

$$N = 10 \times [a \times 10^{n-2} + b \times 10^{n-3} + c \times 10^{n-4} + \cdots + s \times 10^1 + t + 5u] = 7(k + 7u)$$

Como $7 \nmid 10$, então

$$7 \mid [a \times 10^{n-2} + b \times 10^{n-3} + c \times 10^{n-4} + \cdots + s \times 10^1 + t + 5u]. \quad \blacksquare$$

Se aplicarmos o critério acima em um número de muitos dígitos e ainda sim, for difícil de visualizar, podemos repetir o processo até chegarmos num número menor em que se possa afirmar que ele é ou não divisível por 7.

Exemplo 15. Verifique se os números abaixo são divisíveis por 7, usando o critério acima.

(a) 24.836

Usando o primeiro critério temos, 2483 + 5.6 = 2513, ainda está difícil de saber, aplicaremos de novo o critério e teremos 251 + 5.3 = 266, aplicando novamente 26 + 5.6 = 56 e 7 | 56, portanto 24836 é divisível por 7.

(b) 28.632

Usando o primeiro critério temos, 2863 + 5.2 = 2873, ainda está difícil de saber, aplicaremos de novo o critério e teremos 287 + 5.3 = 302, aplicando novamente 30 + 5.2 = 40 e $7 \nmid 40$, portanto 28.632 não é divisível por 7.

C_2) Divisibilidade por 11.

Teorema 16. Um número N é divisível por 11, se o resultado da diferença entre o número formado pelos algarismos excluindo o digito da unidade e o algarismo das unidades, for divisível por 11.

Demonstração.

Seja (2.7) um número com n algarismos e que seja divisível por 11, isto é,

$$N = abc \cdots stu = 11k, \text{ com } k \in \mathbb{Z}.$$

Explicitando esse número na forma polinômica, teremos

$$N = a \times 10^{n-1} + b \times 10^{n-2} + c \times 10^{n-3} + \cdots + s \times 10^2 + t \times 10^1 + u \times 10^0 = 11k$$

$$N = a \times 10^{n-1} + b \times 10^{n-2} + c \times 10^{n-3} + \cdots + s \times 10^2 + t \times 10^1 + u = 11k$$

Somando $-11u$ nos dois membros da expressão acima, tem-se

$$N = a \times 10^{n-1} + b \times 10^{n-2} + c \times 10^{n-3} + \cdots + s \times 10^2 + t \times 10^1 + u - 11u$$

$$N = 11k - 11u$$

$$N = 11(k - u)$$

Percebemos que N é formado pela soma de vários múltiplos de 10, logo podemos tirar o 10 em evidência.

$$N = 10 \times [a \times 10^{n-2} + b \times 10^{n-3} + c \times 10^{n-4} + \cdots + s \times 10^1 + t - u] = 11(k - u)$$

Como $11 \nmid 10$, então

$$11 \mid [a \times 10^{n-2} + b \times 10^{n-3} + c \times 10^{n-4} + \cdots + s \times 10^1 + t - u] \quad \blacksquare$$

Se aplicarmos o critério acima em um número de muitos dígitos e ainda sim, for difícil de visualizar, podemos repetir o processo até chegarmos num número menor em que se possa afirmar que ele é ou não divisível por 11.

Exemplo 16. Verifique se os números abaixo são divisíveis por 11, usando o critério acima.

(a) 81.631

Aplicando o critério, temos então 8163 − 1 = 8162, só olhando para o número não conseguimos, ainda, saber se ele é ou não divisível por 11. Então aplicaremos o critério até o número resultante ser suficiente para sabermos se é ou não divisível por 11. Logo, 816 − 2 = 814; 81 − 4 = 77 e 11 | 77. Portanto, 81.631 é divisível por 11.

(b) 43.896

Aplicando o critério, temos então 4389 − 6 = 4383, só olhando para o número não conseguimos, ainda, saber se ele é ou não divisível por 11. Então aplicaremos o critério até o número resultante ser suficiente para sabermos se é ou não divisível por 11. Logo, 438 − 3 = 435; 43 − 5 = 38 e $11 \nmid 38$. Portanto, 43.896 não é divisível por 11.

C_3) Divisibilidade por 13.

Teorema 17. Um número N é divisível por 13 se o resultado da soma do quadruplo do algarismo da unidade do número N somado com o número formado pelos outros algarismos, for divisível por 13.

Demonstração.

Seja (2.7) um número com n algarismos e que seja divisível por 13, isto é,

$N = abc \cdots stu = 13k$, com $k \in \mathbb{Z}$. Explicitando esse número na forma polinômica, teremos

$$N = a \times 10^{n-1} + b \times 10^{n-2} + c \times 10^{n-3} + \cdots + s \times 10^2 + t \times 10^1 + u \times 10^0 = 13k$$

$$N = a \times 10^{n-1} + b \times 10^{n-2} + c \times 10^{n-3} + \cdots + s \times 10^2 + t \times 10^1 + u = 13k$$

Somando $39u$ nos dois membros da expressão acima, teremos

$$N = a \times 10^{n-1} + b \times 10^{n-2} + c \times 10^{n-3} + \cdots + s \times 10^2 + t \times 10^1 + u + 39u$$

$$N = 13k + 39u$$

$$N = 13(k + 3u)$$

Percebemos que N é formado pela soma de vários múltiplos de 10, logo podemos tirar o 10 em evidência.

$$N = 10 \times [a \times 10^{n-2} + b \times 10^{n-3} + c \times 10^{n-4} + \cdots + s \times 10^1 + t + 4u] = 13(k + 3u)$$

Como $13 \nmid 10$, então

$$13 \mid [a \times 10^{n-2} + b \times 10^{n-3} + c \times 10^{n-4} + \cdots + s \times 10^1 + t + 4u] \qquad \blacksquare$$

Se aplicarmos o critério em um número de muitos dígitos e ainda sim, for difícil de visualizar, podemos repetir o processo até chegarmos num número menor em que se possa afirmar que ele é ou não divisível por 13.

Exemplo 17. Verifique se os seguintes números são divisíveis por 13, usando o critério de divisibilidade por 13.

(a) 34.814

Aplicando o critério, temos então 3481 + 4.4 = 3497, só olhando para o número não conseguimos, ainda, saber se ele é ou não divisível por 13. Então aplicaremos o critério até o número resultante ser suficiente para sabermos se é ou não divisível por 13. Logo, 349 + 4.7 = 377; 37 + 4.7 = 65 e 13 | 65. Portanto, 34.814 é divisível por 13.

(b) 68.530

Aplicando o critério, temos então 6853 + 4.0 = 6853, só olhando para o número não conseguimos, ainda, saber se ele é ou não divisível por 13. Então aplicaremos o critério até o número resultante ser suficiente para sabermos se é ou não divisível por 13. Logo, 685 + 4.3 = 697; 69 + 4.7 = 97 e $13 \nmid 97$. Portanto, 68.530 não é divisível por 13.

D) Divisibilidade por $6, 15, 21, 33, 35, 55, 65, 77, \ldots$

Esse grupo de divisores é formado apenas por números compostos, isto é, números formados a partir do produto entre números primos, o que além de reforçar a importância dos critérios já apresentados, funciona também como uma aplicação de combinações dos critérios estudados nos grupas A, B e C. Nele utilizaremos apenas um teorema como base de sustentação, uma vez que os demais se fazem presentes nele, assim como a condição geral de multiplicidade, permite-nos justificar certos critérios de divisibilidade já estudados, mas também permite enunciar outros.

Teorema 18. Se um número for divisível por vários outros primos entre si, dois a dois, então será divisível pelo produto deles.

Demonstração.

Seja N um número dado e $a, b, c, \cdots$ vários números primos entre si, dois a dois.

Se $\frac{\mathrm{N}}{\mathrm{a}} = q_1 \Longrightarrow N = a \times q_1$

Se $\frac{\mathrm{N}}{\mathrm{b}} = q_2 \Longrightarrow N = b \times q_2$

Se $\frac{\mathrm{N}}{\mathrm{c}} = q_3 \Longrightarrow N = c \times q_3$

$\vdots$

Queremos mostrar que $N = (a \times b \times c \times \cdots) \times q$.

Como $N = a \times q_1$, implica que $a \times q_1$ será divisível por b e, sendo b primo com a, então b dividirá q_1, logo, $q_1 = b \times q'$, ou ainda, $N = a \times b \times q'$.

Como $a \times b \times q'$ é divisível por c, e c é primo com a e b, então, N será primo com $a \times b$, portanto, c irá dividir q', logo, $q' = c \times q''$, portanto, $N = a \times b \times c \times q''$ ou ainda

$$N = (a \times b \times c) \times q''.$$

Seguindo o mesmo raciocínio adotado, teremos que $N = (a \times b \times c \times \cdots) \times q$.

■

d_1) Divisibilidade de um número N por 6.

$$\frac{\mathrm{N}}{6} = \frac{\mathrm{N}}{2 \times 3}$$

Ou seja, um número N só será divisível por 6 quando for divisível por 2 e 3, simultaneamente. Assim, N só será divisível por 6 se for par e a soma dos seus algarismos for um múltiplo de 3.

Exemplo 18. Verifique se o número 34.746 é divisível por 6.

Como o algarismo das unidades é seis, então o número 34.746 é par, logo é divisível por 2.

A soma dos algarismos $3 + 4 + 7 + 4 + 6 = 24$, e como 24 é múltiplo de 3, então 34.746 é divisível por 3.

Assim, 34.746 é divisível por 6, pois é divisível por 2 e 3 simultaneamente.

d_2) Divisibilidade de um número N por 15.

$$\frac{\mathrm{N}}{15} = \frac{\mathrm{N}}{3 \times 5}$$

Ou seja, um número N só será divisível por 15 quando for divisível por 3 e 5, simultaneamente. Assim, N só será divisível por 15 se a soma dos seus algarismos for um múltiplo de 3 e o algarismo das unidades desse número for zero ou cinco.

Exemplo 19. Verifique se o número 83.475 é divisível por 15.

A soma dos algarismos $8 + 3 + 4 + 7 + 5 = 27$, e como 27 é múltiplo de 3, então 83.475 é divisível por 3;

Como o algarismo da unidade do número é 5, então 83.475 é divisível por 5;

Assim, 83.475 é divisível por 15, pois é divisível por 3 e 5 simultaneamente.

d_3) Divisibilidade de um número N por 21.

$$\frac{\mathrm{N}}{21} = \frac{\mathrm{N}}{3 \times 7}$$

Ou seja, um número N só será divisível por 21 quando for divisível por 3 e 7, simultaneamente. Assim, N só será divisível por 21 se a soma dos seus algarismos for um múltiplo de 3 e o quíntuplo do seu algarismo da unidade somado com o número formado pelos outros algarismos for divisível por 7

Exemplo 20. Verifique se o número 73.437 é divisível por 21.

A soma dos algarismos $7 + 3 + 4 + 3 + 7 = 24$, e como 24 é múltiplo de 3, então 73.437 é divisível por 3;

Como $7343 + 5.7 = 7378$ e $737 + 5.8 = 777$ e 777 é múltiplo de 7, então 73.437 é divisível por 7.

Assim, 73.437 é divisível por 21, pois é divisível por 3 e 7 simultaneamente.

d_4) Divisibilidade de um número N por n.

Seja $n = p_1 \times p_2 \times p_3 \times \cdots$, onde $p_1, p_2, p_3, \cdots$ são números primos.

$$\frac{\mathrm{N}}{\mathrm{n}} = \frac{\mathrm{N}}{\mathrm{p}_1 \times \mathrm{p}_2 \times \cdots p_s} \tag{2.8}$$

Ou seja, um número N só será divisível por n quando for divisível por $p_1, p_2, \cdots, p_s$ simultaneamente. Assim, N só será divisível por n se for divisível por p_1, se for divisível por p_2, se for divisível por p_s e assim por diante, de forma simultânea.

Portanto, $33 = 3 \times 11, 35 = 5 \times 7, 55 = 5 \times 11, 65 = 5 \times 13, 105 = 3 \times 5 \times 7$ e assim por diante obedecem a esse critério.

2.6. Máximo Divisor Comum (MDC)

Definição 5. (Máximo Divisor Comum). Sejam a e b inteiros, onde um deles é não nulo. O máximo divisor comum de a e b, representado por $mdc(a, b)$, é o maior dentre os divisores positivos comuns de a e b.

Exemplo 21. Sejam $a = 36$ e $b = 60$. Indicando por D_{36} e D_{60} o conjunto dos divisores positivos de 36 e 60, respectivamente, temos

$D_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$ e $D_{60} = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$

Assim, a intersecção dos dois conjuntos é $D_{36} \cap D_{60} = \{1, 2, 3, 4, 6, 12\}$.

Logo, 12 é o maior divisor comum de 36 e 60, isto é, $mdc(36, 60) = 12$.

Definição 6. Diremos que dois números inteiros a e b são primos entre si, se $mdc(a, b) = 1$, ou seja, se o máximo divisor comum de ambos for igual a 1.

Proposição 17. Sejam a e b inteiros positivos. Assim,

i) Se b é divisor de a, então $mdc(a, b) = b$;

$ii)$ Se $a = bq + c$, com $c \neq 0$, então o conjunto dos divisores comuns dos números b e c é igual ao conjunto dos divisores comuns de a e b. Em particular, $mdc(a, b) = mdc(b, c)$.

Demonstração.

$i)$ Sendo todo divisor comum de a e b é um divisor de b. Como b é divisor de a, tem-se todo divisor de b é também divisor de a, ou seja, um divisor comum de a e b. Portanto, o conjunto dos divisores comuns dos números a e b é igual ao conjunto dos divisores de b. Como o maior divisor de b é ele mesmo, tem-se $mdc(a, b) = b$.

$ii)$ Fazendo o uso das proposições 10 e 11, tem-se que todo divisor comum de a e b também divide c, consequentemente, é um divisor comum de b e c. Assim, podemos usar o mesmo argumento para afirmar que todo divisor comum de b e c também divide a, consequentemente, é um divisor comum de a e b. Logo, os divisores comuns de a e b são os mesmos que os divisores comuns de b e c. Em particular, também coincidem os maiores divisores comuns, ou seja, $mdc(a, b) = mdc\ (b, c)$. ■

Teorema 18. ***(Algoritmo de Euclides)***. Sejam a e b números inteiros positivos. Aplica-se sucessivamente a divisão euclidiana para obter a seguinte sequência de igualdades:

$$a = b.q_1 + r_1\ , 0 \leq r_1 \leq b$$
$$b = r_1.q_2 + r_2\ , 0 \leq r_2 \leq r_1,$$
$$r_1 = r_2.q_3 + r_3\ , 0 \leq r_3 \leq r_2,$$
$$\vdots \qquad \vdots \qquad \vdots$$
$$r_{n-3} = r_{n-2}.q_{n-1} + r_{n-1}\ , 0 \leq r_{n-1} \leq r_{n-2}$$
$$r_{n-2} = r_{n-1}.q_n + r_n\ , 0 \leq r_n \leq r_{n-1}$$
$$r_{n-1} = r_n.q_{n+1} + 0$$

até algum r_n dividir r_{n-1}. Assim o $mdc(a, b) = r_n$, ou seja, é o último resto não nulo do procedimento de divisão.

Demonstração.

Podemos iniciar com a última divisão $r_{n-1} = r_n.q_{n+1} + 0$, pois nela decorre que r_n divide r_{n-1}. Logo, pela proposição 17 (item i), $mdc(r_{n-1}, r_n) = r_n$. Aplicando o (item ii) da mesma proposição 17 na penúltima divisão, concluímos que $mdc(r_{n-2}, r_{n-1}) = mdc(r_{n-1}, r_n) = r_n$. Usando novamente esse mesmo item, na antepenúltima divisão, temos que $mdc(r_{n-3}, r_{n-2}) = mdc(r_{n-2}, r_{n-1}) = r_n$. Prolongando esse raciocínio até se chegar a primeira divisão, temos que $mdc(a, b) = r_n$, que é exatamente o que desejávamos provar. ■

Vale observar que se escrevermos as desigualdades dos restos do algoritmo de Euclides, uma seguida da outra, ou seja, $b > r_1 > r_2 > r_3 \cdots \geq 0$. Como entre b e 0 há apenas uma quantidade

finita de inteiros, essa sequência não pode continuar indefinidamente, pois caso assim o fosse ela não iria possuir o menor elemento, o que não é possível pelo princípio da Boa Ordenação, o que garante que ela só chega ao final se um dos restos for zero, isso ratifica que o algoritmo tem um fim.

Exemplo 22. Encontre o mdc dos números 210 e 864, usando o algoritmo de Euclides.

$$864 = 210.4 + 24$$
$$210 = 24.8 + 18$$
$$24 = 18.1 + 6$$
$$18 = 6.3 + 0$$

Logo, o $mdc(210, 864) = 6$. Podemos também usar o algoritmo em forma de dispositivo.

Tabela 02 – Algoritmo de Euclides no Cálculo do MDC

Uso do Algoritmo de Euclides no MDC					
Quociente		4	8	1	3
Números	864	210	24	18	6
Resto	24	18	6	0	

Fonte: O próprio Autor

Se fizermos uma comparação entre a tabela acima e as divisões sucessivas, vamos observar que ambas são equivalentes.

Mas, o Algoritmo de Euclides usado de trás para frente nos fornece uma informação adicional muito valiosa. Para mostrar essa informação, vamos reescrever as divisões sucessivas do exemplo 24, isolando os restos, nosso ponto de partida será o $mdc(210, 864) = 6$.

$$6 = 24 - 18.1$$
$$18 = 210 - 24.8$$
$$24 = 864 - 210.4$$

Logo,

$$\begin{aligned} 6 &= 24 - (210 - 24.8).1 \\ &= 24.9 - 210 \\ &= (864 - 210.4).9 - 210 \\ &= 864.(9) + 210.(-37) \end{aligned}$$

Sendo assim, podemos escrever

$$6 = mdc(210, 864) = 864.(9) + 210.(-37)$$

Esse dispositivo sempre funciona nos conduzindo a uma importante ferramenta na resolução de problemas que envolvem o máximo divisor comum de dois números. O mesmo foi provado pela primeira vez no início do século XVII por Claud-Gaspard Bachet de Méziriac(1581-1638) e logo mais tarde generalizado por Étienne Bézout[1] (1730-1783), matemático francês.

Teorema 20. ***(Relação de Bachet-Bézout).*** Considere a e b inteiros, com um deles diferente de zero. Existem dois números inteiros m e n, de modo que

$$mdc(a,b) = am + bn. \tag{2.9}$$

Demonstração.

Consideremos a combinação linear $am + bn$, onde $m,\ n \in \mathbb{Z}$. Este conjunto de inteiros, denotado por $C(a,b) = \{am + bn; m,n\ \in \mathbb{Z}\}$, possui elementos positivos e negativos.

Além disso, escolhendo $m = n = 0$, vemos que $0 \in C(a,b)$.

Pelo Princípio da Boa Ordenação, podemos escolher m_0 e n_0 de tal modo que $\lambda = am_0 + bn_0$ seja o menor inteiro positivo em $C(a,b)$.

Mostraremos primeiramente que $\lambda|a$.

Suponhamos por absurdo que $\lambda \nmid a$, logo pela divisão Euclidiana, existem inteiros q e r tais que $a = \lambda q + r$, com $0 < r < \lambda$. Portanto

$$r = a - \lambda q = a - q(am_0 + bn_0) = a.(1 - qm_0) + b.(-qn_0)$$

De onde vemos que $r \in C(a,b)$, o que contradiz o fato de λ ser o menor elemento positivo em $C(a,b)$.

Da mesma forma suponhamos por absurdo que $\lambda \nmid b$, logo pela divisão Euclidiana, existem inteiros q_1 e r_1 tais que $a = \lambda q_1 + r_1$ com $0 < r_1 < \lambda$. Logo

$$r_1 = b - \lambda q_1 = b - q_1(am_0 + bn_0) = b - q_1 am_0 - q_1 n_0 = a.(-q_1 m_0) + b.(1 - q_1 n_0)$$

E isso nos mostra que $r_1 \in C(a,b)$, contrariando novamente o fato de λ ser o menor elemento positivo em $C(a,b)$. Logo $\lambda|a$ e $\lambda|b$.

Resta agora provar que $\lambda = d$. Como $d = mdc(a,b)$ existem $a_1, b_1 \in \mathbb{Z}$, tais que $a = da_1$ e $b = db_1$, logo

$$\lambda = am_0 + bn_0 = da_1 m_0 + db_1 n_0 = d(a_1 m_0 + b_1 n_0)$$

De onde temos que $\lambda|d$. Logo pela proposição 13, concluímos que $d \leq \lambda$, mas $d < \lambda$ é impossível pois d é o máximo divisor comum de a e b, portanto $d = \lambda = am_0 + bn_0$. ■

[1] Étiene Bézout, matemático francês (1730 – 1783), foi um dos precursores da área da Matemática hoje conhecida como Geometria Algébrica. Famoso pelo teorema sobre MDC, seu livro didático se tornou referência a ponto de os professores da época usarem a expressão "vou dar explicação como o Bézout". A expressão foi transformada, aos poucos, em "vou dar o Bézout". Especialmente em escolas militares, é comum usar-se o termo "bizu", que tem exatamente essa origem.

Proposição 19. Sejam a e $b \in \mathbb{Z}$, não ambos nulos e $d = mdc(a,b)$. Se d_1 é um divisor comum de a e b, então $d_1 | d$

Demonstração.

Sendo $d = mdc(a,b)$, pela relação de Bézout, existem inteiros x e y, tais que $ax + by = d$. Como $d_1 | a$ e $d_1 | b$, pelas proposições 10 e 11, temos que $d_1 | ax + by$.

Logo, por conseguinte, $d_1 | d$. ■

Proposição 20. Sejam a e b inteiros, onde um deles é não nulo. Então,

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

Demonstração.

Para cada c e d inteiros, tem-se que $d \mid c$ se, e somente se, $d \mid |c|$. Dessa forma, os divisores comuns de a e b são exatamente os divisores comuns de $|a|$ e $|b|$. Em particular, também coincidem os maiores divisores comuns, ou seja, $mdc(a,b) = mdc(|a|,|b|)$. ■

Exemplo 23. Qual o máximo divisor comum de

(a) -8 e 12.

- $mdc(-8,12) = mdc(|-8|,|12|) = mdc(8,12) = 4$;

(b) 14 e -35.

- $mdc(14,-35) = mdc(|14|,|-35|) = mdc(14,35) = 7$;

Corolário 2. Sejam $a, b \in \mathbb{Z}$ e $c \in \mathbb{N}$. Se $c \mid a$ e $c \mid b$, então $c \mid mdc(a,b)$.

Demonstração.

Como $c \mid a$ e $c \mid b$ existem $a_1, b_1 \in \mathbb{Z}$, tais que $a = ca_1$ e $b = cb_1$ e sabendo que

$$mdc(a,b) = am + bn, \text{ com } m, n \in \mathbb{Z}$$

$$mdc(a,b) = ca_1 m + cb_1 n$$

$$mdc(a,b) = c(a_1 m + b_1 n)$$

De onde temos que $c \mid mdc(a,b)$. ■

Corolário 3. Quaisquer que sejam $a, b \in \mathbb{N}$, não ambos nulos, e $\lambda \in \mathbb{Z}$, tem-se que

$$mdc(\lambda a, \lambda b) = \lambda . mdc(a,b)$$

Demonstração.

Primeiramente observamos que:

$$\lambda am + \lambda bn = \lambda(am + bn), \text{ onde } m, n \in \mathbb{Z}$$

Usando o corolário 2. e o fato de λ ser positivo na igualdade acima temos

$$mdc(\lambda a, \lambda b) = \min\{\lambda am + \lambda bn; m, n \in \mathbb{Z}\}$$

$$= \lambda . \min\{am + bn; m, n \in \mathbb{Z}\}$$

$$= \lambda . mdc(a,b).$$

■

Corolário 4. Dados $a, b \in \mathbb{Z}$, ambos não nulos, tem-se que

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

Demonstração.

Fazendo $d = mdc(a, b)$ e pelo corolário 3 temos que

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

De onde temos que a igualdade acima só se verifica se tivermos:

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

Proposição 21. Dois números inteiros a e b são primos entre si se, e somente se, existirem m e n inteiros tais que $ma + nb = 1$.

Demonstração.

Supondo que a e b são primos entre si, temos pela definição 6 que $mdc(a, b) = 1$. Agora pelo teorema 20 existem inteiros m e n tais que $ma + nb = mdc(a, b) = 1$. Logo, a primeira parte da proposição fica demonstrada.

Agora supondo que existam m e n tais que $ma + nb = 1$. Se $mdc(a, b) = d$, temos que $d \mid (am + bn)$, o que mostra que $d \mid 1$, e, portanto, $d = 1$.

Provando assim que a e b são primos entre si. ■

2.7. Mínimo Múltiplo Comum (MMC)

Definição 7. (Mínimo Múltiplo Comum). Considere a e b inteiros não nulos. O mínimo múltiplo comum de a e b , indicado por $mmc(a, b)$, é o menor dentre os múltiplos positivos comuns de a e b.

Proposição 22. Sejam a e b inteiros positivos. Se a é múltiplo de b, então $mmc(a, b) = a$.

Demonstração.

Todo múltiplo comum de a e b é múltiplo de a. Todo múltiplo de a é múltiplo de b, ou seja, um múltiplo comum de a e b. Portanto, o conjunto dos múltiplos comuns de a e b é igual ao conjunto dos múltiplos de b. Como o menor múltiplo positivo de a é ele mesmo, tem-se que $mmc(a, b) = a$. ■

Teorema 21. Se a e b são inteiros positivos, então

$$mmc(a, b) = \frac{\mathrm{a.b}}{\mathrm{mdc(a,b)}} \qquad (2.10)$$

Demonstração.

Vamos inicialmente considerar que $m = \frac{\text{ab}}{\text{mdc(a,b)}}$ e $d = mdc(a,b)$. Uma vez que $d = mdc(a,b)$, devem existir inteiros a' e b', de forma que $a = a'd$ e $b = b'd$. Como $m = \frac{\text{ab}}{\text{mdc(a,b)}} = \frac{\text{a}}{\text{d}} \cdot b = a'b = ab'$, tem-se que m é um múltiplo comum de a e b. Seja M um múltiplo comum de a e b. Dessa forma, há inteiros p e q, de modo que $ap = bq = M$. Cancelando o fator d em todos os membros, obtemos $a'p = b'q = \frac{\text{M}}{\text{d}}$. O fato de $d = mdc(a,b)$, pela relação de Bézout, acarreta a existência de números inteiros x e y, tais que $ax + by = d$. E isso implica em $a'x + b'y = 1$. Multiplicando todos os membros dessa última igualdade por p, obtém-se $a'px + b'py = p$. Substituindo $a'p$ por $b'q$, temos $b'qx + b'py = p$. Logo, $b' \mid p$. Porém, isso garante que $a'b \mid ap$. Portanto, $m \mid M$. Consequentemente, $m \leq M$. Segue daí que $m = mmc(a,b)$. ■

Proposição 23. Sejam a e b inteiros não nulos e $m = mmc(a,b)$. Se m_1 é um múltiplo comum de a e b, então $m \mid m_1$

Demonstração.

Pela divisão euclidiana, devem existir inteiros q e r, tais que $m_1 = mq + r$, com $0 \leq r < m$. Como $a \mid m$ e $a \mid m_1$, segue da proposição 11, que $a \mid m_1 - mq$, ou seja, $a \mid r$. Analogamente $b \mid r$. Logo, r, com $0 \leq r < m$, é um múltiplo comum de a e b. Desde que m é o menor múltiplo comum positivo de a e b, então a única possibilidade é de termos $r = 0$, o que acarreta $m \mid m_1$. ■

Proposição 24. Considere a e b inteiros, com um deles não nulo. Assim,

$$mmc(a,b) = mmc(|a|,|b|).$$

Demonstração.

Para cada c e d inteiros, tem-se que $d = ck$ se, e somente se, $d = |c|k$. Dessa forma, os múltiplos comuns de a e b são exatamente os múltiplos comuns de $|a|$ e $|b|$. Em particular, também coincidem os maiores múltiplos comuns, ou seja, $mmc(a,b) = mmc(|a|,|b|)$. ■

Exemplo 24. Qual o mínimo múltiplo comum de

(a) -12 e -18

$$mmc(-12,-18) = mmc(|-12|,|-18|) = mmc(12,18) = \frac{12.18}{\text{mdc}(12,18)} = \frac{12.18}{6} = 12.3$$

$$mmc(-12,-18) = 36$$

(b) 15 e -40

$$mmc(15,-40) = mmc(|15|,|-40|) = mmc(15,40) = \frac{15.40}{\text{mdc}(15,40)} = \frac{15.40}{5} = 15.8$$

$$mmc(15,-40) = 120$$

2.8. Equações Diofantinas Lineares

Definição 8. Uma equação diofantina linear de duas variáveis é uma equação do tipo:

$$aX + bY = c \qquad (2.11)$$

Com $a, b, c \in \mathbb{Z}$, sendo X e Y variáveis a ser determinadas em $\mathbb{Z}$.

Ao nos depararmos com equações do tipo de (2.11) certamente alguns ponto precisam ser muito bem esclarecidos.

- Quais são as condições para que a equação possua solução?
- Quantas são as soluções?
- Como calcular as soluções, caso existam?

Exemplo 25. Considere as equações diofantinas abaixo:

(a) $4X + 7Y = 3$

(b) $2X + 6Y = 11$

Observe que na equação do item (a) temos que o $mdc(4, 7) = 1$, ou seja, $mdc(4, 7) \mid 3$ e é visível que $x_0 = -1$ e $y_0 = 1$ é uma solução para $4X + 7Y = 3$, porém esta solução não é única, já que $x_0 = 6$ e $y_0 = -3$ é outra solução para a mesma equação.

Agora observando a equação do item (b), verificamos que $mdc(2, 6) \nmid 11$ e também podemos notar que não existem x e $y \in \mathbb{Z}$, tais que $2x + 6y = 11$, uma vez que $2x + 6y$ é um número par e, portanto nunca igual a 11.

Com o auxílio da proposição e do teorema a seguir iremos fornecer as respostas mais gerais para os questionamentos levantados anteriormente.

Proposição 25. Sejam $a, b, c \in \mathbb{Z}$, a equação $aX + bY = c$, admite solução em $\mathbb{Z}$ se, e somente se,

$$mdc(a, b) \mid c.$$

Demonstração.

Suponhamos que a equação admita uma solução x_0, y_0.

Então vale a igualdade $ax_0 + by_0 = c$. Como o $mdc(a, b) \mid a$ e $mdc(a, b) \mid b$, segue que ele divide $ax_0 + by_0$, logo divide c.

Agora, suponhamos que o $mdc(a, b) \mid c$, ou seja, que $c = d.\lambda$, onde $d = mdc(a, b)$ e com $\lambda \in \mathbb{Z}$. Por outro lado, o teorema 20 nos garante que existem inteiros m e n tais que

$$d = am + bn$$

Multiplicando ambos os lados da igualdade acima por λ, obtemos

$$c = d.\lambda = a(m\lambda) + b(n\lambda)$$

Logo, a equação $aX + bY = c$ admite pelo menos uma solução $x_0 = m\lambda$ e $y_0 = n\lambda$. ■

Consideremos que na equação $aX + bY = c$, com $a \neq 0$ ou $b \neq 0$ tenhamos $d \mid c$. Dividindo esta equação por d, temos:

$$\frac{aX}{d} + \frac{bY}{d} = \frac{c}{d}$$

Fazendo $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$ e $c_1 = \frac{c}{d}$

Teremos

$$a_1X + b_1Y = c_1$$

Que é uma equação equivalente a $aX + bY = c$ e do corolário 4, $(a_1, b_1) = 1$ e da proposição 21 está equação sempre tem solução.

Exemplo 26. Mostre que a equação $4X + 7Y = 3$ sempre tem solução em $\mathbb{Z}$ e determine um par de números x e y que satisfaça a equação.

Como o $mdc(4, 7) = 1$ e $1 \mid 3$, temos pela proposição 25 que $4X + 7Y = 3$ admite solução em $\mathbb{Z}$. Claramente o par de inteiros $x = -1$ e $y = 1$ é solução da equação $4X + 7Y = 3$. Poderíamos também encontrar outras soluções para essa mesma equação, como por exemplo $x = 6$ e $y = -3$, ou ainda, $x = 13$ e $y = -7$. Na verdade, se tivermos uma equação diofantina linear $aX + bY = c$, com $mdc(a, b) = 1$ ela terá infinitas soluções é o que o próximo teorema irá nos garantir.

Teorema 22. Seja x_0 e y_0 uma solução da equação $aX + bY = c$, onde $mdc(a, b) = 1$. Então, as soluções de x e y em $\mathbb{Z}$ da equação são:

$$x = x_0 + bt, \quad y = y_0 - at; \quad t \in \mathbb{Z}.$$

Demonstração.

Consideremos x e y uma solução de $aX + bY = c$, logo

$$ax + by = c = ax_0 + by_0$$

$$ax + by = ax_0 + by_0$$

$$ax - ax_0 = by_0 - by$$

$$a(x - x_0) = b(y_0 - y)$$

Como $mdc(a, b) = 1$, temos que $b \mid (x - x_0)$, assim existe $t \in \mathbb{Z}$ tal que

$$x - x_0 = tb$$

$$x = x_0 + tb \tag{2.12}$$

Substituindo $x - x_0 = tb$ em $a(x - x_0) = b(y_0 - y)$, temos

$$a(x - x_0) = b(y_0 - y)$$

$$atb = b(y_0 - y)$$

$$at = y_0 - y$$

$$y = y_0 - at \tag{2.13}$$

Provando que as soluções da equação são do tipo proposto, e como

$$\begin{aligned} ax + by &= a(x_0 + tb) \\ &= ax_0 + atb + by_0 - bta \\ &= ax_0 + by_0 \end{aligned}$$

$$ax + by = c$$

Provando que os números x e y são soluções da equação $aX + bY = c$. ■

Devemos observar também que, se caso tivéssemos $mdc(a, b) = d$ no teorema 22, então teríamos as soluções x e y de $aX + bY = c$, dadas por

$$x = x_0 + \frac{b}{d}t \text{ e } y = y_0 - \frac{a}{d}t$$

De fato, seja x e y uma solução de $aX + bY = c$ da mesma forma que x_0 e y_0, logo

$$ax + by = ax_0 + by_0 \Rightarrow a(x - x_0) = b(y_0 - y)$$

Dividindo esta última equação por $d = mdc(a, b)$, temos

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$$

Assim, $\frac{b}{d} \mid (x - x_0)$, já que $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Logo, $\exists\ t \in \mathbb{Z}$ tal que $x - x_0 = \frac{b}{d}t \Rightarrow x = x_0 + \frac{b}{d}t$. Substituindo $x - x_0$ por $\frac{b}{d}t$ na equação acima, obtemos de modo análogo que $y = y_0 - \frac{a}{d}t$.

Se os valores de $|a|, |b|$ e $|c|$ forem pequenos fica fácil encontrar uma solução particular por inspeção, como no exemplo 28. Caso contrário poderemos recorrer ao método descrito a seguir.

Dada a equação $aX + bY = c$, com $mdc(a, b) \mid c$, vimos que é possível tornar uma equação $a_1X + b_1Y = c_1$ equivalente a $aX + bY = c$, com $mdc(a, b) = 1$.

Agora usando o algoritmo de Euclides de trás para frente, é possível determinar $m, n \in \mathbb{Z}$ tais que

$$ma + nb = 1$$

Multiplicando ambos os lados da igualdade acima por c_1, obtemos

$$c_1ma + c_1nb = c_1$$

De onde temos que $x_0 = c_1m$ e $y_0 = c_1n$ é uma solução particular da equação dada.

Exemplo 27. Resolva a equação diofantina $60x + 42y = 6$.

A equação tem solução pois $mdc(60, 42) = 6 \mid 6$. Dividindo ambos os lados da equação por $6 = mdc(60, 42)$, obtemos

$$10x + 7y = 1$$

Vamos agora usando o algoritmo de Euclides achar uma solução particular x_0 e y_0.

Tabela 03 – Algoritmo de Euclides no Cálculo do MDC em Equações Diofantinas

Algoritmo de Euclides no MDC em Equações Diofantinas				
Quociente		1	2	3
Números	10	7	3	1
Resto	3	1	0	

Fonte: O próprio Autor

$$1 = 7 - 2.3$$

$$3 = 10 - 7$$

$$1 = 7 - 2.(10 - 7)$$

$$10.(-2) + 7.(3) = 1$$

De onde temos que $x_0 = -2$ e $y_0 = 3$, logo as soluções são

$$x = -2 + 7t \text{ e } y = 3 - 10t, \text{ com } t \in \mathbb{Z}$$

2.8.1. Equação Diofantina em Duas Variáveis nos Naturais

Quando estamos resolvendo uma equação diofantina, há uma possibilidade de as variáveis tratadas não poderem assumir valores negativos, isto é, faz-se necessário resolver a equação no conjunto $\mathbb{N} \cup \{0\}$, ou seja, as equações do tipo $aX + bY = c$, onde $a, b, c \in \mathbb{N}$ e $X, Y \in \mathbb{N} \cup \{0\}$, contudo, para conseguirmos resolver equações desse tipo precisamos do seguinte resultado.

Proposição 26. Sejam $a, b \in \mathbb{N}$, com $mdc(a, b) = 1$. Todo número inteiro c pode ser escrito de modo único da forma: $c = ma + nb$, com $0 \leq m < b$ e $n \in \mathbb{Z}$.

Demonstração.

Existência: Pelo teorema 20, sabemos que existem $\alpha, \beta \in \mathbb{Z}$ tais que

$$\alpha a + \beta b = mdc(a, b) = 1$$

Multiplicando ambos os lados da igualdade acima por c, temos que

$$\alpha ac + \beta bc = c$$

Da divisão euclidiana, sabemos que existem $q, m \in \mathbb{Z}$ com $0 \leq m < b$ tais que $\alpha c = qb + m$.

Substituindo esse valor de αc na igualdade acima, obtemos

$$c = \alpha ac + \beta bc$$

$$c = a(qb + m) + \beta bc$$

$$c = aqb + am + \beta bc$$

$$c = am + b(aq + \beta c)$$

Agora tomando $n = aq + \beta c \in \mathbb{Z}$, obtemos

$$c = ma + nb, \text{ com } 0 \leq m < b \text{ e } n \in \mathbb{Z}$$

Unicidade: Suponhamos que

$$ma + nb = m_1 a + n_1 b, \text{ com } 0 \leq m, m_1 < b$$

Logo,

$$ma - m_1 a = n_1 b - nb$$

$$a(m - m_1) = b(n_1 - n)$$

Temos que $|m - m_1| < b$. Como o $mdc(a, b) = 1$ devemos ter $b \mid (m - m_1)$, o que só é possível quando $m - m_1 = 0 \Rightarrow m = m_1$, de onde temos imediatamente que $n = n_1$. ■

Consideremos a partir de agora o seguinte conjunto:

$$S(a, b) = \{xa + yb; x, y \in \mathbb{N}\} \cup \{0\},$$

onde $a, b \in \mathbb{N}$.

A proposição a seguir caracteriza os elementos de $S(a, b)$.

Proposição 27. Tem-se que $c \in S(a, b)$ se, e somente se, existem inteiros $m, n \in \mathbb{N} \cup \{0\}$ únicos, com $m < b$ tais que $c = ma + nb$.

Demonstração.

Se $c = ma + nb$, com $m, n \in \mathbb{N} \cup \{0\}$, então $c \in S(a, b)$.

Agora, se $c \in S(a, b)$, então existem $x, y \in \mathbb{N} \cup \{0\}$ tal que $c = xa + yb$. Pela divisão euclidiana, temos $x = bq + m$ com $0 \leq m < b$, substituindo o valor de x nesta última igualdade, temos:

$$c = (bq + m)a + yb = ma + (aq + y)b$$

Tomando $n = aq + y \in \mathbb{N} \cup \{0\}$, temos:

$$c = am + nb$$

É verdade que m e n são únicos. A veracidade dessa afirmação decorre imediatamente da proposição 26. ■

Definição 9. O conjunto de lacunas de $S(a, b)$ é o conjunto:

$$L(a, b) = \mathbb{N} \backslash S(a, b)$$

Proposição 28. Temos que: $L(a, b) = \{ma - nb \in \mathbb{N}; m, n \in \mathbb{N}, m < b\}$

Demonstração.

Seja l pertencente ao conjunto de lacunas $L(a, b)$. Notamos que l não pode ser escrito como $ma + nb$, pois não existem $m, n \in \mathbb{N} \cup \{0\}$ tal que $l = ma + nb$. Se m e n fossem determinados

então $l \in S(a,b)$ que é um absurdo. No entanto, a proposição 26 garante que existe um único n' tal que $l = ma + n'b$. Tomemos então $n' = -n$, com $n \in \mathbb{Z}$. Logo, $l = ma - nb$. ■

Teorema 23. A equação $aX + bY = c$, onde $mdc(a,b) = 1$, tem solução em $\mathbb{N}$ se, e somente se,

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

Demonstração.

Como a equação $aX + bY = c$, tem solução se, e somente se, $c \in S(a,b)$ e já que $L(a,b) = \mathbb{N} \backslash S(a,b)$, temos que $c \notin L(a,b)$. ■

Corolário 5. Seja $a, b \in \mathbb{N}$ tais que $mdc(a,b) = 1$. Tem-se que $(a-1)(b-1)$ é o menor inteiro tal que $c \in S(a,b)$ para todo $c \geq (a-1)(b-1)$.

Demonstração.

Como $L(a,b)$ é finito e o seu maior elemento ocorre quando $m = (b-1)$ e $n = 1$, temos que:

$$Max\, L(a,b) = (b-1)a - b$$

Portanto se,

$$\begin{aligned} c \geq (b-1)a - b + 1 &= ab - a + 1 \\ &= a(b-1) - (b-1) \\ &= (a-1)(b-1) \end{aligned}$$

a equação $aX + bY = c$ admite solução em $\mathbb{N}$. Agora se $c = (a-1)(b-1) - 1$, ela não admite solução em $\mathbb{N}$. ■

Diante dos resultados até aqui apresentados fica fácil determinar se a equação $aX + bY = c$ admite solução.

Se $mdc(a,b) \nmid c$, a equação não tem solução no conjunto dos inteiros, logo não tem solução em $\mathbb{N}$. Se $mdc(a,b) \mid c$, a equação é equivalente a outra da forma $a_1X + b_1Y = c_1$, com

$$a_1 = \frac{\mathrm{a}}{\mathrm{mdc(a,b)}},\ b_1 = \frac{\mathrm{b}}{\mathrm{mdc(a,b)}},\ c_1 = \frac{\mathrm{c}}{\mathrm{mdc(a,b)}}\ e\ mdc(a_1, b_1) = 1$$

Pelo algoritmo de Euclides, escrevemos:

$$1 = mdc(a_1, b_1) = m_1 a - n_1 b$$

Logo

$$c = cm_1 a - cn_1 b$$

Agora, usando a divisão euclidiana, escrevemos $cm_1 = qb + m$ com $m < b$, logo

$$c = \begin{cases} ma + (qa - cn_1)b \in S(a,b), & se \quad qa \geq cn_1 \\ ma - (cn_1 - qa)b \in L(a,b), & se \quad cn_1 \geq qa \end{cases}$$

Vimos que no segundo caso a equação $a_1X + b_1Y = c_1$ não tem solução.

No primeiro caso a equação tem solução. Definimos então a solução minimal m e n da equação $a_1X + b_1Y = c_1$, com $m < b$, minimal no sentido de que se x e y são soluções, então $x \geq m$.

Dessa forma, enunciamos o resultado a seguir.

Proposição 29. Suponhamos que a equação $aX + bY = c$ com o $mdc(a, b) = 1$, tenha solução e seja $x_0 = m$ e $y_0 = n$ a solução minimal. As soluções x e y da equação são dadas por:

$$x = m + tb, \;\; e \;\; y = n - ta, \;\; t \in \mathbb{N}, \text{com } n - ta \geq 0$$

Exemplo 28. Determinar para quais valores de $c \in \mathbb{N}$ a equação $7X + 3Y = c$ admite solução no conjunto $\mathbb{N} \cup \{0\}$.

Como o conjunto das lacunas de $S(7, 3)$ é:

$$L(a, b) = \{7m - 3n \in \mathbb{N}, m, n \in \mathbb{N}, m < 3\} = \{1, 2, 4, 5, 8, 11\}$$

Portanto, a equação $7X + 3Y = c$ admite solução em $\mathbb{N} \cup \{0\}$ se, e somente se, $c \notin L(7, 3)$.

Exemplo 29. Resolva a equação $7X + 3Y = 13$ em $\mathbb{N} \cup \{0\}$.

Do exemplo 30, temos que $13 \notin L(7, 3)$, logo a equação possui solução em $\mathbb{N} \cup \{0\}$. Usando o algoritmo de Euclides, temos

$$7 = 3.2 + 1 \Rightarrow 1 = 7 - 3.2 \Rightarrow 13 = 7.13 - 3.26 \Rightarrow 13 = 7.(3.4 + 1) - 3.26$$

$$\Rightarrow 13 = 3.28 + 7.1 - 3.26 \Rightarrow 13 = 7.1 + 3.2$$

De onde segue que $x_0 = 1$ e $y_0 = 2$ é a solução minimal da equação, logo, as soluções são

$$x = 1 + 3t, \;\; y = 2 - 7t, \text{com } t \in \mathbb{N} \cup \{0\}$$

Portanto a equação tem $x_0 = 1$ e $y_0 = 2$ como a única solução natural.

Nesse momento, cabe ressaltarmos que não se faz necessário usar toda a técnica desenvolvida acima, pois para valores de b pequenos, é mais oportuno encontramos as soluções por inspeção. No exemplo 31, bastaríamos ter testado quais dos valores $x = 0$ ou $x = 1$ tornava o número $13 - 7X$ divisível por 3, que como vimos é quando $x = 1$.

Capítulo 3

Neste capítulo, iniciaremos a apresentação de uma das noções mais profícuas de toda a aritmética, introduzida por Gauss, no seu livro *Disquisitiones Arithmeticae,* um tratado em latim sobre teoria dos números, publicado em 1801. A notação usada na obra é a mesma utilizada até hoje no estudo da congruência.

Com o auxílio do estudo da congruência vamos provar um famoso teorema de Pierre de Fermat, conhecido na literatura como *pequeno teorema de Fermat,* bem como a sua generalização, igualmente famosa, devida a Euler e conhecida como o *teorema de Euler*. A existência desses resultados em teoria elementar dos números se deve, dentre outros, ao fato dos mesmos iniciarem um estudo sistemático do comportamento dos restos da divisão das potências de um número natural a por um número natural $m > 1$ fixado, no caso em que a e m são relativamente primos. Apresentaremos, também o não menos famoso *teorema chinês dos restos*, o qual possui muitas aplicações interessantes em teoria elementar dos números.

3.1. Congruência módulo m

Definição 10. Sejam a, b e m inteiros dados, sendo $m > 1$. Dizemos que a é congruente a b, módulo m, denotamos $a \equiv b \ (mod\ m)$, se $m \mid (a - b)$. Se a não for congruente a b módulo m, denotamos $a \not\equiv b \ (mod\ m)$.

Exemplos 30. De acordo com a definição acima, podemos escrever:

(a) $3 \equiv 5 \ (mod\ 2)$, pois $2 \mid (3 - 5)$

(b) $-1 \equiv 11 \ (mod\ 12)$, pois $12 \mid (-1 - 11)$

(c) $x \equiv -x \ (mod\ 2)$, pois $2 \mid (x - (-x))$

Após a análise dos exemplos, provavelmente surja o seguinte questionamento: o que estamos realmente investigando em um número quando consideramos a congruência módulo m? Para responder a este questionamento, observemos o que ocorre com os números inteiros módulo 4, por exemplo:

$4k \equiv 0 \ (mod\ 4)$, $4k + 1 \equiv 1 \ (mod\ 4)$, $4k + 2 \equiv 2 \ (mod\ 4)$ e $4k + 3 \equiv 3 \ (mod\ 4)$.

Assim, a sequência $\cdots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \cdots$ dos números inteiros é igual, módulo 4, à sequência $\cdots, 3, 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, \cdots$, e vemos que todo inteiro é congruente, módulo 4, ao resto de sua divisão por 4. Esse resultado será generalizado com o uso da próxima proposição.

Proposição 30. Sejam a e m inteiros dados, com $m > 1$.

(i) Se a deixa resto r na divisão por m, então $a \equiv r \ (mod\ m)$. Em particular, todo inteiro é congruente módulo m, a exatamente um dos números $0, 1, 2, \cdots, m-2, m-1$.

(ii) $a \equiv b \ (mod\ m)$ se e somente se a e b deixam um mesmo resto na divisão por m.

Demonstração.

(i) Suponha que a deixa resto r quando dividido por m. Pelo algoritmo da divisão, temos $a = qm + r$ para algum inteiro q. Assim, $a - r = qm$, ou seja, $m \mid (a - r)$.

Na notação, que escrevermos $a \equiv r \ (mod\ m)$. O resto é imediato.

(ii) $(\Rightarrow)$ Se $a \equiv b \ (mod\ m)$, então $m \mid (a - b)$. Considere $a = m.q + r$ e que $a - b = m.q_1$, substituindo $m.q + r - b = m.q_1 \Rightarrow -b = mq_1 - mq - r \Rightarrow b = m(q - q_1) + r$, onde q_2 é a diferença entre $(q - q_1) = q_2$, logo $b = m.q_2 + r$. Segue que a e b deixam um mesmo resto na divisão por m. $(\Leftarrow)$ Reciprocamente, se a, b deixam um mesmo resto r na divisão por m, podemos escrever que $a = mq_1 + r$ e $b = mq_2 + r$, com $q_1, q_2 \in \mathbb{Z}$. Logo, $a - b = m(q_1 - q_2)$, ou seja, $m \mid (a - b)$. Portanto, $a \equiv b \ (mod\ m)$. ■

Na definição da relação de congruência, a razão pela qual não consideramos o módulo $m = 1$ é a seguinte: se usássemos a congruência módulo 1, obteríamos $a \equiv b \ (mod\ 1)$ como sinônimo de que $1 \mid (a - b)$, o que é sempre verdade. Portanto, dois inteiros quaisquer seriam indistinguíveis módulo 1.

Uma vez que a notação de congruência módulo m enfatiza apenas o resto da divisão de um número por m, notamos que o primeiro ganho ao se usar congruência é operacional: nas duas proposições a seguir 31 e 32, provaremos algumas propriedades elementares de congruência, as quais irão nos permitir, por exemplo, calcular rapidamente o resto da divisão de 17^{2002} por 13, tarefa que não é fácil de cumprir com os métodos de que dispomos até o presente momento.

Proposição 31. Dados inteiros a, b, c e m, sendo $m > 1$, temos:

(a) $a \equiv a \ (mod\ m)$

(b) $a \equiv b \ (mod\ m) \ \Rightarrow b \equiv a \ (mod\ m)$

(c) $a \equiv b \ (mod\ m)$ e $b \equiv c \ (mod\ m) \Rightarrow a \equiv c \ (mod\ m)$

Demonstração.

O item (a) é imediato, pois $m \mid (a - a)$, isto é, $m \mid 0$, já o item (b) como a e b tem o mesmo resto módulo m, então $m \mid (a - b)$ e $m \mid (b - a)$.

Quanto ao último item (c), se $a \equiv b \ (mod\ m)$ e $b \equiv c \ (mod\ m)$, então podemos escrever que $m \mid (a - b)$, $m \mid (b - c)$ e $m \mid (a - c)$, assim $a - c = (a - b) + (b - c)$. Mas isso é o mesmo que $a \equiv c \ (mod\ m)$. ■

Proposição 32. Sejam a, b, c, d, m e n inteiros dados, com $m, n > 1$.

(a) Se $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$, então $a + c \equiv b + d\ (mod\ m)$ e $ac \equiv bd\ (mod\ m)$. Em particular, $ac \equiv bc\ (mod\ m)$.

(b) Se $a \equiv b\ (mod\ m)$, então $a^k \equiv b^k\ (mod\ m)$, para todo $k \in \mathbb{N}$.

(c) Se $c_0, c_1, \cdots, c_n \in \mathbb{Z}$ e $f(x) = c_n x^n + \cdots + c_1 x + c_0$, então

$$a \equiv b\ (mod\ m) \Rightarrow f(a) \equiv f(b)(mod\ m).$$

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

(e) Se $a + c \equiv b + c\ (mod\ m)$, então $a \equiv b\ (mod\ m)$.

(f) Se $ac \equiv bc\ (mod\ m)$ e $mdc(c, m) = d$, então $a \equiv b\ (mod\ \frac{m}{d})$. Em particular, se $mdc\ (c, m) = 1$, então $a \equiv b\ (mod\ m)$.

(g) Se $a \equiv b\ (mod\ mn)$, então $a \equiv b\ (mod\ m)$ e $a \equiv b\ (mod\ n)$.

(h) Se $a \equiv b\ (mod\ m_i), \forall\ i = 1, \cdots, r \iff a \equiv b\ (mod[m_1, \cdots, m_r])$ onde

$$[m_1, \cdots, m_r] = mmc(m_1, \cdots, m_r)$$

Demonstração.

(a) Como $(a + c) - (b + d) = (a - b) + (c - d)$, $ac - bd = a(c - d) + (a - b)d$ e ainda $m\ |(a - b)$, $m\ |(c - d)$, segue da proposição 11 que $m\ |\ [(a + c) - (b + d)]$ e $m\ |\ (ac - bd)$. Por outro lado, isso é o mesmo que $a + c \equiv b + d\ (mod\ m)$ e $ac \equiv bd\ (mod\ m)$. Por fim, o caso particular segue de $c \equiv c\ (mod\ m)$.

(b) Fazendo $c = a$ e $d = b$ na segunda parte do item (a), obtemos $a^2 \equiv b^2\ (mod\ m)$. Se já mostramos que $a^\ell \equiv b^\ell\ (mod\ m)$, para um certo $\ell \in \mathbb{N}$, então novamente da segunda parte de (a) (dessa vez com $c = a^\ell$ e $d = b^\ell$), obtemos $a^{\ell+1} = a \cdot a^\ell \equiv b \cdot b^\ell = b^{\ell+1}\ (mod\ m)$. O restante, segue por indução em k.

(c) Se $a \equiv b\ (mod\ m)$, temos, a partir dos itens (a) e (b), que $c_k a^k \equiv c_k b^k\ (mod\ m)$, para $0 \leq k \leq m$. Portanto,

$$f(a) = \sum_{k=0}^{m} c_k a^k \equiv \sum_{k=0}^{m} c_k b^k = f(b)(mod\ m)$$

(d) Como $a \equiv b\ (mod\ m)$, existe $q \in \mathbb{Z}$ tal que $a = b + mq$. Queremos, pois, mostrar que

$$mdc(b + mq, m) = mdc(b, m).$$

Sejam $d = mdc(a + bc, b)$ e $d' = mdc(a, b)$. Como $d'\ |a, b$, temos que $d'\ |a, a + bc$. Portanto, temos que $d'\ |\ d$.

Reciprocamente, como $d \mid (a + bc)$ e $d \mid b$, temos que $d \mid [(a + bc) - bc]$, isto é, $d \mid a$ e $d \mid b$, logo, $d \mid d'$, assim $d = d'$.

Dessa maneira, o $mdc(a + bc, b) = mdc(a, b)$, ou seja, $mdc(b + mq, m) = mdc(b, m)$.

(e) Se $a + c \equiv b + c \ (mod\ m)$, então $m \mid [(a + c) - (b + c) = a - b]$, o que é o mesmo que $a \equiv b \ (mod\ m)$

(f) Sejam $m = dm'$ e $c = dc'$, com c' e m' inteiros primos entre si. De $ac \equiv bc \ (mod\ m)$, segue que $(dm') \mid [dc'(a - b)]$ ou, ainda, que $m' \mid c'(a - b)$.

Mas, como $mdc\ (m', c') = 1$, então $m' \mid\ (a - b)$, o que é o mesmo que $a \equiv b \ (mod\ \frac{\mathrm{m}}{\mathrm{d}})$. O restante é imediato.

(g) Se $a \equiv b \ (mod\ mn)$, então $mn \mid\ (a - b)$, o que possibilita que $m \mid\ (a - b)$. Porém, isso é equivalente a $a \equiv b \ (mod\ m)$; analogamente, $a \equiv b \ (mod\ n)$.

(h) Se $a \equiv b \ (mod\ m_i),\ i = 1, \cdots, r$, então $m_i \mid\ (a - b)$, para todo i. Sendo $a - b$ um múltiplo de cada m_i, segue que $[m_1, \cdots, m_r] \mid\ (a - b)$, o que prova que $a \equiv b \ (mod\ [m_1, \cdots, m_r])$. A reciproca segue do item (g). ■

De posse dessa proposição, agora podemos encontrar o resto da divisão de um número muito grande, escrito na forma de potência a^k por outro valor m.

Exemplos 31. Calcule o resto da divisão do número 17^{2002} por 13.

Solução. Como $17 \equiv 4 \ (mod\ 13)$ e $16 \equiv 3 \ (mod\ 13)$, segue do item (b) da proposição 32, módulo 13,

$$17^{2002} \equiv 4^{2002} = 16^{1001} \equiv 3^{1001}$$

Notando, agora, que $3^3 \equiv 1 \ (mod\ 13)$ e aplicando os itens (a) e (b) da proposição 32, obtemos

$$3^{1001} = 3^2 . 3^{999} = 9 . (3^3)^{333} \equiv 9 . 1^{333} = 9,\ 3^{1001} \equiv 9 \ (mod\ 13)$$

Então, segue da proposição 31 que 17^{2002} deixa resto 9 na divisão por 13.

O uso das congruências também pode ser associado as equações diofantinas, como pode ser visto no próximo exemplo.

Exemplos 32. Encontre o menor múltiplo inteiro positivo de 7 que deixa resto 1 quando dividido por 2, 3, 4, 5 e 6.

Solução. Queremos achar a menor solução positiva x do seguinte sistema de congruências:

$$\begin{cases} 7X \equiv 1 \ (mod\ 2) \\ 7X \equiv 1 \ (mod\ 3) \\ 7X \equiv 1 \ (mod\ 4) \\ 7X \equiv 1 \ (mod\ 5) \\ 7X \equiv 1 \ (mod\ 6) \end{cases}$$

Pela proposição 32, item (h), temos que toda solução simultânea das congruências acima é solução da congruência $7X \equiv 1\ (mod\ [2,3,4,5,6])$, e reciprocamente. Portanto, devemos achar a solução positiva mínima u da congruência $7X \equiv 1\ (mod\ 60)$, que é equivalente a resolver a equação diofantina $7X - 60Y = 1$. Pelo algoritmo de euclidiano encontramos que a solução geral é dada por $x = -17 + 60t$ e $y = -2 - 7t$, com $t \in \mathbb{Z}$.

Portanto, o menor valor positivo de x de modo que exista y para os quais x, y é uma solução da equação diofantina $7X - 60Y = 1$ é $x = -17 + 60.1 = 43$. Segue-se, então que o número procurado é $7.43 = 301$.

3.2. Pequeno Teorema de Fermat

O uso efetivo de congruências para calcular restos é consideravelmente simplificado se encontrarmos expoentes que tornem uma certa potência congruente a 1. Por exemplo, sabendo que $7^3 \equiv 1\ (mod\ 9)$ fica muito mais simples calcular o resto da divisão de 25^{1001} por 9, já que 25 deixa resto 7 quando dividido por 9 ou ainda que $25 \equiv 7\ (mod\ 9)$, temos

$$25^{1001} \equiv 7^{1001} = (7^3)^{333}.7^2 \equiv 1^{333}.49 \equiv 4\ (mod\ 9).$$

Nessa direção, o propósito agora é, uma vez fixados os inteiros a e m primos entre si, com $m > 1$, encontrar um expoente $k \in \mathbb{N}$ para o qual

$$a^k \equiv 1\ (mod\ m). \qquad (3.1)$$

Para isso, analisaremos inicialmente o caso em que m é primo, provando assim um dos mais importantes resultados da teoria elementar de congruências, conhecido na literatura como o pequeno teorema de Fermat.

Desde, pelo menos, 500 anos antes de Cristo, os chineses sabiam que, se m é um número primo (a partir desse momento usaremos p para representar esse número primo), então $p|2^p - 2$. Coube a Pierre de Fermat, no século XVII, generalizar esse resultado, enunciando um pequeno, porém notável teorema.

Para demonstrar o Teorema de Fermat, necessitamos do lema a seguir.

Lema 1. Seja p um número primo. Os números $\binom{p}{i}$, onde $0 < i < p$, são todos divisíveis por p.

Demonstração.

O resultado vale trivialmente para $i = 1$. Podemos, então, supor $1 < i < p$.

Nesse caso, $i!\ |p(p-1)\cdots(p-i+1)$, e o $mdc\ (i!, p) = 1$, decorre assim que

$$i!\ |(p-1)\cdots(p-i+1)$$

e o resultado se segue, pois

$$\binom{p}{i} = p\,\frac{(\mathrm{p}-1)\cdots(\mathrm{p}-\mathrm{i}+1)}{\mathrm{i}!}$$

■

Teorema 24. (Fermat) Dado um número primo p, tem-se que p divide o número $a^p - a$, para todo $a \in \mathbb{Z}$.

Demonstração.

Se $p = 2$, o resultado é óbvio já que $a^2 - a = a(a-1)$ é par. Suponhamos p ímpar. Nesse caso, claramente basta mostrar o resultado para $a \geq 0$. Vamos provar o resultado por indução em a.

O resultado vale claramente para $a = 0$, pois $p \mid 0$.

Supondo o resultado válido para a, iremos prova-lo para $a+1$. Pela fórmula do Binômio de Newton,

$$(a+1)^p - (a+1) = a^p - a + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a$$

Como, pelo Lema 1 e pela hipótese de indução, o segundo membro da igualdade acima é divisível por p, o resultado segue. ■

Exemplos 33. Dado um número qualquer $n \in \mathbb{N}$, tem-se que n^9 e n, quando escritos na base 10, têm o mesmo algarismo das unidades.

Solução. A afirmação acima é equivalente a $10 \mid n^9 - n$. Como n^9 e n têm a mesma paridade, segue-se que $n^9 - n$ é par, isto é, $2 \mid n^9 - n$.

Por outro lado,

$$n^9 - n = n(n^4-1)(n^4+1) = (n^5 - n)(n^4+1)$$

Logo, pelo Pequeno Teorema de Fermat, temos que $5 \mid n^5 - n$ e, portanto, $5 \mid n^9 - n$. Tem-se, então que $10 \mid n^9 - n$.

Corolário 6. Se p é um número primo e se a é um número natural não divisível por p, então p divide $a^{p-1} - 1$.

Demonstração.

Como, pelo Pequeno Teorema de Fermat, $p \mid a(a^{p-1} - 1)$ e como o $mdc\ (a,p) = 1$, segue-se, imediatamente, que p divide $a^{p-1} - 1$. ■

O corolário 6 também é chamado de *Pequeno Teorema de Fermat ou reformulação do Pequeno Teorema de Fermat*. Vale ressaltar também que o Pequeno Teorema de Fermat fornece-nos um teste de não primalidade. De fato, dado um número $m \in \mathbb{N}$, com $m > 1$, se existir algum $a \in \mathbb{N}$, com $mdc(a,m) = 1$, tal que $m \nmid a^{m-1} - 1$, então m não é primo.

Até mesmo os chineses achavam também que se m era composto, então $m \nmid 2^m - 2$, uma recíproca do Teorema de Fermat, no caso de $a = 2$. Muitos matemáticos acreditavam nesse resultado, até que, em 1819, Sarrus[2] mostrou que o número $341 = 31 \times 11$ divide $2^{341} - 2$.

Poder-se-ia perguntar se vale a recíproca mais restritiva do Pequeno Teorema de Fermat:

Seja um inteiro $m > 1$, a condição $m \mid (a^{m-1} - 1)$ para todo $a \in \mathbb{N}$ tal que o $mdc\ (a, m) = 1$, acarreta necessariamente, que m é primo?

O próximo exemplo nos mostrará que isso também é falso.

Exemplos 34. Seja $a \in \mathbb{N}$ tal que $mdc(a, 3) = mdc(a, 11) = mdc(a, 17) = 1$. Note que essa condição é equivalente a $mdc(a, 561) = 1$, pois $3 \times 11 \times 17 = 561$.

Por outro lado,

$$mdc(a^{280}, 3) = mdc(a^{56}, 11) = mdc(a^{35}, 17) = 1$$

e, portanto, pelo Pequeno Teorema de Fermat, 3 divide $(a^{280})^2 - 1 = a^{560} - 1$, 11 divide $(a^{56})^{10} - 1 = a^{560} - 1$ e 17 divide $(a^{35})^{16} - 1 = a^{560} - 1$.

Segue-se assim que 561 divide $a^{561} - 1$, para todo a tal que $mdc(a, 561) = 1$, sem que 561 seja primo.

3.3. Teorema de Euler

O matemático suíço Leonhard Paul Euler (1707 – 1783) fez grandes descobertas para várias áreas da matemática. Euler ficou conhecido por desenvolver várias fórmulas como, por exemplo, a fórmula de Euler, os números de Euler, a constante de Euler-Mascheroni, os ângulos de Euler, a conjetura de Euler, entre outras. Ele trabalhou em quase todas as áreas da matemática sendo elas: geometria, cálculo infinitesimal, álgebra e teoria dos números.

Segundo D'Ambrosio (2009), Euler foi considerado o matemático mais prolífico da história. Suas obras completas estão reunidas em 84 volumes, sendo que 40% dessas obras são sobre a matemática. Euler chegou a demonstrar quase todos os teoremas de Fermat, exceto o teorema conhecido como "*Último Teorema de Fermat*". Um dos sonhos de todo matemático é encontrar uma fórmula que gere números primos, Fermat morreu com a certeza de que sua fórmula da primalidade $2^{2^n} + 1$ sempre gerava números primos. Porém, Euler derrubou sua convicção quando demonstrou e provou que ela não era válida para todos os números. Euler fez grandes descobertas na matemática e até hoje elas vêm

[2] Pierre Frédéric Sarrus (1798 – 1861) – Matemático francês autor de vários tratados, incluindo uma solução de equações numéricas com múltiplas incógnitas e outra com múltiplas integrais. Ele também descobriu uma regra mnemônica para solucionar o determinante de uma matriz 3x3.

sendo discutidas e analisadas. Seu amplo conhecimento ficou registrado na história, sendo amplamente utilizada no presente e, com certeza, será aplicada também no futuro.

Como profundo conhecedor da obra de Fermat, Euler produziu uma generalização do teorema de Fermat, que permite, por exemplo, encontrarmos o resto da divisão de 3^{2021} por 34, observe que o fato de 34 não ser primo pode a princípio causar algum desconforto, mas na prática o desafio se limita em encontrarmos a potência de 3 que deixe resto 1 ao ser dividido por 34, ou seja, $3^k \equiv 1\ (mod\ 34)$. Mas antes de mergulharmos no Teorema de Euler, precisamos de alguns resultados.

É necessário primeiro, que se verifique se a congruência $aX \equiv 1\ (mod\ m)$ possui alguma solução em X.

Proposição 33. Sejam $a, m\ \in \mathbb{Z}$, com $m > 1$. A congruência $aX \equiv 1\ (mod\ m)$ possui solução se, e somente se, $mdc(a, m) = 1$. Além disso, se $x_0 \in \mathbb{Z}$ é uma solução, então x é uma solução da congruência se, e somente se, $x \equiv x_0\ (mod\ m)$.

Demonstração.

A congruência acima tem uma solução x_0 se, e somente se, $m\ |ax_0 - 1$, o que equivale a dizer que a equação diofantina $aX - mY = 1$ possui solução em números inteiros se, e somente se o $mdc(a, m) = 1$. Por outro lado, se x_0 e x são soluções da congruência $aX \equiv 1\ (mod\ m)$, então $ax \equiv ax_0\ (mod\ m)$ e o $mdc\ (a, m) = 1$, o que implica em $x \equiv x_0\ (mod\ m)$. Observamos ainda que, se x_0 é solução da congruência $aX \equiv 1\ (mod\ m)$, e $x \equiv x_0\ (mod\ m)$, então x é também solução da mesma congruência, pois $ax \equiv ax_0 \equiv 1\ (mod\ m)$. ■

Uma solução da congruência $aX \equiv 1\ (mod\ m)$ determina e é determinada por qualquer outra solução. Se considerarmos que duas soluções congruentes módulo m são, essencialmente, a mesma, temos a unicidade da solução da congruência $aX \equiv 1\ (mod\ m)$.

Proposição 34. Sejam $a, k, m \in \mathbb{Z}$, com $m > 1$ e $mdc(k, m) = 1$. Se $a_1, \cdots, a_m$ é um sistema completo de resíduos módulo m, então $a + ka_1, \cdots, a + ka_m$ também é um sistema completo de resíduos módulo m.

Demonstração.

Para $i, j = 0, \cdots, m - 1$, temos que

$$a + ka_i \equiv a + ka_j\ (mod\ m) \Leftrightarrow ka_i \equiv ka_j\ (mod\ m) \Leftrightarrow a_i \equiv a_j\ (mod\ m) \Leftrightarrow i = j$$

Isso mostra que $a + ka_1, \cdots, a + ka_m$ são, dois a dois, não congruentes módulo m e, portanto, formam um sistema completo de resíduos módulo m. ■

Um *sistema reduzido de resíduos* módulo m é um conjunto de números inteiros $r_1, \cdots, r_s$, tais que

a) $mdc\ (r_i, m) = 1$, para todo $i = 1, \cdots, s$;

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

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

Designamos por $\varphi(m)$ o número de elementos de um sistema reduzido de resíduos módulo $m > 1$, que corresponde à quantidade de números naturais entre 0 e $m - 1$ que são primos com m. Pondo $\varphi(1) = 1$, isso define uma importante função

$$\varphi: \mathbb{N} \longrightarrow \mathbb{N}$$

chamada *função fi de Euler*.

Pela definição, temos que $\varphi(m) \leq m - 1$, para todo $m \geq 2$. Além disso, se $m \geq 2$, então $\varphi(m) = m - 1$ se, e somente se, m é um número primo. De fato, m é primo se, e somente se, $1, 2, \cdots, m - 1$ formam um sistema reduzido de resíduos módulo m, o que equivale a dizer que $\varphi(m) = m - 1$.

Teorema 25. (Euler). Sejam $m, a \in \mathbb{Z}$ com $m > 1$ e $mdc\ (a, m) = 1$. Então,

$$a^{\varphi(m)} \equiv 1\ (mod\ m) \qquad (3.2)$$

Demonstração.

Seja $r_1, \cdots, r_{\varphi(m)}$ um sistema reduzido de resíduos módulo m. Logo $ar_1, \cdots, ar_{\varphi(m)}$ também forma um sistema reduzido de resíduos módulo m e, portanto,

$$ar_1 \cdot ar_2 \cdot \cdots \cdot ar_{\varphi(m)} \equiv r_1 \cdot r_2 \cdot \cdots \cdot r_{\varphi(m)}\ \ (mod\ m)$$

Consequentemente

$$a^{\varphi(m)} r_1 \cdot r_2 \cdot \cdots \cdot r_{\varphi(m)} \equiv ar_1 \cdot ar_2 \cdot \cdots \cdot ar_{\varphi(m)} \equiv r_1 \cdot r_2 \cdot \cdots \cdot r_{\varphi(m)}\ \ (mod\ m)$$

Como o $mdc\ (r_1 \cdot r_2 \cdot \cdots \cdot r_{\varphi(m)}, m) = 1$, segue pela Proposição 32, item (a) que

$$a^{\varphi(m)} \equiv 1\ (mod\ m)$$ ■

Proposição 35. Sejam $m, m' \in \mathbb{N}$ tais que o $mdc(m, m') = 1$. Então $\varphi(mm') = \varphi(m)\varphi(m')$.

Demonstração.

O resultado é trivial se $m = 1$ ou $m' = 1$. Portanto, vamos supor que $m > 1$ e $m' > 1$. Considere a seguinte tabela formada pelos números naturais de 1 a $m \cdot m'$:

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

Como se tem que o $mdc(t, m \cdot m') = 1$ se, e somente se, o $mdc(t, m') = mdc(t, m) = 1$, para calcular $\varphi(m \cdot m')$, devemos determinar os inteiros na tabela acima que são simultaneamente primos com m e m'.

Se o primeiro elemento de uma coluna não for primo com m', então todos os elementos da coluna não são primos com m'. Portanto, os elementos primos com m' estão necessariamente nas colunas

restantes que são em número $\varphi(m')$, cujos elementos são primos com m', como é fácil verificar. Vejamos agora quais são os elementos primos com m em cada uma dessas colunas.

Como o $mdc(m, m') = 1$, a sequência

$$k, m' + k, \cdots, (m-1)m' + k$$

forma um sistema completo de resíduos módulo m, (Proposição 34) e, portanto, $\varphi(m)$ desses elementos são primos com m. Logo, o número de elementos simultaneamente primos com m' e m é $\varphi(m) \cdot \varphi(m')$. ■

Proposição 36. Se p é um número primo e r, um número natural, então tem-se que

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

Demonstração.

De 1 até p^r, temos p^r números naturais. Temos que excluir, desses, os números que não são primos com p^r, ou seja, todos os múltiplos de p, que são precisamente $p, 2p, \cdots, p^{r-1}p$, cujo número é p^{r-1}. Portanto, $\varphi(p^r) = p^r - p^{r-1}$, provando o resultado. ■

Agora, podemos obter a expressão de $\varphi(m)$ para qualquer $m \in \mathbb{N}$.

Teorema 26. Seja $m > 1$ e seja $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ a decomposição de m em fatores primos. Então,

$$\varphi(m) = p_1^{\alpha_1} \cdots p_n^{\alpha_n}\left(1 - \frac{1}{\mathrm{p}_1}\right) \cdots \left(1 - \frac{1}{\mathrm{p}_n}\right) \qquad (3.3)$$

A demonstração desse resultado decorre imediatamente das Proposições 35 e 36.

A fórmula do teorema acima pode assim ser reescrita como se segue:

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

Para calcular o resto da divisão de uma potência a^n por um número natural $m > 1$, é conveniente achar um expoente $h \in \mathbb{N}$ de modo que $a^h \equiv 1\ (mod\ m)$, pois, se $n = hq + r$ é a divisão euclidiana de n por h, teremos $a^n \equiv a^{hq}a^r \equiv a^r\ (mod\ m)$. Portanto, é clara a utilidade do Teorema de Euler para resolução de questões como veremos no exemplo seguinte.

Exemplos 35. Qual o resto da divisão de 3^{2021} por 34.

Solução. Note que

$$\varphi(34) = \varphi(2 \cdot 17) = 2^0.17^0.(2-1).(17-1) = 16$$

Pelo Teorema de Euler, temos que $3^{16} \equiv 1\ (mod\ 34)$, logo

$$3^{2021} \equiv 3^{16.126+5} \equiv 3^5 \equiv 5\ (mod\ 34)$$

Portanto, 5 é o resto da divisão de 3^{2021} por 34.

Observe que com o uso do Teorema de Euler na obtenção do resto da divisão que a princípio poderia levar muito tempo, no exemplo acima, foi feito de forma rápida, simples e prática, evidenciando assim a importância da generalização do Teorema de Fermat, feita por Euler.

3.4. Teorema Chinês dos Restos

O Teorema Chinês dos Restos tem como primeiro registro o livro "*Manual de Aritmética do Sol*" do matemático chinês Sun Zi Suanjung, a data exata do livro é incerta, sabendo-se apenas que foi nos primeiros séculos entre 280 d.C a 483 d.C. A obra divide-se em três capítulos, em que o primeiro capítulo contém apenas dois problemas que tratam de métodos para fazer multiplicações e divisões, utilizando palitinhos chineses, já o capítulo dois trata de vinte e oito problemas envolvendo frações, extrações de raiz quadrada, cálculo de áreas e volumes, proporções e regra de três simples, e finalmente o capítulo três que contém 36 problemas aritméticos e no problema vigésimo sexto conhecido como problema do mestre Sun, utiliza-se pela primeira vez o Teorema Chinês dos Restos.

O chinês Sun-Tsu escreveu num livro intitulado Suan-Ching (Aritmética), que abordava num verso o chamado tai-yen (grande generalização), o seguinte problema: Achar um número que dividido por 3, 5 e 7 deixa restos 2, 3 e 2, respectivamente. Sua resolução tinha como base a determinação de números auxiliares 70, 21 e 15 e observar que $233 = 2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15$ é solução. Dividindo esse resultado por $3 \cdot 5 \cdot 7$, resultava em 23 como resto, que é a menor solução positiva do problema. Somente em 1852, esses resultados tornaram-se conhecidos na Europa, após algumas divergências sobre a validade do método de trabalho, mas em 1874 essa técnica era essencialmente a mesma contida na *Disquisitiones Arithmeticae*, de K. F. Gauss.

Na prática o problema de Sun-Tsu pode ser resumido em encontrar um inteiro que seja a solução do seguinte sistema de congruências.

$$\begin{cases} X \equiv 2 \ (mod\ 3) \\ X \equiv 3 \ (mod\ 5) \\ X \equiv 2 \ (mod\ 7) \end{cases}$$

De modo geral, estamos diante de um sistema de congruências da forma:

$$a_i X \equiv b_i \ (mod\ n_i), \text{ para } i = 1, 2, \cdots, r.$$

Para que tal sistema possua solução, é necessário que o $mdc(a_i, n_i) | \, b_i$, para todo $i = 1, 2, \cdots, r$. Nesse caso, o sistema é equivalente a um da forma

$$X \equiv c_i \ (mod\ m_i), \text{ onde } i = 1, 2, \cdots, r$$

Teorema 27. (Teorema Chinês dos restos) Se o $mdc\left(m_i, m_j\right) = 1$, para todo par de m_i, m_j com $i \neq j$, então o sistema $X \equiv c_i \ (mod\ m_i)$ possui uma única solução módulo $M = m_1 m_2 \cdots m_r$. As soluções são

$$x = M_1 y_1 c_1 + \cdots + M_r y_r c_r + tM, \tag{3.4}$$

onde $t \in \mathbb{Z}$, $M_i = M/m_i$ e y_i é solução de $M_i Y = 1 \ (mod\ m_i), i = 1, 2, \cdots, r$.

Demonstração.

Vamos, inicialmente, provar que x é uma solução simultânea do sistema $X \equiv c_i \ (mod\ m_i)$. De fato, como $m_i \mid M_j$, se $i \neq j$, e $M_i y_i \equiv 1 \ (mod\ m_i)$, segue que

$$x = M_1 y_1 c_1 + \cdots + M_r y_r c_r \equiv M_i y_i c_i \equiv c_i \ (mod\ m_i),$$

Por outro lado, se x' é outra solução do sistema $X \equiv c_i \ (mod\ m_i)$, então

$$x \equiv x' (mod\ m_i), \forall\ i, i = 1, 2, \cdots, r$$

Como o $mdc\left(m_i, m_j\right) = 1$, para $i \neq j$, segue-se que $mmc(m_1, \cdots, m_r) = m_1 \cdots m_r = M$ e consequentemente pela Proposição 32, item (h), temos que $x \equiv x' (mod\ M)$. ■

Exemplos 36. Agora, vamos ao problema de Sun-Tsu. Achar um número que dividido por 3, 5 e 7 deixa restos 2, 3 e 2, respectivamente.

Solução.

Nesse caso, temos que $M = 3 \cdot 5 \cdot 7 = 105$, $M_1 = 5 \cdot 7 = 35$, $M_2 = 3 \cdot 7 = 21$ e ainda que $M_3 = 3 \cdot 5 = 15$. Por outro lado, $y_1 = 2$, $y_2 = 6$ e $y_3 = 8$ são soluções, respectivamente, das congruências $2Y \equiv 1 \ (mod\ 3)$, $Y \equiv 1 \ (mod\ 5)$ e $Y \equiv 1 \ (mod\ 7)$. Portanto, uma solução módulo $M = 105$ é dada por $x = M_1 y_1 c_1 + M_2 y_2 c_2 + M_3 y_3 c_3$, isto é, $x = 758$.

Como $758 \equiv 23 \ (mod\ 105)$, segue que 23 é uma solução única, módulo 105, do problema de Sun-Tsu e qualquer outra solução é da forma $x = 23 + 105.\ t$, com $t \in \mathbb{Z}$.

Outro famoso problema na antiguidade, era que os generais chineses costumavam contar suas tropas perdidas após uma batalha da seguinte forma: ordenavam que as tropas formassem várias colunas com um determinado tamanho e depois contavam quantas sobravam e faziam isso para vários tamanhos diferentes.

Exemplos 37. Um general chinês possuía 2000 soldados para uma batalha. Após o confronto ele precisou verificar suas baixas. Assim alinhou os soldados de 7 em 7 e sobraram 5. Quando alinhou de 9 em 9 sobraram 4. E quando alinhou de 10 em 10 sobrou apenas 1. Quantos soldados haviam na formatura, sabendo que há mais de 1500 indivíduos na formatura?

Solução.

Escrevendo na forma de um sistema de congruências, temos

$$\begin{cases} X \equiv 5\ (mod\ 7) \\ X \equiv 4\ (mod\ 9) \\ X \equiv 1\ (mod\ 10) \end{cases}$$

Nesse caso, temos que $M = 7 \cdot 9 \cdot 10 = 630$, $M_1 = 9 \cdot 10 = 90$, $M_2 = 7 \cdot 10 = 70$ e $M_3 = 7 \cdot 9 = 63$. Por outro lado, $y_1 = 6$, $y_2 = 4$ e $y_3 = 7$ são soluções, respectivamente, das congruências $6Y \equiv 1\ (mod\ 7)$, $7Y \equiv 1\ (mod\ 9)$ e $3Y \equiv 1\ (mod\ 10)$. Portanto, uma solução módulo $M = 630$ é dada por $x = M_1 y_1 c_1 + M_2 y_2 c_2 + M_3 y_3 c_3$, isto é, $x = 4261$.

Como $2000 > x > 1500$, temos que:

$$4261 \equiv 3631 \equiv 3001 \equiv 2371 \equiv 1741\ (mod\ 630)$$

Portanto, haviam 1741 soldados na formatura.

Cabe a ressalva que essa não é a única maneira de se utilizar o Teorema Chinês dos restos, porém optamos por esse método, pois ele se torna mais simples e rápido, se levamos em consideração que ele será utilizado para alunos no nível básico de ensino.

Capítulo 4

Neste capítulo iremos apresentar algumas aplicações contextualizadas relacionando divisibilidade e congruência modular. Essas aplicações serão discutidas em duas perspectivas com o propósito de relacionar os conteúdos, primeiro envolvendo critérios de divisibilidade no ensino fundamental II, com ênfase no 6º e 7º anos e depois estudaremos usando congruência modular, que é uma componente curricular do ensino superior.

A Base Nacional Comum Curricular (BNCC) de 2017 distribui os conteúdos de Matemática em 5 unidades temáticas; Números, Álgebra, Geometria, Grandezas e Medidas, Probabilidade e Estatística. O foco do nosso trabalho está na unidade Números, uma vez que praticamente todos os conteúdos de Aritmética neste ciclo de ensino se concentram nessa unidade.

> "A unidade temática **Números** tem como finalidade desenvolver o pensamento numérico, que implica o conhecimento de maneiras de quantificar atributos de objetos e de julgar e interpretar argumentos baseados em quantidades. No processo da construção da noção de número, os alunos precisam desenvolver, entre outras, as ideias de aproximação, proporcionalidade, equivalência e ordem, noções fundamentais da Matemática. Para essa construção, é importante propor, por meio de situações significativas, sucessivas ampliações dos campos numéricos. No estudo desses campos numéricos, devem ser enfatizados registros, usos, significados e operações." (BRASIL, BNCC, 2017. p.270)

Nessa estrutura curricular, a construção da ideia de números, suas propriedades e operações são abordadas dentro de uma visão de progressão vertical em torno dos objetos de conhecimento e habilidades apresentadas ao longo dos eixos, de forma que as construções e procedimentos acerca dos conceitos sejam conectados e ampliados ao longo de todo o processo. Dessa forma, para o eixo dos Números, espera-se que o aluno ao concluir os anos finais do ensino fundamental, tenha domínio e clareza sobre esse eixo de conhecimento, mas na prática a realidade tem sido outra.

> "Embora o estudo dos números e das operações seja um tema importante no currículo do ensino fundamental, constata-se, com frequência, que muitos alunos chegam ao final dessa fase de formação, com um conhecimento insuficiente sobre como eles são utilizados e sem ter desenvolvido uma ampla compreensão dos diferentes significados das operações." (BRASIL, 1998, p.95)

No entanto, dentro do contexto escolar o que se percebe é uma abordagem do eixo de Números voltada principalmente para a resolução de algoritmos, com escassa ênfase ao olhar qualitativo, investigativo e associativo em torno das propriedades que os envolvem. É no 6º ano, que assuntos importantes da Aritmética, tais como múltiplos, divisores, divisão euclidiana e critérios de divisibilidade são apresentados, sendo no 7º ano ampliados com o mmc, o mdc, módulo, potenciação e radiciação de

um número inteiro, porém o que se verifica na prática é que essa apresentação está voltada apenas a exposição simples de um conjunto de regras e cálculos desconectados de situações cotidianas, concretas, não proporcionando ao aluno percepções de implicações gerais que seus conceitos e ideias podem proporcionar.

Sendo assim, algumas das relações mais significativas no conjunto dos números inteiros, em torno das operações e validações de propriedades numéricas, são praticamente inexploradas no contexto regular da sala de aula. Um exemplo pode ser encontrado na operação de divisão euclidiana, pois não se observa a exploração sobre a condição de existência e unicidade do quociente e do resto em caráter associativo a outras ideias aritméticas, como o papel do quociente numa sequência de múltiplos e divisores de um número inteiro ou mesmo o comportamento cíclico dos restos. A abordagem do sistema de numeração decimal configura outro exemplo, uma vez que tal conteúdo acaba se restringindo ao reconhecimento de ordens e classes numéricas e ao valor posicional de um algarismo, sem qualquer vinculação ou exploração de seu uso no entendimento de relações de igualdade, equivalência e propriedades relacionadas as operações básicas.

Ampliando o nosso olhar sobre os aspectos aritméticos, temos a oportunidade de uma reflexão sobre a abordagem desses assuntos no ambiente escolar e acadêmico, pois a partir de uma pesquisa de natureza aplicada, com uma abordagem qualitativa, utilizando procedimentos técnicos de análise bibliográfica e documental, realizada no primeiro momento no 6º e 7º anos do ensino fundamental e posteriormente na pós-graduação, podemos contribuir na elaboração de hipóteses, comparações e formulações mais abrangentes na utilização dos números e suas construções. Essas implicações convergem para uma preocupação concreta sobre o ensino da matemática, no que se configura uma abordagem fragmentado e independente dos tópicos presentes no eixo Números do currículo. Com essa abordagem verifica-se a causa de uma série de paradigmas e insucessos relacionados ao interesse e aprendizagem matemática. Portanto, neste trabalho usamos aplicações que possibilitam uma relação entre essas formas de registro, no sentido de que

> A originalidade da atividade matemática está na mobilização simultânea de ao menos dois registros de representação ao mesmo tempo, ou na possibilidade de trocar a todo momento de registro de representação. Certamente, segundo os domínios ou as fases da pesquisa, em uma resolução de problema um registro pode aparecer explicitamente privilegiado, mas deve existir a possibilidade de passar de um registro a outro. (DUVAL, 2003, p. 14-15)

Sob outra perspectiva, a abstração do raciocínio hipotético, a transposição da linguagem verbal para a simbólica, própria da matemática, as transformações de padrões percebidos em generalizações, a comparação entre grandezas, são bases para o tratamento e aprendizado algébrico. Desse modo, para que se possa sair de casos particulares e conseguir observar e estabelecer algumas relações, tais como

a de igualdade ou de equivalência, de modo a manipular operações e propriedades numéricas para que se possa formular uma ideia geral, é necessário que se conheça, domine, entenda e aplique com segurança conceitos já estabelecidos, isto é, necessita-se que a relação entre os conhecimentos aritméticos resulte de forma associativa e contínua na construção da base algébrica, pois é nesse campos que se encontram as equações diofantinas, também foco deste trabalho.

Segundo (BRASIL, 2017), o eixo Álgebra presente no currículo de matemática, tem como finalidade a construção do pensamento algébrico e ressalta o caráter contributivo e relacional do eixo de Números nessa construção. Como afirma (LINS; GIMENEZ, 1997, p. 159) “devemos buscar é a coexistência da educação algébrica com a aritmética, de modo que uma esteja implicada na outra”.

Nessa lógica, compreende-se que a abordagem aplicada em alguns tópicos da Teoria dos Números, presentes no currículo de Matemática, pode ser vista como uma ferramenta de alto poder construtivo no processo de transição sem rupturas, entre a Aritmética e a Álgebra. Com isso, também se interfere diretamente em questões como o resultado no processo de ensino aprendizado, pois segundo (GIL, 2008.118f) a relação entre Aritmética e a Álgebra pode também justificar as dificuldades apresentadas pelos alunos no aprendizado de matemática. Ainda acrescenta que, em observação e reflexão sobre a introdução e tratamento aplicado ao ensino de Álgebra, percebe-se que alguns dos procedimentos algébricos escolhidos são contraditórios ou diferentes aos aritméticos dos quais os alunos estavam acostumados, esse cenário acentua-se ao fato dos alunos muitas vezes acumularem e carregarem para as situações de aprendizado atual, dificuldades herdadas em contextos aritméticos anteriores.

Assim, percebemos que mediante esse olhar diferenciado e reflexivo sobre alguns conteúdos e processos aritméticos, em especial, divisibilidade e congruência modular, estamos atendendo a uma demanda significativa do ensino da matemática, promovendo tanto uma melhor percepção e domínio das bases aritméticas, quanto a construção de uma linearidade direta e associativa ao uso algébrico, consequentemente, ampliando os subsídios para o alcance das competências do currículo de Matemática do 6º e 7º anos do Ensino Fundamental, especificados na BNCC.

Dessa forma, vamos agora iniciar a apresentação de algumas aplicações que possam ser resolvidas apenas com o uso dos critérios de divisibilidade e de congruência, em uma linguagem acessível aos alunos do ensino fundamental II e aos alunos do ensino superior uma vez que a notação de congruência usada nesse trabalho é a mesma usada na academia.

Aplicação 01. Divisão Euclidiana

Cinco amigas ganham um pacote de balas e começam a dividir: Uma para Alice, uma para Bia, uma para Carla, uma para Dani e uma para Ester; novamente uma para Alice, uma para Bia, uma para Carla, uma para Dani e uma para Ester; e assim por diante até que termine as 1.786 balas que haviam no pacote. Qual das cinco meninas recebeu a última bala?

Solução.

Note que como a quantidade de balas é muito elevada, continuar a distribuição até que se chegue no número 1.786 não é recomendado. Perceba também que a quantidade de amigas que irá dividir as balas é cinco, portanto, vamos analisar essa situação usando apenas o critério de divisibilidade do 5, isto é, uma congruência módulo 5. Para que um número seja divisível por 5, o algarismo das unidades deve ser zero ou cinco, e como o algarismo das unidades na aplicação proposta é o 6, significa dizer que estamos uma unidade a mais de um ciclo completo, logo quem receberá a última bala será a mesma pessoa que recebeu a primeira, portanto, a Alice.

Podemos também usar tabelas ou mesmo uma figura para ajudar na resolução da questão e ao fazermos uso desses mecanismos estamos utilizando as ferramentas de congruência modular. Além disso, o uso da tabela e da figura ampliam os horizontes de aplicabilidade dos critérios de divisibilidade e da própria congruência.

Tabela 04 – Distribuição da Quantidade de Balas

Alice	1	6	11	16	⋯	1781	1786
Bia	2	7	12	17	⋯	1782	
Carla	3	8	13	18	⋯	1783	
Dani	4	9	14	19	⋯	1784	
Ester	5	10	15	20	⋯	1785	

Fonte: O Próprio Autor

Tabela 05 – Generalização da Quantidade de Balas distribuídas

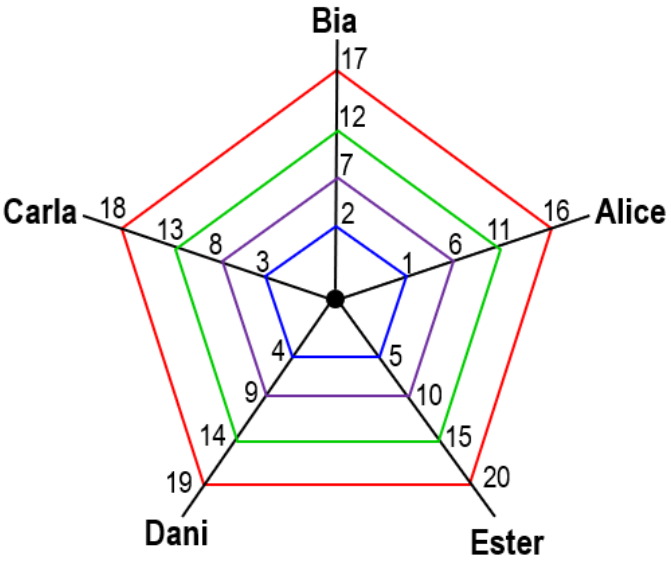
Alice	**Bia**	**Carla**	**Dani**	**Ester**
1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
⋮	⋮	⋮	⋮	⋮
$5q+1$	$5q+2$	$5q+3$	$5q+4$	$5q$

Fonte: O Próprio Autor

Ao analisar as tabelas o aluno irá observar que por maior que seja a quantidade de balas N, ele só precisará trabalhar com o algarismo das unidades, assim ele notará que se o número tiver 1 ou 6 como último algarismo, quem receberá a última bala será a Alice, isto é, $6 \equiv 1 \equiv 1\ (mod\ 5)$. Se o algarismo das unidades fosse o 2 ou 7, quem receberia a última bala seria a Bia, $7 \equiv 2 \equiv 2\ (mod\ 5)$, se fosse 3 ou 8, seria a Carla, $8 \equiv 3 \equiv 3\ (mod\ 5)$, se fosse 4 ou 9, seria a Dani, $9 \equiv 4 \equiv 4\ (mod\ 5)$ e finalmente, se o número tiver como algarismo das unidades o 0 ou 5, a última bala é da menina Ester, $5 \equiv 0 \equiv 0\ (mod\ 5)$. Nota-se também que a tabela 05, permite uma generalização, que valerá para qualquer quantidade N de balas, possibilitando ao aluno estender este raciocínio para outras aplicações.

Outra forma de ilustrar a divisão euclidiana é usando figuras em formato de teias de aranha. Esse método surgiu de uma questão aplicada na prova da OBMEP, além disso, conseguimos distribuir as congruências por cada uma das amigas, isto é, Alice ficará com todas as $N \equiv 1\ (mod\ 5)$, já a Bia ficará com todas as $N \equiv 2\ (mod\ 5)$, a Carla com $N \equiv 3\ (mod\ 5)$, a Dani com $N \equiv 4\ (mod\ 5)$ e por fim a Ester com as $N \equiv 0\ (mod\ 5)$. A esse modelo de ilustração denominamos de “Teia de Congruências”.

Figura 01 – Teia de Congruências módulo 5



Fonte: O Próprio Autor.

Aplicação 02. Divisão Euclidiana

No dia 3 de julho de 2021 foi inaugurado na cidade de Bragança o restaurante Marujos. Sabendo que o dia da inauguração foi um sábado e que o funcionamento do restaurante acontece em escalas a cada três dias, não importando o dia da semana, responda:

(a) Em que dia da semana foi o 100º dia de funcionamento do restaurante Marujos?

(b) Para que o restaurante complete 50 sábados abertos, quantos dias de funcionamento precisarão?

(c) Qual será o dia da semana do aniversário de 2 anos da inauguração do restaurante?

Solução.

Desta vez, vamos iniciar com a construção de uma tabela, na qual destacaremos o dia da semana em que ocorreram as 21 primeiras aberturas do restaurante.

Tabela 06 – Distribuição dos 21 primeiros dias de abertura do Restaurante

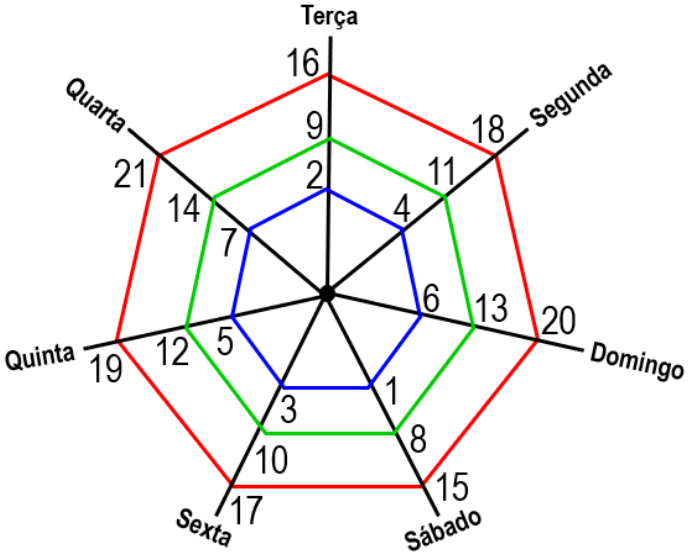
Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
6º	4º	2º	7º	5º	3º	1º
13º	11º	9º	14º	12º	10º	8º
20º	18º	16º	21º	19º	17º	15º

Fonte: O Próprio Autor

Com o auxílio da tabela 06, é possível explorar algumas relações e características, tais como o fato de nos 7 primeiros dias de abertura ocorrerem em dias diferentes da semana. Dessa forma, podemos extrair como conclusão que a resolução do problema é uma divisão euclidiana de 100 dividido por 7, isto é, $100 = 7q + r$, ou ainda, $100 = 7.14 + 2$. Assim, podemos observar que o dia da semana em que o restaurante abrirá pela 100º vez, é aquele que deixa resto 2 na divisão por 7, ou seja, será numa terça-feira.

Usando a teia de congruências, conseguimos distribuir as congruências pelos sete dias da semana, isto é, os sábados serão $N \equiv 1\ (mod\ 7)$, aos domingos temos $N \equiv 6\ (mod\ 7)$, as segundas $N \equiv 4\ (mod\ 7)$, as terças $N \equiv 2\ (mod\ 7)$, as quartas $N \equiv 0\ (mod\ 7)$, as quintas $N \equiv 5\ (mod\ 7)$ e por fim as sextas $N \equiv 3\ (mod\ 7)$. Observe que as congruências não seguem uma sequência linear como na aplicação anterior.

Figura 02 – Teia de Congruências módulo 7



Fonte: O Próprio Autor.

Para resolvermos o item (b), vamos usar uma generalização do número de aberturas do restaurante, a partir do resto deixado na divisão euclidiana.

Tabela 07 – Generalização dos dias de funcionamento do Restaurante

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
6º	4º	2º	7º	5º	3º	1º
13º	11º	9º	14º	12º	10º	8º
⋮	⋮	⋮	⋮	⋮	⋮	⋮
$7q + 6$	$7q + 4$	$7q + 2$	$7q$	$7q + 5$	$7q + 3$	$7q + 1$

Fonte: O Próprio Autor

Note que os dias de funcionamento aos sábados são representados por números que deixam resto 1 na divisão euclidiana por 7, então ele é da forma $7q + 1$, onde q representa quantos ciclos semanais, completam-se desde o início da contagem. Uma maneira de expor esse raciocínio é o de montar uma tabela.

Tabela 08 – Generalização da quantidade de abertura do Restaurante aos sábados

Ordenação dos Sábados de funcionamento q	Total de dias de funcionamento
1º	$7.0 + 1 = 1$
2º	$7.1 + 1 = 8$
3º	$7.2 + 1 = 15$
⋮	⋮
q	$7.(q - 1) + 1$

Fonte: O Próprio Autor

Para respondermos ao questionamento do item (b), isto é, para que o restaurante complete 50 sábados abertos, quantos dias de funcionamento precisarão?

Assim, podemos supor que para $q = 50$, temos

$$7.(50 - 1) + 1 = 344,$$

ou seja, após 344 dias de funcionamento o restaurante completará 50º sábados de abertura.

Para o item (c), isto é, qual será o dia da semana do aniversário de 2 anos da inauguração do restaurante?

Verificamos que o total de dias existentes nos 2 anos após a abertura é de $2.365 = 730\ dias$. Como esses dias estão organizados em ciclos de 7 dias, podemos escrever nas seguintes notações: $730 = 7.104 + 2$ (divisão euclidiana), $730 - 2 = 7q$ (múltiplo de 7), que $7|\ 730 - 2$ (divisor de 7)

ou ainda $730 \equiv 2\ (mod\ 7)$ (congruência). Como temos 104 ciclos semanais completos e mais dois dias e a abertura do restaurante foi no sábado 03 de julho, então dois dias a frente será uma segunda-feira.

As duas primeiras aplicações que acabam de ser apresentadas, proporcionam um olhar mais prático e concreto ao aluno, uma vez que elas surgem de situações problemas rotineiros, o que facilitará o envolvimento do aluno. Nas aplicações seja usando as tabelas ou a teia de congruências observamos a generalização que essas aplicações oferecem, pois elas ampliam e conectam conteúdos como divisão euclidiana e critérios de divisibilidade além disso, possibilitam também o contato do aluno com as congruências, isso tudo de uma maneira clara, simples e objetiva.

Outra importante contribuição que essas aplicações oferecem é o de estabelecer uma relação entre divisibilidade e congruência modular, permitindo uma conexão entre os conteúdos trabalhados na disciplina Aritmética na pós-graduação e a sua utilização no ciclo básico, atendendo assim um dos objetivos centrais do programa de mestrado profissional.

Aplicação 03. Sistema de Congruências.

Daniela e Manuel são irmãos e juntos têm mais de trinta e menos de oitenta livros. Um dia eles foram arrumar os livros no armário, quando separavam de 2 em 2 sempre sobrava 1, quando separavam de 3 em 3 sempre sobrava 2 e quando separavam de 5 em 5 sempre sobravam 4. Qual é a quantidade de livros que os irmãos possuem?

Solução:

Esse é o típico problema em que a análise dos critérios de divisibilidade é suficiente para solucionarmos a questão, sem ter que fazer uso de ferramentas mais elaboradas, como o Teorema Chinês dos Restos ou mesmo das congruências, por exemplo.

Note que estamos em busca de um número N, em que, $30 < N < 80$. Usando o critério de divisibilidade do 2, observamos que o número procurado é ímpar, pois separados de 2 em 2 sobra 1, ou seja, o algarismo das unidades só pode ser $\{1, 3, 5, 7, 9\}$. No entanto, ao usarmos o critério de divisibilidade do 5, observamos que N não pode ter como algarismo das unidades o 5, pois se assim o fosse, o número N seria divisível por 5, o que não ocorre, logo devemos descartar o 5 do conjunto dos últimos algarismos, restando apenas $\{1, 3, 7, 9\}$. No entanto, ao analisarmos que o número N deixa resto 4 quando dividido por 5, evidenciamos que esse número só pode ter como algarismo das unidades o 4 ou o 9, mas o 4 se descarta pelo fato do número procurado ser ímpar, então concluímos que o número procurado tem o nove como último algarismo, descartando assim o $\{1, 3, 7\}$ da posição de algarismo das unidades.

Então, as possibilidades para o número N são $39, 49, 59, 69, 79$. Para finalmente chegarmos ao valor procurado, vamos usar o critério de divisibilidade do 3, isto é, para que um número seja divisível por 3 a soma dos seus algarismos precisa ser múltiplo de 3. Como N deixa resto 2 quando dividido por 3, descartamos o $39 = 3.13 + 0$ e o $69 = 3.23 + 0$, que já que eles são múltiplos de 3, ou seja, $3|39$ e $3|69$, já o 49 e o 79 são descartado por deixarem resto 1 quando divididos por 3, $49 = 3.16 + 1$ e $79 = 3.26 + 1$, portanto o número de livros procurado é $N = 59$, já que $5 + 9 = 14$ e $14 = 3.4 + 2$ deixa resto 2 quando dividido por 3.

Vamos agora resolver utilizando o Teorema Chinês dos Restos, teorema abordado na componente curricular de Aritmética no ensino superior.

Escrevendo na forma de um sistema de congruências, temos

$$\begin{cases} N \equiv 1\ (mod\ 2) \\ N \equiv 2\ (mod\ 3) \\ N \equiv 4\ (mod\ 5) \end{cases}$$

Nesse caso, temos que $M = 2 \cdot 3 \cdot 5 = 30$, $M_1 = 3 \cdot 5 = 15$, $M_2 = 2 \cdot 5 = 10$ e ainda $M_3 = 2 \cdot 3 = 6$. Por outro lado, $y_1 = 3$, $y_2 = 4$ e $y_3 = 6$ são soluções, respectivamente, das congruências $Y \equiv 1\ (mod\ 2)$, $Y \equiv 1\ (mod\ 3)$ e $Y \equiv 1\ (mod\ 5)$. Portanto, uma solução módulo $M = 30$ é dada por $N = M_1 y_1 c_1 + M_2 y_2 c_2 + M_3 y_3 c_3$, isto é, $N = 269$.

Como $30 < N < 80$, temos que

$$269 \equiv 269 - 30 \equiv 239\ (mod\ 30)$$
$$239 \equiv 239 - 30 \equiv 209\ (mod\ 30)$$
$$209 \equiv 209 - 30 \equiv 179\ (mod\ 30)$$
$$179 \equiv 179 - 30 \equiv 149\ (mod\ 30)$$
$$149 \equiv 149 - 30 \equiv 119\ (mod\ 30)$$
$$119 \equiv 119 - 30 \equiv 89\ (mod\ 30)$$
$$89 \equiv 89 - 30 \equiv 59\ (mod\ 30)$$

Portanto, os irmãos possuem 59 livros.

Aplicação 04. Sistema de Congruências.

Subindo uma escada de dois em dois degraus, sobra um degrau. Subindo a mesma escada de três em três degraus, sobram dois degraus. Determine quantos degraus possui a escada, sabendo que o número de degraus é um múltiplo de 7 e está compreendido entre 40 e 100.

Solução.

Usando o critério de divisibilidade do 2, o número que estamos procurando é ímpar, já que o mesmo deixa resto 1, quando dividido por 2. Como o número é múltiplo de 7, então devemos analisar apenas os múltiplos ímpares de 7, compreendidos entre 40 e 100. Ao fazermos isso, ficamos apenas

com os seguintes valores $\{49, 63, 77, 91\}$. Por fim, usamos o critério de divisibilidade do 3, onde para que um número seja divisível por 3 a soma dos seus algarismos precisa ser múltiplo de 3, assim descartamos o $63 = 3.21 + 0$, pois, $3|63$, e estamos em busca de um valor que deixa resto 2 quando dividido por 3, logo devemos eliminar o 49 e o 91 já que fazendo a soma dos seus algarismos, vemos que $4 + 9 = 13$ e $9 + 1 = 10$, ou seja, ambos deixam resto 1 quando divididos por 3. Portanto o número de degraus dessa escada é $N = 77$, pois o mesmo é múltiplo de 7, é ímpar e deixa resto 2 quando dividido por 3, uma vez que $7 + 7 = 14$ e $14 = 3.4 + 2$.

Vamos agora resolver utilizando o Teorema Chinês dos Restos

Escrevendo na forma de um sistema de congruências, temos

$$\begin{cases} N \equiv 1\ (mod\ 2) \\ N \equiv 2\ (mod\ 3) \\ N \equiv 0\ (mod\ 7) \end{cases}$$

Nesse caso, temos que $M = 2 \cdot 3 \cdot 7 = 42$, $M_1 = 3 \cdot 7 = 21$, $M_2 = 2 \cdot 7 = 14$ e ainda $M_3 = 2 \cdot 3 = 6$. Por outro lado, $y_1 = 5$, $y_2 = 8$ e $y_3 = 6$ são soluções, respectivamente, das congruências $Y \equiv 1\ (mod\ 2)$, $2Y \equiv 1\ (mod\ 3)$ e $6Y \equiv 1\ (mod\ 7)$.

Portanto, uma solução módulo $M = 42$ é dada por

$$N = M_1 y_1 c_1 + M_2 y_2 c_2 + M_3 y_3 c_3$$

isto é, $N = 329$.

Como $40 < N < 100$, temos que:

$$329 \equiv 329 - 42 \equiv 287\ (mod\ 42)$$
$$287 \equiv 287 - 42 \equiv 245\ (mod\ 42)$$
$$245 \equiv 245 - 42 \equiv 203\ (mod\ 42)$$
$$203 \equiv 203 - 42 \equiv 161\ (mod\ 42)$$
$$161 \equiv 161 - 42 \equiv 119\ (mod\ 42)$$
$$119 \equiv 119 - 42 \equiv 77\ (mod\ 42)$$

Portanto, a escada possui 77 degraus.

Podemos resolver também esse problema com o uso de uma equação de duas variáveis (equação diofantina), para isso vamos escrever

$$N = 2x + 1 \qquad (*)$$
$$N = 3y + 2 \qquad (**)$$

Igualando $(*)$ e $(**)$, temos que $2x - 3y = 1$. Observe que agora estamos diante de uma equação diofantina que possui solução já que o $mdc(2, -3) = 1$, e que por simples inspeção

encontramos a solução minimal $x_0 = 2$ e $y_0 = 1$, que nos permite escrever as soluções gerais para as duas variáveis $x = 2 + 3k$ e $y = 1 + 2k$, $k \in \mathbb{Z}$.

Substituindo as soluções gerais em $(*)$ e $(**)$ encontramos

$$N = 6k + 5$$

onde k é um inteiro.

Como $40 < N < 100$, podemos achar os valores inteiros de k que satisfazem essas inequações, $40 < 6k + 5 < 100 \Rightarrow 35 < 6k < 95$, dessa forma observamos que os possíveis valores de são $k = \{6, 7, \cdots, 15\}$.

De posse desses resultados podemos tabelar esses valores para que possamos destacar os restos da divisão de N por 7, afim de identificar o que deixa resto zero, ou seja, o N que é múltiplo de 7.

Tabela 09 – Análise dos valores de $40 < N < 100$

k	$N = 6k + 5$	$N = 2q + r$	$N = 3q + r$	$N = 7q + r$	$resto$
6	41	$2.20 + 1$	$3.13 + 2$	$7.5 + 6$	6
7	47	$2.23 + 1$	$3.15 + 2$	$7.6 + 5$	5
8	53	$2.26 + 1$	$3.17 + 2$	$7.7 + 4$	4
9	59	$2.29 + 1$	$3.19 + 2$	$7.8 + 3$	3
10	65	$2.32 + 1$	$3.21 + 2$	$7.9 + 2$	2
11	71	$2.35 + 1$	$3.23 + 2$	$7.10 + 1$	1
12	77	$2.38 + 1$	$3.25 + 2$	$7.11 + 0$	0
13	83	$2.41 + 1$	$3.27 + 2$	$7.11 + 6$	6
14	89	$2.44 + 1$	$3.29 + 2$	$7.12 + 5$	5
15	95	$2.47 + 1$	$3.31 + 2$	$7.13 + 4$	4

Fonte: O Próprio Autor

Analisando a tabela 09 observamos que todos os valores na forma $N = 6k + 5$, deixam resto 1 quando divididos por 2 e deixam resto 2 quando dividido por 3, no entanto, apenas um desses valores é múltiplo de 7, ou seja, $N = 77$ é o número que atende a todas as condições do problema.

As aplicações 03 e 04 são sistemas de congruências que podem ser resolvidas apenas com o uso dos critérios de divisibilidade, porém podem ser resolvidas também através do Teorema Chinês dos Restos ou ainda por equações diofantinas (aplicação 04) o que possibilita uma ampliação nas possibilidades de uso dessas aplicações, isto é, se usarmos apenas os critérios de divisibilidade estamos realizando uma resolução aritmética que pode ser abordada no 6º e 7º anos, e quando optamos por uma

solução com o uso de congruências e equações diofantinas estamos justamente fazendo uma resolução algébrica, assim temos a oportunidade de oferecer uma ligação entre o pensamento aritmético e o algébrico, de acordo com (LINS. 1997).

Aplicação 05. Mínimo Múltiplo Comum

Uma festa de casamento será realizada em um salão que comporta no máximo 200 pessoas. O organizador sabe que, se distribuir 8 convidados por mesa, uma mesa ficará com apenas um convidado. O mesmo irá ocorrer se ele distribuir 6 ou 7 convidados por mesa. Se ele distribuir 9 convidados por mesa, uma mesa ficará com menos do que 9 pessoas. Quantas pessoas ficarão nessa última mesa?

Solução.

Vamos primeiramente encontrar o número N, que representa a quantidade de convidados. Observe também que a quantidade de convidados será das formas $N = 6q + 1, N = 7q' + 1$ e ainda $N = 8q'' + 1$, para $q, q' e\ q'' \in \mathbb{Z}$, isto é, se o número N deixa resto 1 nas divisões por 6, 7 e 8, então ele também deixará resto 1 quando dividido pelo $mmc(6,7,8) = 168$, sendo assim, o número de convidados também poderá ser escrito da forma $N = 168k + 1$, para $k \in \mathbb{Z}$. Mas, note que o valor de $N \leq 200$, o que só será possível se o quociente $k = 1$, o que possibilita um $N = 169$. Sendo o número de convidados igual a 169, se os mesmos forem distribuídos em mesas com 9 convidados teremos $169 = 9.18 + 7$, ou seja, a última mesa terá apenas 7 convidados.

Essa aplicação também pode ser resolvida por congruências, escrevendo

$$\begin{cases} N \equiv 1\ (mod\ 6) \\ N \equiv 1\ (mod\ 7) \\ N \equiv 1\ (mod\ 8) \end{cases}$$

Usando a proposição 32 item (h), podemos simplificar o sistema de congruências para apenas uma congruência $N \equiv 1\ (mod\ 168)$, sendo 168 o mínimo múltiplo comum de 6, 7 e 8. Em seguida podemos escrever essa congruência no formato de uma divisão euclidiana $N = 168k + 1$, a partir desse momento verificamos que o único valor possível para o quociente $k = 1$, uma vez que qualquer outro valor inteiro e positivo maior que um iria significar um número superior a 200 convidados, dessa forma temos que o valor de $N = 168.1 + 1 = 169$, e como essa quantidade de convidados será distribuída em mesas de 9 convidados assim $169 \equiv 7\ (mod\ 9)$, pois $169 = 9.18 + 7$, isto é, teremos 18 mesas com 9 convidados cada e uma última mesa com 7 convidados.

Aplicação 06. Máximo Divisor Comum

Beto, Caio e Davi possuem 72, 90 e 150 figurinhas respectivamente, eles querem guardar as figurinhas em pacotes de igual quantidade, utilizando para isso a menor quantidade possível de pacotes. Quantas figurinhas serão guardadas em cada pacote utilizado por eles?

Solução.

Fazendo uma análise de divisibilidade dos três valores, observamos que todos eles são pares, logo a quantidade de figurinhas que será depositada nos pacotes, também será um múltiplo de 2. Em seguida podemos analisar os valores pelo critério de divisibilidade do 3 e do 9, e logo veremos que todos são divisíveis por 3, pois, $7 + 2 = 9$, $9 + 0 = 9$ e $1 + 5 + 0 = 6$, porém apenas o 72 e 90 são divisíveis por 9 uma vez que todo múltiplo de 9 também é múltiplo de 3. Seguindo na análise, vemos que apenas o número 72 é divisível por 4, o que também já exclui a divisibilidade por 8 dos três valores juntos. Continuando a análise, vemos que apenas os valores 90 e 150 são divisíveis por 5 e por 10, já que 72 deixar resto 2, quando dividido por 5 ou por 10. Fazendo a análise da divisibilidade por 7 do valor 72, vemos que $7 + 5.2 = 17$, e 17 não é divisível por 7, o que também já impossibilita o uso do 7. Por fim, observamos que 72 também não é divisível por 11, já que $7 - 2 = 5$ e 5 não é divisível por 11. Concluída as análises vemos que, os três valores só obedecem de forma simultânea os critérios de divisibilidade do 2 e do 3, o que permite também a sua divisibilidade por 6, já que todo número que é divisível por 2 e por 3 também será divisível por 6. Portanto, em cada pacote utilizado pelos garotos teremos 6 figurinhas.

Nessa aplicação podemos explorar também o uso das congruências

$$90 \equiv 18\ (mod\ 72)$$

$$150 \equiv 6\ (mod\ 72)$$

Analisando os dois restos da congruência observamos que ambos são múltiplos de 6, logo

$$18 \equiv 6 \equiv 0\ (mod\ 6)$$

E como 72 é múltiplo de 6, então

$$\begin{cases} 72 \equiv 0\ (mod\ 6) \\ 90 \equiv 0\ (mod\ 6) \\ 150 \equiv 0\ (mod\ 6) \end{cases}$$

Portanto o número de figurinhas em cada pacote será 6.

Ao observarmos as aplicações 05 e 06 notamos a possibilidade do uso dos critérios de divisibilidade e da divisão euclidiana na determinação do mmc e mdc, uma vez que foi possível resolver as situações apresentadas sem o uso da tradicional fatoração, ou seja, é mais uma janela de oportunidades que se abre para que se possa aplicar os critérios de divisibilidade e a divisão euclidiana, prolongando ainda mais os horizontes de aplicação desse importante conteúdo aritmético. O uso das congruências nessas aplicações pode ser usado no ambiente acadêmico para exemplificar a relação entre mmc e mdc, ressaltando inclusive a importância do mdc nas equações diofantinas como pode ser observado pelo uso do Teorema de Bézout.

Aplicação 07. Radiciação

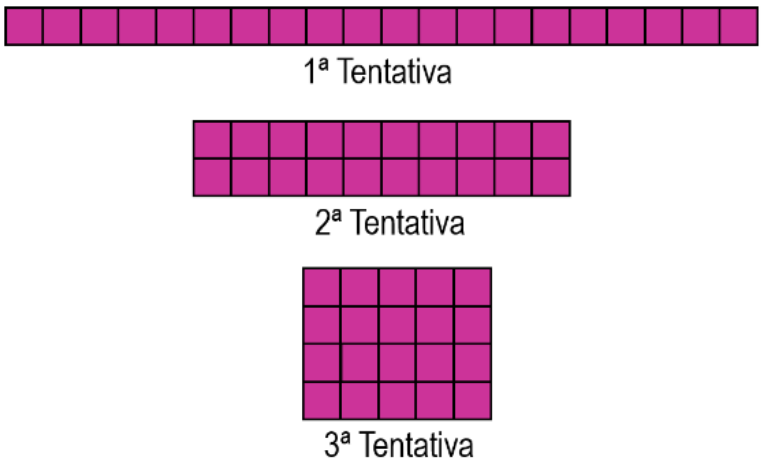
Pedro e Lucas possuem 20 e 36 placas quadradas cada um, respectivamente. Eles estão brincando de formar figuras com as suas placas de tal forma que não sobre nenhuma placa, vencerá a disputa aquele que conseguir formar um quadrado, usando todas as suas peças. Quem será o vencedor?

Solução.

Nessa disputa será vencedor aquele que possuir uma quantidade de blocos a que ao ser dividida por um valor b, terá no quociente um valor igual ao próprio divisor b. Vamos analisar essas possibilidades usando os critérios de divisibilidade:

Primeiramente para o Pedro (20 placas). Como sabemos, o 1 divide qualquer número, porém se enfileirarmos as 20 placas um ao lado do outro não formaremos um quadrado, pelo mesmo motivos que se colocarmos as vinte placas uma sobre a outra. Usando o critério de divisibilidade do 2, vemos que a quantidade de placas do Pedro é par, logo divisível por 2, porém a quantidade de placas não é divisível por 3, já que $2 + 0 = 2$ e 3 não divide 2. As placas podem ser agrupadas de 4 em 4, já que 20 é divisível por 4, ele também pode agrupar as placas de 5 em 5 ou de 10 em 10, já que o número vinte termina em zero, atendendo assim os critérios do 5 e do 10, isto é, as placas do Pedro podem ser agrupadas de 6 maneiras $D_{(20)} = \{1, 2, 4, 5, 10, 20\}$. Como a quantidade de divisores que representa as placas que o Pedro tem a sua disposição $d(20) = 6$ é um número par não temos um quadrado perfeito, então ele não conseguirá formar um quadrado com essa quantidade de peças utilizando todas, pois $\sqrt{20} \notin \mathbb{Z}$. Podemos inclusive representar as suas 6 tentativas de formar um quadrado, com apenas três figuras, que elas se diferem apenas por uma rotação.

Figura 03 – Tentativas de montagem de um quadrado com 20 placas



Fonte: O Próprio Autor.

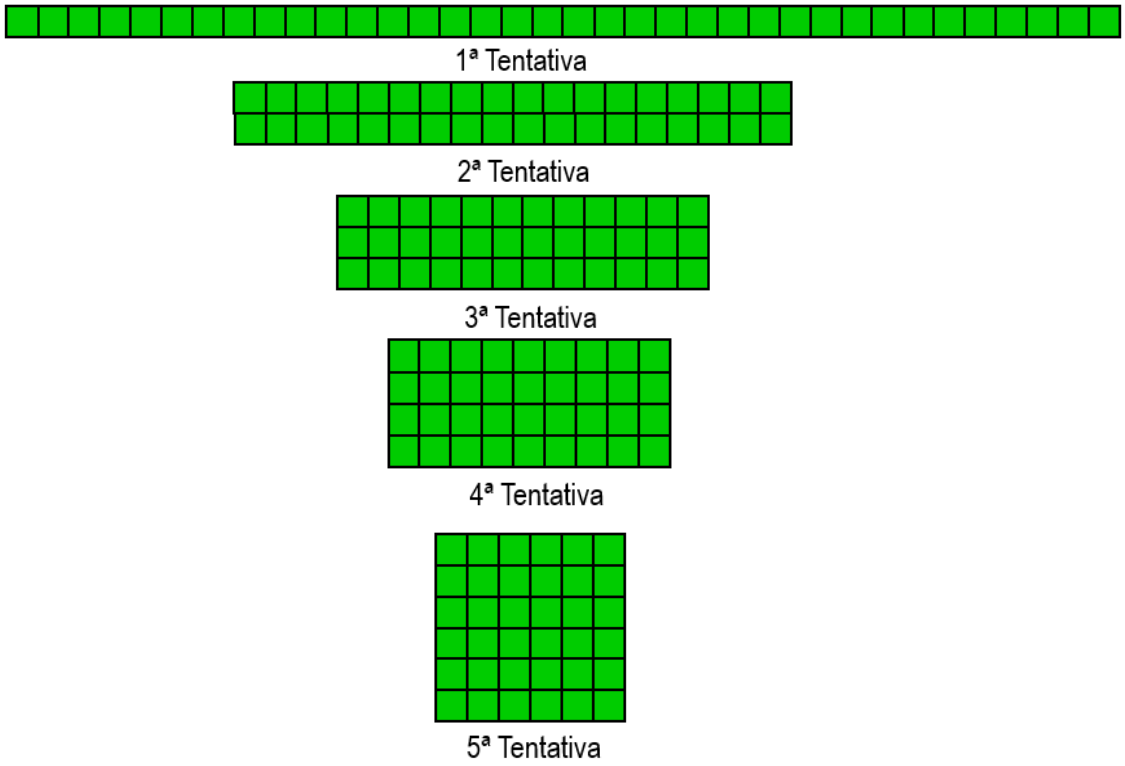
Agora vamos analisar as 36 placas do Lucas. Como sabemos, o 1 divide qualquer número, porém se enfileirarmos as 36 placas uma ao lado da outra não formaremos um quadrado, pelo mesmo motivos que se colocarmos as trinta e seis placas uma sobre o outra. Usando o critério de divisibilidade do 4,

vemos que a quantidade de placas do Lucas é um número par e divisível por 4, logo divisível por 2 também, já que todo múltiplo de 4, também é múltiplo de 2. Notamos também que a quantidade 36 é divisível por 9, já que $3 + 6 = 9$, e 9 é múltiplo de 9, logo divisível por 3 também, já que todo múltiplo de 9, também é múltiplo de 3. Como 36 é múltiplo de 2 e de 3 simultaneamente, também será de 6, e como 36 também é múltiplo de 3 e 4 simultaneamente, também será de 12 e por fim será de 18 também, pois 36 é múltiplo de 2 e 9 simultaneamente. Assim, as peças de Lucas podem ser agrupadas de 9 maneiras $D_{(36)} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$. Como a quantidade de divisores que representa as placas que o Lucas tem a sua disposição $d(36) = 9$ é um número ímpar, será um quadrado perfeito, então ele conseguirá formar um quadrado com essa quantidade de peças utilizando todas, uma vez que $\sqrt{36} \in \mathbb{Z}$.

Assim consequentemente a paridade da quantidade de divisores de um número se apresenta como uma excelente possibilidade de apresentação para a operação de radiciação, pois apesar de ser uma operação nova para os alunos dessas séries a sua chegada pode ser feita com ferramentas já conhecidas o que favorece e intensifica a importância de conteúdos como múltiplos, divisores e fatoração.

Podemos inclusive representar as tentativas de formar um quadrado, com apenas 5 figuras, que se diferem apenas por uma rotação.

Figura 04 – Tentativas de montagem de um quadrado com 36 placas



Fonte: O Próprio Autor.

Essa aplicação é relevante, pois oferece uma conexão entre os critérios de divisibilidade e a operação de radiciação, permitindo mais uma vez ao aluno a ampliação e a ligação entre vários conteúdos, pois podemos também explorar nessa aplicação: a quantidade de divisores de um número, a determinação de quais são os divisores desse número, os divisores comuns, a paridade da quantidade de divisores, a definição de múltiplo, a fatoração em termos primos e a potenciação, além disso as tentativas de agrupamento das placas (Figuras 03 e 04) que oferece ao aluno uma visão lúdica de todo o processo.

Aplicação 08. Equações Diofantinas

Uma fábrica de gelo precisa entregar 26 toneladas de gelo para um barco. A entrega será efetuada usando os dois caminhões da fábrica, um deles com capacidade para transportar 3 toneladas, e o outro com capacidade para 2 toneladas. Se, em cada viagem, os caminhões estiverem preenchidos com sua capacidade máxima, e os dois caminhões forem utilizados na entrega, de quantas maneiras diferentes a entrega pode ser feita?

Solução:

Vamos chamar de x o número de viagens dadas pelo caminhão que transporta 3 toneladas e de y o que transporta 2 toneladas, assim montamos a equação $3x + 2y = 26$, onde $x, y \in \mathbb{N}$.

Isolando uma das variáveis da equação $3x + 2y = 26$, obtemos

$$3x = 26 - 2y$$

$$3x = 2(13 - y)$$

$$x = 2.\frac{(13 - \mathrm{y})}{3}$$

$$x = 2.k, \text{ sendo } k = \frac{13-\mathrm{y}}{3}$$

Sendo $x, y \in \mathbb{N}$, note que $0 < y < 13$, assim estamos em busca dos valores de y, que ao serem subtraídos de 13, tornam-se divisíveis por 3, isto é, $3 \,|(13 - y)$. Dessa forma, o primeiro valor de y é 1, pois, $3 \,|(13 - 1)$, e em sendo $y = 1$, o valor de x é 8, pois $x = 2.4 = 8$.

O segundo valor possível para y seria 4, o que iria gerar um $x = 2.3 = 6$. O terceiro valor para y seria 7, o que produziria um $x = 2.2 = 4$, e por fim poderíamos ter um $y = 10$, gerando assim um $x = 2$. Totalizando 4 possibilidades de entrega.

Essas possibilidades podem ser organizadas em uma tabela.

Tabela 10 – Análise das possibilidades de entrega por inspeção da variável y

y	k	$x = 2.k$
1	4	8
4	3	6
7	2	4
10	1	2

Fonte: O Próprio Autor

Caso tivéssemos optado por isolar a variável y, teríamos:

$$3x + 2y = 26$$
$$2y = 26 - 3x$$
$$2y = 26 - 3x$$
$$y = \frac{(26 - 3x)}{2}$$

Sendo x, $y \in \mathbb{N}$, note que $2 \mid (26 - 3x)$, assim podemos usar a paridade para afirmar que x será necessariamente um número par, já que ele está sendo multiplicado por um número ímpar e a diferença entre $(26 - 3x)$, precisar ser par, já que é divisível por 2. Outro aspecto importante é que $x < 10$, pois $3x = 30$ e $(26 - 30) \notin \mathbb{N}$, assim a variável x, é um número par compreendido entre 2 e 8, ou seja, $x = \{2, 4, 6, 8\}$. Logo, os valores y são 10, 7, 4 e 1. Organizando na tabela, encontramos as mesmas 4 possibilidades de entrega.

Tabela 11 – Análise das possibilidades de entrega por inspeção da variável x

x	y
2	10
4	7
6	4
8	1

Fonte: O Próprio Autor

Temos a possibilidade de resolver essa equação diofantina com o uso das congruências.

$$3x + 2y = 26 \Rightarrow 3x + 2y - 26 = 0$$

Fazendo cada termo da equação congruência módulo 2, e em seguida usando a proposição 32, item (e), obtemos

$$3x \equiv x \ (mod\ 2)$$
$$2y \equiv 0 \ (mod\ 2)$$
$$-26 \equiv 0 \ (mod\ 2)$$

$$3x + 2y - 26 \equiv x \equiv 0\ (mod\ 2) \Rightarrow x \equiv 0\ (mod\ 2)$$

O que nos fornece os valores de $x = \{0, 2, 4, 6, 8, 10, \cdots, 2k\}$, porém devemos atentar para o fato da variável x representar a quantidade de viagens realizadas pelo caminhão de 3 toneladas. Como o comando deixa claro que o caminhão será usado excluímos o valor $x = 0$, assim como todos os valores de $x \geq 10$, pois dez viagens representariam um valor acima das 26 toneladas transportadas, o que possibilita apenas 4 valores para x, sendo eles $x = \{2, 4, 6, 8\}$.

Agora vamos fazer cada termo da equação congruência módulo 3, e em seguida usaremos novamente a proposição 32, item (e), obtemos

$$3x \equiv 0\ (mod\ 3)$$
$$2y \equiv -y\ (mod\ 3)$$
$$-26 \equiv 1\ (mod\ 3)$$
$$3x + 2y - 26 \equiv -y + 1\ (mod\ 3)$$
$$y \equiv 1\ (mod\ 3)$$

O que nos fornece os valores de $y = \{1, 4, 7, 10, 13, \cdots, 3k + 1\}$, porém devemos atentar para o fato da variável y representar a quantidade de viagens realizadas pelo caminhão de 2 toneladas. Como o comando deixa claro que o caminhão será usado excluímos os valores $y \geq 13$, pois treze viagens representariam o valor total da carga por apenas um caminhão e como sabemos os dois veículos são usados, o que possibilita apenas 4 valores para y, sendo eles $y = \{1, 4, 7, 10\}$.

Reunindo as 4 possibilidades de cada variável tabela 12, concluímos que só há 4 maneiras de se fazer essa entrega de 26 toneladas usando os dois caminhões.

Tabela 12 – Análise das possibilidades de entrega por congruência

x	$3x$	y	$2y$	$3x + 2y$	$= 26$
8	24	1	2	$24 + 2$	$= 26$
6	18	4	8	$18 + 8$	$= 26$
4	12	7	14	$12 + 14$	$= 26$
2	6	10	20	$6 + 20$	$= 26$

Fonte: O Próprio Autor

Nessa última aplicação destacamos a relação entre divisibilidade, equações diofantinas e congruências, uma vez que as mesmas podem ser resolvidas através do algoritmo de Euclides ou por congruência, e ao fazermos uso dos conceitos de múltiplo, divisor e os critérios de divisibilidade do 2 e do 3, possibilitamos mais uma vez a ligação entre os conteúdos aritméticos e algébricos defendida por (LINS; 1997), criando um ambiente de familiaridade e de fluxo contínuo entre os eixos de Números e Álgebra, exposta na BNCC (2017).

Capítulo 5

Considerações Finais

Encontramos com muita frequência no ensino médio alunos que não dominam os principais critérios de divisibilidade e que não conseguem realizar a transposição da linguagem verbal para a simbólica, pensando nisso já inserimos em nossos planejamentos anuais revisões de temas aritméticos do ensino fundamental, é nesse momento que os conteúdos são novamente apresentados aos alunos, porém essa nova abordagem é rápida e busca apenas aspectos pontuais, não permitindo uma ligação entre divisibilidade e outros assuntos, sejam eles aritméticos ou algébricos.

Dessa forma, observamos que a melhor maneira de minimizarmos esse problema é solucionar essas dificuldades ainda no ensino fundamental, especificamente no 6º e 7º anos. No entanto, essa abordagem não deve ser feita de forma mecânica, produzindo apenas uma memorização rápida de tópicos isolados, precisamos inserir aplicações que possibilitem uma ampliação do uso da divisibilidade, permitindo uma ligação entre divisão euclidiana e critérios de divisibilidade, criando uma continuidade entre os aspectos aritméticos e algébricos que favoreçam a transposição da linguagem verbal para a simbólica matemática.

Usando uma linguagem compatível ao ciclo de ensino, apresentamos aplicações que capacitam os alunos a estabelecer uma conexão entre os critérios de divisibilidade, a divisão euclidiana, o uso de divisores e múltiplos, o mmc e o mdc, a operação de radiciação e equações lineares com até duas variáveis, além disso é apresentado ao aluno a notação de congruência modular, notação essa que não oferece dificuldades por tratar-se de uma simplificação de todo o processo de divisão com restos. As aplicações expostas nesse trabalho são feitas em diferentes linguagens, com o auxílio de tabelas e da teia de congruências, o que possibilitou a generalização de muitos resultados o que beneficia a transposição de linguagens pelos alunos. Portanto, essas aplicações configuram uma excelente oportunidade de solução para as dificuldades encontradas no ensino médio.

Outro ponto de destaque nessas aplicações é a relação entre os tópicos trabalhados no ensino fundamental e os conteúdos abordados na disciplina Aritmética na pós-graduação, gerando exemplos que relacionam conteúdos como divisibilidade, equações diofantinas e congruências, sendo este último tópico, fundamental para a utilização do Teorema de Fermat, do Teorema de Euler e o Teorema Chinês dos Restos. A utilização dessas aplicações no ensino superior oferece aos discentes deste ciclo uma relação entre os critérios de divisibilidade e a teoria das congruências modulares permitindo uma ligação entre a teoria e a prática.

A utilização dessas aplicações também configura a possibilidade de criação ou de reavaliação de sequências didáticas no ensino fundamental, reforçando a ligação entre as unidades temáticas Números e Álgebra. Além disso, essas aplicações configuram uma fonte de pesquisa para professores do ensino básico e para alunos do ensino superior que desejarem estabelecer uma relação entre estes conteúdos nestes ciclos de ensino. As relações oferecidas nas aplicações propostas nesse estudo têm como limites a relação entre os aspectos aritméticos e algébricos, porém isso pode ser transposto em futuros trabalhos sejam eles dentro desses campos ou com a inserção da unidade Geometria.

O presente trabalho também pode ser explorado como ponto de partida para outras dificuldades apresentadas pelos alunos do ensino médio, mas que na verdade tem sua origem no ensino fundamental como por exemplo as equações do 2º grau. O que permitiria mais uma vez a ligação entre o eixo Números e Álgebra, agora com o uso de congruências quadráticas, podendo chegar até as criptografias. Assim, teríamos outra oportunidade de enriquecer com mais exemplos os conteúdos da pós-graduação.

Ao concluir está pesquisa podemos observar que as nossas expectativas foram atendidas e superadas, pois contávamos em estabelecer três ou no máximo quatro relações entre os critérios de divisibilidade e as congruências modulares, ao final conseguimos evidenciar mais que o dobro do esperado, reforçando assim a relevância da pesquisa e dos resultados obtidos.

Referências

[1] AABOE, A. **Episódios da História Antiga da Matemática**. Rio de Janeiro, 3º Edição. SBM, 2013.

[2] AMARAL, L.F.C. **Divisibilidade por 7: Um novo método?** Revista do Professor de Matemática. Rio de Janeiro, SBM, 2020. Edição 101.

[3] BARBOSA, R.; FEITOSA, S. **OBMEP – Banco de Questões 2017**. Rio de Janeiro: IMPA, 2017.

[4] **BRASIL**. Parâmetros Curriculares Nacionais: Matemática. Brasília: MEC/SEF, 1998. P. 90-148.

[5] **BRASIL.** Base Nacional Comum Curricular. Brasília: MEC, 2017. Disponível em: https://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf. Acesso em: 03/10/2021.

[6] BRUXELAS, A. C. **Aritmética modular e aplicações: criptografia RSA e calendário perpétuo**. Dissertação (Mestrado/PROFMAT) - Apresentada como dissertação de Mestrado, Universidade de São Paulo, São Carlos. Disponível em: https://www.teses.usp.br/teses/disponiveis/55/55136/tde-22012021-113841/publico/AnaCatarinaBruxelas_revisada.pdf. Acesso em 06/10/2021.

[7] CARVALHO, P. C. P; MORGADO, A. C. **Matemática-Discreta.** Coleção PROFMAT. Rio de Janeiro, 2º Edição, SBM, 2013.

[8] D´AMBROSIO, U. **A Matemática ao longo da história: novas direções impulsionadas pelas guerras**. In: VIII Seminário Nacional de História da Matemática, 2009, *Atas do VIII Seminário Nacional de História da Matemática*. Belém: Universidade da Amazônia, 2009. Disponível em: http://ubiratan.mat.br/publicacoes/2009.html. Acesso em: 22/09/2021

[9] DUVAL, Raymond. Registros de representações semióticas e funcionamento cognitivo da compreensão em matemática. p.11-33. In MACHADO, Silvia Dias Alcântara (org). **Aprendizagem em Matemática**: Registros de representação semiótica. Campinas, SP: Papirus, 2003.

[10] GIL, K. H. **Reflexões sobre as dificuldades dos alunos na aprendizagem de álgebra**. Dissertação (Mestrado) – Originalmente apresentada como dissertação de Mestrado, Pontifícia Católica do Rio Grande do Sul – Faculdade de Física, Porto Alegre, 2008.118f. Disponível em: http://repositorio.pucrs.br/dspace/bitstream/10923/2962/1/000401324-Texto%2BCompleto-0.pdf. Acesso em: 04/10/2021.

[11] HARARI, Y. N. **Sapiens: Uma história da Humanidade.** São Paulo, 1º Edição. Companhia das Letras 2020.

[12] HEFEZ, A. **Aritmética**: Coleção PROFMAT. Rio de Janeiro: SBM, 2016.

[13] LACERDA, J. C. A. **Praticando a Aritmética**. Rio de Janeiro, 8º Edição. Editora XYZ, 2014.

[14] LIMA. E. L. **Zero é um número natural?** Revista do Professor de Matemática, Rio de Janeiro. SBM 1982. Edição 1. Disponível em: https://www.rpm.org.br/cdrpm/1/2.htm. Acesso em 13/09/2021.

[15] LINS, R. C.; GIMENEZ, J. **Perspectivas em Aritmética e Álgebra para o século XXI**. 6. ed. Campinas-SP: Papirus, 1997.

[16] MOURA. R. N. **Congruências Modulares e Algumas Aplicações para Educação Básica**. Dissertação (Mestrado/ PROFMAT) - Originalmente apresentada como dissertação de Mestrado, Centro de Ciências e Tecnologia. Fortaleza - CE. 2015

[17] MUNIZ NETO, A. C. **Tópicos da Matemática Elementar, volume 5: Teoria dos Números**. Rio de Janeiro, 2º Edição. SBM, 2013.

[18] PEREIRA DE SÁ, I. **A aritmética modular e suas aplicações no cotidiano.** Disponível em: www.magiadamatematica.com. Acesso em: 28/09/2021

[19] RODRIGUES, J. M. **Criptografia e conteúdos de matemática no ensino fundamental.** Dissertação (Mestrado/ PROFMAT) - Originalmente apresentada como dissertação de Mestrado – Centro de Ciências Exatas e de Tecnologia – Departamento de Matemática. São Carlos. 2013.

[20] ROQUE, T; PITOMBEIRA, J. B. **Tópicos da História da Matemática**. Coleção PROFMAT. Rio de Janeiro, 2º Edição, SBM, 2013.

[21] SILVA, A. C. **As equações diofantinas lineares no currículo da educação básica**. Dissertação (Mestrado/ PROFMAT) – Originalmente apresentada como dissertação de Mestrado, Universidade Estadual de Ponta Grossa – Paraná, Ponta Grossa, 2019.