CENTRO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL - PROFMAT

KÁTIA APARECIDA DA CRUZ

Investigação Matemática em Problemas de Aritmética

Maringá

2018

KÁTIA APARECIDA DA CRUZ

Investigação Matemática em Problemas de Aritmética

Trabalho de Conclusão de Curso apresentado ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como requisito parcial para obtenção do título de Mestre em Matemática.
Área de concentração: Matemática.

Orientador: Prof. Dr. Eduardo de Amorim Neves

Maringá

2018

Dados Internacionais de Catalogação na Publicação (CIP)
(Biblioteca Setorial BSE-DMA-UEM, Maringá, PR, Brasil)

Cruz, Kátia Aparecida da
C957i Investigação matemática em problemas de aritmética / Kátia Aparecida da Cruz. -- Maringá, 2018.
77 f. : il., color.

Orientador: Prof. Dr. Eduardo de Amorim Neves.
Dissertação (mestrado) - Universidade Estadual de Maringá, Centro de Ciências Exatas, Departamento de Matemática, 2018.

1. Investigação matemática. 2. Teoria dos números. 3. Olímpiada de Matemática - Brasil - Problemas. 4. Mathematical research. 5. Number theory. 6. Mathematical Olympics' Problems. I. Neves, Eduardo de Amorim, orient. II. Universidade Estadual de Maringá. Centro de Ciências Exatas. Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT. III. Título.

CDD 22.ed. 513

Edilson Damasio CRB9-1.123

KÁTIA APARECIDA DA CRUZ

INVESTIGAÇÃO MATEMÁTICA EM PROBLEMAS DE ARITMÉTICA

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática tendo a Comissão Julgadora composta pelos membros:

COMISSÃO JULGADORA:

Prof. Dr. Eduardo de Amorim Neves
DMA/Universidade Estadual de Maringá (Orientador)

Prof. Dr. Valter Soares de Camargo
Universidade Estadual do Paraná - Paranavaí

Prof. Dr. Thiago Fanelli Ferraiol
DMA/Universidade Estadual de Maringá

Aprovada em: 29 de junho de 2018.
Local de defesa: Auditório do DMA, Bloco F67, campus da Universidade Estadual de Maringá.

"*O estilo dedutivista, fundamentado nos axiomas, teoremas e provas, oculta a luta, esconde a aventura. Toda a história evapora, as sucessivas formulações provisórias do teorema durante a prova são relegadas ao esquecimento enquanto o resultado final é exaltado como infalibilidade sagrada* "

Imre Lakatos

Resumo

O presente trabalho tem como objetivo apresentar a metodologia e teoria da investigação matemática utilizando, para isso, problemas de aritmética retirados da Olimpíada Brasileira de Matemática das Escolas Públicas. Dessa forma, indicaremos suas características e etapas de modo a proporcionar a sua compreensão e importância no ensino de matemática. Além disso, abordaremos alguns conceitos básicos da teoria dos números afim de contribuir para o entendimento da fundamentação teórica utilizada como base para a realização das atividades investigativas.

Palavras-chave: Investigação Matemática; Teoria dos Números; Problemas de Olimpíada de Matemática.

Abstract

This work aims to present mathematical research methodology and theory by using arithmetic problems withdrawn from Public Schools' Brazilian Mathematical Olympics. Therefore, it will demonstrate its characteristics and phases in order to provide its comprehension and importance in mathematics teaching. Furthermore it will approach some basic concepts of number theory to add to the understanding of theoretical foundation used as base to the conducting research activities.

Key-words: Mathematical Research; Number Theory; Mathematical Olympics' Problems.

AGRADECIMENTOS

Agradeço a Deus pela benção da vida, por me iluminar e fortalecer nos momentos mais difíceis.

Aos meus pais e minhas irmãs por sempre apoiarem as minhas decisões e me incentivarem a alcançar os meus objetivos.

Aos professores do programa PROFMAT da Universidade Estadual de Maringá pela contribuição na minha formação acadêmica.

Aos meus colegas de turma pelo apoio e ajuda no decorrer destes dois anos.

Às minhas amigas Erica e Luana pelo apoio, ajuda e companheirismo nessa jornada.

Ao CAPES pelo auxílio financeiro nesses dois anos.

Ao meu orientador Eduardo de Amorim Neves que disponibilizou tempo, dedicação e atenção me conduzindo ao cumprimento desse trabalho.

SUMÁRIO

INTRODUÇÃO

A matemática, geralmente é abordada nas escolas com uma visão tradicional, como se esta fosse pronta e acabada. No entanto, alguns autores sugerem a importância de apresentarmos aos estudantes a matemática como uma atividade humana e falível, na qual os teoremas podem ser refutados e reformulados.

Esta situação nos leva a refletir que para inserirmos essa outra visão precisa-se de metodologias adequadas que permitam alcançarmos esse objetivo ao mesmo tempo que contribuam no processo de ensino e aprendizagem. Diante desse contexto destaca-se o papel da investigação matemática no ensino e a importância de compreendê-la.

Dessa forma, o presente trabalho justifica-se pela relevância desse estudo, para que a investigação matemática conceda ao aluno a oportunidade de olhar a matemática com um caráter no qual ele pode agir como matemático, ou seja, para que ele consiga compreender como ocorre o processo de criação da matemática. Nesse sentido é necessário que essa metodologia seja aplicada na sala de aula de forma adequada.

Assim, temos com este trabalho o intuito de mostrar a importância da investigação matemática, as suas características, as etapas necessárias no decorrer de sua aplicação, o papel do professor e, para isso, vamos utilizar problemas de aritmética para ilustrar na prática como podemos proceder.

Para alcançar os objetivos citados acima, realizamos pesquisas bibliográficas, visto que elas nos proporcionam a oportunidade de entender a investigação matemática e sua relevância, bem como alguns conceitos básicos da teoria dos números.

O trabalho está dividido da seguinte maneira:

O capítulo 1 está dividido em duas seções. Na primeira apresentamos uma aplicação da investigação matemática em um problema de aritmética, com base no modelo simplificado de Lakatos para a heurística da descoberta matemática. Na segunda seção abordamos as ideias de alguns autores que destacam a importância de considerarmos a matemática como uma atividade humana e falível, a definição de investigação matemática, suas características e suas etapas, isso baseado principalmente em J. P. Ponte; J. Brocardo; H. Oliveira [18], J. Brocardo [3] e M. Lamonato; C. L. B. Passos [14] e finalizamos apontando a visão de Lakatos sobre o conhecimento matemático, enfatizando sua semelhança com a investigação matemática fundamentando-se, principalmente, em P. J. Davis; R. Hersh [5] e I. Lakatos [13].

No capítulo 2 abordamos alguns conceitos básicos da teoria dos números, sendo estes os que foram necessários para realização do capítulo 3, para isso utilizamos na pesquisa, principalmente, as referências A. C. Muniz Neto [16], A. Hefez [11], J. P. Santos [20] e F. C. Milies; S. P. Coelho [15].

No capítulo 3, apresentamos algumas Atividades Investigativas baseadas em problemas de aritmética retirados da Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP). Essas atividades são retratadas, propositalmente, em uma linguagem informal, quase como um relato ou descrição de um diálogo, com o intuito de descrever o mais próximo possível como desenvolveu-se o pensamento no decorrer da realização da investigação.

CAPÍTULO 1

A METODOLOGIA E TEORIA DA INVESTIGAÇÃO MATEMÁTICA

Neste capítulo apresentamos como a investigação matemática é definida de acordo com alguns autores, suas características e sua relevância para o ensino de Matemática. Além disso, faremos uma aplicação da investigação matemática baseado no modelo de Lakatos.

1.1 Aplicação da Investigação Matemática

Iniciaremos a apresentação da investigação matemática através de um exemplo, seguindo o modelo simplificado de Lakatos para a heurística da descoberta matemática, baseado em Davis e Hersh, o qual veremos com mais detalhe na subseção 1.2.1 . Temos, com isso, o intuito de familiarizar o leitor com o processo de desenvolvimento da investigação matemática.

Para exemplificarmos como funciona esse modelo, utilizaremos um exercício proposto na Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP) no ano de 2017 para o nível 2, ou seja, para estudantes do oitavo e nono ano do ensino fundamental II. No entanto, ele será adaptado de maneira a não deixar explícito o que o exercício questionava, começa aqui a diferença entre trabalhar com resolução de problemas na qual há uma pergunta pré estabelecida enquanto na investigação não há perguntas a priori, mas sim alguma dinâmica. O enunciado original da questão que iremos investigar é o seguinte:

Júlia faz o seguinte cálculo com números inteiros positivos: ela escolhe um número, eleva esse número ao cubo e subtrai desse cubo o próprio número. Veja na figura que o resultado do cálculo de Júlia com o número 2 *é igual a* 6*.*

a) *Qual é o resultado do cálculo de Júlia com o número* 3*?*

b) *Qual é o número que deve ser escolhido por Júlia para que o resultado do cálculo seja* 1320*?*

c) *Explique por que, para qualquer número que Júlia escolher, o resultado final do cálculo será sempre um múltiplo de* 6*.*[*]

Agora para trabalharmos com a investigação vamos retirar as perguntas e deixar apenas a dinâmica, da seguinte maneira:

Exemplo 1.1 *Júlia faz o seguinte cálculo com números inteiros positivos: ela escolhe um número, eleva esse número ao cubo e subtrai desse cubo o próprio número. Veja na figura que o resultado do cálculo de Júlia com o número* 2 *é igual a* 6*.*

Antes de iniciarmos a investigação é importante ressaltarmos que ela será realizada com bases nas nossas experiências pessoais, sendo assim é possível que o leitor encontre outras ideias que possam ser desenvolvidas a partir desse mesmo enunciado. Além disso, seguiremos o modelo simplificado de Lakatos, nesse sentido, destacaremos as etapas da investigação como exemplos, contra-exemplos, tentativa

[*] Questão 3, nível 2, 2ª fase, ano 2017

de teorema, comentário, conjectura, reformulação, refutação, observação e demonstração.

Comentário: Inicialmente vamos fazer alguns testes com a proposta da dinâmica.

Exemplos:

$$\begin{aligned} 3^3 - 3 &= 27 - 3 = 24 \\ 4^3 - 4 &= 64 - 4 = 60 \\ 5^3 - 5 &= 125 - 5 = 120 \\ 6^3 - 6 &= 216 - 6 = 210 \end{aligned}$$

Observação: Nesses casos nota-se que os resultados são sempre divisíveis por 3.

Demonstração: Seja a um número inteiro positivo, temos que

$$a^3 - a = a(a^2 - 1) = a(a+1)(a-1)$$

Dessa forma, como $(a-1)$, a e $(a+1)$ são números consecutivos, segue que ao menos um desses números é múltiplo de 3, logo o produto deles é múltiplo de 3. Portanto, $a^3 - a$ é divisível por 3.

Comentário: Também é possível alterar o valor do expoente por outros números como, por exemplo, o número 2. Podemos ser ousados sem nos preocuparmos se estamos corretos, como diz Davis e Hersh (1995) "o céu não cairá se for falsa".

Exemplos:

$$\begin{aligned} 2^2 - 2 &= 4 - 2 = 2 \\ 3^2 - 3 &= 9 - 3 = 6 \\ 4^2 - 4 &= 16 - 4 = 12 \\ 5^2 - 5 &= 25 - 5 = 20 \\ 6^2 - 6 &= 36 - 6 = 30 \end{aligned}$$

Observação: Percebemos que esses resultados são sempre divisíveis por 2.

Tentativa de Teorema: Se um número inteiro positivo a for elevado ao número n e subtrairmos o número a, então o resultado será divisível por n.

Contra-exemplo: Se o expoente for o número 4 e a base for o número 2, temos $2^4 - 2 = 16 - 2 = 14$. Mas 14 não é divisível por 4.

Ponto de ordem: No entanto, apesar de não ter sido válido para todo número n, ainda podemos trocar o expoente por outros valores.

Exemplos: Utilizando o número 5 como expoente, temos:

$$\begin{aligned} 2^5 - 2 &= 32 - 2 = 30 \\ 3^5 - 3 &= 243 - 3 = 240 \\ 4^5 - 4 &= 1024 - 4 = 1020 \\ 6^5 - 6 &= 7776 - 6 = 7770 \end{aligned}$$

Observação: Nesses, todos os resultados são divisíveis por 5, então para o expoente igual a 5 a conjectura parece ser válida.

Exemplos: Escolhendo o número 6 para o expoente, temos:

$$\begin{aligned} 2^6 - 2 &= 64 - 2 = 62 \\ 3^6 - 3 &= 729 - 3 = 726 \\ 4^6 - 4 &= 4096 - 4 = 4092 \\ 5^6 - 5 &= 15625 - 5 = 15620 \end{aligned}$$

Observação: Analisando esses resultados, percebe-se que eles não são divisíveis por 6, mas são divisíveis por 2.

Comentário: Podemos também utilizar o número 7 como expoente.

Exemplos:

$$\begin{aligned} 2^7 - 2 &= 128 - 2 = 126 \\ 3^7 - 3 &= 2187 - 3 = 2184 \\ 4^7 - 4 &= 16384 - 4 = 16380 \\ 5^7 - 5 &= 78125 - 5 = 78120 \end{aligned}$$

Observação: Notamos que esses resultados são divisíveis por 7.

Demonstração: Seja a um número inteiro positivo, vamos mostrar que existe $c \in \mathbb{Z}$ tal que $a^7 - a = 7c$. Neste caso, temos que a pode ser escrito como:

$$7k, 7k+1, 7k+2, 7k+3, 7k+4, 7k+5, 7k+6$$

onde $k \in \mathbb{N}$.

Note que:

$$a^7 - a = a(a-1)(a^2+a+1)(a+1)(a^2-a+1).$$

Assim, temos sete casos a considerar:

1. Se $a = 7k$, com $k \in \mathbb{N}$.

$$\begin{aligned} a^7 - a &= 7\underbrace{k \cdot (7k-1) \cdot [(7k)^2 + 7k + 1] \cdot (7k+1) \cdot [(7k)^2 - 7k + 1]}_{\text{c}} \\ &= 7c \end{aligned}$$

2. Se $a = 7k+1$, $k \in \mathbb{N}$.

$$\begin{aligned} a^7 - a &= (7k+1) \cdot (7k+1-1) \cdot [(7k+1)^2 + (7k+1) + 1] \cdot \\ &\quad \cdot (7k+1+1) \cdot [(7k+1)^2 - (7k+1) + 1] \\ &= 7\underbrace{k \cdot (7k+1) \cdot [(7k+1)^2 + 7k + 2] \cdot (7k+2) \cdot [(7k+1)^2 - 7k]}_{\text{c}} \\ &= 7c \end{aligned}$$

3. Se $a = 7k+2$, com $k \in \mathbb{N}$.

$$\begin{aligned} a^7 - a &= (7k+2) \cdot (7k+2-1) \cdot [(7k+2)^2 + (7k+2) + 1] \cdot \\ &\quad \cdot (7k+2+1) \cdot [(7k+2)^2 - (7k+2) + 1] \\ &= (7k+2) \cdot (7k+1) \cdot (49k^2 + 35k + 7) \cdot (7k+3) \cdot [(7k+2)^2 - 7k - 1] \\ &= 7\underbrace{(7k+2) \cdot (7k+1) \cdot (7k^2 + 5k + 1) \cdot (7k+3) \cdot [(7k+2)^2 - 7k - 1]}_{\text{c}} \\ &= 7c \end{aligned}$$

4. Se $a = 7k+3$, $k \in \mathbb{N}$.

$$\begin{aligned} a^7 - a &= (7k+3) \cdot (7k+3-1) \cdot [(7k+3)^2 + (7k+3) + 1] \cdot \\ &\quad \cdot (7k+3+1) \cdot [(7k+3)^2 - (7k+3) + 1] \\ &= (7k+3) \cdot (7k+2) \cdot [(7k+3)^2 + 7k + 4] \cdot (7k+4) \cdot (49k^2 + 35k + 7) \\ &= 7\underbrace{(7k+3) \cdot (7k+2) \cdot [(7k+3)^2 + 7k + 4] \cdot (7k+4) \cdot (7k^2 + 5k + 1)}_{\text{c}} \\ &= 7c \end{aligned}$$

5. Se $a = 7k + 4$, $k \in \mathbb{N}$.

$$\begin{aligned}
a^7 - a &= (7k+4)\cdot(7k+4-1)\cdot[(7k+4)^2+(7k+4)+1]\cdot\\
&\quad \cdot(7k+4+1)\cdot[(7k+4)^2-(7k+4)+1]\\
&= (7k+4)\cdot(7k+3)\cdot(49k^2+63k+21)\cdot(7k+5)\cdot[(7k+4)^2-7k-3]\\
&= 7\underbrace{(7k+4)\cdot(7k+3)\cdot(7k^2+9k+3)\cdot(7k+5)\cdot[(7k+4)^2-7k-3]}_{\text{c}}\\
&= 7c
\end{aligned}$$

6. Se $a = 7k + 5$, $k \in \mathbb{N}$.

$$\begin{aligned}
a^7 - a &= (7k+5)\cdot(7k+5-1)\cdot[(7k+5)^2+(7k+5)+1]\cdot\\
&\quad \cdot(7k+5+1)\cdot[(7k+5)^2-(7k+5)+1]\\
&= (7k+5)\cdot(7k+4)\cdot[(7k+5)^2+7k+6]\cdot(7k+6)\cdot(49k^2+63k+21)\\
&= 7\underbrace{(7k+5)\cdot(7k+4)\cdot[(7k+5)^2+7k+6]\cdot(7k+6)\cdot(7k^2+9k+3)}_{\text{c}}\\
&= 7c
\end{aligned}$$

7. Se $a = 7k + 6$, $k \in \mathbb{N}$.

$$\begin{aligned}
a^7 - a &= (7k+6)\cdot(7k+6-1)\cdot[(7k+6)^2+(7k+6)+1]\cdot\\
&\quad \cdot(7k+6+1)\cdot[(7k+6)^2-(7k+6)+1]\\
&= 7\underbrace{(7k+6)\cdot(7k+5)\cdot[(7k+6)^2+7k+7](k+1)\cdot[(7k+6)^2-7k-5]}_{\text{c}}\\
&= 7c
\end{aligned}$$

Como em todos os casos $a^7 - a = 7c$, logo, $a^7 - 7$ é divisível por 7.

Comentário: É possível escolhermos para o expoente o número 8.

Exemplos:

$$\begin{aligned}
2^8 - 2 &= 256 - 2 = 254\\
3^8 - 3 &= 6561 - 3 = 6558\\
4^8 - 4 &= 65536 - 4 = 65536\\
5^8 - 5 &= 390625 - 5 = 390620
\end{aligned}$$

Observação: Nesse caso, os resultados não são divisíveis por 8, mas são divisíveis por 2.

Comentário: Vamos utilizar o número 9 como expoente.

Exemplos:

$$\begin{aligned} 2^9 - 2 &= 512 - 2 = 510 \\ 3^9 - 3 &= 19683 - 3 = 19680 \\ 4^9 - 4 &= 262144 - 4 = 2621440 \\ 5^9 - 5 &= 1953125 - 5 = 1953120 \end{aligned}$$

Observação: Notamos que os resultados encontrados não são divisíveis por 9, mas são divisíveis por 2. Neste último caso, percebemos que a conjectura parece ser válida somente quando o expoente for um número primo, o que nos leva a seguinte reformulação.

Reformulação: Se um número inteiro positivo a for elevado ao número primo p e subtrairmos o número a, então o resultado será divisível por p.

Neste momento, consideramos importante destacar que todo o processo acima nos levou a essa última reformulação da conjectura, que é o famoso Pequeno Teorema de Fermat (Teorema 2.46), ressaltamos ainda que como dizem Davis e Hersh (1995), a partir de "sementes" simples, ou seja, de enunciados simples, damos a oportunidade ao aluno de participar do processo da criação da matemática.

Mas, ainda é possível continuar a nossa investigação, afinal o que acontece se o expoente não for um número primo?

Observação: Com os exemplos realizados anteriormente notamos que quando o expoente não for um número primo os resultados serão divisíveis por 2.

Nova Conjectura: Se um número inteiro positivo a for elevado ao número n, sendo que n não é um número primo, e subtrairmos a, então o resultado será divisível por 2.

Refutação: Para todo expoente os resultados serão divisíveis por 2.

Reformulação: Se um número inteiro positivo a for elevado ao número n e subtrairmos a, então o resultado será divisível por 2.

Demonstração: Devemos mostrar que $2|a^n - a$, ou seja, que $a^n - a = 2s$. Para isso vamos considerar dois casos:

1° caso - Se a é um número da forma $2q$, temos:

$$(2q)^n - 2q = 2^n q^n - 2q = 2(2^{n-1} \cdot q^n - q)$$

Logo, $a^n - a$ é divisível por 2.

2° caso - Se a é um número da forma $2q+1$, segue que:

$$(2q+1)^n - (2q+1) = (2q+1)[(2q+1)^{n-1} - 1].$$

Como a é ímpar então a^n também é ímpar, logo $[(2q+1)^{n-1} - 1]$ é par e consequentemente $(2q+1)[(2q+1)^{n-1} - 1]$ também é par.

Portanto, $a^n - a$ é divisível por 2.

Esse exemplo nos permite perceber que a investigação matemática propicia ao aluno a participação no processo da criação da matemática. Além disso, podemos observar a relevância das refutações e reformulações durante o processo enfatizando ao mesmo tempo a contribuição do modelo simplificado de Lakatos.

Assim, para que possamos compreender melhor a teoria da investigação matemática apresentamos na próxima seção um pouco da sua fundamentação teórica.

1.2 A Investigação Matemática

A matemática geralmente é tratada como uma ciência pronta e acabada. De acordo com Ponte, Brocardo e Oliveira (2005) essa ciência é vista, usualmente, como um corpo de conhecimentos organizado de forma lógica e dedutiva, como um edifício sólido, paradigma do rigor e das certezas absolutas.

Nesse contexto, a investigação matemática vem a contrastar essa perspectiva, visto que propõe um processo no qual ocorra a criação matemática. Segundo Polya:

> A matemática tem dois aspectos: é a rigorosa ciência de Euclides, mas é também uma outra coisa. A matemática apresentada da maneira euclidiana, revela-se uma ciência dedutiva, sistemática, mas a Matemática em desenvolvimento apresenta-se como uma ciência indutiva, experimental. Ambos os aspectos são tão antigos quanto a própria ciência (POLYA, 2005, p. vi).

Ainda sobre essa visão da matemática, Lamonato e Passos dizem que

> A matemática vista como uma disciplina que se encerra em si mesma, que já está pronta e que deve ser aprendida, desqualifica-a enquanto ciência e campo de conhecimento e pesquisa, outorgando apenas a alguns o poder de conhecê-la e estudá-la. Dessa maneira, estaríamos reduzindo a Matemática, incluindo seu processo de construção, a uma Matemática estática, presente no currículo escolar, ainda entendendo este como rol de conteúdos.
>
> Por outro lado, necessitamos entender, compreender e tratar a Matemática como um processo, como uma ciência, de fato, que tem caráter de investigação, que é um conhecimento historicamente em construção e não somente construído (LAMONATO; PASSOS, 2011, p. 57).

Assim, a investigação matemática se torna uma metodologia que contribui para que essa visão da matemática seja apresentada aos estudantes.

Nesse sentido, Brocardo traz que

> [...] a visão da Matemática como um corpo de conhecimentos é incompleta. A Matemática é também uma actividade humana, uma construção social que, em última análise, é falível. Assim, é importante que a actividade matemática dos alunos consista essencialmente em experenciar um tipo de trabalho como o dos matemáticos profissionais. Neste, a investigação é uma actividade central e o ensino da Matemática deve dar relevância à realização de actividades de investigação por parte dos alunos (BROCARDO, 2001, p. 92).

Diante dessa visão da matemática, torna-se importante compreendermos o que representa a investigação matemática para o ensino e como esta acontece de fato. Segundo Ponte, Brocardo e Oliveira (2005, p. 13) "para os matemáticos profissionais, investigar é descobrir relações entre objetos matemáticos conhecidos ou desconhecidos, procurando identificar as respectivas propriedades".

Sobre o significado de investigar, Lamonato e Passos (2001, p. 62) consideram que "investigar é procurar o que ainda não se conhece; investigar é questionar e procurar responder. Para investigar, é necessário querer saber; para investigar, é preciso estar curioso".

A importância da investigação matemática no ensino é enfatizado por Braumann quando este diz que

> Aprender Matemática não é simplesmente compreender a Matemática já feita, mas ser capaz de fazer investigação de natureza matemática (ao nível adequado a cada grau de ensino). Só assim se pode verdadeiramente perceber o que é a Matemática e a sua utilidade na compreensão do mundo e na intervenção sobre o mundo. Só assim se pode realmente dominar os conhecimentos adquiridos. Só assim se pode ser inundado pela paixão "detectivesca" indispensável à verdadeira fruição da Matemática. Aprender Matemática sem forte intervenção da sua faceta investigativa é como tentar aprender a andar de bicicleta vendo os outros andar e recebendo informação sobre como o conseguem. Isso não chega. Para verdadeiramente aprender é preciso montar a bicicleta e andar, fazendo erros e aprendendo com eles (BRAUMANN, 2002, p. 5).

Para Ponte, Brocardo e Oliveira (2005) uma investigação matemática tem seu desenvolvimento baseado em um ou mais problemas, podendo assim considerar que o primeiro passo de uma investigação é identificar de forma clara o problema a resolver. Além disso, quando trabalhamos com um problema, o nosso intuito é resolvê-lo, porém além de resolver o problema proposto, é possível fazermos outras descobertas, que, em alguns casos, podem ser consideradas mais relevantes que a própria solução do problema original. Assim, a investigação matemática parece se apresentar muito próxima da resolução de problemas. Nesse sentido, Ponte, Brocardo e Oliveira explicam que

> Numa investigação, as coisas são um pouco diferentes. Trata-se de situações mais abertas - a questão não está bem definida no início, cabendo a quem investiga um papel fundamental na sua definição. E uma vez que os pontos de partida podem não ser exatamente

> os mesmos, os pontos de chegada podem ser também diferentes (PONTE; BROCARDO; OLIVEIRA, 2005, p. 23).

De acordo com Brocardo (2001) em uma investigação matemática o contexto representa uma situação que direciona a um objetivo que é escolhido como compondo o resultado da exploração dessa situação. Assim, o aluno apresenta um papel de suma importância, pois este deve optar sobre o modo de explorar a situação.

A investigação de matemática segundo Ponte, Brocardo e Oliveira envolve quatro momentos principais:

> O primeiro abrange o reconhecimento da situação, a sua exploração preliminar e a formulação de questões. O segundo momento refere-se ao processo de formulação de conjecturas. O terceiro inclui a realização de testes e o eventual refinamento das conjecturas. E, finalmente, o último diz respeito à argumentação, à demonstração e avaliação do trabalho realizado (PONTE; BROCARDO; OLIVEIRA, 2005, p. 20).

Estes momentos podem acontecer simultaneamente, por exemplo, ao mesmo tempo que surgir uma conjectura podem ser formuladas questões. Além disso, esses momentos podem envolver diversas atividades. Segundo Lamonato e Passos,

> A primeira etapa - a exploração e a formulação de questões - constitui os momentos iniciais da atividade, em que os alunos observam ou recolhem dados, buscam diferenças, semelhanças, regularidades e põem questões que buscarão desvendar. Posteriormente, a formulação de conjecturas consiste num processo de elaboração de hipóteses para suas questões, explicações que serão testadas e reformuladas, utilizando-se de exemplos e contraexemplos, caminhando, assim, para a justificação das conjecturas, com o uso de argumentações, provas ou demonstrações. E, finalmente, a avaliação do trabalho prevê a discussão, a argumentação, a socialização e o debate, processos estes nem sempre lineares, mas que abarcaram a negociação de significados em diversos momentos (LAMONATO; PASSOS, 2011, p. 64).

Conforme Ponte, Brocardo e Oliveira (2005), a aplicação da investigação matemática em uma aula (ou conjunto de aulas) se desenvolve em três fases: introdução da tarefa, realização da investigação e discussão dos resultados. Na primeira fase, o professor faz a proposta à turma, sendo esta oralmente ou por escrito. Esta fase é de suma importância para o desenvolvimento do trabalho, assim o professor precisa levar os alunos a compreenderem a tarefa proposta e o que se espera deles no decorrer da atividade. A segunda fase pode ser desenvolvida individualmente, em pares, em pequenos grupos ou com toda a turma. É nessa fase que ocorrem a exploração e formulação de questões, a elaboração de conjecturas, o teste e reformulação de conjecturas, a justificação de conjecturas e a avaliação, sendo assim torna-se importante o professor estar atento a todo o trabalho realizado pelos alunos prestando o apoio que for necessário. Na terceira fase é o momento em que se realiza uma discussão acerca do que foi realizado no decorrer do trabalho. Dessa forma, os alunos podem apresentar suas estratégias, conjecturas e justificações, sendo assim o professor assume o papel de moderador, garantindo que os resultados mais significativos sejam apresentados de modo a estimular o questionamento entre os estudantes.

Ainda sobre esta terceira fase Ponte, Brocardo e Oliveira enfatizam que

> A fase de discussão é, pois, fundamental para que os alunos, por um lado, ganhem um entendimento mais rico do que significa investigar e, por outro, desenvolvem a capacidade de comunicar matematicamente e de refletir sobre o seu trabalho e o seu poder de argumentação. Podemos mesmo afirmar que, sem a discussão final, se corre o risco de perder o sentido da investigação (PONTE; BROCARDO; OLIVEIRA, 2005, p. 41).

Na investigação matemática segundo Ponte, Brocardo e Oliveira (2005, p. 23) "o aluno é chamado a agir como um matemático, não só na formulação de questões e conjecturas e na realização de provas e refutações, mas também na apresentação de resultados e na discussão e argumentação com os seus colegas e o professor".

No entanto, para que a investigação matemática alcance o seu intuito, destaca-se que o professor apresenta um papel fundamental. Nesse processo o docente assume diversos papéis; de acordo com Ponte, Brocardo e Oliveira (2005, p. 47) o professor deve "desafiar os alunos, avaliar o seu progresso, raciocinar matematicamente e apoiar o trabalho deles".

Assim, ressalta-se que a investigação matemática, quando bem preparada por um professor e conduzida de forma adequada em sala de aula, pode trazer grande contribuição para o desenvolvimento matemático dos estudantes.

1.2.1 Modelo Simplificado de Lakatos

Imre Lakatos foi um filósofo que apresentava uma teoria sobre o descobrimento matemático que se assemelha a investigação matemática. De acordo com Silva e Moura,

> [...] Lakatos considerava a matemática tão falível quanto o conhecimento do mundo externo. O cerne de sua preocupação está no crescimento do conhecimento matemático, propriciado principalmente pelas conjecturas informais e provas heurísticas de teorias já formalizadas (SILVA; MOURA, 2015, p. 279).

Segundo Silva e Moura (2015), Lakatos considera melhor uma matemática que cresce e se desenvolve a partir de um problema e uma conjectura, do que uma matemática esqueletizada e fossilizada.

Essa visão de Lakatos (1978, p. 29) se enfatiza no trecho de seu livro *A lógica do descobrimento matemático: provas e refutações*, que descreve um diálogo entre um professor e seus alunos. "Você está interessado apenas em provas que "provem" o que pretendemos provar. Estou interessado em provas mesmo que elas não realizem a tarefa pretendida".

Assim, Silva e Moura (2015) dizem que tanto na obra de Lakatos como na metodologia da investigação matemática, a atividade matemática é de suma importância. Além disso, a visão da matemática como uma atividade humana e falível pode ser considerada uma característica central das duas teorias.

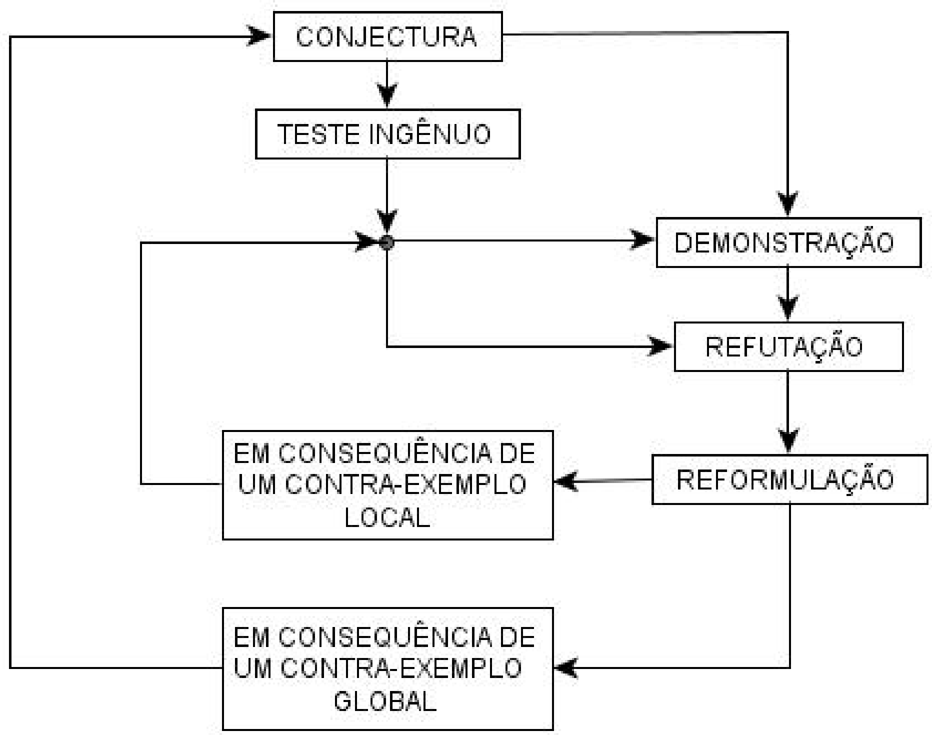
De acordo com Silva e Moura (2015), comparando as duas teorias, destaca-se que a grande diferença está no fato de Lakatos não apresentar preocupação pedagógica com a matemática e sim com a construção de novos conhecimentos matemáticos, enquanto que na investigação matemática a preocupação principal é o processo pedagógico.

Conforme Davis e Hersh (1995) o modelo heurístico de Lakatos de demonstrações e refutações, que se apresenta como uma forma para que ocorra o desenvolvimento do conhecimento matemático em geral, pode ser utilizado por um indivíduo com o intuito de criar nova matemática.

Dessa forma, acredita-se que esse processo possa ser aplicado em sala de aula por meio de questões abertas, nas quais os enunciados propiciem aos estudantes a oportunidade de desenvolverem novas matemáticas, vivenciando, assim, um pouco da realidade das atividades desenvolvidas pelos pesquisadores em matemática.

Apresentamos, a seguir, o esquema proposto por Davis e Hersh (1995) referente ao modelo de Lakatos.

Figura 1.1: Modelo Simplificado de Lakatos para a heurística da descoberta matemática



Fonte: Davis e Hersh (1995, p. 276).

Nesse modelo, são apresentadas as relações entre vários processos presentes no decorrer de uma atividade, sendo que segundo Lakatos (1978) contra-exemplo local é aquele que refuta um lema, sem precisamente refutar a conjectura principal, enquanto que o contra-exemplo global é aquele que refuta a própria conjectura principal.

A compreensão desse modelo fica mais clara relacionado-o com as três regras que Lakatos apresenta sobre o método de prova e refutações.

> Norma 1. Se tivermos uma conjectura, disponhamos-nos a comprová-la e a refutá-la. Inspecionemos a prova cuidadosamente para elaborar um rol de lemas não triviais (análise de prova); encontremos contra-exemplos tanto para a conjectura (contra-exemplos globais) como para os lemas suspeitos (contra-exemplos locais).
>
> Norma 2. Se tivermos um contra-exemplo global, desfaçamo-nos de nossa conjectura, acrescentemos à nossa análise de prova

> um lema apropriado que venha a ser refutado pelo contra-exemplo, e substituamos a nova conjectura desprezada por outra melhorada que incorpore o lema como uma condição. Não permitamos que uma refutação seja destituída como um monstro. Esforcemo-nos por tornar explícitos todos os “lemas implícitos”.
>
> Norma 3. Se tivermos um contra-exemplo local, confiramos para verificar se ele não é também contra-exemplo global. Se for, podemos facilmente aplicar a Regra 2 (LAKATOS, 1978, p. 73).

Dessa forma, quando compreendemos as regras apresentadas por Lakatos percebemos o quanto sua teoria se assemelha com a investigação matemática e, consequentemente, o quanto esta pode contribuir para que o aluno desenvolva uma nova matemática.

CAPÍTULO 2

CONCEITOS BÁSICOS DA TEORIA DOS NÚMEROS

Neste capítulo, apresentaremos alguns conceitos básicos da Teoria dos Números que serão utilizados no Capítulo 3. Neste sentido, destacamos que não pretendemos explorar todos os conceitos da Teoria dos Números, mas somente os resultados que foram necessários para a realização deste trabalho. No decorrer deste capítulo utilizamos as seguintes referências: A. C. Muniz Neto [16], A. Hefez [11], J. P. O. Santos [20] e F. C. P. Milies; S. P. Coelho [15]. Além disso, para os exemplos foram usadas as referências R. Ribeiro [19], C. W. A. Freitas [10], D. S. Bispo [1], E. Chagas [4], S. Feitosa [6], [7], [8] e D. Fomin; S. Genkin; I. Itenberg [9].

2.1 Divisibilidade

Nesta seção abordaremos a divisibilidade apresentando definições, teoremas, proposições, propriedades e alguns exemplos, com o intuito de destacarmos conceitos relevantes para as investigações matemáticas que serão apresentadas no capítulo 3.

Sabemos que a divisão de um número inteiro por outro nem sempre é possível, assim expressamos essa possibilidade por meio da relação de divisibilidade e, se essa relação não existir, será possível realizarmos uma "divisão com resto pequeno", denominada divisão euclidiana.

Assim, apresentamos inicialmente a definição de divisibilidade.

Definição 2.1 *Dados a e b números inteiros, com $a \neq 0$, diremos que a divide b e denotamos por $a|b$, se existir um inteiro c tal que $b = ca$.*

Neste caso, dizemos que a é um divisor ou fator de b, que b é divisível por a ou que b é um múltiplo de a.

No caso em que a não divide b escrevemos $a \nmid b$.

Exemplo 2.2 $6|42$, *pois existe um número inteiro* $c = 7$, *tal que* $42 = 6 \cdot 7$.

Exemplo 2.3 $4 \nmid 14$, *pois não existe um número inteiro* c, *tal que* $14 = 4 \cdot c$

Em relação a divisibilidade estabelece-se algumas propriedades.

Proposição 2.4 *Dados* $a, b, c \in \mathbb{Z}$. *Temos que:*
i) $1|a, a|a$ *e* $a|0$
ii) $0|a \Leftrightarrow a = 0$
iii) a divide b se, e somente se, $|a|$ *divide* $|b|$
iv) se $a|b$ *e* $b|c$, *então* $a|c$

Pelo fato de sempre ser possível efetuar a divisão de a por b com resto, apresentamos o teorema a seguir que é conhecido como algoritmo da divisão para números inteiros.

Teorema 2.5 *(Divisão Euclidiana) Sejam* a *e* b *números inteiros com* $b \neq 0$, *existem inteiros* q *e* r, *únicos, tais que:*

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

Os inteiros q e r são chamados, respectivamente, de quociente e de resto da divisão de a por b.

Demonstração: Suponha que $b > 0$ e considere q o maior inteiro tal que $bq \leq a$. Dessa forma, $bq \leq a < b(q+1)$, subtraindo bq em todos os membros da desigualdade segue que $0 \leq a - bq < b$ e definimos $r = a - bq$. Agora, suponha $b < 0$, então $-b > 0$, assim existem q, r inteiros tais que $a = (-b)q + r$, com $0 \leq r < -b$ e $a = b(-q) + r$, com $0 \leq r < -b = |b|$.

Para mostrar a unicidade, vamos supor que $a = bq + r = bq' + r'$, sendo q, q', r, $r' \in \mathbb{Z}$ e $0 \leq r, r' < |b|$. Dessa forma, segue que:

$$|r' - r| < |b|$$

e

$$b(q - q') = r' - r.$$

Agora, se $q \neq q'$, então $|q - q'| \geq 1$, logo

$$|b| \leq |b| \cdot |q - q'| = |r - r'| < |b|$$

o que é uma contradição. Portanto, $q = q'$, e consequentemente, $r = r'$. $\square$

Além disso, podemos destacar que o resto da divisão de a por b é igual a zero se, e somente se, b divide a. Mas ainda é importante ressaltar que na divisão desses números, com $a > 1$, a é divisível por b, ou deixa resto 1 ou 2 ou 3 ou $\cdots$ ou $b - 1$.

Exemplo 2.6 *Dados os números inteiros* 17 *e* 5*, temos que* $17 = 5 \times 3 + 2$*. Logo, na divisão de* 17 *por* 5 *o quociente e o resto, são respectivamente,* $q = 3$ *e* $r = 2$*.*

Exemplo 2.7 *(OBM 1ª fase) Uma professora tem* 237 *balas para dar a seus* 31 *alunos. Qual é o número mínimo de balas a mais que ela precisa conseguir para que todos os alunos recebam a mesma quantidade de balas, sem sobrar nenhuma para ela?*[†]

Solução: Vamos dividir 237 *por* 31*, assim obtemos quociente* $q = 7$ *e resto* $r = 20$*. Dessa forma, para que não sobre nenhuma bala para a professora é preciso que ela consiga uma quantidade de balas que somada ao resto* $r = 20$ *seja possível distribuir mais uma bala para cada aluno. Portanto, são necessárias mais* 11 *balas.*

Exemplo 2.8 *Mostre que de três números inteiros consecutivos um e apenas um é múltiplo de* 3*.*

Solução: Sejam os três números inteiros consecutivos representados por $a, a+1, a+2$*. Na divisão do número* a *por* 3 *existem três possibilidades para o resto, ou seja, o resto será igual a* 0*,* 1 *ou* 2*. Assim, analisando os três casos temos:*

1° *caso - Seja* $a = 3q$*, ou seja, a dividido por 3 deixa resto 0. Dessa forma, segue que* $a + 1 = 3q + 1$ *e* $a + 2 = 3q + 2$*. Logo, existe um e apenas um dos três números consecutivos que é múltiplo de 3.*

2° *caso - Seja* $a = 3q + 1$*, ou seja, a deixa resto 1 quando dividido por 3. Assim,* $a + 1 = 3q + 1 + 1 = 3q + 2$ *e* $a + 2 = 3q + 1 + 2 = 3q + 3 = 3(q + 1)$*. Portanto, somente um desses números é múltiplo de* 3*.*

[†]Questão 7, nível 1, 1ª fase, ano 2004

3° *caso - Seja* $a = 3q+2$, *ou seja, a divisão de a por 3 deixa resto 2. Desse modo,* $a+1 = 3q+2+1 = 3q+3 = 3(q+1)$ *e* $a+2 = 3q+2+2 = 3q+4 = 3(q+1)+1$. *Logo, um e apenas um desses números é múltiplo de* 3.

A partir da unicidade do quociente e do resto na divisão euclidiana é possível definir duas funções importantes.

Definição 2.9

1. *Escrevendo por* $q_b(a)$ *o quociente da divisão do número a por b, a função quociente por b é definida como:*

$$\begin{aligned} q_b \quad : \quad & \mathbb{Z} \to \mathbb{Z} \\ & a \mapsto q_b(a) \end{aligned}$$

2. *Denotando* $r_b(a)$ *como resto da divisão de a por b, definimos a função resto como:*

$$\begin{aligned} r_b \quad : \quad & \mathbb{Z} \to \mathbb{Z} \\ & a \mapsto r_b(a) \end{aligned}$$

Exemplo 2.10 *Dado o número* 16 *podemos escrever* $16 = 3 \cdot 5 + 1$. *Logo, temos que* $q_5(16) = 3$ *e* $r_5(16) = 1$.

Em relação ao números inteiros, temos que estes podem ser classificados em números pares, quando são da forma $2q$ para algum $q \in \mathbb{Z}$ e em número ímpares, quando são da forma $2q + 1$.

2.2 Representação dos Números Inteiros

Ao longo desta seção vamos abordar alguns conceitos relacionados ao sistema decimal posicional que é adotado atualmente para representar os números inteiros.

Neste sistema, são utilizados apenas os dez símbolos

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9$$

chamados de algarismos, para representar todo número inteiro, por isso é chamado de *sistema decimal*. Além disso, cada algarismo apresenta um peso de acordo com a posição que ele ocupa no número, por isso esse é chamado *sistema posicional*.

Esse peso, sempre uma potência de dez, relacionado ao algarismo, varia da direita para a esquerda da seguinte forma: o algarismo da direita tem peso um; o seguinte tem peso dez; o seguinte possui peso cem, etc.

Contando da direita para a esquerda cada algarismo tem uma ordem e a cada terna de ordens, também da direita para a esquerda, forma-se uma classe.

Assim, um número a pode ser expresso como $r_n \cdots r_1 r_0$ que no sistema decimal representa o número

$$r_n 10^n + r_{n-1} 10^{n-1} + \cdots + r_1 10 + r_0.$$

Essa representação é baseada no seguinte teorema:

Teorema 2.11 *Dados os números inteiros a e b, com $a > 0$ e $b > 1$. Existem números inteiros $n \geq 0$ e $0 \leq r_0, r_1, \cdots, r_n < b$, com $r_n \neq 0$, univocamente determinados, tais que $a = r_0 + r_1 b + r_2 b^2 + \cdots + r_n b^n$.*

Demonstração: Ver A. Hefez [11]. □

Exemplo 2.12 *O número 5436, na base 10, representa*

$$5 \cdot 10^3 + 4 \cdot 10^2 + 3 \cdot 10 + 6.$$

É interessante destacarmos que essa representação na base 10 é essencial para as demonstrações dos critérios de divisibilidade.

2.3 Máximo Divisor Comum

Nesta seção apresentaremos a definição de máximo divisor comum e alguns resultados que podem ser significativos para as investigações matemáticas propostas no capítulo 3.

Dados os números inteiros a e b, dizemos que um número inteiro d é divisor comum de a e b se $d|a$ e $d|b$.

Em relação à definição de máximo divisor comum, temos que:

Definição 2.13 *Denomina-se máximo divisor comum de a e b o maior de seus divisores comuns.*

Note que o único caso que não exite o máximo divisor comum de a e b é quando ambos são nulos.

Além disso, podemos apresentar a definição dada por Euclides, que denota uma caracterização diferente para o máximo divisor comum.

Definição 2.14 *Um número inteiro $d \geq 0$ é dito um máximo divisor comum de a e b, denotado por $mdc(a, b)$ ou simplesmente (a, b), se possuir as seguintes propriedades:*
i) d é um divisor comum de a e b;
ii) d é divisível por todo divisor comum de a e b.

Observe que o máximo divisor comum não depende da ordem em que são considerados a e b, isto é, $(a, b) = (b, a)$. Além disso, se existir o (a, b), tem-se

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

Exemplo 2.15 *Determine o* $(15, 20)$.

Solução: Vamos determinar os divisores de 15 *que são:* $\pm 1, \pm 3, \pm 5, \pm 15$ *e os divisores de* 20 *que são:* $\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20$.

Tomando o maior divisor comum de 15 *e* 20*, temos que o* $(15, 20) = 5$.

Existem casos nos quais determinar o máximo divisor comum utilizando apenas a definição se torna inviável, como por exemplo $(6785, 18432)$, assim apresentamos um resultado abaixo que pode facilitar esse processo.

Lema 2.16 *(Lema de Euclides) Dados $a, b, n \in \mathbb{Z}$. Se existe $(a, b - na)$, então, (a, b) existe e*

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

Demonstração: Considere $d = (a, b - na)$. Como $d|a$ e $d|(b - na)$, temos d que divide $b = b - na + na$. Portanto, d é um divisor comum de a e b. Suponha que c é um divisor comum de a e b. Assim, c é um divisor comum de a e $(b - na)$, logo $c|d$. Dessa forma, prova-se que $d = (a, b)$. □

Exemplo 2.17 *Determine o* $(141, 255)$.

Solução: Utilizando o Lema de Euclides, com $a = 141$ *e* $b = 255$ *temos*

$$(141, 255) = (141, 114) = (27, 114) = (27, 6)$$

$$= (3, 6) = (3, 6) = (3, 3) = 3.$$

Agora vamos enunciar o Algoritmo de Euclides que representa um método de grande relevância para obtermos o máximo divisor comum de dois números.

Teorema 2.18 *Sejam* b *e* c*, com* $c > 0$*. Se o algoritmo da divisão for aplicado sucessivamente obtemos a série de equações.*

$$\begin{aligned}
b &= cq_1,\ 0 < r_1 < c,\\
c &= r_1q_2 + r_2,\ 0 < r_2 < r_1,\\
r_1 &= r_2q_3 + r_3,\ 0 < r_3 < r_2,\\
&\vdots\\
r_{j-2} &= r_{j-1}q_j + r_j,\ 0 < r_j < r_{j-1},\\
r_{j-1} &= r_jq_{j+1}
\end{aligned}$$

Como a sequência de restos não pode diminuir indefinidamente pois $0 \leq r_1 < r_{i-1}$ *e existe apenas um número finito de naturais menores que* c*. Dessa forma, para algum* j*, encontraremos* $r_{j+1} = 0$*. Então,* r_j *será o maior divisor comum* b *e* c*, isto é, o último resto não nulo da sequência de divisões acima.*

Na prática, para obtermos o (a, b) utilizando o Algoritmo de Euclides podemos realizar os seguintes cálculos:

Primeiramente, efetuamos a divisão $a = bq_1 + r_1$ e organizamos os números no seguinte esquema:

	q_1	
a	b	
r_1		

Em seguida, efetuamos a divisão $b = r_1q_2 + r_2$ e colocamos os números no esquema a seguir:

	q_1	q_2	
a	b	r_1	
r_1	r_2		

Assim, prosseguindo, enquanto for possível, obtemos:

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

Exemplo 2.19 *Calcule o mdc de* 300 *e* 245.

Solução: Utilizando o Algoritmo de Euclides, temos:

	1	4	2	5
300	245	55	25	5
55	25	5		

Portanto, $(300, 245) = 5$.

Note que, no exemplo acima, pelo Algoritmo de Euclides temos que:

$$55 = 2 \cdot 25 + 5 \Leftrightarrow 5 = 55 - 2 \cdot 25 \tag{2.1}$$

$$245 = 4 \cdot 55 + 25 \Leftrightarrow 25 = 245 - 4 \cdot 55 \tag{2.2}$$

$$300 = 1 \cdot 245 + 55 \Leftrightarrow 55 = 300 - 1 \cdot 245 \tag{2.3}$$

Assim, substituindo 2.2 em 2.1 , segue que:

$$5 = 55 - 2 \cdot (245 - 4 \cdot 55) = 9 \cdot 55 - 2 \cdot 245 \tag{2.4}$$

Agora, substituindo 2.3 em 2.4, temos:

$$5 = 9 \cdot (300 - 1 \cdot 245) - 2 \cdot 245 = 9 \cdot 300 - 11 \cdot 245 \tag{2.5}$$

Desse modo, temos que $(300, 245) = 5 = 9 \cdot 300 + (-11) \cdot 245$.

A partir desse exemplo e do Algoritmo de Euclides podemos enunciar o Teorema de Bézout.

Teorema 2.20 *Dados* a, b *inteiros e* $d = (a, b)$. *Então existem inteiros* m *e* n *tais que* $d = ma + nb$.

Definição 2.21 *Sejam a e b dois números inteiros, diremos que a e b são primos entre si ou coprimos quando $(a, b) = 1$.*

Proposição 2.22 *Dois números inteiros a e b são primos entre si se, e somente se, existem números inteiros m e n tais que $ma + nb = 1$.*

Demonstração: Ver A. Hefez [11] □

Exemplo 2.23 *(IOM - 1959) Prove que $\dfrac{21n+4}{14n+3}$ é irredutível para todo número natural n.*

Observação: uma fração $\dfrac{a}{b}$ é dita irredutível quando apresenta numerador a e denominador b primos entre si.

Solução: Devemos mostrar que $(21n+4, 14n+3) = 1$. Assim, utilizando o lema de Euclides temos que:

$$(\underbrace{21n+4}_{a}, \underbrace{14n+3}_{b}) = (7n+1, 14n+3) = (7n+1, 1) = 1.$$

Portanto, $\dfrac{21n+4}{14n+3}$ é irredutível para todo número natural n.

2.4 Equações Diofantinas Lineares

Nesta seção vamos abordar as equações do tipo $ax + by = c$, com $a, b, c \in \mathbb{Z}$.

Em homenagem a Diofanto de Alexandria, que foi o primeiro a considerar problemas dessa forma, essas equações são chamadas de equações diofantinas lineares. Algumas equações desse tipo não possuem solução, por exemplo, a equação $2x + 6y = 5$.

Assim, torna-se interessante observar em quais condições essas equações apresentam soluções.

Proposição 2.24 *Sejam a, b e c números inteiros. A equação diofantina*

$$ax + by = c$$

possui solução se, e somente se, $(a, b) | c$.

Demonstração: Ver A. Hefez [11] $\square$

É importante destacar que as equações do tipo $ax + by = c$, com (a, b) = 1, sempre possuem soluções.

Dessa forma, vamos mostrar como essas equações diofantinas podem ter suas soluções determinadas a partir de soluções particulares quaisquer.

Proposição 2.25 *Seja x_0, y_0 uma solução particular da equação $ax + by = c$, onde $(a, b) = 1$. Então, as soluções x, y em $\mathbb{Z}$ da equação são:*

$$x = x_0 + tb, \ y = y_0 - ta; \ t \in \mathbb{Z}$$

Demonstração: Consideremos x, y uma solução de $ax + by = c$, portanto:

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

$$\Leftrightarrow ax - ax_0 = by_0 - by$$

$$\Leftrightarrow a(x - x_0) = b(y_0 - y). \tag{2.6}$$

Como $(a, b) = 1$, temos que $b|(x - x_0)$. Portanto,

$$x - x_0 = tb, \ t \in \mathbb{Z}. \tag{2.7}$$

Agora substituindo 2.7 em 2.6, temos que:

$$b(y_0 - y) = atb \Leftrightarrow y_0 - y = ta.$$

Portanto, as soluções são da forma:

$$x = x_0 + tb \ \text{ e } \ y = y_0 - ta.$$

Por outro lado, se $x = x_0 + tb$ e $y = y_0 - ta$, tem-se:

$$ax + by = a(x_0 + tb) + b(y_0 - ta) = ax_0 + atb + by_0 - bta = ax_0 + by_0 = c.$$

Portanto, x, y é solução. $\square$

Assim, pela proposição acima temos que a equação diofantina $ax + by = c$, com $(a, b) = 1$, apresenta infinitas soluções em $\mathbb{Z}$.

Quando $|a|$, $|b|$ e $|c|$ forem números "pequenos", então uma solução para a equação $ax + by = c$, pode ser obtida por inspeção. No entanto, existem casos em que isso se torna inviável, por isso podemos descrever o seguinte método para encontrar uma solução particular da equação.

Inicialmente é possível determinar $m, n \in \mathbb{Z}$ tais que

$$ma + nb = (a, b) = 1.$$

Agora, multiplicando os dois membros dessa igualdade por c, segue que:

$$cma + cnb = c.$$

Portanto, $x_0 = cm$ e $y_0 = cn$ é uma solução particular da equação.

Exemplo 2.26 *Determinar todas as soluções inteiras da equação diofantina*

$$18x + 5y = 48.$$

Solução: Inicialmente vamos determinar o $(18, 5)$ *utilizando o algoritmo de Euclides.*

	3	1	1	2
18	5	3	2	1
3	2	1		

Portanto, o $(18, 5) = 1$*, como* $1|48$*, temos que essa equação possui solução.*

Pelo algoritmo de Euclides, temos que:

$$3 = 1 \cdot 2 + 1 \Leftrightarrow 1 = 3 - 1 \cdot 2$$

$$5 = 1 \cdot 3 + 2 \Leftrightarrow 2 = 5 - 1 \cdot 3$$

$$18 = 3 \cdot 5 + 3 \Leftrightarrow 3 = 18 - 3 \cdot 5$$

Agora, substituindo as equações acima umas nas outras, segue que:

$$1 = 3 - 1 \cdot (5 - 1 \cdot 3) = 2 \cdot 3 - 1 \cdot 5 = 2 \cdot (18 - 3 \cdot 5) - 1 \cdot 5 = 18 \cdot 2 - 7 \cdot 5$$

ou seja,

$$1 = 18 \cdot 2 + 5 \cdot (-7)$$

Multiplicando essa equação por 48, obtemos:

$$48 = 18 \cdot 96 + 5 \cdot (-336)$$

Logo, uma solução particular da equação proposta é $x_0 = 96$ *e* $y_0 = -336$. *Dessa forma, segue que as soluções são:*

$$x = 96 + 5t, \; y = -336 - 18t; \; t \in \mathbb{Z}$$

Exemplo 2.27 *Anita comprou um número ímpar de canetas e borrachas, gastando R\$ 37,40. Sabendo-se que os preços unitários das canetas e borrachas são, respectivamente, R\$ 1,70 e R\$ 0,90, determine quantas canetas e quantas borrachas ela comprou.*

Solução: Sejam x *o número de canetas e* y *o número de borrachas. Temos a equação* $1,70x + 0,90y = 37,40$, *multiplicando por 10, obtemos:*

$$17x + 9y = 374$$

Como $(17, 9) = 1$ *e* $1|374$, *então essa equação tem solução.*

Agora, usando o algoritmo de Euclides, segue que:

$$\begin{array}{c|c|c|c} & 1 & 1 & 8 \\ \hline 17 & 9 & 8 & 1 \\ \hline 8 & 1 & & \end{array}$$

e podemos escrever

$$9 = 1 \cdot 8 + 1 \Leftrightarrow 1 = 9 - 1 \cdot 8$$

$$17 = 1 \cdot 9 + 8 \Leftrightarrow 8 = 17 - 1 \cdot 9.$$

Substituindo as equações acima umas nas outras, temos que:

$$1 = 9 - 1 \cdot (17 - 1 \cdot 9) = -1 \cdot 17 + 2 \cdot 9$$

ou seja,

$$1 = 17 \cdot (-1) + 9 \cdot 2.$$

Multiplicando essa equação por 374, obtemos:

$$374 = 17 \cdot (-374) + 9 \cdot 748.$$

Logo, $x_0 = -374$ *e* $y_0 = 748$ *é uma solução particular da equação e a solução geral é:*

$$x = -374 + 9t, \; y = 748 - 17t; \; t \in \mathbb{Z}.$$

Como $x > 0$ *e* $y > 0$*, temos que:*

$$-374 + 9t > 0 \Rightarrow t > 41,5$$

e

$$748 - 17t > 0 \Rightarrow t < 44.$$

Logo, $t = 42$ *ou* $t = 43$*.*

Se $t = 42$*, temos* $x = 4$ *e* $y = 34$ *e se* $t = 43$*, obtemos* $x = 13$ *e* $y = 17$*. Como* x *deve ser ímpar, segue* $x = 13$ *e* $y = 17$*, ou seja, foram compradas* 13 *canetas e* 17 *borrachas.*

Em alguns casos precisamos resolver as equações diofantinas lineares da forma $ax + by = c$, com $a, b, c \in \mathbb{N}$, em $\mathbb{N} \cup \{0\}$. Dessa forma, torna-se importante apresentarmos a proposição a seguir.

Proposição 2.28 *Dados* $a, b \in \mathbb{N}$*,com* $(a, b) = 1$ *temos que todo número inteiro* c *pode ser escrito de maneira única do seguinte modo:*

$$c = ma + nb$$

com $0 \leq m < b$ *e* $n \in \mathbb{Z}$*.*

Demonstração: Existência: Como existem $u, v \in \mathbb{Z}$ tais que

$$ua + vb = (a, b) = 1.$$

Assim, multiplicando os membros dessa igualdade por c, obtemos:

$$cua + cvb = c. \tag{2.8}$$

Além disso, temos que existem, pela divisão euclidiana, $q, m \in \mathbb{Z}$ com $0 \leq m < b$ tais que

$$uc = qb + m. \tag{2.9}$$

Dessa forma, substituindo 2.9 em 2.8, segue que:

$$a(qb + m) + bvc = c$$

$$\Leftrightarrow aqb + am + bvc = c$$

$$\Leftrightarrow ma + (aq + vc)b = c.$$

Considerando $n = (aq + vc)$, temos que $c = ma + nb$, com $0 \leq m < b$.

Unicidade: Suponha que exista duas soluções assim $ma + nb = m'a + n'b$, com $0 \leq m, m' < b$.

Assim, segue que:

$$ma - m'a = n'b - nb \Leftrightarrow (m - m')a = (n' - n)b$$

com $|m - m'| < b$. Como $(a, b) = 1$, temos que $b|(m - m')$, o que é possível somente se $m = m'$, e neste caso $n = n'$. □

Como nem sempre uma equação diofantina do tipo $ax + by = c$, onde $(a, b) = 1$ possui solução em $\mathbb{N} \cup \{0\}$, a seguir apresentamos definições e resultados importantes que contribuem para determinarmos quando isso ocorre.

Definição 2.29 *Dados $a, b \in \mathbb{N}$. Define-se o conjunto:*

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

que é denominado de semigrupo gerado por a e b.

Assim, a equação diofantina $ax + by = c$, onde $(a, b) = 1$, possui solução $\mathbb{N} \cup \{0\}$ em se, e somente se, $c \in S(a, b)$.

Proposição 2.30 *Temos que $c \in S(a, b)$ se, e somente se, existem $m, n \in \mathbb{N} \cup \{0\}$, com $m < b$ tais que $c = ma + nb$.*

Demonstração: Ver A. Hefez [11]. □

Definição 2.31 *Define-se o conjunto de lacunas de $S(a, b)$ como sendo o conjunto*

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

Corolário 2.32 *Tem-se que*

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

Teorema 2.33 *Dada a equação $ax + by = c$, onde $(a,b) = 1$, esta possui solução em números naturais se, e somente se,*

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

Demonstração: Temos que a equação $ax + by = c$ possui solução se, e somente se, $c \in S(a,b)$ e $\mathcal{L}(a,b) = \mathbb{N} \backslash S(a,b)$, logo a equação tem solução se $c \notin \mathcal{L}(a,b)$. □

Corolário 2.34 *Dados $a, b \in \mathbb{N}$ tais que $(a,b) = 1$. Temos 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: Temos que $\mathcal{L}$ é um conjunto finito e o seu maior elemento é

$$max\mathcal{L}(a,b) = (b-1)a - b$$

Logo, se

$$c \geq (b-1)a - b + 1 = (b-1)(a-1)$$

a equação $aX + bY = c$ tem solução nos naturais.

Por outro lado, se $c = (b-1)(a-1) - 1$ a equação não possui solução. □

Exemplo 2.35 *Para quais valores de c em $\mathbb{N}$ a equação $7x + 5y = c$ não possui soluções em $\mathbb{N} \cup \{0\}$?*

Solução: O conjunto de lacunas de $S(7,5)$ é o conjunto:

$$\mathcal{L}(7,5) = \{m7 - n5 \in \mathbb{N}, m, n \in \mathbb{N}, m < 5\}$$

Dessa forma, segue que:

Se $m = 1$ temos que $(1 \cdot 7 - n5) \in \mathbb{N}$ quando $n = 1$.

Se $m = 2$ temos que $(2 \cdot 7 - n5) \in \mathbb{N}$ quando $n = 1, 2$.

Se $m = 3$ temos que $(3 \cdot 7 - n5) \in \mathbb{N}$ quando $n = 1, 2, 3, 4$.

Se $m = 4$ temos que $(4 \cdot 7 - n5) \in \mathbb{N}$ quando $n = 1, 2, 3, 4, 5$.

Portanto, $\mathcal{L}(7,5) = \{1, 2, 3, 4, 6, 8, 9, 11, 13, 16, 18, 23\}$.

Logo, a equação $7x + 5y = c$ não possui solução em $\mathbb{N} \cup \{0\}$ se, e somente se, $c \in \mathcal{L}(7,5)$.

2.5 Números primos

Vamos apresentar nesta seção a definição de Números primos e alguns resultados de grande relevância como o Teorema Fundamental da Aritmética.

Definição 2.36 *Um número natural p com $p > 1$, é dito número primo se possui somente dois divisores positivos 1 e p.*

Sejam p e q números primos e a um numero natural qualquer, da definição de números primos, segue que:

i) Se $p|q$ então $p = q$.

   Com efeito, por hipótese, q é primo e $p|q$, assim segue da definição de números primos que $p = 1$ ou $p = q$. Como p é primo temos que $p > 1$, logo $p = q$.

ii) Se $p \nmid a$ então $(p, a) = 1$.

   Seja $(p, a) = d$, temos que $d|p$ e $d|a$. Logo, $d = p$ ou $d = 1$. No entanto se $p = d$, então $p|a$ o que contradiz a hipótese, portanto $d = 1$.

Dado um número n, tal que $n > 1$, se este número não for primo diremos que é um número composto.

Exemplo 2.37 *Temos que os números* 2, 3 *e* 5 *são números primos, enquanto que os números* 6, 8 *e* 10 *são compostos.*

Proposição 2.38 *Dados $a, b, p \in \mathbb{Z}$, com p primo. Se $p|ab$, então $p|a$ ou $p|b$.*

Demonstração: Ver J.P.O. Santos [20]. □

Como a partir dos números primos é possível gerar todos os números naturais, apresentamos, a seguir, o resultado que nos garante esse fato e que nos mostra a relevância dos números primos na Teoria dos números.

Teorema 2.39 *(Teorema Fundamental da Aritmética) Todo número natural maior do que* 1 *ou é primo ou pode ser escrito de maneira única (a menos da ordem dos fatores) como um produto de números primos.*

Demonstração: Vamos utilizar o segundo Princípio da Indução. Para $n = 2$ a afirmação é verdadeira. Agora vamos supor que o resultado é válido para todo número natural menor do que n. Assim, devemos mostrar que vale para n. Se n for um número primo, não há nada para demonstrar. Suponhamos que n seja um número composto. Portanto, existem números n_1 e n_2 tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$.

Dessa forma, pela hipótese de indução, segue que existem números primos $p_1, \cdots, p_r$ e $q_1, \cdots, q_s$ tais que $n_1 = p_1 \cdots p_r$ e $n_2 = q_1 \cdots q_s$. Logo, $n = p_1 \cdots p_r q_1 \cdots q_s$.

Agora, para provar a unicidade, vamos supor que n apresenta duas fatorações distintas, ou seja,

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

Assim, devemos mostrar que $r = s$. Como $p_1 | q_1 \cdots q_s$, então p_1 divide pelos menos um dos fatores q_j, ou seja, $p_1 = q_j$ para algum j. Suponhamos que $p_1 = q_1$, portanto

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

Como $p_2 \cdots p_r < n$, pela hipótese de indução temos que $r = s$ e, portanto, as fatorações $p_1 \cdots p_r$ e $q_1 \cdots q_s$ são iguais. □

Exemplo 2.40 *As fatorações em números primos dos números* 100 *e* 2625 *são:*

$100 = 2 \cdot 2 \cdot 5 = 2^2 \cdot 5$

$2625 = 3 \cdot 5 \cdot 5 \cdot 5 \cdot 7 = 3 \cdot 5^3 \cdot 7$

Note, nos exemplos acima, que quando os fatores primos se repetem é possível agrupá-los. Além disso, podemos organizar esses fatores primos em ordem crescente, sendo assim podemos enunciar o seguinte resultado:

Teorema 2.41 *Dado um número inteiro* $n \neq 0, 1, -1$, *existem números primos* $p_1 < p_2 < \cdots < p_r$ *e* $\alpha_1, \cdots, \alpha_r \in \mathbb{N}$, *univocamente determinados, tais que*

$$n = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

Quando tratamos da fatoração em números primos de um número natural n, podemos ressaltar a relação existente entre essa fatoração com os divisores de n por meio do seguinte resultado:

Proposição 2.42 *Seja* $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ *um número natural. Se* n' *é um divisor positivo de* n*, então ele será da forma*

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

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

Em relação ao número de divisores positivos do número natural n, que indicamos por $d(n)$, nota-se, a partir de uma contagem simples, que se n está escrito na forma $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, sendo $p_1, \cdots, p_r$ números primos e $\alpha_1, \cdots, \alpha_r \in \mathbb{N}$, segue que:

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 2) \cdots (\alpha_r + 1).$$

Teorema 2.43 *Dados* $a = \pm p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ *e* $b = \pm p_1^{\beta_1} \cdots p_n^{\beta_n}$*. Pondo*

$$\gamma_i = min\{\alpha_i, \beta_i\}$$

temos que

$$(a, b) = p_1^{\gamma_1} \cdots p_n^{\gamma_n}.$$

Demonstração: Ver em A. Hefez [11]. □

Exemplo 2.44 *Determine o número de divisores positivos de* 2008^8.

Solução: Temos que $2008^8 = (2^3 \cdot 251)^8 = 2^{24} \cdot 251^8$.

Logo, $d(2008^8) = (24 + 1) \cdot (8 + 1) = 225$.

Exemplo 2.45 *Um número natural* n *possui exatamente dois divisores e* $n + 1$ *possui exatamente* 3 *divisores. Encontre o número de divisores de* $n + 2$.

Solução: Como n *possui exatamente* 2 *divisores, segue que* $n = p$ *é um número primo. Como todo número quadrado perfeito possui uma quantidade ímpar de divisores, temos que* $n + 1$ *que possui exatamente* 3 *divisores é um quadrado perfeito. Portanto,* $n + 1 = x^2$*, para algum* x *inteiro positivo. Dessa forma, segue que*

$$n = n + 1 - 1 = x^2 - 1 = (x - 1)(x + 1) = p,$$

como p *é um número primo, só é possível termos* $x - 1 = 1$ *o que implica que* $x = 2$ *e portanto* $n = 3$.

Logo, $n + 2 = 3 + 2 = 5$ *e seu número de divisores é igual a* 2.

Além dos resultados apresentados até este momento envolvendo números primos, podemos destacar também o Pequeno Teorema de Fermat que possui grande relevância na teoria dos números.

Teorema 2.46 *(Pequeno Teorema de Fermat) Dado um número primo p, temos que p divide o número $a^p - a$, para todo $a \in \mathbb{Z}$.*

Demonstração: Ver em A. Hefez [11]. $\square$

Corolário 2.47 *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: Ver em A. Hefez [11]. $\square$

2.6 Congruências

Nesta seção apresentaremos a definição de congruência, alguns exemplos e resultados de grande relevância para a Teoria dos números como, por exemplo, o Pequeno Teorema de Fermat.

Definição 2.48 *Dados a, b e m números inteiros, com $m > 1$. Diremos que a é congruente a b módulo m, e indicamos por $a \equiv b \ (mod\ m)$, se $m|(a-b)$, ou seja, se os restos de sua divisão euclidiana por m são os mesmos. Se a não for congruente a b módulo m, indicamos $a \not\equiv b \ (mod\ m)$.*

Como essa definição diz que $a \equiv b \ (mod\ m)$, se e somente se $m|(a-b)$, segue que

$$a \equiv b \ (mod\ m) \Leftrightarrow m|(a-b) \Leftrightarrow a - b = km \Leftrightarrow a = b + km, para\ algum\ k \in \mathbb{Z}.$$

Exemplo 2.49 *Temos que $5 \equiv 2 \ (mod\ 3)$, pois $3|(5-2)$ e $7 \not\equiv 4 \ (mod\ 2)$, pois $2 \nmid (7-4)$.*

Note que dados quaisquer $a, b \in \mathbb{Z}$ o resto da divisão desses números por 1 sempre será o zero, devido a esse fato utilizamos $m > 1$ na definição de congruência.

A partir da definição de congruência temos que ela representa uma relação de equivalência, o que apresentamos na proposição a seguir.

Proposição 2.50 *Dados inteiros a, b, c e m, com $m > 1$, segue que:*

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

ii) *se* $a \equiv b \ (mod\ m)$, *então* $b \equiv a \ (mod\ m)$,

iii) *se* $a \equiv b \ (mod\ m)$ *e* $b \equiv c \ (mod\ m)$, *então* $a \equiv c \ (mod\ m)$.

Demonstração:

i) Temos que $m|0$ o que implica que $m|(a-a)$, logo $a \equiv a \ (mod\ m)$.

ii) Se $a \equiv b \ (mod\ m)$, então $a = b + km$, sendo k algum inteiro. Portanto, $b = a - km$ o que implica que $b \equiv a \ (mod\ m)$.

iii) Se $a \equiv b \ (mod\ m)$ e $b \equiv c \ (mod\ m)$, segue que $m|(a-b)$ e $m|(b-c)$. Dessa forma, $m|(a-b)+(b-c)$, ou seja, $m|(a-c)$. Portanto, $a \equiv c \ (mod\ m)$.

□

Em relação a congruência, podemos destacar que existem semelhanças consideráveis entre suas propriedades e as propriedades da igualdade.

Proposição 2.51 *Sejam a, b, c e d inteiros dados, sendo $m > 1$.*

i) *se* $a \equiv b \ (mod\ m)$ *e* $c \equiv d \ (mod\ m)$, *então* $a + c \equiv b + d \ (mod\ m)$.

ii) *se* $a \equiv b \ (mod\ m)$, *então* $a + c \equiv b + c \ (mod\ m)$.

iii) *se* $a \equiv b \ (mod\ m)$ *e* $c \equiv d \ (mod\ m)$, *então* $ac \equiv bd \ (mod\ m)$.

iii) *se* $a \equiv b \ (mod\ m)$, *então* $a^n \equiv b^n \ (mod\ m)$, *para todo* $n \in \mathbb{N}$.

iv) *se* $a + c \equiv b + c \ (mod\ m)$, *então* $a \equiv b \ (mod\ m)$.

Exemplo 2.52 *Calcule o resto de* 4^{100} *por* 3.

Solução: Temos que $4 \equiv 1 \ (mod\ 3)$. *Dessa forma elevando a 100, segue que*

$$4^{100} \equiv 1^{100} \equiv 1 \ (mod\ 3)$$

Portanto, o resto é 1.

Como qualquer número inteiro a é congruente módulo m a algum dos restos $0, 1, 2, \cdots, m-1$, sendo que dois desses números distintos não são congruentes módulo m, temos a seguinte definição.

Definição 2.53 *Um sistema completo de resíduos módulo m é um conjunto de números inteiros tais que os restos na divisão por m, são os números* $0, 1, 2, \cdots, m-1$, *em qualquer ordem e sem repetições.*

Além disso, também podemos apresentar essa definição do seguinte modo.

Definição 2.54 *O conjunto dos inteiros* $\{r_1, r_2, \cdots, r_s\}$ *representa um sistema completo de resíduos módulo m se*

i) $r_i \not\equiv r_j \ (mod\ m)$ *para* $i \neq j$.

ii) para todo inteiro n existe r_i *tal que* $n \equiv r_i \ (mod\ m)$.

Assim, nota-se que um sistema completo de resíduos módulo m tem m elementos.

Exemplo 2.55 *O conjunto* $\{24, 31, 45, 62\}$ *é um sistema completo de resíduos módulo* 4, *pois dividindo esses números por* 4 *obtemos, respectivamente,* 0, 3, 1 *e* 2.

Exemplo 2.56 *Prove que* $n^2 + 1$ *não é divisível por* 3 *qualquer seja o inteiro* n.

Solução: Sabemos que todo inteiro n é congruente módulo 3 *a* 0, 1 *ou* 2. *Assim, temos três casos a considerar.*

1° *caso - se* $n \equiv 0 \ (mod\ 3)$, *segue que*

$$n^2 \equiv 0^2 \ (mod\ 3) \Rightarrow n^2 \equiv 0 \ (mod\ 3) \Rightarrow n^2+1 \equiv 0+1 \ (mod\ 3) \Rightarrow n^2+1 \equiv 1 \ (mod\ 3).$$

2° *caso - se* $n \equiv 1 \ (mod\ 3)$, *temos que*

$$n^2 \equiv 1^2 \ (mod\ 3) \Rightarrow n^2 \equiv 1 \ (mod\ 3) \Rightarrow n^2+1 \equiv 1+1 \ (mod\ 3) \Rightarrow n^2+1 \equiv 2 \ (mod\ 3).$$

3° *caso - se* $n \equiv 2 \ (mod\ 3)$, *segue que*

$$n^2 \equiv 2^2 \ (mod\ 3) \Rightarrow n^2 \equiv 4 \equiv 1 \ (mod\ 3) \Rightarrow n^2+1 \equiv 1+1 \ (mod\ 3) \Rightarrow n^2+1 \equiv 2 \ (mod\ 3).$$

Dessa forma, como nunca temos $n^2+1 \equiv 0 \ (mod\ 3)$*, podemos concluir que* n^2+1 *não é divisível por* 3.

Em algumas situações é importante considerarmos congruências lineares, ou seja, congruências da forma

$$ax \equiv b \ (mod\ m)$$

onde a, b, m são números inteiros dados, com $a \neq 0$ e $m > 1$.

Neste caso, temos que $m|(ax - b)$. Assim, se x é solução de $ax - b$, então essa equação precisa ser múltiplo de m. Portanto, temos que existe $y \in \mathbb{Z}$ tal que $ax = b - my$, isto é, $ax + my = b$.

Para determinar quando uma congruência linear da forma $ax \equiv b \ (mod\ m)$ tem solução temos o seguinte resultado.

Teorema 2.57 *A congruência* $ax \equiv b \ (mod\ m)$ *possui solução se, e somente se* $d = (a, m)$ *divide* b.

Agora, vamos apresentar um dos resultados mais importantes da teoria de congruências, visto que este pode auxilar de forma considerável algumas situações propostas sobre esse tema.

Teorema 2.58 *(Pequeno Teorema de Fermat) Sejam* p *primo e* $a \in \mathbb{Z}$*. Se* $p \nmid a$*, tem-se que*

$$a^{p-1} \equiv 1 \ (mod\ p).$$

Demonstração: Sejam os números $a, 2a, 3a, \cdots, (p-1)a$. Como $mdc(a, p) = 1$ temos que nenhum destes números é divisível por p, isto é, nenhum deles é congruente a zero módulo p. Dessa forma, o conjunto dos restos destes números coincide com o conjunto dos restos não nulos na divisão por p, ou seja, coincide com o conjunto $\{1, 2, 3, \cdots, p-1\}$.

Assim, segue que:

$$a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \ (mod\ p)$$

$$a^{p-1}(p-1)! \equiv (p-1)! \ (mod\ p).$$

No entanto, $mdc((p-1)!, p) = 1$ o que nos permite cancelar o termo $(p-1)!$ nos dois membros da congruência, assim obtemos:

$$a^{p-1} \equiv 1 \ (mod \ p)$$

o que conclui a demonstração. $\square$

Corolário 2.59 *Se p é um número primo e a um inteiro positivo, então:*

$$a^p \equiv a \ (mod \ p).$$

Demonstração: Temos dois casos a considerar, se $p|a$ e se $p \nmid a$.

Se $p \nmid a$, então a partir do teorema acima, multiplicando ambos os membros por a, segue que $a^{p-1} \cdot a \equiv 1 \cdot a \ (mod \ p)$ e consequentemente $a^p \equiv a \ (mod \ p)$.

Se $p|a$, temos que $p|(a^p - a)$, ou seja, $p|a(a^{p-1} - 1)$, logo $a^p \equiv a \ (mod \ p)$.

Portanto, em ambos os casos tem-se que $a^p \equiv a \ (mod \ p)$. $\square$

Exemplo 2.60 *Verifique que* 17 *divide* $11^{104} + 1$.

Solução: Como 17 *é um número primo e* $17 \nmid 11$*, pelo Pequeno Teorema de Fermat, temos que* $11^{16} \equiv 1 \ (mod \ 17)$*. Além disso, pelo Algoritmo da divisão segue que* $104 = 16 \cdot 6 + 8$.

Dessa forma, temos:

$(11^{16})^6 \equiv 1^6 \ (mod \ 17)$

$11^{96} \equiv 1 \ (mod \ 17)$

$11^{96} \cdot 11^8 \equiv 1 \cdot 11^8 \ (mod \ 17)$

$11^{104} \equiv 11^8 \ (mod \ 17)$

Note que $11^2 = 121 \equiv 2 \ (mod \ 17)$ *e* $11^8 = (11^2)^4 \equiv 2^4 \equiv -1 \ (mod \ 17)$.

Portanto, temos que $11^{104} \equiv 11^8 \equiv -1 \ (mod \ 17)$*, ou seja, 17 divide* $11^{104} + 1$.

CAPÍTULO 3

A INVESTIGAÇÃO NA PRÁTICA

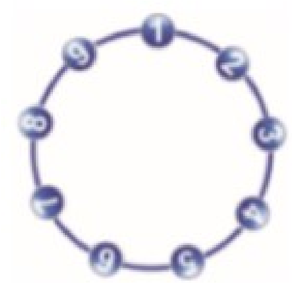
Neste capítulo, faremos investigações baseadas em exercícios de aritmética da Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP). Em cada atividade proposta seguiremos os seguintes passos: inicialmente apresentamos o enunciado do exercício como foi proposto pela OBMEP, em seguida resolvemos o que foi sugerido e, por fim, realizamos a investigação tendo como base questões que foram surgindo. Consideramos importante ressaltar que essas investigações serão conduzidas com base nas nossas experiências pessoais, o que torna possível que o leitor perceba caminhos diferentes dos nossos para conduzi-las.

3.1 Atividade Investigativa 1: Pulando em uma circunferência

Apresentamos nesta seção uma investigação na qual exploramos alguns conceitos da Teoria dos Números como Congruência, Sistema completo de resíduos, Máximo divisor comum e Quantidade de divisores de um número. A seguir, trazemos o exercício no qual baseamos a nossa investigação e a descrição desta.

(OBMEP - Nível 2 - 2016) Luciana marcou os números de 1 a 9 em uma circunferência, como na figura. A partir do número 1, ela começou a pular de 4 em 4. No primeiro pulo ela foi do 1 ao 5, no segundo, do 5 ao 9, no terceiro, do 9 ao 4 e assim por diante. Depois de pular 1000 vezes, em que número ela parou? [‡]

[‡]Questão 11, nível 2, 1ª fase, ano 2016



Inicialmente vamos resolver o que o exercício propõe.

Solução: Pulando de 4 em 4, verificamos que para retornar ao ponto de partida temos que fazer a seguinte sequência:

$$1 \smile 5 \smile 9 \smile 4 \smile 8 \smile 3 \smile 7 \smile 2 \smile 6 \smile 1$$

Assim, percebemos que é necessário pular 9 vezes para voltar ao ponto de partida e que, para isso, iremos passar em todos os números que estão na circunferência. Como $1000 = 9 \cdot 111 + 1$, segue que para Luciana pular 1000 vezes ela deve fazer 111 voltas completas e mais um pulo, logo ela irá parar no número 5. $\square$

Agora, analisando o enunciado, começaram a surgir alguns questionamentos que nos levaram a começar a nossa investigação.

Por exemplo, a primeira pergunta que nos ocorreu foi o que aconteceria se mudássemos a quantidade de "espaço" entre os pulos? Isto é, e se Luciana pulasse de 5 em 5, de 2 em 2 ou de 7 em 7?

Se Luciana pular de 5 em 5 a partir do número 1, temos que no primeiro pulo ela irá do 1 ao 6, no segundo, do 6 ao 2, no terceiro, do 2 ao 7 e assim por diante, conforme a sequência abaixo:

$$1 \smile 6 \smile 2 \smile 7 \smile 3 \smile 8 \smile 4 \smile 9 \smile 5 \smile 1$$

Nesse caso percebemos que ela precisa pular 9 vezes para retornar ao ponto de partida e para isso passar em todos os números, portanto se ela pulasse 1000 vezes de 5 em 5 como $1000 = 9 \cdot 111 + 1$ ela irá parar no número 6.

Por outro lado, se ela pular de 2 em 2, verificamos novamente que para retornar ao ponto de partida é necessário pular 9 vezes e também precisa passar por todos os números como verificamos na sequência abaixo:

$$1 \smile 3 \smile 5 \smile 7 \smile 9 \smile 2 \smile 4 \smile 6 \smile 8 \smile 1$$

Assim como $1000 = 9 \cdot 111 + 1$, segue que depois de pular 1000 vezes ela irá parar no número 3.

Incrivelmente percebemos que, se ela pular de 7 em 7, também será preciso pular 9 vezes para voltar ao ponto de partida, mais ainda, notamos que novamente ela passa por todos os números, o que nos leva a fazer a seguinte conjectura:

"Para retornar ao ponto de partida, pulando de n em n, sempre será preciso pular 9 vezes, logo será preciso passar por todos os números de 1 a 9".

No entanto, ao analisar a possibilidade de ela pular de 3 em 3 percebemos que nossa conjectura não é válida, pois para retornar ao ponto de partida é preciso pular 3 vezes, passando apenas nos números 1, 4 e 7 e o mesmo ocorre se pular de 6 em 6, obviamente se ela pular de 9 em 9 será preciso apenas 1 pulo para retornar ao ponto de partida.

Assim, notamos que pulando de n em n quando o $(n, 9) = 1$ será preciso pular 9 vezes para retornar ao ponto de partida, passando por todos os números, enquanto que quando $(n, 9) = 3$ será necessário pular 3 vezes parar retornar ao ponto de partida, passando pelos números 1, 4 e 7, o que nos leva a reformular a nossa conjectura.

1. *"Seja n o tamanho do pulo, tal que $(n, 9) = 1$, então para retornar ao ponto de partida, pulando de n em n, será preciso pular 9 vezes e passar por todos os números de 1 a 9".*

2. *"Seja n o tamanho do pulo, tal que $(n, 9) = 3$, então para retornar ao ponto de partida, pulando de n em n, será preciso pular 3 vezes e passar pelos números 1, 4 e 7".*

Demonstração: Seja n o tamanho do pulo e m_i o número onde Luciana está parada, temos que $m_i = 1, 2, 3, 4, 5, 6, 7, 8$ ou 9 que são os números que estão presentes na circunferência e $i = 0, 1, 2, \cdots$, que indica o número do pulo.

1. Quando $(n, 9) = 1$, segue que $9 \nmid n$, portanto n pode ser escrito nas formas $9k + 1, 9k + 2, 9k + 4, 9k + 5, 9k + 7, 9k + 8$, com $k \in \mathbb{N}$.

   Assim, podemos organizar em uma tabela os resultados das somas de $m_i + n$. Nela vamos considerar m_i na ordem crescente e não na ordem em que iríamos parar e $k + 1 = s$.

n / m_i	$9k+1$	$9k+2$	$9k+4$	$9k+5$	$9k+7$	$9k+8$
1	$9k+2$	$9k+3$	$9k+5$	$9k+7$	$9k+8$	$9s$
2	$9k+3$	$9k+4$	$9k+6$	$9k+7$	$9k+9$	$9s+1$
3	$9k+4$	$9k+5$	$9k+7$	$9k+8$	$9s+1$	$9s+2$
4	$9k+5$	$9k+6$	$9k+8$	$9s$	$9s+2$	$9s+3$
5	$9k+6$	$9k+7$	$9s$	$9s+1$	$9s+3$	$9s+4$
6	$9k+7$	$9k+8$	$9s+1$	$9s+2$	$9s+4$	$9s+5$
7	$9k+8$	$9s$	$9s+2$	$9s+3$	$9s+5$	$9s+6$
8	$9s$	$9s+1$	$9s+3$	$9s+4$	$9s+6$	$9s+7$
9	$9s+1$	$9s+2$	$9s+4$	$9s+5$	$9s+7$	$9s+8$

Analisando a tabela percebemos que para todo n a soma $m_i + n$ formam um conjunto de números que quando divididos por 9 deixa os restos 0, 1, 2, 3, 4, 5, 6, 7 e 8 portanto esse conjunto representa um sistema completo de resíduos módulo 9. Logo, para retornar ao ponto de partida será preciso passar por todos os números que estão na circunferência.

2. Quando $(n, 9) = 3$, temos que $3|n$ e $9 \nmid n$, portanto n pode ser escrito nas formas $9k + 3$ e $9k + 6$, com $k \in \mathbb{N}$.

   Para $n = 9k + 3$ e partindo de $m_0 = 1$, segue que:

$$1 + 9k + 3 = 9k + 4 \Rightarrow m_1 = 4$$

   Para $m_1 = 4$, temos:

$$4 + 9k + 3 = 9k + 7 \Rightarrow m_2 = 7$$

   Para $m_2 = 7$, segue que:

$$7 + 9k + 3 = 9(k + 1) + 1 \Rightarrow m_3 = 1$$

   De forma análoga, mostra-se para $n = 9k + 6$.

   Portanto, será preciso pular 3 vezes para retornar ao ponto de partida, passando sempre pelos números 4 e 7.

□

Ainda é possível irmos um pouco mais além. O que será que acontece se alterarmos a quantidade de números marcados na circunferência? Isto é, e se na circunferência marcássemos números de 1 a 3, de 1 a 4 e assim por diante?

Fazendo algumas tentativas no caso em que marcamos números de 1 a 3 na circunferência, temos que se pular de 2 em 2 é preciso pular 3 vezes para retornar ao ponto de partida, se pular de 4 em 4 também é necessário pular 3 vezes para voltar ao ponto de partida e que ocorre o mesmo se pular de 5 em 5. No entanto, se pular de 6 em 6 observamos que ela precisará pular 1 vez para retornar ao ponto de partida.

Agora se marcarmos na circunferência números de 1 a 4, percebemos que se pular de 2 em 2 é preciso 2 pulos para retornar ao ponto de partida, se pular de 3 em 3 é necessário 4 pulos para voltar ao ponto de partida, se pular de 4 em 4 precisará de 1 pulo para retornar ao ponto de partida, de 5 em 5 são precisos 4 pulos e de 6 em 6 são necessários 2 pulos.

Assim, considerando que c representa a quantidade de números marcados na circunferência, que está se iniciando no número 1 e n representa de quanto em quanto irá se pular, percebemos pela análise acima que considerando $c = 3$, temos que quando o máximo divisor comum de 3 e n é igual a 1, $(3, n) = 1$, são necessários 3 pulos para retornar ao ponto de partida e 1 pulo quando $(3, n) = 3$.

Fazendo $c = 6$, quando $(6, n) = 1$ será necessário pular 6 vezes para voltar ao ponto de partida, quando $(6, n) = 3$ é preciso pular 2 vezes para retornar ao ponto de partida, quando $(6, n) = 2$ deve-se pular 3 vezes e quando $(6, n) = 6$ é preciso pular apenas uma vez.

Para $c = 7$, temos que quando $(7, n) = 1$ será preciso pular 7 vezes para retornar ao ponto de partida e quando $(7, n) = 7$ basta pular uma vez.

Fazendo $c = 30$, quando $(30, n) = 1$ deve-se pular 30 vezes para retornar ao ponto de partida, se $(30, n) = 2$ é preciso pular 15 vezes, quando $(30, n) = 3$ será necessário pular 10 vezes, se $(30, n) = 5$ precisa-se pular 6 vezes, quando $(30, n) = 6$ é necessário pular 5 vezes, se $(30, n) = 10$ deve-se pular 3 vezes, quando $(30, n) = 15$ é preciso pular 2 vezes e basta pular apenas uma vez quando $(30, n) = 30$.

Dessa forma, analisando esses resultados notamos que a quantidade de pulos está relacionada com os divisores de c, o que nos leva a conjecturar que:

"Seja c a quantidade de números dispostos em uma circunferência, organizados de 1 a c, partindo de 1 e pulando de n em n as possíveis quantidades necessárias de pulos para retornar ao ponto de partida será $\dfrac{c}{(c, n)}$".

Demonstração: Como c e n são números naturais , eles podem ser escritos na forma $c = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ e $n = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_r^{\beta_r}$, onde $p_1, p_2, \cdots, p_r$ são números primos e $\alpha_1, \alpha_2, \cdots, \alpha_r, \beta_1, \beta_2, \cdots, \beta_r \in \mathbb{N} \cup \{0\}$.

Agora, considerando $\gamma = min\{\alpha_i, \beta_i\}$, com $i = 1, 2, 3, \cdots, r$, tem-se pelo Teorema 2.43 que:

$$(c, n) = p_1^{\gamma_1} \cdots p_r^{\gamma_r}.$$

Dessa forma, as possíveis quantidades de pulos para retornar ao ponto de partida será as possíveis combinações de $p_1, p_2, \cdots, p_r$, com $0 \leq \lambda_i \leq \alpha_i$, para $i = 1, 2, \cdots, r$, que podem ser expressas por:

$$\frac{c}{(c, n)} = \frac{p_1^{\alpha_1} \cdots p_r^{\alpha_r}}{p_1^{\gamma_1} \cdots p_r^{\gamma_r}} = p_1^{\lambda_1} \cdots p_r^{\lambda_r}$$

com $\lambda_i = \alpha_i - \gamma_i$.

$\square$

Analisando essa investigação percebemos que, mesmo não estando explícito, ela foi baseada no modelo heurístico de Lakatos e sua importância, visto que nos permite explorar vários conceitos matemáticos.

3.2 Atividade Investigativa 2: Pulos dos grilos

Nesta seção, desenvolvemos uma investigação que nos proporcionou a possibilidade de abordarmos outros conceitos da Teoria dos Números tais como Divisão euclidiana, Função quociente, Função resto, Equação diofantina e Conjunto das lacunas, sendo estes necessários no decorrer da investigação ou para demonstrar algumas conjecturas elaboradas no durante o processo.

Apresentamos, a seguir, o exercício utilizado como base para a realização da investigação e a exposição das etapas e resultados desta.

(OBMEP - Nível 2 - 2013) Dois grilos, Adonis e Basílio, pulam sempre para frente; Adonis só dá pulos de 1 cm ou 8 cm e Basílio só dá pulos de 1 cm ou 7 cm. Eles percorrem qualquer distância com o menor número de pulos possível. Por exemplo, Adonis percorre 16 cm com apenas dois pulos de 8 cm cada, enquanto Basílio precisa de quatro pulos, sendo dois de 7 cm e outros dois de 1 cm. Por outro lado, para percorrer 15 cm, Adonis precisa de oito pulos, sendo um de 8 cm e sete de 1 cm, enquanto Basílio precisa de apenas três pulos, sendo dois de 7 cm e um de 1 cm.

Indicando por $A(d)$ e $B(d)$, respectivamente, o número de pulos que Adonis e Basílio dão para percorrer d centímetros, temos $A(15) = 8$, $B(15) = 3$, $A(16) = 2$ e $B(16) = 4$. §

Analisando essa questão resolvemos montar uma tabela relacionando a distância percorrida com a quantidade de pulos. Assim, obtemos:

Distância d	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
A(d)	1	2	3	4	5	6	7	1	2	3	4	5	6	7	8	2	3
B(d)	1	2	3	4	5	6	1	2	3	4	5	6	7	2	3	4	5

Observando esses dados notamos que cada distância d pode ser escrita, de modo único, na forma $d = 8 \cdot k + r$, sendo k o quociente da divisão de d por 8 e r o resto dessa divisão e ao mesmo tempo pode ser escrita, de modo único, na forma $d = 7 \cdot q + s$, sendo q o quociente da divisão de d por 7 e s o resto dessa divisão, o que nos permitiu conjecturar que:

"O número de pulos pode ser escrito como $A(d) = k + r$ e $B(d) = q + s$".

Demonstração: Denotando por $k_8(d)$ o quociente da divisão do número d por 8, é possível definirmos a função quociente por 8, como:

$$\begin{aligned} k_8 \ : \ & \mathbb{Z} \to \mathbb{Z} \\ & d \mapsto k_8(d) \end{aligned}$$

Também pode-se definir a função resto, como:

$$\begin{aligned} r_8 \ : \ & \mathbb{Z} \to \mathbb{Z} \\ & d \mapsto r_8(d) \end{aligned}$$

Logo, a quantidade de pulos necessários para percorrer cada distância será a soma das funções k_8 e r_8, ou seja,

$$A(d) = k_8 + r_8.$$

De forma análoga, provamos o fato de que $B(d) = q + s$. □

§Questão 6, nível 2, 2ª fase, ano 2013

Nesse casos, como Adonis dá pulos de 1 cm ou 8 cm e Basílio dá pulos de 1 cm ou 7 cm torna-se possível escrever qualquer número natural por meio da soma de um múltiplo de 8 com um múltiplo de 1 ou por meio da soma de um múltiplo de 7 e um múltiplo de 1.

No entanto, nos surgiu uma outra pergunta: e se variarmos o tamanho dos pulos ainda será possível escrevermos qualquer número natural?

Por exemplo, se Adonis der pulos de 1 cm ou 3 cm, podemos escrever 1 como $1 = 3 \cdot 0 + 1$, 2 da forma $2 = 3 \cdot 0 + 2$, 3 como $3 = 3 \cdot 1 + 0$, 4 do seguinte modo $4 = 3 \cdot 1 + 1$, 5 como $5 = 3 \cdot 1 + 2$ e 13 da forma $13 = 3 \cdot 4 + 1$. Assim, conjecturamos que:

"Qualquer que seja o tamanho dos pulos é possível escrever todos os números naturais."

Supondo agora que Adonis, por exemplo, dá pulos de 2 cm ou 7 cm, temos que não é possível escrever o número 1 como uma combinação desses dois números, que 2 pode ser escrito como $2 = 2 \cdot 1 + 7 \cdot 0$, que é não possível escrever o número 3, o número 4 pode ser escrito na forma $4 = 2 \cdot 2 + 7 \cdot 0$ e o número 13 é escrito como $2 \cdot 3 + 7 \cdot 1$. A partir desses contra-exemplos percebemos que nossa conjectura não é verdadeira.

Portanto, reformulando-a temos:

"Se um dos tamanhos do pulo for diferente de 1 *cm não é possível escrever todos os números naturais como uma combinação dos tamanhos dos pulos".*

Demonstração: Considerando a e b os tamanhos dos pulos, temos a equação diofantina $ax + by = d$, onde d representa a distância percorrida, ou seja, os números naturais e $(a, b) = 1$.

Como essa equação só possui solução nos naturais se, e somente se, d não pertence ao conjunto das lacunas, logo, d só poderá ser escrito por meio de uma combinação de a e b se d não pertencer ao conjunto das lacunas de a e b. Portanto, não é possível escrever todos os números naturais como combinação dos tamanhos dos pulos. $\square$

Ainda analisando os dados na tabela que relaciona a quantidade de pulos com as distâncias, percebemos que em alguns momentos Adonis dá mais pulos e em outros momentos Basílio dá mais pulos e notamos que essas mudanças, como se fossem "ultrapassagens", começam a ocorrer sempre que uma distância d representa um múltiplo de 8 ou um múltiplo de 7.

Por exemplo, quando a distância é igual a 7 cm, temos que $A(d) = 7$ e $B(d) = 1$.

Fazendo a distância igual a 8 cm, segue que $A(d) = 1$ e $B(d) = 2$.

Agora, considerando a distância igual a 14, verificamos que $A(d) = 7$ e $B(d) = 2$ e quando a distância é igual a 16 cm, percebemos que $A(d) = 2$ e $B(d) = 4$.

Além disso, observamos que quem começa a ultrapassar é aquele que a distância d não representa um múltiplo do tamanho do seu pulo, o que nos levou a conjecturarmos que:

"Quem ultrapassa é aquele que tem o resto da divisão de d pelo tamanho do seu pulo diferente de zero".

No entanto, existem números que são múltiplos de 7 e de 8 ao mesmo tempo como, por exemplo, o 56 para o qual temos $A(d) = 7$ e $B(d) = 8$, o que representa um contra-exemplo para a nossa conjectura. Vamos encerrar essa investigação sem conseguir chegar a uma conclusão para essa última conjectura.

Sim, isso pode acontecer! Deixar problemas em aberto é frequente e saudável na pesquisa matemática.

3.3 Atividade Investigativa 3: Brincando com números

A partir do exercício proposto nesta seção, apresentamos uma investigação na qual exploramos os conceitos de Máximo Divisor Comum e Lema de Euclides, sendo este último utilizado para a demonstração de uma conjectura sugerida.

(OBMEP - Nível 2 - 2008) Ana e Daniela brincam de escrever números no quadro negro. A brincadeira começa com cada uma delas escrevendo um número natural. Depois disso:

- quem tiver o menor número mantém esse número;
- quem tiver escrito o maior número troca-o pela diferença entre seu número e o número da outra.

Elas repetem esse procedimento até que os dois números escritos no quadro negro fiquem iguais. Se Ana começou escrevendo 100 e Daniela 88, qual o número que vai ficar escrito no quadro negro ao final da brincadeira?[¶]

Solução: A partir da situação descrita na questão, conseguimos montar uma tabela com as jogadas realizadas até chegarmos ao resultado final, respondendo assim à questão proposta.

Números iniciais	100	88
1ª jogada	12	88
2ª jogada	12	76
3ª jogada	12	64
4ª jogada	12	52
5ª jogada	12	40
6ª jogada	12	28
7ª jogada	12	16
8ª jogada	12	4
9ª jogada	8	4
10ª jogada	4	4

Portanto, a brincadeira irá parar quando ficar escrito o número 4. □

Agora, o que acontece se começarmos a brincadeira com números diferentes?

Por exemplo, se começarmos por 50 e 20, temos:

Números iniciais	50	20
1ª jogada	30	20
2ª jogada	10	20
3ª jogada	10	10

Quando utilizamos os números 10 e 3, notamos que:

Números iniciais	10	3
1ª jogada	7	3
2ª jogada	4	3
3ª jogada	1	3
4ª jogada	1	2
5ª jogada	1	1

Iniciando com 21 e 14, obtemos:

[¶]Questão 9, nível 2, 1ª fase, ano 2008

Números iniciais	21	14
1ª jogada	7	14
2ª jogada	7	7

Observando o número escrito no final das brincadeiras, percebemos que esse número foi sempre o máximo divisor comum dos dois números iniciais, o que nos permitiu conjecturar que:

"Dados os números inteiros a e b se mantermos o menor deles e trocarmos o maior pela diferença entre os dois, repetindo esse processo até que os dois números sejam iguais, então o número final é o máximo divisor comum de a e b."

Demonstração: Sejam a, b e n números inteiros, temos pelo Lema de Euclides (Lema 2.16) que se existe $(a, b-na)$, então $(a, b) = (a, b-na)$. Logo, considerando $n = 1$ segue que, repetindo esse procedimento, encontraremos o máximo divisor comum de a e b, ou seja, quando chegarmos a dois números iguais, determinamos (a, b). □

Nessa atividade investigativa não conseguimos abordar muitas questões, o que nos levou a elaborarmos apenas uma conjectura. Assim, notamos que nem todos os exercícios nos proporcionam a oportunidade de realizar uma investigação muito enriquecedora, a qual nos conduz a um relevante desenvolvimento matemático.

3.4 Atividade Investigativa 4: Algarismos afilhados

Nesta seção, apresentamos uma investigação realizada em relação a um exercício que aborda o conceito de Divisores. Dessa forma, explorando este mesmo conceito buscamos encontrar novas conjecturas.

(OBMEP - Nível 2 - 2007) Um algarismo é afilhado de um número se ele é o algarismo das unidades de algum divisor desse número. Por exemplo, os divisores de 56 são 1, 2, 4, 7, 8, 14, 28 e 56, logo os afilhados de 56 são 1, 2, 4, 6, 7 e 8.

a) Quais são os afilhados de 57? [‖]

Solução: Incialmente verificamos que os divisores de 57 são 1, 3, 19 e 57, logo os seus afilhados são 1, 3, 7 e 9. □

[‖] Questão 3, nível 2, 2ª fase, ano 2007

Mas temos infinitos números, por isso nos questionamos: e quem são os afilhados desses outros números?

Se considerarmos o número 2 temos que seus divisores são 1 e 2, logo seus afilhados são 1 e 2. Da mesma forma, para o número 3 notamos que seus afilhados são 1 e 3.

Analisando o número 4 conclui-se que seus divisores são 1, 2 e 4 e consequentemente seus afilhados são 1, 2 e 4.

No caso do número 5 seus afilhados são 1 e 5 e do número 7 são 1 e 7.

Assim, comparando a quantidade de divisores de um número e a quantidade de afilhados, conjecturamos que:

"A quantidade de afilhados que um número possui é igual à quantidade de divisores que ele apresenta."

No entanto, observando o exemplo dado no enunciado do exercício e outros como, por exemplo, o número 11 que tem como os divisores os números 1 e 11 e seu afilhado é o 1, percebemos que essa conjectura não é verdadeira.

Agora, observando mais alguns números, notamos que para o número 12 seus divisores são 1, 2, 3, 4, 6 e 12, logo seus afilhados são 1, 2, 3, 4 e 6.

Considerando o número 13 temos que ele possui como divisores o 1 e 13 e consequentemente como seus afilhados 1 e 3.

Quando analisamos o número 14 verificamos que seus divisores são 1, 2, 7 e 14 e portanto seus afilhados são 1, 2, 4 e 7. Da mesma forma, para o número 15 temos que seus divisores são 1, 3, 5 e 15 e consequentemente tem como afilhados o 1, 3 e 5.

Desse modo, comparando a quantidade de divisores e a quantidade de afilhados dos números 12, 13, 14 e 15, conjecturamos que:

"Somente os números maiores que 10 *e que são múltiplos de* 3 *possuem a quantidade de afilhados igual a* $(n-1)$*, onde* n *representa a quantidade de divisores desse número".*

No entanto, os divisores de 18 são 1, 2, 3, 6, 9 e 18 e seus afilhados são 1, 2, 3, 6, 8 e 9, então neste caso a quantidade de divisores é igual a quantidade de afilhados, portanto este é um contra-exemplo para a conjectura.

Verificando mais alguns números, temos que o número 20 tem como divisores o

1, 2, 4, 5, 10 e 20 e como afilhados são 0, 1, 2, 4 e 5.

No caso do número 25 segue que seus divisores são 1, 5 e 25 e consequentemente seus afilhados são 1 e 5.

Agora, considerando o número 30 percebemos que seus divisores são 1, 2, 3, 5, 6, 10, 15 e 30, portanto seus afilhados são 0, 1, 2, 3, 5 e 6.

A partir desses resultados podemos conjecturar que:

"Os números maiores que 10 *e que são múltiplos de* 5 *possuem a quantidade de afilhados igual a* $(n-1)$*, onde n representa a quantidade de divisores desse número".*

Porém, notamos que os divisores de 40 são 1, 2, 4, 5, 8, 10, 20 e 40 e seus afilhados são 0, 1, 2, 5 e 8. Portanto, o número 40 tem 8 divisores e 6 afilhados, logo este é um contra- exemplo para a conjectura.

Após algumas tentativas de conjecturas, decidimos encerrar essa atividade investigativa mesmo sem nenhuma conclusão verdadeira. No entanto, acreditamos que mesmo assim ela pode contribuir para o desenvolvimento matemático do estudante.

3.5 Atividade Investigativa 5: Brincadeira do dobra ou apaga

Nesta seção, realizamos uma investigação onde o principal conceito explorado foi a Representação dos números inteiros na base 10. No entanto, no decorrer do processo, com o intuito de elaborar novas conjecturas, também abordamos o Teorema Fundamental da Aritmética.

A seguir apresentamos o exercício em que nos baseamos para a investigação, bem como para a descrição desta.

(OBMEP - Nível 1 - 2005) Numa aula de Matemática, a professora inicia uma brincadeira, escrevendo no quadro negro um número. Para continuar a brincadeira, os alunos devem escrever outro número, seguindo as regras abaixo:

1. Se o número escrito só tiver um algarismo, ele deve ser multiplicado por 2.

2. Se o número tiver mais de um algarismo, os alunos podem escolher entre apagar o algarismo das unidades ou multiplicar esse número por 2.

Depois que os alunos escrevem um novo número a brincadeira continua com este número, sempre com as mesmas regras.

Veja a seguir dois exemplos desta brincadeira, um começando com 203 e outro com 4197:

$$203 \xrightarrow{dobra} 406 \xrightarrow{apaga} 40 \xrightarrow{apaga} 4\ldots$$

$$4197 \xrightarrow{apaga} 419 \xrightarrow{dobra} 838 \xrightarrow{apaga} 83 \ldots$$

a) Comece a brincadeira com o número 45 e mostre uma maneira de prosseguir até chegar ao número 1.**

Solução: Podemos seguir os seguintes passos para chegar ao número 1 e consequentemente resolver a questão proposta.

$$45 \xrightarrow{apaga} 4 \xrightarrow{dobra} 8 \xrightarrow{dobra} 16 \xrightarrow{apaga} 1$$

□

A partir da ideia proposta pelo exercício a primeira questão que nos ocorreu foi: se alterarmos esse número, quais são os passos necessários para chegar ao número 1?

Assim, começamos a realizar tentativas com o intuito de observar o que aconteceria. Por exemplo, se utilizarmos o número 42 temos:

$$42 \xrightarrow{apaga} 4 \xrightarrow{dobra} 8 \xrightarrow{dobra} 16 \xrightarrow{apaga} 1$$

Usando o número 43 segue que:

$$43 \xrightarrow{apaga} 4 \xrightarrow{dobra} 8 \xrightarrow{dobra} 16 \xrightarrow{apaga} 1$$

Agora trocando pelo número 46 temos:

$$46 \xrightarrow{apaga} 4 \xrightarrow{dobra} 8 \xrightarrow{dobra} 16 \xrightarrow{apaga} 1$$

Substituindo o número por 31 temos:

$$31 \xrightarrow{apaga} 3 \xrightarrow{dobra} 6 \xrightarrow{dobra} 12 \xrightarrow{apaga} 1$$

**Questão 1, nível 2, 2ª fase, ano 2005

Alterando o número por 23 segue que:

$$23 \xrightarrow{apaga} 2 \xrightarrow{dobra} 4 \xrightarrow{dobra} 8 \xrightarrow{dobra} 16 \xrightarrow{apaga} 1$$

Observando esses resultados conjecturamos que:

"Dado um número formado com dois algarismos e com o algarismo da dezena diferente de 1*, é possível chegar ao* 1 *com o seguinte procedimento: apagar o algarismo da unidade, em seguida dobrar o novo número até obtermos um número múltiplo de* 2 *que tenha o algarismo* 1 *na dezena e finalmente apagar o algarismo da unidade."*

Demonstração: Seja ab um número formado por dois algarismos, escrevendo esse número na base 10 temos:

$$ab = a \cdot 10 + b$$

Assim, utilizando as regras das brincadeiras, para apagarmos o algarismo da unidade estaríamos subtraindo o número b, ou seja:

$$a \cdot 10 + b - b = a \cdot 10$$

Agora, para continuarmos apenas com o algarismo a temos que:

$$(a \cdot 10) \div 10 = a$$

Como $1 < a \leqslant 9$, temos dois casos a considerar:

1° caso - se $1 < a < 5$, então, ao multiplicarmos por dois, obtemos um número c tal que $2 \leq c \leq 8$, multiplicando o resultado obtido por dois encontramos um número d tal que $4 \leq d \leq 16$. Assim, fazendo sucessivas multiplicações por 2 obtemos um número do tipo $1 \cdot 10 + t$, ou seja, $1t$, apagando o algarismo t chega-se ao número 1.

2° caso - se $5 \leq a \leq 9$, então basta multiplicar por 2 e obteremos um número c tal que $10 \leq c \leq 18$, ou seja, encontraremos um número do tipo $1 \cdot 10 + t$, ou seja, $1t$ apagando o algarismos t chegamos ao número 1.

$\square$

Analisamos por enquanto números com dois algarismos. Mas, existem números com mais algarismos. E nesses casos o que será que acontece?

Aplicando as regras da brincadeira em alguns exemplos, como 238, 345 e 8567 obtemos:

$$238 \xrightarrow{apaga} 23 \xrightarrow{apaga} 2 \xrightarrow{dobra} 4 \xrightarrow{dobra} 8 \xrightarrow{dobra} 16 \xrightarrow{apaga} 1$$

$$345 \xrightarrow{apaga} 34 \xrightarrow{apaga} 3 \xrightarrow{dobra} 6 \xrightarrow{dobra} 12 \xrightarrow{apaga} 1$$

$$8567 \xrightarrow{apaga} 856 \xrightarrow{apaga} 85 \xrightarrow{apaga} 8 \xrightarrow{dobra} 16 \xrightarrow{apaga} 1$$

Dessa forma, podemos conjecturar que:

"Para chegar ao número 1 *a partir de qualquer número natural que não comece com* 1*, basta apagarmos sucessivamente os algarismos da unidade dos números obtidos em sequência até obtermos um número com um algarismo, em seguida dobrar este número até encontrarmos um múltiplo de* 2 *que inicie com o algarismo* 1 *e apagar o algarismo da unidade."*

Demonstração: Seja a um número tal que $a = r_n \cdots r_1 r_0$, escrevendo esse número na base 10, temos:

$$a = r_n \cdot 10^n + \cdots + r_1 \cdot 10 + r_0.$$

Utilizando as regras da brincadeira podemos apagar o algarismo da unidade, para isso é possível subtrair o número r_0, ou seja,

$$r_n \cdot 10^n + \cdots + r_1 \cdot 10 + r_0 - r_0 = r_n \cdot 10^n + \cdots + r_1 \cdot 10.$$

Como pela brincadeira r_1 deve se tornar o novo algarismo da unidade, então devemos dividir esse novo número por 10, assim segue que:

$$r_n \cdot 10^n + \cdots + r_1 \cdot 10 = 10 \cdot (r_n \cdot 10^{n-1} + \cdots + r_2 \cdot 10 + r_1).$$

Agora dividindo por 10, temos:

$$[10 \cdot (r_n \cdot 10^{n-1} + \cdots + r_2 \cdot 10 + r_1)] \div 10 = r_n \cdot 10^{n-1} + \cdots + r_2 \cdot 10 + r_1.$$

Assim, repetindo esse processo sucessivamente obteremos o número b tal que:

$$b = r_n.$$

Dessa forma, como $1 < r_n \leqslant 9$, temos dois casos a considerar de forma análoga a demonstração da conjectura anterior.

$\square$

Agora, aplicando as mesmas regras dessa brincadeira, quais serão os passos para chegar no final a outros algarismos?

Vamos começar utilizando alguns exemplos como, 45, 67 e 123, para observar o que acontece para chegarmos ao número 2, ou seja,

$$45 \xrightarrow{apaga} 4 \xrightarrow{dobra} 8 \xrightarrow{dobra} 16 \xrightarrow{apaga} 1 \xrightarrow{dobra} 2$$

$$67 \xrightarrow{apaga} 6 \xrightarrow{dobra} 12 \xrightarrow{apaga} 1 \xrightarrow{dobra} 2$$

$$123 \xrightarrow{apaga} 12 \xrightarrow{apaga} 1 \xrightarrow{dobra} 2$$

Esses resultados nos permitem afirmar que:

"Dado qualquer número natural que não inicie com o algarismo 2*, é possível chegar ao número* 2*, com a seguinte estratégia:*

1° *caso - se o número começar com o algarismo* 1*, basta apagar os algarismos da unidade dos números obtidos sucessivamente até chegar em* 1 *e em seguida dobrar;*

2° *caso - se o número não começar com o algarismo* 1*, deve-se usar o mesmo processo para chegar ao número* 1 *e em seguida dobrar."*

Demonstração: Seja a um número que não comece com o algarismo 2, tal que $a = r_n \cdots r_1 r_0$, escrevendo esse número na base 10, temos:

$$a = r_n \cdot 10^n + \cdots + r_1 \cdot 10 + r_0.$$

Assim, no primeiro caso segue que $r_n = 1$, portanto o número a pode ser escrito como:

$$a = 1 \cdot 10^n + \cdots + r_1 \cdot 10 + r_0.$$

Utilizando as regras da brincadeira é possível apagar o algarismo da unidade, logo é possível subtrair o número r_0, ou seja,

$$1 \cdot 10^n + \cdots + r_1 \cdot 10 + r_0 - r_0 = 1 \cdot 10^n + \cdots + r_1 \cdot 10.$$

Como pela brincadeira r_1 se tornará o novo algarismo da unidade, então precisamos dividir esse novo número por 10, dessa forma temos:

$$1 \cdot 10^n + \cdots + r_1 \cdot 10 = 10 \cdot (1 \cdot 10^{n-1} + \cdots + r_2 \cdot 10 + r_1).$$

Agora dividindo por 10, segue que:

$$[10 \cdot (1 \cdot 10^{n-1} + \cdots + r_2 \cdot 10 + r_1] \div 10 = 1 \cdot 10^{n-1} + \cdots + r_2 \cdot 10 + r_1.$$

Portanto, repetindo sucessivamente esse processo obtemos:

$$b = 1.$$

Em seguida multiplicando 1 por 2, chegamos ao número 2.

No segundo caso, a demonstração é análoga ao caso em que queremos chegar ao número 1.

□

E o que ocorre quando pretendemos chegar ao número 3?

Podemos utilizar alguns exemplos como, 13, 54, 423 e 857 para observamos o que ocorre, quando temos como objetivo chegar ao número 3.

$$13 \xrightarrow{apaga} 1 \xrightarrow{dobra} 2 \xrightarrow{dobra} 4 \xrightarrow{dobra} 8 \xrightarrow{dobra} 16 \xrightarrow{dobra} 32 \xrightarrow{apaga} 3$$

$$54 \xrightarrow{apaga} 5 \xrightarrow{dobra} 10 \xrightarrow{apaga} 1 \xrightarrow{dobra} 2 \xrightarrow{dobra} 4 \xrightarrow{dobra} 8 \xrightarrow{dobra} 16 \xrightarrow{dobra} 32 \xrightarrow{apaga} 3$$

$$423 \xrightarrow{apaga} 42 \xrightarrow{apaga} 4 \xrightarrow{dobra} 8 \xrightarrow{dobra} 16 \xrightarrow{dobra} 32 \xrightarrow{apaga} 3$$

$$857 \xrightarrow{apaga} 85 \xrightarrow{apaga} 8 \xrightarrow{dobra} 16 \xrightarrow{dobra} 32 \xrightarrow{apaga} 3$$

Assim, podemos conjecturar que:

"Dado qualquer número natural que não comece com o algarismo 3, é possível chegar ao número 3, com a seguinte estratégia:

1° *caso - se o número começar com os algarismos 1, 2, 4 ou 8 deve-se apagar os algarismos da unidade dos números obtidos sucessivamente até chegar ao algarismo que iniciava o número, em seguida dobrá-lo até obter o número 32 e no final apagar o algarismo da unidade;*

2° *caso - se o número inicia com os algarismos 5, 6, 7 ou 9, basta utilizar o processo para chegar ao número 1, em seguida dobrar até obter o número 32 e por fim apagar o algarismo da unidade."*

Demonstração: Seja a um número que não inicia com o algarismo 3, tal que $a = r_n \cdots r_1 r_0$, escrevendo esse número na base 10, temos:

$$a = r_n \cdot 10^n + \cdots + r_1 \cdot 10 + r_0.$$

No primeiro caso, temos que r_n é igual a 1, 2, 4 ou 8. Assim, utilizando as regras da brincadeira é possível apagar o algarismo da unidade, portanto é possível subtrair o número r_0, ou seja,

$$r_n \cdot 10^n + \cdots + r_1 \cdot 10 + r_0 - r_0 = r_n \cdot 10^n + \cdots + r_1 \cdot 10.$$

Pela brincadeira r_1 deve-se tornar o novo algarismo da unidade, podemos assim dividir esse novo número por 10, dessa forma temos:

$$r_n \cdot 10^n + \cdots + r_1 \cdot 10 = 10 \cdot (r_n \cdot 10^{n-1} + \cdots + r_1).$$

Agora dividindo por 10, temos:

$$[10 \cdot (r_n \cdot 10^{n-1} + \cdots + r_1)] \div 10 = r_n \cdot 10^{n-1} + \cdots + r_1.$$

Portanto, repetindo sucessivamente esse processo obtemos:

$$b = r_n.$$

Como r_n é igual a 1, 2, 4 ou 8 e todos esse números representam uma potência de 2, basta multiplicá-los por 2 até o obtermos 32 e assim apagar o algarismo da unidade para chegarmos ao número 3.

No segundo caso, o início da demonstração é análoga ao caso em que queremos chegar ao número 1, pois depois que encontramos o número 1, que representa uma potência de 2, a partir daí basta multiplicarmos por 2 até obtermos o número 32 e apagarmos o algarismo da unidade. □

Ainda é possível ir um pouco mais além, isto é, como podemos proceder para chegar ao número 5, 6 ou 7? Ou mais ainda, como fazer para chegar a qualquer número de um algarismo, ou seja, para chegar a um número p?

Agora analisando os exemplos apresentados nos surgiu uma outra questão que mudou um pouco o rumo da nossa investigação. Será que é possível encontrar um número mínimo de passos para chegarmos ao número 1?

Notamos que os números com dois algarismos e que começam pelo mesmo algarismo sempre precisam da mesma quantidade de passos para chegar ao número 1. Dessa forma, vamos analisar o que acontece se o número tiver somente um algarismo.

Se for o número 2, temos:

$$2 \xrightarrow{dobra} 4 \xrightarrow{dobra} 8 \xrightarrow{dobra} 16 \xrightarrow{apaga} 1$$

Percebe-se que nesse caso são necessários no mínimo 4 passos para chegar ao número 1.

Agora, utilizando o número 3, segue que:

$$3 \xrightarrow{dobra} 6 \xrightarrow{dobra} 12 \xrightarrow{apaga} 1$$

Nesse caso, foram necessários 3 passos.

Quando temos o número 4, segue que:

$$4 \xrightarrow{dobra} 8 \xrightarrow{dobra} 16 \xrightarrow{apaga} 1$$

Assim, são preciso 3 passos para chegar ao número 1.

Se for o número 5, temos que:

$$5 \xrightarrow{dobra} 10 \xrightarrow{apaga} 1$$

Nesse caso, foram necessários 2 passos para chegar ao número 1.

Agora, se considerarmos o número 8, segue que:

$$8 \xrightarrow{dobra} 16 \xrightarrow{apaga} 1$$

Percebemos que nesse caso foram necessários 2 passos para chegar ao número 1.

Se for o número 9, temos:

$$9 \xrightarrow{dobra} 18 \xrightarrow{apaga} 1$$

Nesse caso, precisamos de 2 passos para chegar ao número 1.

Observando esses exemplos notamos que no caso do número 9 e do número 6 o número de passos é igual à soma dos expoentes presentes em sua decomposição em fatores primos. Assim, conjecturamos que:

"Dado um número $n = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}$ a quantidade de passos para chegar ao número 1 é dada por $\alpha_1 + \dots + \alpha_r$".

No entanto, partindo do número 2 são preciso 4 passos e seu expoente na decomposição em fatores primos é igual a 1. Portanto, essa conjectura não é verdadeira.

Agora, analisando a quantidade que foi preciso dobrar o número para chegar a um múltiplo de 2 que comece com o algarismo 1 e a sua quantidade de algarismos, percebemos que existe uma relação entre essas quantidades tanto no caso de um algarismo como quando o número possui dois algarismo ou mais. Dessa forma, temos uma nova conjectura

"Seja $n = a_1 a_2 \cdots a_s$ um número natural, onde $a_1, \cdots, a_s$ são seus algarismos.

1. *Se $a_1 = 1$, a quantidade mínima de passos para chegar ao número 1 será dada por $q = s - 1$;*
2. *Se $a_1 \neq 1$, a quantidade mínima de passos para chegar em 1 será dada por $q = k + s$, onde s é o número de algarismos de n e k é o primeiro índice da sequência $(B_k) = 2^k \cdot a_1$, com $k = 0, 1, 2, \cdots$, que tenha dois algarismos."*

Observando alguns dos exemplos realizados como o caso do número 42 notamos que é possível começar o mesmo processo de modo diferente, ou seja,

$$42 \xrightarrow{dobra} 84 \xrightarrow{dobra} 168 \xrightarrow{apaga} 16 \xrightarrow{apaga} 1$$

Agora, fazendo o mesmo processo 52, temos:

$$52 \xrightarrow{dobra} 104 \xrightarrow{apaga} 10 \xrightarrow{apaga} 1$$

Dessa forma, percebemos que a quantidade de passos para chegar ao número 1 é a mesma independente do processo escolhido, ou seja, se optamos por apagar ou dobrar. Assim, temos a seguinte conjectura:

"Esse processo apresenta a propriedade comutativa, ou seja, optando por apagar ou dobrar, atingiremos a mesma quantidade de passos para chegar ao número".

Analisando outros exemplos segue que:

$$238 \xrightarrow{dobra} 476 \xrightarrow{dobra} 952 \xrightarrow{apaga} 95 \xrightarrow{apaga} 9 \xrightarrow{dobra} 18 \xrightarrow{dobra} 36 \xrightarrow{dobra}$$
$$72 \xrightarrow{apaga} 7 \xrightarrow{dobra} 14 \xrightarrow{apaga} 1$$

$$345 \xrightarrow{dobra} 690 \xrightarrow{dobra} 1380 \xrightarrow{apaga} 138 \xrightarrow{apaga} 13 \xrightarrow{apaga} 1$$

Comparando esses resultados com os que já foram realizados, percebemos que não é em todo o processo que obtemos o mesmo resultado optando por qualquer umas das opções, ou seja, optando tanto por apagar como por dobrar. Portanto, essa conjectura não é verdadeira.

Além dessas questões formuladas sobre essa atividade seria possível levantar outras como, por exemplo, o que ocorreria se alterássemos a regra trocando dobrar por triplicar? Dessa forma, destacamos que nessa atividade apresentamos algumas sugestões de questões que podem conduzir a investigação matemática, todavia é possível elaborar outras questões.

No decorrer deste capítulo notamos que podemos aplicar a investigação matemática a diferentes exercícios, mas que a partir de cada um deles obtemos resultados distintos. Assim, considerarmos importante destacar novamente que essas investigações são particulares, ou seja, foram realizadas com base nas nossas experiências pessoais o que torna possível que outras pessoas percorram caminhos diferentes a partir dos mesmos enunciados de exercícios.

Além disso, esse fato evidencia a relevância da discussão ao final da investigação, pois esta proporciona a oportunidade de debatermos sobre as conjecturas e demonstrações realizadas levando-nos a aperfeiçoa-las.

Alguns desses exercícios apresentados nos levam a realizar uma grande quantidade de questionamentos, o que enriquece a atividade investigativa e consequentemente o desenvolvimento matemático.

No entanto, outros exercícios, mesmo nos conduzindo a algum resultado interessante, não nos proporcionam a oportunidade de desenvolver uma investigação baseadas em diversas questões, limitando assim, um pouco, o desenvolvimento matemático. Em outros casos não conseguimos obter conjecturas válidas, mais ainda nesse processo de criação as conjecturas não são formuladas de modo preciso. No entanto, mesmo assim os exercícios nos levam a abordarmos conceitos matemáticos importantes no decorrer das tentativas.

Dessa forma, percebemos a importância que o exercício escolhido apresenta para a investigação matemática e que, mesmo quando não obtemos um resultado que pareça satisfatório, ele pode contribuir para que o aluno se desenvolva matematicamente.

CAPÍTULO 4

CONSIDERAÇÕES FINAIS

Na atual realidade das escolas percebe-se a necessidade dos professores estarem buscando constantemente por metodologias diferenciadas que possam contribuir para a aprendizagem. Assim, no presente trabalho abordamos os tópicos que consideramos de grande relevância sobre a investigação matemática com o intuito principal de proporcionar ao leitor compreender essa metodologia e direcionar como pode ser a sua aplicação na sala de aula.

Compreende-se que a visão da matemática passível de erros, associada à investigação matemática, se orientada pelo professor de forma adequada, pode proporcionar aos estudantes a oportunidade de se apropriarem e desenvolverem os conhecimentos matemáticos, pois essa concede aos alunos momentos essenciais de aprendizagem, como a fase do desenvolvimento que envolve a formulação de questões, elaboração de conjecturas, testes e reformulação das conjecturas e, principalmente, a fase da discussão dos resultados.

Além disso, acredita-se que as atividades investigativas realizadas com os problemas da Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP) podem servir como base para a elaboração de atividades a serem aplicadas aos estudantes, visto que no decorrer do seu desenvolvimento notou-se que elas envolveram vários conceitos importantes da teoria dos números.

Dessa forma, espera-se que esse trabalho contribua significativamente para a compreensão da investigação matemática, ajudando, assim, professores e alunos no processo de ensino e aprendizagem a terem um novo olhar sobre a matemática.

BIBLIOGRAFIA

[1] BISPO, D. S. *Equações Diofantinas Lineares e sua aplicação.* 2013. 76 f. Monografia (Graduação em Licenciatura em Matemática)-Universidade Estadual do Sudoeste da Bahia, Vitória da Conquista, 2013. Disponível em: <http://www.uesb.br/mat/download/Trabamonografia/2013/Dinguiston.pdf>. Acesso em: 25 jan. 2018.

[2] BRAUMANN, C. A. *Divagações sobre investigação matemática e o seu papel na aprendizagem da matemática.* Centro de Investigação em Matemática e Aplicações. Universidade de Évora, 2002. Disponível em: <http://spiem.pt/DOCS/ATAS_ENCONTROS/2002/2002_02_CABraumann.pdf>. Acesso em: 11 mar. 2018

[3] BROCARDO, J. *As investigações na aula de matemática: Um projeto curricular no 8° ano.* 2001. 641 f. Tese (Doutorado) - Curso de Doutorado em Educação, Departamento de Educação da Faculdade de Ciências, Universidade de Lisboa, Lisboa, 2001. Disponível em: <http://repositorio.ul.pt/bitstream/10451/3101/1/ulsd041324_Joana_Brocardo.pdf> Acesso em: 10 mar. 2018

[4] CHAGAS, E. *Múltiplos, Divisores e Primos - Aula 2.* Polos Olímpicos de Treinamento Intensivo. Disponível em: <http://www.mat.ufpr.br/poti/documentos/arquivos/Aula%2002%20-%20Múltiplos%20Divisores%20e%20Primos.pdf>. Acesso em 08 fev. 2018.

[5] DAVIS, P.J; HERSH, R. *A Experiência Matemática.* Lisboa: Gradiva, 1995.

[6] FEITOSA, S. *O Algoritmo de Euclides - Aula 3*. Polo Olímpico de Treinamento. Disponível em: <http://poti.impa.br/uploads/material_teorico/c6aeewhejio8g.pdf>. Acesso em: 08 fev. 2018.

[7] FEITOSA, S. *Congruêcnias I - Aula 6*. Polos Olímpicos de Treinamento. Disponível em: <http://poti.impa.br/uploads/material_teorico/a1170g5pyrs4w.pdf>. Acesso em: 08 fev. 2018.

[8] FEITOSA, S. *Divisores - Aula 10*. Polos Olímpicos de Treinamento. Disponível em: <http://www.urantiagaia.org/educacional/matematica/teoria_numeros2/Aula 10-Divisores.pdf>. Acesso em: 09 fev. 2018.

[9] FOMIN, D.; GENKIN, S.; ITENBERG, I. *Círculos Matemáticos. A Experiência Russa*. Rio de Janeiro: IMPA, 2010.

[10] FREITAS, C. W. A. *Equações Diofantinas*. 2015. 201 f. Dissertação (Mestrado em Matemática)-Programa de Pós-Graduação em Matemática em Rede Nacional, Universidade Federal do Ceará, Fortaleza, 2015. Disponível em: <http://www.repositorio.ufc.br/bitstream/riufc/12990/1/2015_dis_cwafreitas.pdf>. Acesso em: 25 jan. 2018.

[11] HEFEZ, A. *Aritmética*. Coleção Profmat. Rio de Janeiro: SBM, 2014.

[12] IMPA. *Olimpíada Brasileira de Matemática das Escolas Públicas - OBMEP*. Provas e soluções. Disponível em:<http://www.obmep.org.br/provas.htm> Acesso em: 15 set. 2017

[13] LAKATOS, I. *A Lógica do Descobrimento Matemático: Provas e Refutações*. Rio de Janeiro: Zahar, 1978.

[14] LAMONATO, M.; PASSOS, C. L. B. *Discutindo resolução de problemas e exploração-investigação matemática: reflexões para o ensino de matemática*. Zetetiké-FE/Unicamp, v.19,n.36, p.51-74, jul/dez 2011. p. 51-74. Disponível em:<https://periodicos.sbu.unicamp.br/ojs/index.php/zetetike/article/view /8646625/13527>. Acesso em: 24 fev. 2018.

[15] MILIES, F. C. P; COELHO, S. P. *Números: Uma introdução à Matemática.* 3 ed. São Paulo: Universidade Estadual de São Paulo, 2001.

[16] MUNIZ NETO, A. C. *Tópicos de Matemática Elementar: teoria dos números.* Coleção do Professor de Matemática. Vol. 5. 2 ed. Rio de Janeiro: SBM, 2012.

[17] POLYA, G. *A Arte de Resolver Problemas.* Tradução e adaptação Heitor Lisboa de Araújo. Rio de Janeiro: Interciência, 1995.

[18] PONTE, J. P.; BROCARDO, J.; OLIVEIRA, H. *Investigações Matemáticas na Sala de Aula.* Belo Horizonte: Autêntica, 2005.

[19] RIBEIRO, R. *Equações Diofantinas: uma abordagem para o Ensino Médio.* 2014. 43 f. Dissertação (Mestrado em Matemática)- Programa de Mestrado Profissional em Matemática em Rede Nacional, Universidade de Brasília, Brasília, 2014. Disponível em: <http://repositorio.unb.br/bitstream/10482/17328/1/2014_RildoRibeiro.pdf> Acesso em: 04 fev. 2018.

[20] SANTOS, J. P. O. *Introdução à Teoria dos Números.* Coleção Matemática Universitária. Rio de Janeiro: IMPA, 1998.

[21] SILVA, G. H. G.; MOURA, A. Q. *O fabilismo de Lakatos e o trabalho com investigações matemáticas em sala de aula: possíveis aproximações.* Acta Scientiae,v.17, n.2, maio/ago. 2015. Disponível em: <https://www.researchgate.net/publication/286088226_O_falibilismo_de _Lakatos_e_o_trabalho_com_investigacoes_matematicas_em_sala_de_aula_possiveis _aproximacoes> Acesso em: 24 de fev. 2018.