

Betânia Almeida Lopes

**Demonstrações e investigações matemáticas  
básicas: um olhar sobre os números primos**

Alegre - ES

Abril de 2021

Betânia Almeida Lopes

## **Demonstrações e investigações matemáticas básicas: um olhar sobre os números primos**

Trabalho de conclusão de Curso apresentado ao Departamento de Matemática Pura e Aplicada da Universidade Federal do Espírito Santo como parte dos requisitos para a obtenção do título de Licenciado Pleno em Matemática.

Universidade Federal do Espírito Santo – UFES

Departamento de Matemática Pura e Aplicada

Orientador: Prof. Dr. Victor do Nascimento Martins

Alegre - ES

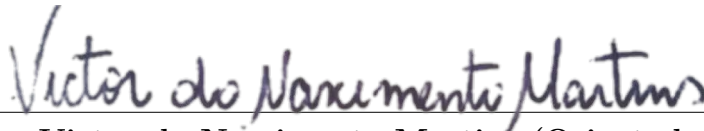
Abril de 2021

Betânia Almeida Lopes

## **Demonstrações e investigações matemáticas básicas: um olhar sobre os números primos**

Trabalho de conclusão de Curso apresentado ao Departamento de Matemática Pura e Aplicada da Universidade Federal do Espírito Santo como parte dos requisitos para a obtenção do título de Licenciado Pleno em Matemática.

Trabalho aprovado. Alegre - ES, 29 de Abril de 2021:



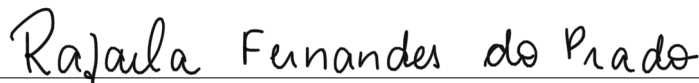
---

**Prof. Dr. Victor do Nascimento Martins (Orientador)**  
(DMPA/CCENS - UFES)



---

**Prof. Me. Bernardo Ignatowski Barcelos**  
(DMPA/CCENS - UFES)



---

**Prof<sup>a</sup>. Dra. Rafaela Fernandes do Prado**  
(IFB - campus Gama)

Alegre - ES  
Abril de 2021

# Agradecimentos

Primeiramente, agradeço à Deus por todas as bênçãos e sabedoria para me ajudar nos momentos mais conturbados em meio ao que vivemos, sem Ele nada disso seria possível.

Aos meus pais que me apoiaram, me ajudaram e sempre me motivaram, me dando forças para continuar. Me sinto imensamente agradecida por Deus ter me abençoado com vocês. Agradeço à minha irmã que me ajudou com sabedoria e entusiasmo em cada parte deste trabalho, sempre me dando sugestões, sanando dúvidas e me incentivando.

Aos meus companheiros de turma, Lucas e Bruno que estão comigo nesses 4 anos, pelas trocas de conhecimentos, experiências e vivências e por momento nenhum me deixaram desanimar, vocês foram verdadeiros amigos, levarei vocês para sempre em minha vida.

Aos meus amigos que nesses meses complicados de pandemia e exaustão mental tem sido verdadeiros motivadores, companheiros e tem me dado forças para continuar.

Ao meu orientador, Victor Martins que sem ele a realização deste trabalho não teria sido possível. Pelos conselhos, pela paciência e compreensão. Meu muito obrigado por ter mostrado a beleza da teoria dos números através dos números primos, sem você talvez eu não teria descoberto o mistério e loucura desses números incríveis.

Aos professores e colegas de graduação que passaram pela minha vida nesses anos, sou grata pelos ensinamentos, pelos conhecimentos trocados e transmitidos, pelas experiências, risadas e brincadeiras de descontração nesse percurso difícil.

Aos membros da banca examinadora que gentilmente aceitaram participar e colaborar com este trabalho.

Enfim, a todos que me ajudaram e acreditaram em mim, muito obrigada!

*“O gosto pelos mistérios dos números é raro... os encantos desta sublime ciência só revelam toda sua beleza àqueles que tem a coragem de perquiri-los.”*

*Carl Friedrich Gauss*

# Resumo

O presente trabalho tem como principal objetivo discutir a necessidade e a importância de utilizar investigações e demonstrações matemáticas ainda na educação básica. Levantamos discussões sobre o quanto benéfica pode ser a apresentação de investigações e demonstrações nas aulas de matemática na educação básica e como isso deve ser apresentado pelo professor, utilizando como base os conceitos e as ferramentas da teoria dos números. Para isso, apresentamos alguns resultados e definições do conjunto dos números inteiros, incluindo o teorema fundamental da aritmética. Mais especificamente nossa pesquisa sobre utilização de demonstrações e da investigação em aulas de matemática se pauta sobre os números primos. Mostramos o quanto a investigação matemática foi fundamental para a forma como os principais resultados e conjecturas se deram a partir da busca por padrões e fórmulas. Fazemos uma breve discussão sobre sua infinidade, sobre como foram e são descobertos e sobre sua distribuição no conjunto dos números inteiros. Desse modo, discutimos os principais tópicos sobre o tema que é ensinado na educação básica e apresentamos algumas ideias intuitivas de aulas e/ou atividades que utilizam demonstrações e investigações matemáticas a fim de incentivar o uso das ferramentas didáticas na educação básica sobre o tema.

**Palavras-chaves:** Números primos, educação básica, investigações e demonstrações matemáticas.

# Sumário

	<b>Introdução</b> . . . . .	<b>7</b>
<b>1</b>	<b>DEMONSTRAÇÕES E INVESTIGAÇÕES MATEMÁTICAS</b> . . . . .	<b>9</b>
1.1	Aulas investigativas . . . . .	10
1.2	Números inteiros em aulas investigativas . . . . .	12
<b>2</b>	<b>NÚMEROS PRIMOS</b> . . . . .	<b>18</b>
2.1	A importância dos números primos . . . . .	19
2.2	Aplicações . . . . .	20
2.3	A busca por padrões e fórmulas . . . . .	22
2.4	Distribuição dos números primos . . . . .	27
<b>3</b>	<b>INVESTIGAÇÕES SOBRE NÚMEROS PRIMOS NO ENSINO FUN-</b> <b>DAMENTAL</b> . . . . .	<b>31</b>
3.1	As fases de uma aula investigativa . . . . .	32
3.2	Alguns exemplos de atividades investigativas e demonstrativas pau- tadas sobre os números primos . . . . .	33
	<b>Considerações Finais</b> . . . . .	<b>41</b>
	<b>REFERÊNCIAS</b> . . . . .	<b>42</b>

# Introdução

Os números primos foram descobertos há mais de 2 mil anos através de investigações matemáticas e desde então geram bastante dúvidas a respeito de seus padrões, fórmulas, distribuição e aplicações. Este é um dos principais conceitos matemáticos que atualmente são ensinados no 6º ano do ensino fundamental e esses conteúdos fazem parte da base do conhecimento matemático ao longo da educação básica. É através deles que aprendemos diversos conceitos como critérios de divisibilidade, soma e subtração de frações que utilizam o mínimo múltiplo comum, decomposição de números naturais bem como a aplicabilidade na criptografia e segurança de dados, por exemplo. No entanto, esses conceitos são vistos de maneira bastante breve. Dessa forma, não recebem, em geral, seu merecido destaque que deixaria mais clara sua relevância.

A teoria dos números apresenta conceitos que, à primeira vista, são de fácil entendimento como, por exemplo, a definição de número primo, que diz que um número natural maior do que 1 é um número primo se ele é divisível apenas pelo número um e por ele mesmo. Apesar da simplicidade dos conceitos existem muitas perguntas sem respostas e isso faz com que muitas pessoas se interessem a estudar sobre o tema.

Os números primos ostentam uma parcela instigante dessas perguntas sem respostas. Esses fascinantes números transmitem mistério e loucura para quem se dispõe a estudá-los. A fim de buscar uma alternativa para apresentar os números primos e seus conteúdos relacionados ensinados na educação básica, investigamos como os principais nomes da história dos números primos chegaram no que sabemos até hoje, ressaltando seus aspectos históricos, importância e motivações investigativas, aplicações e resultados visando tornar o ensino de matemática mais atrativo e interessante. Essa necessidade foi observada a partir de estudo orientado e de uma vasta revisão bibliográfica.

Apresentamos, no Capítulo 1 deste trabalho, uma breve discussão sobre como o ensino de matemática pode ser mais eficiente quando diferentes ferramentas de ensino são apresentadas aos alunos. E que implementar melhorias no ensino, de forma que estes tenham mais autonomia, faz com que o processo de ensino-aprendizagem tenha melhores resultados. Vamos observar que essas metodologias podem ser feitas através de aulas investigativas e demonstrativas e que estas auxiliam no pensamento crítico, criativo e construtivo do aluno, bem como do professor. Apontamos os principais argumentos que defendem o uso dessa metodologia, respaldados por documentos oficiais e de investigações



de autores sobre o assunto.

Além disso, destacamos algumas definições e alguns resultados importantes da teoria dos números, especificamente sobre o conjunto dos números inteiros. Desse modo, apresentamos alguns exemplos e ideias que podem ser utilizadas em sala de aula ou em monitorias e atividades extra-curriculares, bem como algumas definições do conjunto dos números inteiros.

No Capítulo 2, mostraremos que investigações matemáticas enquanto ferramenta no desenvolvimento de uma teoria pode ser motivador e natural para geração de novos resultados e teorias. Apresentamos a evolução dos números primos, partindo da definição e de alguns dos principais resultados e prosseguindo com uma discussão sobre algumas aplicações, a busca por padrões e fórmulas, conjecturas e distribuição dos números primos no conjunto dos números inteiros. Por fim, destacamos como as investigações matemáticas foram fundamentais para evolução da teoria.

No Capítulo 3 e último do trabalho, discutimos sobre os tópicos da teoria dos números, especificamente do 6º ano, mostrando o que os alunos vêem sobre números primos e conteúdos relacionados. Demos apontamento para as fases de uma aula investigativa fazendo conexão com os capítulos anteriores e trazendo uma visão geral de como o professor pode se organizar no planejamento desse tipo de aula. A última seção deste capítulo foi dedicada a apresentar alguns breves exemplos de aulas e atividades que envolvem investigações e demonstrações sobre os tópicos da teoria dos números vistos no ensino fundamental, com o intuito de auxiliar o professor na busca por aulas mais atrativas, fazendo com que os alunos possam vir a ter mais interesse e maior absorção de conhecimento no estudo desse conteúdo tão importante e enigmático.

Em um momento em que tanto se fala na utilização de metodologias ativas no processo de ensino, esperamos, com este trabalho, iniciar e incentivar uma discussão sobre a utilização de aulas investigativas na educação básica, especialmente no ensino dos tópicos da teoria dos números. Além disso, esperamos que os leitores, principalmente licenciandos e licenciados em matemática, reflitam sobre a apresentação de algumas demonstrações matemáticas já na educação básica, como forma de solidificar a aprendizagem da disciplina.

# 1 Demonstrações e investigações matemáticas

Nos últimos anos, tem-se discutido bastante a respeito do ensino de matemática na educação básica no Brasil. Mudanças no currículo têm levantado questões importantes, a fim de redirecionar o caminho do ensino de matemática, tornando-o mais consistente e eficaz.

As discussões levantadas sobre o ensino de matemática na educação básica, trata, entre outras coisas, de questões como a importância das investigações matemáticas em que o aluno (re)constrói o conhecimento, discute, cria hipóteses e conjecturas baseado no que pesquisou e observou sobre determinado conteúdo. Essa perspectiva, segundo (LAMONATO; PASSOS, 2011) “possibilita ao aluno pensar a partir de uma dinâmica que prevê observações, descobertas, erros, acertos e, fundamentalmente, decisões.”

“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. [...] 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 apud (PONTE; BROCARDO; OLIVEIRA, 2016, p. 19)).

Em uma aula de investigação matemática, o aluno é instigado a agir como um matemático de modo a formular, investigar, conjecturar, discutir e apresentar seus resultados. A Base Nacional Comum Curricular, (BRASIL, 2019), cita como competências do ensino de matemática, no ensino fundamental, uma formação contemplada a partir de raciocínio, comunicação, argumentação e representação. De acordo com o documento, “os conhecimentos a serem adquiridos devem estimular processos mais elaborados de reflexão e de abstração, que dêem sustentação a modos de pensar que permitam aos estudantes formular e resolver problemas em diversos contextos com mais autonomia e recursos matemáticos, a fim de desenvolver habilidades relativas aos processos de investigação, de construção de modelos e de resolução de problemas.”

Além disso, a Secretaria de Estado da Educação do Espírito Santo, (SANTO, 2019), defende o uso de técnicas concretas no ensino de matemática. Apesar de tratar superficialmente e não citar efetivamente o uso de demonstrações, é possível entender o

interesse pelo ensino mais sólido e eficaz, no intuito dos alunos serem mais efetivos no próprio aprendizado.

Na visão de Lakatos e Palomar (1978, 2004 apud (SANTO, 2019)) “a matemática é uma atividade humana que contém nela uma lógica de conjecturas, refutações e demonstrações até chegar às conclusões e que cada vez mais deve ser deixada de lado a resolução de problemas de maneira mecânica ou a memorização de processo.”

Mencionadas e discutidas as visões de documentos oficiais, como a BNCC e as orientações da SEDU-ES, sobre como a matemática pode ser mais atraente para os alunos e como processos de investigações matemáticas podem ser importantes aliados no ensino de matemática na educação básica, abordaremos um pouco sobre o que é uma investigação matemática e o que autores falam sobre o assunto.

## 1.1 Aulas investigativas

Em matemática, investigar é descobrir as relações entre objetos matemáticos conhecidos ou não, buscando identificar algumas propriedades. Nesse contexto, investigar não significa, necessariamente, trabalhar com problemas difíceis. Significa trabalhar com questões instigantes de modo que a incerteza da apresentação inicial torne-se um aprendizado claro e organizado ao final do processo.

“O pensamento investigativo, o crítico e o criativo ampliam as possibilidades ou alternativas para tomar decisões, propor soluções, articular informações, decidir no que acreditar, avaliar se uma argumentação, procedimentos ou resultados são viáveis. Identificam hipóteses, implícitas ou explícitas na argumentação, e rejeitam conclusões e pensamentos tendenciosos, avaliando a credibilidade das fontes de informação” (SANTO, 2019, p. 36).

Nessa perspectiva, o professor desempenha um importante papel nesse processo, pois é ele quem guia o aluno na construção do saber contemplado através de investigações matemáticas. Para isso, as instruções devem ser claras, precisas e devem ser instigantes de tal forma que os alunos entendam o que tem que ser feito e se sintam instigado com a tarefa a ser feita.

“[...] o professor tem um papel determinante nas aulas de investigação. [...] o professor deve procurar interagir com os alunos tendo em conta as necessidades particulares de cada um e sem perder de vista os aspectos mais gerais de gestão da situação didática. Desse modo, o professor é chamado a desempenhar um conjunto de papéis: desafiar os alunos, avaliar o seu progresso, raciocinar matematicamente e apoiar o trabalho deles” (PONTE; BROCARDO; OLIVEIRA, 2016, p. 47).

Quando se aborda aulas investigativas é imprescindível discutir sobre o rigor matemático – métodos de provas, demonstrações e práticas matemáticas – a ser cobrado

dos alunos em suas considerações finais. Para isso, o professor deve possuir uma certa experiência com demonstrações e, conseqüentemente, com os métodos e rigor matemático. Certamente, os alunos devem estar familiarizados com tais procedimentos, de forma que seus argumentos se tornarão cada vez mais seguros e precisos, assim como seus métodos e práticas.

Para (LIMA, 2007), as demonstrações que podem ser feitas na educação básica não podem e/ou devem ser óbvias e/ou evidentes do ponto de vista intuitivo. Também não devem apresentar passos lógicos, argumentos e técnicas difíceis. Para ele, devem ser fáceis mas intuitivamente não evidentes e talvez elegantes, isto é, devem exigir que os alunos questionem e pensem sobre a veracidade do resultado, fazendo com que os alunos desenvolvam assim, interesse.

Tendo em vista a discussão acima, apresentaremos a seguir um exemplo clássico de um teorema que poderia ser demonstrado em sala de aula, o Teorema de Pitágoras.

### Teorema de Pitágoras

O teorema de Pitágoras é uma importante relação matemática sobre triângulos retângulos, que diz que dado um triângulo retângulo qualquer, o quadrado do comprimento da hipotenusa ( $c$ ) é igual à soma dos quadrados dos comprimentos dos catetos ( $a$  e  $b$ ). Ou seja,  $c^2 = a^2 + b^2$ .

### Estratégia para a demonstração do Teorema de Pitágoras

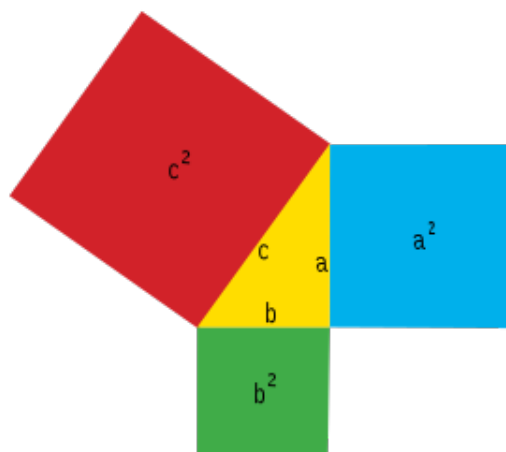
Na Figura 1 vemos uma representação geométrica do teorema de Pitágoras. Se construirmos quadrados sobre os catetos  $a$  e  $b$ , a soma das áreas dos quadrados de lados  $a$  e  $b$ , equivale à área do quadrado construído sobre a hipotenusa  $c$ .

A demonstração do teorema de Pitágoras pode ser feito utilizando softwares animados como GeoGebra, onde encontra-se diversos modelos prontos disponibilizados, um deles é <<https://www.geogebra.org/m/jFFERBdd#material/ZFTGX57r>> e vídeos do YouTube que utilizam experimentos. A demonstração desse resultado foi omitida, pois além de ser extensa para a figura apresentada não é o foco deste trabalho.

A apresentação das demonstrações de alguns resultados pode chamar a atenção dos alunos para a beleza da matemática. Estas além de convencerem os alunos de resultados com base na razão, também proporcionam para os mesmos o senso crítico das inquietações, investigações matemáticas e raciocínio lógico-dedutivo, bem como um amplo conhecimento matemático interpretativo e um aprendizado mais dinâmico e interessante.

Este processo pode amenizar as aulas de resolução mecânica através de fórmulas e problemas sem um sentido claro apresentados durante seus anos no ensino básico, fazendo

Figura 1 – Representação do teorema de Pitágoras.



Fonte: Wikipédia.

com que alunos se interessem pela matemática e conseqüentemente, grandes possibilidades de diminuição dos níveis de reprovações pela matéria.

“[Os alunos podem ter] um sabor da matemática em construção e do trabalho criativo e independente... [Eles podem] generalizar a partir da observação de casos, [usar] argumentos por analogia, reconhecer ou extrair um conceito matemático de uma situação concreta.” (PÓLYA, 1981, p. 157 e 101 apud (PONTE; BROCARD; OLIVEIRA, 2016, p. 19)).

## 1.2 Números inteiros em aulas investigativas

A teoria dos números tem um papel de destaque na educação básica. Apesar de alguns resultados apresentarem demonstrações que exigem uma certa maturidade dos alunos com a matemática e suas técnicas, alguns resultados podem ser utilizados em aulas investigativas. Além de mostrar aos alunos os principais resultados que eles estudam ao longo dos anos, mostra-lhes também a relevância desses resultados em conteúdos diversos e para a matemática.

Basicamente, a teoria dos números no ensino fundamental consiste no estudo dos números inteiros e estes números são facilmente assimilados pelos estudantes. Estes estão entre os principais tipos de números que utilizamos em nosso cotidiano. Os números inteiros ocupam um lugar de destaque na matemática escolar, principalmente no ensino fundamental - anos finais, mais precisamente entre o 6º ano e o 8º ano do ensino fundamental.

Alguns objetos de conhecimentos citados pela BNCC, isto é, base mínima de conteúdos que devem ser ensinados aos alunos são:

- Operações com números inteiros;

- Divisão euclidiana;
- Múltiplos e divisores de um número inteiro;
- Usos e história;
- Ordenação e associação entre pontos da reta numérica e o conjunto dos números inteiros.

Entre os objetos de conhecimentos citados pela BNCC, vamos apresentar alguns resultados que podem ser abordados em aulas investigativas e demonstrativas. Apresentaremos algumas das principais definições e resultados da teoria dos números, que acreditamos que seriam interessantes de serem apresentados utilizando aulas investigativas visando um melhor aprendizado e compreensão sobre o conteúdo e importância destes. Para um maior aprofundamento nos resultados aqui apresentados, sugerimos (VIDIGAL, 2005) ou (TENGAN, 2018).

## Divisibilidade, mdc e mmc

Para alunos que estão descobrindo uma nova matemática, diferente daquela ensinada por pedagogos (que embora façam um ótimo trabalho muitas vezes, não têm formação em matemática e ensinam o básico) apresentar resultados como o lema a seguir, é de suma importância. Professores podem apresentá-lo de maneira geral e solicitar aos alunos que tentem chegar a resultados contrários, a fim de observarem e tirarem suas próprias conclusões acerca do resultado.

A demonstração desse resultado em si exige um nível de conhecimento matemático consideravelmente maior do que os alunos dessa idade (11 - 13) apresentam. Entretanto fica a cargo do professor (que tem conhecimento amplo sobre sua turma) apresentá-lo ou não.

**Lema 1.1.** *Dados dois números naturais  $a$  e  $b$ , com  $b \neq 0$ , existem naturais  $q$  (quociente) e  $r$  (resto), unicamente determinados, tais que  $a = bq + r$ , em que  $0 \leq r < b$ .*

Dados dois inteiros  $a$  e  $b$  dizemos que  $b$  **divide**  $a$  se existe um número inteiro  $q$  tal que  $a = bq$ . Caso contrário, dizemos que  $b$  **não divide**  $a$ . Quando  $b$  dividir  $a$  denotaremos por  $b \mid a$ , isto é, existe  $q \in \mathbb{Z}$  tal que  $a = bq$ . E se  $b$  não dividir  $a$ , denotaremos por  $b \nmid a$ , isto é, não existe  $q \in \mathbb{Z}$  tal que  $a = bq$ .

Por exemplo, escolhendo os números 2, 9 e 18 temos que:

- $9 \mid 18$ ,  $18 = 2 \cdot 9$  e  $2 \in \mathbb{Z}$ .

- $2 \nmid 9$ , pois  $\nexists q \in \mathbb{Z}$  tal que  $9 = 2 \cdot q$ .

Agora considere dois inteiros  $a$  e  $b$ , simultaneamente não nulos. Quando falamos de divisão, a cada número podemos associar um conjunto de divisores,  $D_a$  e  $D_b$ . A intersecção desses dois conjuntos não é vazia, pois 1 pertence a ambos. Seja o conjunto da intersecção, ele é finito, uma vez que o maior elemento de  $D_a$  e o maior elemento de  $D_b$  são menores que  $a$  e  $b$ , respectivamente. O maior elemento da intersecção de  $D_a$  e  $D_b$  é chamado de **máximo divisor comum** de  $a$  e  $b$  e será denotado por  $mdc(a, b)$ .

Por outro lado, também podemos associar os múltiplos positivos comuns de dois números inteiros  $a$  e  $b$ , ou seja, a intersecção dos conjuntos de múltiplos de cada um dos dois números. Esse conjunto (da intersecção) possui um menor elemento. Tal número é chamado **mínimo múltiplo comum** e denotado por  $mmc(a, b)$ .

Formalmente temos:

**Definição 1.1.** *Dados dois inteiros  $a$  e  $b$ , não simultaneamente nulos, dizemos que um inteiro  $m$  é o **máximo divisor comum** de  $a$  e  $b$  e escrevemos  $m = mdc(a, b)$  se:*

- (i)  $m \mid a$  e  $m \mid b$ ;
- (ii) Se existe um inteiro  $c$  tal que  $c \mid a$  e  $c \mid b$  então  $c \leq m$ .

**Definição 1.2.** *Um número inteiro  $n$  é o **mínimo múltiplo comum** dos números não nulos  $a$  e  $b$  ( $mmc(a, b) = n$ ) se:*

- (i)  $n > 0$ ;
- (ii)  $a \mid n$  e  $b \mid n$ ;
- (iii) se existe um inteiro  $c > 0$  tal que  $a \mid c$  e  $b \mid c$  então  $n \leq c$ .

Quando  $a$  e  $b$  são números inteiros tais que  $mdc(a, b) = 1$ , dizemos que  $a$  e  $b$  são **primos entre si**. E, por consequência, o  $mmc(a, b) = ab$ .

Um assunto consideravelmente importante em matemática e pouco explorado na educação básica é o dos números primos. Basicamente, um número inteiro positivo é primo se tiver apenas dois divisores positivos, 1 e ele próprio. Uma ideia de aula investigativa com um olhar sobre estes números poderia ser introduzindo o Teorema Fundamental da Aritmética. Uma simples pergunta ou atividade instigante acerca da decomposição de todos os números inteiros. Por exemplo, propor aos alunos decomposições de alguns números inteiros, levantando alguns questionamentos sobre o processo, observações e resultados.

**Teorema Fundamental da Aritmética:** Dado um número natural  $n > 1$ , existem primos  $p_1 < p_2 < \dots < p_r$  e  $\alpha_1, \alpha_2, \dots, \alpha_r \in \mathbb{N}^*$ , univocamente determinados, tais que

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}.$$

A demonstração desse teorema marca a importância dos números primos para a construção de todos os números maiores que 1. É o início de uma nova matemática, esta que solidifica a base dos blocos de construção de um edifício gigante, que é a matemática. Em resumo, os números primos são a base dessa construção. Todos os números compostos (inteiro positivo  $n$  maior do que 1, escrito como  $n = ab$  com  $1 < a < n$  e  $1 < b < n$ ) podem ser decompostos em pequenas partes, como os átomos do universo, cada elemento é formado por pequenas partículas de maneira única, assim é com os números, os números primos são essas pequenas partículas que compõem todos os números inteiros, e a partir desses, todos os outros números.

## Indução

O princípio de indução é um dos mais importantes métodos de prova da matemática. Com ele provamos uma proposição (uma afirmação) verificando apenas duas condições. Mostrar esse tipo de método para alunos do ensino fundamental é bem interessante e, caso seja possível fazer isso, o professor pode optar por uma abordagem menos rigorosa. O método é de fácil entendimento e pode ser aplicado em atividade investigativa e lúdica como no jogo da Torre de Hanói.

O jogo consiste de  $n$  discos de diâmetros distintos com um furo no seu centro e uma base onde estão fincadas três hastes. Numa das hastes estão enfiados os discos de modo que nenhum disco esteja sobre um outro de diâmetro menor. O jogo consiste em transferir a pilha de discos para uma outra haste, deslocando um disco de cada vez, de modo que, a cada passo, a regra acima seja observada.

Figura 2 – Torre de Hanói



Fonte: (HEFEZ, 2006).

A atividade consiste em mostrar aos alunos o jogo, explicá-lo e colocá-los para jogar com 3 discos apenas. O/A professor/a questiona aos alunos se daria para jogar



com 4 discos, depois 5 discos podendo deixar os alunos jogarem e tirarem suas próprias conclusões. Até que o/a professor/a pergunta aos alunos se daria para jogar com  $n$  discos, solicitando que a turma reflita, discuta e justifique cada resposta. Essa é uma maneira bastante descontraída de apresentar esse prestigiado método de prova matemático.

### Princípio de indução finita

Seja  $n_0$  um número inteiro e suponha que para cada inteiro  $n$ , se tenha uma proposição  $P(n)$ . O chamado **princípio de indução finita**, consiste em verificar duas etapas para provar uma proposição:

- (1) (base da indução)  $P(n_0)$  é verdadeira e;
- (2) (passo indutivo) Se  $P(n)$  é verdadeira para algum número inteiro  $n \geq n_0$ , então  $P(n + 1)$  também é verdadeira.

Ou seja, verificamos que a proposição é verdadeira para o valor inicial  $n = n_0$ . No próximo passo utilizamos a validade da proposição para um dado  $n$  (chamada hipótese de indução) para provar a validade da mesma para o número inteiro seguinte  $n+1$ . Daí, se verificadas as duas etapas, dizemos que  $P(n)$  é verdadeira para todo número inteiro  $n \geq n_0$ .

Para uma compreensão mais efetiva do processo de demonstração por indução, apresentamos a seguir um exemplo de aplicação do resultado. Obviamente, não estamos indicando aqui que demonstrações como a do exemplo devem ser apresentadas a alunos do ensino fundamental. Nosso objetivo é simplesmente deixar o passo a passo formal dessas demonstrações registrado aqui neste trabalho.

**Exemplo 1.** *Vamos mostrar que a soma dos  $n$  primeiros números inteiros positivos pares é  $n(n + 1)$ , isto é,*

$$2 + 4 + 6 + 8 + \dots + 2n = n(n + 1), \quad \forall n \geq 1.$$

*Fazendo indução sobre  $n$  temos:*

(i) *Para  $n = 1$ , o resultado é válido, pois*

$$2 = 1(1 + 1).$$

(ii) *Suponha por hipótese de indução (H.I) que o resultado é válido para  $n = k$ , isto é,*

$$2 + 4 + 6 + 8 + \dots + 2k = k(k + 1).$$

(iii) Devemos mostrar que o resultado é válido para  $n = k + 1$ , isto é

$$2 + 4 + 6 + 8 + \dots + 2k + 2(k + 1) = (k + 1)(k + 2).$$

De fato, para  $n = k + 1$ , temos

$$\underbrace{2 + 4 + 6 + 8 + \dots + 2k}_{k(k+1)} + 2(k + 1) \stackrel{H.I}{=} k(k + 1) + 2(k + 1) = (k + 1)(k + 2),$$

como queríamos demonstrar. Portanto,

$$2 + 4 + 6 + 8 + \dots + 2n = n(n + 1)$$

para todo  $n \geq 1$ .

## 2 Números Primos

Os números primos fascinam os matemáticos desde o seu surgimento. Naturalmente esses números já despertam bastante curiosidades e instigam muitos matemáticos e curiosos do assunto. Para muitos, seus mistérios talvez nunca serão revelados, outros já acreditam que o poder da mente humana pode solucionar qualquer problema relacionado a esses números. Alguns outros até mesmo duvidam de toda a base dessa construção matemática, os números primos. Acreditam que a qualquer momento a base dessa construção irá desmoronar. Afinal, os segredos desses números geradores não foram descobertos até hoje, e parece estarmos longe de desvendar seus mistérios.

Por definição, um número inteiro  $n$  maior que 1 é primo se sempre que escrevermos  $n = a \cdot b$ , com  $a$  e  $b$  inteiros positivos, temos necessariamente  $a = 1, b = n$  ou  $a = n, b = 1$ . Consequentemente um número inteiro  $n$  maior que 1 é composto se existem inteiros positivos  $a$  e  $b$ , com  $1 < a < n$  e  $1 < b < n$ , tais que  $n = ab$ . O número 1 tem apenas um divisor, logo não é considerado primo. E pelo Teorema Fundamental da Aritmética, como o número 1 não é escrito como uma multiplicação de números primos (não pode ser fatorado) este também não é considerado um número composto, sendo tratado apenas como a unidade. Por exemplo 2, 3, 5, 7, 11 são números primos. E 4, 6, 9, 10, 12 são números compostos.

Veremos que não fora por falta de tentativas, gênios matemáticos, assim considerados, se debruçaram sobre livros e cadernos ao longo dos anos para tentar decifrá-los. A busca por padrões e fórmulas, levou matemáticos a conjecturarem resultados que nem eram capazes de verificar. Outros nem viveram para ver todos os resultados de suas conjecturas, morreram acreditando que suas fórmulas mudariam o mundo matemático dos primos. Mesmo assim, tiveram seu nome gravado na história, talvez não do jeito que queriam ou esperavam. Alguns obtiveram sucesso em tirar uma pequena parcela do que esses números escondem, alguns pequenos resultados diante da imensidão dos primos.

Essa busca por padrões e fórmulas dos números primos, feita através de investigações matemáticas, nos mostra o quanto a investigação é importante para o descobrimento de novas teorias, fórmulas e para a construção da matemática em si.

No entanto, é importante ressaltar que uma investigação matemática nem sempre nos trará os resultados que esperamos ou buscamos quando as começamos. Ao longo desta, caminhos podem ser encerrados e/ou iniciados. Quando começamos uma investigação sobre determinado assunto, não sabemos ao certo o que iremos encontrar, por isso é importante estarmos atentos aos assuntos que estão ligados ao que estamos estudando, pois podemos nos deparar com descobertas importantes.

“Quando trabalhando num problema, o nosso objetivo é, naturalmente, resolvê-lo. No entanto, para além de resolver o problema proposto, podemos fazer outras descobertas que, em alguns casos, se revelam tão ou mais importantes que a solução do problema original. Outras vezes, não se conseguindo resolver o problema, o trabalho não deixa de valer a pena pelas descobertas imprevistas que proporciona” (PONTE; BROCARDO; OLIVEIRA, 2016, p. 17).

Euclides como foi o primeiro e o principal nome dessa história. Conseguiu descobrir um dos principais importantes resultados dos números primos. Com um toque de mestre, provou que existem infinitos números primos. O resultado que deu início a história dos primos que virá a seguir, apesar de não estar completa. Existem lacunas a serem cobertas e, sobre elas, conjecturas importantes para tentarmos compreender melhor a imensidão que esses números nos reservam.

## 2.1 A importância dos números primos

Os números primos são um dos números mais importantes da matemática e isso é inegável. É com eles que formamos todos os números inteiros, e com estes criamos todo o universo matemático numérico. O estudo dos números primos vem sendo desenvolvido há mais de 2 mil anos. No entanto, todos os mistérios envolvendo tais números ainda não foram descobertos.

Quando se definiu o que eram os números primos, muitos estudiosos gregos pensaram que se escrevessem todos os números primos em uma tabela teriam seu nome gravado na história da matemática. Diante desse pensamento iniciou-se então a corrida para conseguir o feito, mas o que ninguém previu era que quem havia definido os tais números primos também haveria de provar que eles são infinitos.

Muitas dúvidas surgem acerca desse assunto. Por exemplo, como verificamos a prova de Euclides se não sabemos todas as propriedades desses números? Para um matemático fica claro que a prova que Euclides apresentou é realmente sólida. A verdade é que ninguém é capaz de apresentar um argumento consistente que faça-nos duvidar de Euclides. David Hilbert, um matemático visionário dos anos 80, começou a se questionar sobre o que se havia construído ao longo dos anos sobre esses determinados números, porém a prova matemática de Euclides é tão forte que defende o castelo de blocos firmes para erguer toda a matemática por trás dos números primos. Euclides é considerado dentro da matemática, como pai da arte da prova.

A demonstração que Euclides apresentou foi de extrema facilidade e com um toque de gênio. E é por isso que leva no teorema o próprio nome e é um dos resultados mais fundamentais da teoria dos números.

**Teorema 2.1** (Teorema de Euclides). *O conjunto formado pelos números primos é infinito.*

**Demonstração:** Seja  $A$  uma lista finita qualquer de números primos, a saber,

$$A = \{p_1, p_2, p_3, \dots, p_n\}.$$

Vamos mostrar que existem números primos que não estão nessa lista.

Seja  $p$  o produto de todos os números primos na lista, isto é,  $p = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n$  e seja  $q = p + 1$ . Então,  $q$  pode ser primo ou não:

- Se  $q$  é primo então há pelo menos um número primo a mais que não está listado;
- Se  $q$  não é primo, então algum fator primo  $p_1, p_2, p_3, \dots, p_n$  divide  $q$  e este fator não pode estar na lista  $A$ , pois ao dividirmos  $q = p + 1$  por algum  $p_i$ , sempre teremos resto igual a 1, isso significa que  $p$  não pode estar na lista. Absurdo.

Isso prova que para qualquer lista finita de números primos há um número primo que não está na lista. Portanto, existem infinitos números primos. ■

Fica claro que para essa demonstração ser totalmente consistente, ela tem que ter como base o Teorema Fundamental da Aritmética, visto na Seção 1.2. Sem ele a demonstração não seria possível.

## 2.2 Aplicações

Os números primos não ficam presos somente à aplicação direta do Teorema Fundamental da Aritmética. Estes números estão ligados à segurança de dados (cartões de crédito, comunicação e transações financeiras). Esta segurança de dados é chamada de criptografia que, em grego, *cryptos* significa secreto, oculto.

A criptografia estuda os métodos para codificar uma mensagem de modo que somente seu destinatário legítimo possa interpretá-la. Existem métodos bem simples que são os que consistem em transladar uma letra do alfabeto pela seguinte. Assim como existe a criptografia que codifica uma mensagem, existe também a criptoanálise que decifra uma mensagem, ou seja, quebra o código da mensagem codificada.

Todo código possui dois algoritmos fundamentais. O primeiro utilizado para codificar uma mensagem e o segundo é responsável pela decodificação de uma mensagem. Decodificar é o que um usuário legítimo do código faz quando recebe uma mensagem codificada e deseja lê-la. Quando alguém decifra uma mensagem codificada significa que ele leu uma mensagem codificada recebida sem ser o destinatário legítimo da mesma.

No mundo moderno da internet, onde milhões de transações comerciais entre bancos, pessoas, empresas entre outras situações são feitas, foi preciso que novos métodos e códigos mais difíceis fossem criados, a fim de garantir que uma “mensagem” pudesse ser enviada e

entregue ao destinatário certo. Esses novos códigos foram criados exclusivamente para o uso de aplicações comerciais e são chamados de *criptografia de chave pública*. A criptografia de chave pública foi proposta inicialmente em 1976, em um artigo seminal escrito por dois matemáticos da Universidade de Stanford, na Califórnia, Whit Diffie e Martin Hellman.

Nas palavras de (SAUTOY, 2008, p. 243), “o sistema de criptografia de chave pública é como uma porta com duas chaves diferentes: a chave A tranca a porta, mas uma chave diferente, B, a destranca.”

O RSA (Rivest-Shamir-Adleman) é o método de criptografia de chave pública mais conhecido e usado no mundo e tem como base do seu código, números primos. O RSA foi criado por Ron Rivest, Adi Shamir e Leonard Adleman em 1978. Para poder implementar o RSA precisamos de dois parâmetros básicos, que consiste em dois *números primos*  $p$  e  $q$  e para codificar uma mensagem usando o RSA é suficiente conhecer o produto  $n$  destes dois primos. A *chave de codificação* do RSA é, portanto, constituída essencialmente pelo número  $n = pq$ . Cada usuário do método tem sua própria chave de codificação. Esta chave é tornada pública, daí  $n$  também é conhecido como a chave pública. Já a *chave de decodificação* é constituída pelos primos  $p$  e  $q$ . Cada usuário tem que manter sua chave de decodificação secreta ou a segurança do método estará comprometida.

A segurança do RSA depende totalmente da chave de criptografia  $n$ , embora pareça simples quebrar a segurança do RSA, pois se soubermos qual o valor de  $n$  basta fatorarmos e encontrarmos os fatores primos ( $p$  e  $q$ ) e assim quebrarmos a criptografia. Porém, atualmente não existe uma tecnologia ou método para fatorar tais números, uma vez que a chave de criptografia do RSA utiliza números muito grandes – números de mais de 150 algarismos – e fatorar esse número levaria milhares de anos. A ineficiência do mundo matemático (ou não matemático) de decifrar os números primos garante a segurança da era da internet. Para uma explicação mais detalhada sobre a criptografia, em especial o método RSA, e os elementos matemáticos envolvidos no assunto, sugerimos (COUTINHO, 2011).

Os números primos aparecem não só na matemática, como também na natureza. Em (SAUTOY, 2008, p. 36) são apresentadas duas espécies de cigarras que viviam em uma mesma floresta. O ciclo de vidas dessas duas espécies eram de 17 e 13 anos, respectivamente. O ciclo de vida de uma cigarra consiste em permanecer no solo durante toda sua vida exceto durante o último ano, em que as ninfas sofrem metamorfose, transformam-se em adultos e emergem do solo em massa. Em uma noite elas tomam contas das florestas num evento de canto para alimentação e acasalamento. Assim, colocam seus ovos e morrem seis semanas depois. A floresta permanece em silêncio até a próxima espécie emergir.

Ao longo dos anos surgiram algumas possíveis explicações do porquê dessas espécies de cigarras escolherem um ciclo de vida com um número primo. As espécies viviam em uma mesma floresta e com o ciclo de vida sendo um número primo, a sincronização dos

ciclos de vidas são raros, ou seja, elas raramente vão emergir no mesmo período, pois isso só aconteceria a cada  $221=17 \times 13$  anos. Suponha que essas espécies tivessem escolhido os números não primos 12 e 16, durante o mesmo período de tempo (221 anos) a emergência dessas cigarras estariam sincronizadas 4 vezes, nos anos 48, 96, 144 e 192. A "escolha" de números primos faz com que essas cigarras evitem competir pelo ambiente.

A outra possível explicação é o surgimento de um fungo que era letal para essas duas espécies de cigarras e emergiam no mesmo período que as cigarras. Atentando para o surgimento do fungo as espécies desenvolveram ciclos de vida que o evitassem. Da mesma maneira que as espécies se evitavam, escolhendo números primos para seus ciclos de vida, o mesmo acontecia com os fungos adotando os números primos 17 e 13 anos para o tempo de seus ciclos de vida. As cigarras se certificariam que não emergiriam no mesmo período dos fungos com tanta frequência como se escolhessem ciclos de vida com números não primos. Os números primos se tornaram não apenas números comuns para os ciclos de vida das cigarras mas números que garantiam a sua sobrevivência.

Apesar de apresentarmos poucos exemplos de aplicações nessa seção, encontrar aplicações e a presença dos números primos no dia a dia não é algo difícil. O que nos faz notar que os números primos são altamente importantes para a matemática, segurança da internet, mundo financeiro e além disso, que a natureza se “desenvolve” utilizando a matemática dos números primos.

## 2.3 A busca por padrões e fórmulas

Embora alguns estudos apontem que os primeiros a descobrirem os números primos foram os chineses, até onde se sabe, a primeira pessoa a estudar sobre os primos foi o professor matemático grego Euclides quando publicou “Os Elementos” em 300 a.C. que já apresentava importantes resultados acerca dos números primos. Em seu livro IX de “Os Elementos” demonstrou que existem uma infinidade deles. Essa demonstração foi uma das primeiras provas conhecidas que utiliza o método de prova por contradição. Foi também quem descobriu a capacidade dos primos de decompor os números secundários em fatores de primários.

O grego Eratóstenes em 276 a.C. foi um dos primeiros a desenvolver um método para encontrar números primos que se deu através de tabela de primos. Ele descobriu um método para determinar quais números eram primos em uma lista com um valor limite de números, por exemplo, dos 120 primeiros números naturais. Esse método é conhecido como **Crivo de Eratóstenes** e consiste em escrever todos os números de 1 até  $n$  em uma tabela, no nosso caso até 120. Em seguida ele localizava o primeiro primo da lista, o número 2, riscava todos os seus múltiplos, depois localizava o próximo número que não estava riscado, o número 3 e novamente riscava seus múltiplos.

Através de suas inquietações e observações na busca pelos infinitos números primos, Eratóstenes descobriu e desenvolveu um método no qual não era necessário que o procedimento fosse realizado até o último número estabelecido da tabela, a explicação se da através do seguinte resultado que foi proposto e demonstrado pelo próprio.

**Lema 2.1** (Lema de Eratóstenes). *Se um número inteiro  $n > 1$  não é divisível por nenhum número primo  $p$  tal que  $p^2 \leq n$ , então ele é primo.*

**Demonstração:** Seja  $n$  um número inteiro maior que 1 que não é divisível por nenhum número primo  $p$  tal que  $p^2 \leq n$ . Suponha, por absurdo, que  $n$  não seja primo. Seja  $q$  o menor número primo que divide  $n$ , então  $n = qn_1$ . Daí,  $q^2 \leq qn_1 = n$ . Logo,  $n$  é divisível por um número primo  $q$  tal que  $q^2 \leq n$ , absurdo. ■

Portanto, em nossa tabela (Figura 3), 7 é o ultimo primo da tabela que contém múltiplos, pois o próximo primo é 11, cujo quadrado supera 120.

Figura 3 – Crivo de Eratóstenes



Fonte: Elaborada pela autora.

A nova era matemática sobre os números primos demorou longos anos até que ressurgiu com uma gama de matemáticos corajosos a buscar fórmulas para expressar e encontrar números primos e assim desvendar o maior enigma da área. Era de se esperar que matemáticos de formação fossem os primeiros a surgir com uma tentativa de resolução para esse enigma. Vamos ver a seguir que não foi bem um matemático formado que no século XVII anunciava uma fórmula para encontrar números primos.



Pierre de Fermat não era de fato um matemático de carreira, porém fez descobertas importantíssimas para a disciplina. Fermat anunciava suas descobertas por meio de cartas aos seus colegas. Por volta de 1640 anunciou em carta ao colega matemático Bernard Frenicle de Bessey que tinha criado um “Pequeno Teorema de Fermat”, um teste simples e eficaz para verificar se um número é ou não é primo. Este só foi demonstrado quase um século depois em 1736 por Leonhard Euler. Para falarmos e demonstrarmos o Pequeno Teorema de Fermat precisaremos de um lema.

**Observação 2.1.** *Usaremos o teorema do binômio de Newton para demonstrar os próximos resultados. O teorema se escreve da seguinte maneira:*

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k.$$

Os coeficientes  $\binom{n}{k}$  são chamados coeficientes binominais e são definidos como:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!},$$

em que  $n, k \in \mathbb{Z}$  e  $k \leq n$ .

**Lema 2.2.** *Seja  $p$  um número primo. Os números  $\binom{p}{i}$ , em que  $0 < i < p$ , são todos divisíveis por  $p$ .*

**Teorema 2.2** (Pequeno Teorema de Fermat). *Dado um número primo  $p$ , tem-se que  $p$  divide o número  $a^p - a$ , para todo inteiro positivo  $a$ .*

**Demonstração:** Vamos provar por indução sobre  $a$ . Note que o resultado vale para  $a = 1$ , pois  $1^p - 1 = 0$  e todo número real não nulo divide zero, então  $p \mid 0$ . Supondo que é válido para  $a$ , vamos provar que é válido para  $a + 1$ . Usando o binômio de Newton, temos:

$$(a + 1)^p - (a + 1) = a^p - a + \binom{p}{1} a^{p-1} + \dots + \binom{p}{p-1} a.$$

Pelo Lema 2.2 e a hipótese de indução o segundo membro da igualdade acima é divisível por  $p$ . Portanto, segue o resultado. ■

**Corolário 2.1.** *Sejam  $p$  um número primo e  $a$  um número inteiro positivo não divisível por  $p$ , então  $p$  divide  $a^{p-1} - 1$ .*

**Demonstração:** Pelo Teorema 2.2,  $p \mid a(a^{p-1} - 1)$  e por hipótese  $p \nmid a$  logo,  $p$  divide  $a^{p-1} - 1$ . ■

Pierre de Fermat na mesma época anunciava ter encontrado uma fórmula para os números primos. Ele afirmava que todos os números da forma  $2^{2^n} + 1$ , em que  $n$  é um inteiro não negativo, eram primos. De fato para os primeiros 5 números sua fórmula

funcionava. Fermat morreu convicto de ter descoberto a tão sonhada fórmula para os números primos. No entanto, em 1732, Leonhard Euler mostrou que a fórmula de Fermat falhava para  $n = 5$ .

**Definição 2.1.** *É dito **primo de Fermat** todos os números primos da forma  $F_n = 2^{2^n} + 1$ , onde  $n$  é um inteiro não negativo.*

Apesar de Fermat admitir não poder provar, sua fórmula ficara conhecida por **números de Fermat**. Ainda não foram descobertos outros e, assim, não sabemos se existem ou não. A conjectura diante deste resultado é se números primos de Fermat são finitos. Até hoje só são conhecidos cinco números primos de Fermat são eles:

$$F_0 = 2^{2^0} + 1 = 2^1 + 1 = 2 + 1 = 3$$

$$F_1 = 2^{2^1} + 1 = 2^2 + 1 = 4 + 1 = 5$$

$$F_2 = 2^{2^2} + 1 = 2^4 + 1 = 16 + 1 = 17$$

$$F_3 = 2^{2^3} + 1 = 2^8 + 1 = 256 + 1 = 257$$

$$F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65536 + 1 = 65.537$$

Outra tentativa de listar os números primos veio com Marin Mersenne, que conjecturou que todos os números da forma  $2^n - 1$  eram primos, porém  $n$  tinha que ser primo. Entretanto, depois de algum tempo estudando sua fórmula, Marin Mersenne, ainda na primeira metade do século, em 1644, publicou uma lista de primos que acreditava funcionar em sua fórmula  $2^n - 1$ , a saber 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257. Não se sabe até hoje como Mersenne chegou a essa lista. Como nessa época só haviam as tábuas de primos, os expoentes mais altos não foram verificados e com isso, Mersenne nunca soube se estava realmente certo.

Alguns séculos mais tarde, a lista que Mersenne havia projetado para funcionar em sua fórmula foi verificada até o expoente 257, ou seja, para todos os expoentes entre 2 e 257. Com isso alguns erros foram descobertos. Apesar dos erros, Mersenne ainda ganhou seu nome na história da matemática. Tais números primos ficaram conhecidos como primos de Mersenne.

**Definição 2.2.** *É dito **primo de Mersenne** todo número primo da forma  $M_n = 2^n - 1$ , com  $n$  um inteiro positivo.*

**Proposição 2.1.** *Se  $2^n - 1$  é primo, então  $n$  é primo.*

**Demonstração:** Vamos demonstrar essa proposição pela contrapositiva, ou seja, vamos provar que se  $n$  é composto então  $2^n - 1$  é composto.

Se  $n = ab$  com  $a, b \geq 2$  então

$$1 < 2^a - 1 < 2^n - 1,$$

pois  $2^n - 1 = (2^a)^b - 1$ .

Note que  $2^n - 1$  é divisível por  $2^a - 1$ , pois

$$2^n - 1 = (2^a)^b - 1 = (2^a - 1) \cdot (2^{a(b-1)} + 2^{a(b-2)} + \dots + 2^{2a} + 2^a + 1),$$

logo  $2^n - 1$  é composto. ■

Em 1742, o matemático Christian Goldbach enviou uma carta a seu colega Leonhard Euler na qual propunha que todo número par maior do que dois podia ser expresso como a soma de dois números primos e que todo número ímpar maior do que cinco podia ser expresso como a soma de três números primos.

Ao longo dos anos, a proposta de Goldbach foi nomeada como conjectura forte de Goldbach e conjectura fraca de Goldbach, respectivamente. Nem Goldbach nem Euler foram capazes de provar as afirmações, por isso permaneceram como suposições ou conjecturas. O problema perdurou por quase 300 anos até que em 2006, Harald Helfgott, um matemático peruano, provou o que antes era chamada de conjectura fraca de Goldbach.

A conjectura forte de Goldbach é bastante simples, mas até hoje ninguém a conseguiu provar, e assim este é um dos problemas mais antigos da matemática na teoria dos números.

**Teorema 2.3** (“Conjectura” fraca de Goldbach). *Todo número ímpar  $n > 5$  pode ser escrito como soma de três números primos.*

Outra importante conjectura sobre os números primos é a conjectura dos primos gêmeos. Os primos gêmeos são aqueles primos que tem a diferença entre eles de 2 unidades.

**Definição 2.3.** *Sejam  $x$  e  $y$  dois números primos. Então  $x$  e  $y$  são chamados de **primos gêmeos** se  $|x - y| = 2$ .*

Por exemplo, os números primos 5 e 7 são primos gêmeos, assim como 11 e 13, 17 e 19, 137 e 139. Conjectura-se que existem uma infinidade de primos gêmeos, porém até agora ninguém conseguiu demonstrar.

Atualmente os maiores números primos descobertos são graças a computação, através de softwares. Uma grande desenvolvedora de um desses softwares que nos permite calcular esses números primos gigantes é a GIMPS (Great Internet Mersenne Prime Search) que foi criada por George Woltman no início de 1996. A GIMPS é responsável por um excelente software livre, ou seja, grátis de fácil instalação e que exige pouco do

usuário. Os maiores primos descobertos hoje foram por usuários desse software. Quando um novo número primo é descoberto por meio deste, matemáticos verificam se o resultado é verdadeiro antes de ser divulgado.

Tabela 1 – 10 maiores números primos descobertos.

Posição	Primo	Dígitos	Descoberto por	Ano
1	$2^{82589933} - 1$	24.862.048	Usuário da GIMPS	2018
2	$2^{77.232.917} - 1$	23.249.425	Usuário da GIMPS	2017
3	$2^{74.207.281} - 1$	22.338.618	Usuário da GIMPS	2016
4	$2^{57.885.161} - 1$	17.425.170	Usuário da GIMPS	2013
5	$2^{43.112.609} - 1$	12.978.189	Usuário da GIMPS	2008
6	$2^{42.643.801} - 1$	12.837.064	Usuário da GIMPS	2009
7	$2^{37.156.667} - 1$	11.185.272	Usuário da GIMPS	2008
8	$2^{32.582.657} - 1$	9.808.358	Usuário da GIMPS	2006
9	$10223 \cdot 2^{31.172.165} + 1$	9.383.761	Usuário da GIMPS	2016
10	$2^{30.402.457} - 1$	9.152.052	Usuário da GIMPS	2005

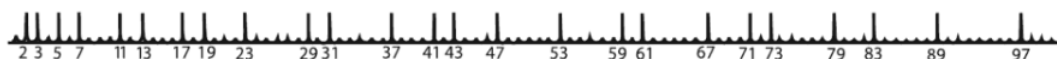
Fonte: GIMPS.

## 2.4 Distribuição dos números primos

Os números primos são para os matemáticos como a tabela periódica é para os químicos, pois os números primos geram todos os outros números. O que intriga quando estudamos sobre os primos é que eles são imprevisíveis. É impossível prevermos quando surgirá o próximo primo, apesar de sua simplicidade e caráter essencial, ninguém em milhares de anos foi capaz de decifrá-los.

Quando olhamos para a reta numérica, eles aparecem de forma totalmente aleatória. Alguns matemáticos chegam a brincar que eles são uma brincadeira da natureza, um lançar de moedas para escolher quando eles apareceriam.

Figura 4 – Os números primos até 100.



Fonte: (SAUTOY, 2008).

Em consequência da natureza desconhecida, quando a busca por padrões para tentar encontrar fórmulas que os gerassem já se mostrava extenuada, surge uma nova perspectiva em relação a essa parte importante da matemática. Iniciam-se estudos para determinar

com que frequência eles se encontram dentro do conjunto dos números naturais/inteiros. Denotaremos por  $\pi(x)$  a função que resulta na quantidade de números primos menores ou iguais a  $x$ , isto é  $\pi(x) : \mathbb{N} \rightarrow \mathbb{N}$ , é dada por

$$\pi(x) = \text{quantidade de números primos menores ou iguais a } x.$$

Assim a probabilidade de que um elemento do conjunto  $\{1, 2, \dots, x\}$  seja primo é dada por  $\frac{\pi(x)}{x}$ .

**Exemplo 2.**  $\pi(10) = 4$ , ou seja, a quantidade de números primos até 10 é 4 e  $\pi(11) = 5$ , pois há cinco números primos até 11, precisamente, 2, 3, 5, 7, 11.

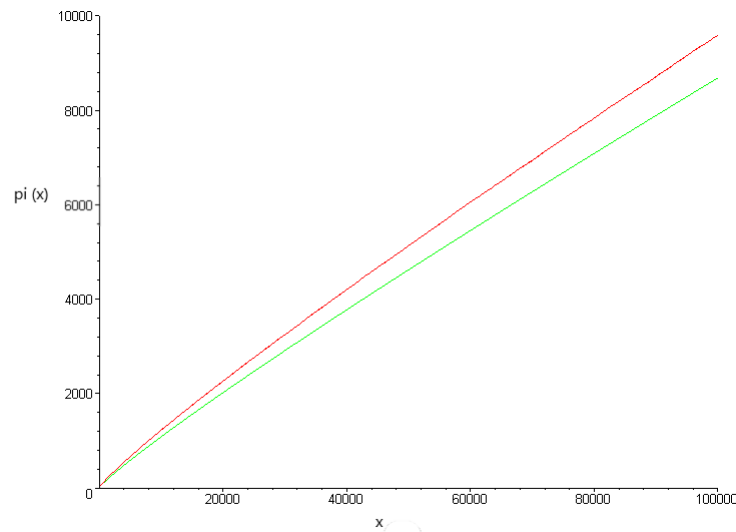
Segundo (SAUTOY, 2008, p. 34), “em vez de abordar diretamente o problema do professor, Gauss observou a questão por um outro ângulo, utilizando o pensamento lateral — o ato de revirar o problema de cabeça para baixo na tentativa de vê-lo por uma nova perspectiva. Esse é um tema extremamente importante nas descobertas matemáticas, sendo um dos motivos pelos quais as pessoas que pensam como o jovem Gauss se tornam bons matemáticos.”

Apesar desse trecho não ser contado em uma história sobre os números primos, a maneira de Gauss observar e investigar problemas de modo geral é bastante perspicaz e eficiente na busca de conhecimentos matemáticos bem como tantos outros assuntos escolares ou não. A tentativa de enxergar um problema ou até mesmo um conteúdo matemático por uma nova perspectiva pode nos trazer novos entendimentos, assimilações, dúvidas e busca por mais conhecimentos. Isso faz com que o aprendizado em matemática seja alcançado com entusiasmo.

Durante anos o que se tratou foi criar fórmulas para gerar todos os números primos, até que Carl Friedrich Gauss (1777 - 1855), por volta de 1792, cansado de encarar suas tabelas de primos sem conseguir qualquer padrão sequer, mudou a pergunta que todo mundo matemático fazia e não obtinha resposta. Gauss pensou que ao invés de tentar prever a exata localização do próximo primo tentasse descobrir a quantidade de primos entre 1 e 100, 1.000, 10.000, 100.000 e assim por diante.

Gauss nessa época também era bastante interessado por logaritmos, e por coincidência conheceu as tabelas de primos por meio de um livro sobre logaritmos que ganhara de presente de seu pai, cuja contracapa apresentava uma tabela de números primos. Aos dezoito anos de idade construiu uma tabela que permitia descobrir que a chance de um número entre 1 e  $x$  ser primo era aproximadamente  $\frac{1}{\ln(x)}$ . Ele então conjecturou que a quantidade real de números primos de 1 até  $x$  era aproximadamente  $\frac{x}{\ln(x)}$  (ver Figura 5). No entanto alguns estudos apontam que quem fizera esta descoberta foi o matemático francês Adrien-Marie Legendre e que Gauss anos mais tarde conjecturou algo equivalente.

Figura 5 – Gráfico comparação entre  $\pi(x)$  (vermelho) e  $\frac{x}{\ln(x)}$  (verde).



Fonte: Wikipédia [Adaptado].

Esse resultado originou o Teorema dos Números Primos em 1896 quando foi demonstrado por Jacques Hadamard e Charles Jean de la Vallée-Poussin, independentemente.

**Teorema 2.4** (Teorema dos Números Primos).

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x} \cdot \left( \frac{1}{\ln(x)} \right)^{-1} = 1$$

Em 1845, um matemático francês, Joseph Bertrand estimou o quanto teríamos que contar para ter a certeza de que encontraríamos um primo. Sua conjectura consistia em que se tomássemos qualquer número  $N$  maior do que 1 e contássemos até duas vezes esse número,  $2N$ , certamente encontraríamos um número primo pelo caminho. Embora Bertrand não tivesse conseguido provar sua estimativa, sua formidável previsão se tornou conhecida como o Postulado de Bertrand. Não demorou muito até que a estimativa de Bertrand fosse provada. Entre 1850 e 1852, o matemático russo Pafnuti Tchebychev (1821-1894) demonstrou o resultado. Atualmente, o postulado de Bertrand também é conhecido como Teorema de Tchebychev.

Este capítulo foi essencial para mostrarmos, mesmo que de maneira breve, que as investigações matemáticas resultam no desenvolvimento de teorias importantes. E quanto mais cedo essa ferramenta didática for incentivada, melhores serão os resultados para a matemática no futuro. As perguntas feitas pelos maiores descobridores da área mostraram que procurar os problemas por outras perspectivas pode elevar as buscas pelo entendimento da matemática. Despertando o interesse dos alunos pela investigação, mais pontos de

vista e perguntas diferentes teremos para encontrar as grandes respostas para enriquecer o conhecimento matemático.

### 3 Investigações sobre números primos no ensino fundamental

Diante do exposto no Capítulo 1 sobre a aplicação da investigação matemática em sala de aula a fim de melhorar o processo de ensino-aprendizagem, e no Capítulo 2, onde o nosso foco são os números primos, neste capítulo apresentaremos os conteúdos relacionados aos números primos que os documentos oficiais, em especial as orientações da SEDU-ES, indicam para os anos finais do ensino fundamental. Nosso objetivo é falar um pouco sobre estes tópicos apresentando exemplos de atividades que envolvam investigações e/ou demonstrações matemáticas.

Orientado pela BNCC, o currículo da SEDU-ES propõe a introdução do conceito de números primos no 6º ano do Ensino Fundamental, como podemos observar na Figura 6.

Figura 6 – Números primos em abordagem curricular.

Objeto de Conhecimento	Habilidade
Fluxograma para determinar a paridade de um número natural Múltiplos e divisores de um número natural Números primos e compostos	Construir algoritmo em linguagem natural e representá-lo por fluxograma que indique a resolução de um problema simples (por exemplo, se um número natural qualquer é par).
Fluxograma para determinar a paridade de um número natural Múltiplos e divisores de um número natural Números primos e compostos	Classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos "é múltiplo de", "é divisor de", "é fator de", e estabelecer, por meio de investigações, critérios de divisibilidade por 2, 3, 4, 5, 6, 8, 9, 10, 100 e 1000.
Fluxograma para determinar a paridade de um número natural  Múltiplos e divisores de um número natural  Números primos e compostos  Mínimo Múltiplo Comum  Máximo Divisor Comum	Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor, incluindo a noção de máximo divisor comum ou mínimo múltiplo comum.

Fonte: (SANTO, 2019).



O estudo de números primos na educação básica é bem reduzido como vemos na Figura 6. Dentro do que se aprende sobre os números primos, nota-se que não são apresentados a história dos números primos, como surgiram, os resultados importantes sobre esses números, como esses números são importantes tanto para a construção da matemática como para o dia-a-dia da humanidade, bem como na natureza, como vimos na Seção 2.2.

Compreensivelmente, não há possibilidade de que todo o conteúdo sobre números primos seja abordado na educação básica porém os números primos podem ser usados como um interessante tema para o professor em aulas investigativas e demonstrativas.

### 3.1 As fases de uma aula investigativa

Nesta seção abordaremos as fases que o professor deve ter consciência ao realizar uma atividade investigativa. Como o professor se organizará, o que esperar ao final da aula, bem como os processos da aula.

No capítulo anterior, vimos que uma aula investigativa pode tomar rumos diferentes dos quais imaginamos. Quando o problema é apresentado, não sabemos como uma investigação irá acabar. Cada aluno ou grupo de alunos fará observações e terá percepções diferentes, portanto, os caminhos a serem percorridos, acertos, erros e discrepâncias poderão variar, pois cada aluno tem seus entendimentos matemáticos.

Com isso, o professor tem um papel crucial durante as aulas. Ele deve estar atento aos questionamentos dos alunos e lhes dar direcionamento correto para que situações das quais os alunos fujam do objetivo, que é investigar matematicamente determinado conteúdo, não ocorram. Além disso, o professor deve ser incentivador para que os alunos se sintam encorajados e motivados a realizar a tarefa.

Segundo (PONTE; BROCARD; OLIVEIRA, 2016), uma atividade investigativa parte de três fases (ver Tabela 2): a introdução da atividade, na qual o professor faz a apresentação e explicação da atividade; a realização da atividade (podendo ser individual ou em grupos) e a discussão dos resultados, em que os alunos expõem suas conclusões/resultados aos demais colegas.

Tabela 2 – Fases da aula de investigação.

Fase da atividade	Elementos da fase
Introdução da atividade	Proposta da atividade Introdução do problema Reconhecer o problema
Realização da atividade	Exploração do problema Investigação dos fatos Formular questões Organizar dados e conjecturar Realização de testes Justificar conjecturas
Discussão dos resultados	Apresentação dos resultados Debate com os colegas

Fonte: Elaborada pela autora.

A fase da introdução da atividade deve ser feita pelo professor de forma clara e objetiva, de modo que, todos os alunos entendam o conteúdo a ser trabalhado e o que precisa ser feito para a realização da atividade. A fase de realização é a parte em que os alunos vão se debruçar sobre a atividade proposta e a partir dos conhecimentos e investigações do grupo ou do aluno, farão observações, explorações e testes. Sempre anotando e justificando cada observação feita durante o processo. A última fase envolverá toda a turma em conjunto e será moderada pelo professor. Ele solicitará que os grupos ou alunos apresentem seus resultados justificando-os, abrindo espaço para discussão/diálogo dos demais colegas. É importante que os alunos se sintam a vontade para debater os resultados e justificativas, bem como, se houver, apresentar diferentes justificativas do mesmo resultado.

### 3.2 Alguns exemplos de atividades investigativas e demonstrativas pautadas sobre os números primos

Com relação ao conceito de números primos e sua parte introdutória, uma ideia de investigação, manipulação, observação de resultados sobre os números inteiros utilizando números primos para os/(as) professores/(as) é de que, quando introduzir o estudo de números primos pode por bem apresentar a demonstração de Euclides para o teorema da infinidade dos números primos. Mudando os argumentos e a forma de apresentar a demonstração, tornando-a didática para que alunos de 11-12 anos, com o mínimo de “maturidade matemática” (entendimento de alguns conceitos matemáticos), compreendam a demonstração, o resultado e a importância dele.

**Teorema 3.1** (Teorema de Euclides). *O conjunto formado pelos números primos é infinito.*

**Demonstração:** Suponhamos que o conjunto dos números primos seja finito:  $A = \{2, 3, 5, \dots, p\}$ . Assim, tomemos o número  $m$  tal que  $m = (2 \cdot 3 \cdot 5 \cdots p) + 1$ .

Note que  $m$  não é divisível por nenhum elemento de  $A$ , pois o resto da divisão é sempre 1.

Dessa forma, temos duas situações: ou  $m$  é outro número primo que não está na lista ou é um número composto cujos fatores são números primos que não estão na lista.

Logo, nossa suposição inicial é falsa, portanto, temos a prova do teorema. ■

Desta forma, gera abertura para citar e apresentar o Teorema Fundamental da Aritmética e com isso, como visto na Seção 1.2, deixar com que os alunos brinquem com determinados números selecionados pelo professor a fim de descobrir se o número é um número primo ou não e se não for, desvendar seus fatores primos de modo que o torna único.

Dessa atividade podemos incorporar os conceitos de mínimo múltiplo comum e máximo divisor comum entre os números trabalhados, podendo dar abertura para criação de fluxogramas para trabalhar múltiplos e divisores de um número inteiro. Uma vez classificados os números entre primos e compostos, o/a professor/(ra) pode solicitar que os alunos escolham os números dois a dois para que os expressem em termos de “é fator de”, “é múltiplo de”, “é divisor de” e apresentar o máximo e mínimo divisor comum entre eles marcando, assim, a importância dos números primos, *mmc* e *mdc* no aprendizado de matemática.

Após essa apresentação inicial aos números primos e diferenciação dos primos e compostos, o/(a) professor/(ra) pode apresentar uma atividade utilizando a história dos números primos.

“[...] É importante incluir a história da Matemática como recurso que pode despertar interesse e representar um contexto significativo para aprender e ensinar Matemática [...]” (BRASIL, 2019, Seção 4.2.1.2).

### Crivo de Eratóstenes

Através da história da matemática apresentar o crivo de Eratóstenes destacando a importância da investigação matemática, como vimos na Seção 2.3 deste trabalho. Como recurso para que os alunos compreendam a classificação dos números primos e compostos, desenvolver a atividade aplicando o crivo de forma investigativa, da seguinte maneira.

Peça que os alunos construam uma tabela (ou pode já entregar uma tabela pronta) de 1 ao número que desejar, como no crivo de Eratóstenes. O número um pode ou não ser um elemento da tabela, a fim de garantir que os alunos tenham entendido o porquê do número 1 não ser primo. Solicite que circulem o número 2 e excluam seus múltiplos, feito isso, peça que circulem o 3 e excluam seus múltiplos e, a partir daí peça que continuem de

maneira análoga para os demais números da tabela, anotando sempre suas observações, ideias de conjecturas e modos de pensar para que justifiquem seus avanços na tabela.

O/(A) professor/(ra), após a realização da atividade, deve abrir espaço para que alunos comparem e discutam seus resultados através de suas anotações já estabelecidas. A atividade deverá ser realizada individualmente tendo em vista sua simplicidade.

A título de curiosidade, pode-se apresentar o lema de Eratóstenes (visto em 2.1) aos alunos para que tenham um exemplo de como as investigações matemáticas trouxeram resultados que ajudaram em um determinado problema da época, onde os números primos estavam sendo descobertos. O/(A) professor/(ra) conhecendo sua turma e a capacidade de absorção e entendimento matemático, poderá optar por demonstrar o resultado de Eratóstenes. Ou optar por apresentar o resultado a um grupo de alunos que fazem parte de algum grupo de estudos ou tutoria da escola, como alunos selecionados a participarem da segunda fase da OBMEP, por exemplo, que costumam ter tutores e/ou monitores no contra-turno.

**Lema 3.1** (Lema de Eratóstenes). *Se um número inteiro  $n > 1$  não é divisível por nenhum número primo  $p$  tal que  $p^2 \leq n$ , então ele é primo.*

**Demonstração:** Do enunciado do lema extraímos as seguintes afirmações (hipóteses):

$$n > 1, p \nmid n \text{ se } p^2 \leq n \text{ e } p \text{ é primo.}$$

Queremos mostrar (tese) que  $n$  é primo.

Suponhamos, por absurdo<sup>1</sup>, que  $n$  não é primo. Seja  $p$  um número primo de tal forma que  $p$  é o menor divisor de  $n$ . Dessa forma, podemos escrever  $n = p.k$ , onde  $p \leq k$  e  $k \in \mathbb{Z}$ . Multiplicando  $p \leq k$  por  $p$  de ambos os lados, temos:

$$p.p \leq p.k \Rightarrow p^2 \leq p.k$$

Substituindo  $p.k$  por  $n$ , pois  $n = p.k$ , obtemos:  $p^2 \leq n$ . Isso implica dizer que  $n$  é divisível por  $p$  (escolhemos  $p$  sendo o menor divisor de  $n$ ) de tal forma que  $p^2 \leq n$ . Com isso, chegamos a um absurdo, pois por hipótese se  $p$  é primo e  $p^2 \leq n$  então  $p \mid n$ . Portanto,  $n$  é primo. ■

## Criptografia

Podemos destacar uma atividade envolvendo uma das aplicações dos números primos vista neste trabalho, a criptografia. Esse material foi extraído de (SILVA, 2019) e o objetivo dessa atividade é mostrar como acontece o processo de codificação e decodificação

<sup>1</sup> Uma prova por absurdo é um método de prova matemática. Assume-se como verdade o contrário do que queremos provar e então chega-se a uma contradição (em um absurdo).

de uma mensagem pelo método RSA, destacando os conceitos matemáticos importantes em cada etapa a fim de enfatizar a utilização dos números primos em aplicações do cotidiano. Essa atividade pode ser desenvolvida por alunos a partir do 6º ano do ensino fundamental e tem como pré-requisitos apenas divisões de números grandes e cálculo de potências.

Essa atividade consiste em codificar e decodificar a palavra CÓDIGO. A atividade descrita mostra passo a passo o que acontece, por meio de um exemplo. Porém, utiliza-se cálculos mais simples, adequando o processo ao que seria feito em uma sala de aula da educação básica. Assim não será evidenciado, por exemplo, as congruências mas o processo de divisão e a utilização dos restos de tais divisões. Serão utilizados primos pequenos com o objetivo de facilitar as operações, quando são utilizados primos grandes o processo é análogo.

O primeiro momento da atividade, chamaremos de codificação que consiste em escolher um número  $n$  tal que  $n = p.q$  em que  $p$  e  $q$  são números primos, tal número será a nossa chave pública. Consideraremos os números primos  $p = 3$  e  $q = 7$ , logo  $n = pq = 3.7 = 21$ . Precisaremos determinar a chave de codificação, isto é, o par  $(k, \varphi(n))$ , onde  $k$  é o menor número primo e  $\text{mdc}(k, \varphi(n)) = 1$  e  $\varphi(n)$  é a função de Euler definida como sendo o número de inteiros positivos menores ou iguais a  $n$  que possuem máximo divisor comum com  $n$  sendo 1, isto é, que são coprimos com  $n$ . Sabemos que dada a decomposição de  $n$  como produto de dois primos, então  $\varphi(n) = (p - 1)(q - 1)$ . Como temos  $p$  e  $q$  definidos é fácil calcular  $\varphi(n)$  logo,  $\varphi(n) = (3 - 1)(7 - 1) = 12$  e  $k$ , que será o menor primo que não divide  $\varphi(n)$ , logo  $k = 5$ , já que  $\text{mdc}(12, 5) = 1$ .

Utilize a tabela a seguir para fazer a conversão das letras da palavra para números:

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

Fazendo a conversão teremos a sequência: 122413181624. Separando os números em blocos, de modo que cada bloco seja menor que  $n = 21$ , temos:

$$12 - 2 - 4 - 13 - 18 - 16 - 2 - 4.$$

Seja  $b$  um bloco. Para codificá-lo considere o resto da divisão de  $b^k$  por  $n$ . Ou ainda, no bloco 12 temos que  $12^5 = 248.832$ , dividindo-o por 21: (ver Figura 7).

Figura 7 – Divisão de 248.832 por 21.

$$\begin{array}{r}
 \mathbf{248832} \quad \big| \mathbf{21} \\
 \underline{-21} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \\
 \mathbf{38} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \\
 \underline{-21} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \\
 \mathbf{178} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \\
 \underline{-168} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \\
 \mathbf{103} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \\
 \underline{-84} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \\
 \mathbf{192} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \\
 \underline{-189} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \\
 \mathbf{3} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000}
 \end{array}$$

Fonte: (SILVA, 2019)[Adaptado].

Sendo  $C(b)$  o bloco codificado, temos  $C(12) = 3$ . Fazendo o mesmo processo para os outros blocos obtemos:

$$C(2) = 11; C(4) = 16; C(13) = 13; C(18) = 9; C(16) = 4; C(2) = 11 \text{ e } C(4) = 16.$$

A sequência de blocos codificados é 3 - 11 - 16 - 13 - 9 - 4 - 11 - 16. Logo, a mensagem codificada será: 3111613941116.

O segundo momento, chamaremos de decodificação. Para decodificar a mensagem que acabamos de codificar também é utilizado o resto da divisão. Porém precisamos determinar  $d$  que é fácil já que conhecemos  $\varphi(n) = 12$  e  $k = 5$ .

Em nosso caso, o número  $d$  é tal que este multiplicado por  $k$  deixa resto 1 na divisão por  $\varphi(n) = 12$ . Ou ainda, basta pensar no número em que  $\text{mdc}(12, d) = 1$ , que é o menor primo que não divide 12. Logo,  $d = 5$ .

Seja um bloco  $a$  da sequência de blocos codificados, a decodificação deste bloco será o resto da divisão de  $a^d$  por  $n$ . Assim, no bloco 3 temos que  $3^5 = 243$ , dividindo-o por 21 temos:

Figura 8 – Divisão de 243 por 21.

$$\begin{array}{r}
 \mathbf{243} \quad \big| \mathbf{21} \\
 \underline{-21} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \\
 \mathbf{33} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \\
 \underline{-21} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \\
 \mathbf{12} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000} \phantom{00000}
 \end{array}$$

Fonte: (SILVA, 2019)[Adaptado].

Sendo  $D(a)$  o bloco decodificado, note que neste caso o resto da divisão é exatamente o valor do primeiro bloco da mensagem original, ou ainda,  $D(3) = 12$ . De modo análogo obtemos os blocos:

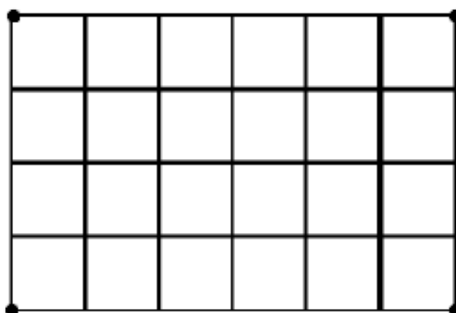
$$D(11) = 2; D(16) = 4; D(13) = 13; D(9) = 18; D(4) = 16; D(11) = 2 \text{ e } D(16) = 4.$$

A sequência de blocos decodificados é 12 - 2 - 4 - 13 - 18 - 16 - 2 - 4. E a mensagem decodificada (numericamente) 122413181624. Considerando os pares de números, obtemos a correspondência (em letras) pela tabela inicial a palavra CÓDIGO, a qual queríamos de fato obter. Os alunos, em duplas, podem ser instigados a codificarem e decodificarem palavras que queiram, cada aluno codifica uma palavra para o outro aluno decodificar. Os alunos decodificam a palavra do outro, anotando os avanços, inquietações, observações que fizeram no processo e depois verificam se chegaram na palavra codificada pelo colega. Essa é uma forma de trazer a matemática dos números primos de maneira descontraída para que os alunos vejam o quanto esses números são importantes para a matemática e para a humanidade, além de reforçar conceitos matemáticos básicos, como a divisão.

#### Máximo divisor comum e mínimo múltiplo comum

A atividade a seguir trabalha os conceitos de *mdc* (máximo divisor comum) e *mmc* (mínimo múltiplo comum) geometricamente. Chamada de mesa de Snooker ou sinuca de snooker, traz a ideia de interpretar o retângulo como uma mesa de sinuca. Além da exploração do *mmc* e *mdc*, uma análise importante é o número de batidas da bola nas laterais da mesa até entrar na “caçapa”. Vamos considerar o retângulo cujas dimensões são os números em questão. Vamos calcular o *mmc* entre 4 e 6. Para isso, considere um retângulo  $4 \times 6$  subdividido em quadrados cuja medida do lado é 1.

Figura 9 – Retângulo de lados 4 e 6.

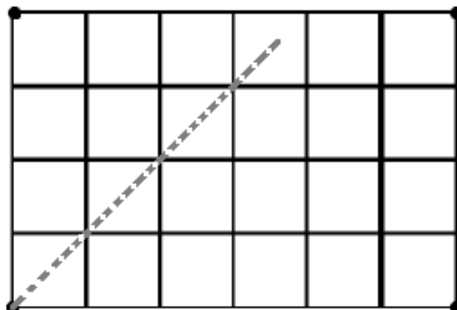


Fonte: Elaborada pela autora.

Imagine que os vértices são as quatro caçapas da mesa. A “bola” se move sempre saindo de uma das caçapas e se “movimenta” pela diagonal dos quadradinhos do retângulo. Quando essa bola toca um dos lados do retângulo, ela faz uma rotação de  $90^\circ$  no sentido

anti-horário e continua a trajetória com a mesma regra, até a bola cair na caçapa (um dos vértices) e daí “acaba o jogo”.

Figura 10 – Percurso da bola.



Fonte: Elaborada pela autora.

De acordo com (PONTE; BROCARD; OLIVEIRA, 2016, p. 57), essa atividade permite que alunos investiguem questões como:

- Quantos quadrados a bola vai atravessar?
- Quantas vezes a bola vai bater nas tabelas (arestas do retângulo)?
- É possível saber as respostas dos itens anteriores antes mesmo de jogar?
- Teste, observe e conjecture com as dimensões da mesma sendo dois números primos entre si.
- Existe/(em) alguma/(as) relação/(ções) que podem ser extraídas das observações feitas?

A introdução da atividade é feita apenas explicando as regras do jogo e apresentando as questões acima. Os alunos deverão trabalhar em pequenos grupos e o professor deve solicitar que cada aluno elabore um “relatório” para anotar as observações, conjecturas e justificativas.

O intuito dessa atividade é deixar que os alunos joguem o jogo com dimensões de retângulo diferentes a fim de analisar, investigar e conjecturar padrões para o jogo, deixar que os alunos façam descobertas e relacionem o jogo com o *mmc* e *mdc*. Para essa aula é interessante que o professor disponibilize malhas quadriculadas para que os alunos testem o jogo com diversas dimensões. É importante também levar em conta o tempo disponibilizado para realização da atividade, o indicado é que sejam utilizadas duas aulas geminadas. Mais detalhes sobre uma experiência com essa atividade pode ser encontrada em (PONTE; BROCARD; OLIVEIRA, 2016, p. 56).



Os exemplos citados acima corroboram para o ensino de matemática focado na teoria dos números, mais precisamente, nos números primos. Certamente todas as propostas de aulas investigativas e demonstrativas auxiliam para, de certa forma, facilitar o trabalho do professor que se dispõe a sair do tradicionalismo, direcionando-o a atividades e propostas que podem e já foram utilizadas em sala de aula. No entanto, não sendo possível o aprofundamento do conteúdo em sala de aula, justificado pela abordagem curricular orientado pela SEDU-ES, por exemplo, é importante que o professor se coloque à disposição de incentivar os alunos como investigadores em matemática. Além da relevância de uma demonstração, evidenciar que os resultados servem tanto para mostrar que os argumentos matemáticos são incontestáveis bem como a utilidade destes no meio matemático e, consequentemente, para a humanidade. O professor atua bem como o motivador e influenciador além de ser detentor da informação, assim sendo, deve agir como um mediador, facilitador e articulador do conhecimento.

## Considerações Finais

Durante este trabalho, constatamos que, cada vez mais tem se discutido a autonomia dos alunos em relação a aprendizagem e apontamos como essa autonomia pode ser desenvolvida por meio de aulas investigativas e demonstrativas. Para enriquecer a discussão, trouxemos autores importantes que nos ajudam a embasar o trabalho com suas experiências e apresentamos os pontos mais relevantes para o curso deste.

Buscamos neste trabalho apresentar formas e conhecimentos prévios que direcionam professores do ensino básico para atividades investigativas e demonstrativas, pautado sobre números primos. Embora o estudo de números primos tenha começado há milhares de anos, a busca por entendimento e aprimoramento dos resultados vem se desenvolvendo. Assim, pode se tornar um importante aliado na busca por aulas mais instigantes. Algumas definições, principais resultados, utilidades e aplicações realçam a sua importância para a construção do conhecimento matemático na educação básica.

Apresentamos um breve estudo da evolução dos números primos, sua importância, aplicações e sua distribuição na reta numérica dos inteiros. Pautamos em como investigações matemáticas enquanto ferramenta foi e ainda é importante para construção da matemática dos números primos. Além de mostrar alguns dos principais resultados e conjecturas sobre números primos e assuntos relacionados, como da infinitude dos números primos, conjectura forte de Goldbach e o teorema fundamental da aritmética.

Mostramos que o estudo dos números primos em aulas investigativas e demonstrativas corroboram para o saber matemático dos alunos. Dessa forma, a fim de amenizar o aprendizado mecânico e desinteressante, empenhamos em apresentar aulas investigativas e demonstrativas que podem ser utilizadas em sala de aula na educação básica como uma forma de estimular e despertar o interesse dos alunos para a matemática. Dessa forma, trouxemos exemplos e propostas de atividades investigativas além de adaptar alguns resultados importantes sobre os números primos, que podem auxiliar professores a direcionarem suas metodologias em sala de aula.

# Referências

- BRASIL, M. da E. *Base Nacional Comum Curricular*. Brasília: MEC, 2019. [9](#), [34](#)
- COUTINHO, S. C. *Números Inteiros e Criptografia RSA*. Rio de Janeiro, RJ: 2. edição, Coleção Matemática e Aplicações, IMPA, 2011. [21](#)
- HEFEZ, A. *Elementos de aritmética*. Rio de Janeiro, RJ: 2. edição, Coleção Textos Universitários, SBM, 2006. [15](#)
- LAMONATO, M.; PASSOS, C. L. B. Discutindo resolução de problemas e exploração-investigação matemática: reflexões para o ensino de matemática. *Zetetiké*, v. 19, n. 2, 2011. [9](#)
- LIMA, E. L. *Matemática e Ensino*. [S.l.]: Sociedade Brasileira de Matemática, 2007. ISBN 9788583370185. [11](#)
- PONTE, J. P. da; BROCARD, J.; OLIVEIRA, H. *Investigações matemáticas na sala de aula*. [S.l.]: 2ª edição. Autêntica Editora, 2016. v. 7. [9](#), [10](#), [12](#), [19](#), [32](#), [39](#)
- SANTO, E. Currículo básico escola estadual. *Guia de Implementação/Secretaria de Educação (SEDU)*, Vitória, 2019. [9](#), [10](#), [31](#)
- SAUTOY, M. *A música dos números primos: A história de um problema não resolvido na matemática*. Rio de Janeiro, RJ: Tradução: Diego Alfaro. Zahar, 2008. [21](#), [27](#), [28](#)
- SILVA, V. B. da. *Números primos e criptografia: Do conceito ao sistema RSA*. Arraias, Tocantins: Universidade Federal do Tocantins - PROFMAT, 2019. [35](#), [37](#)
- TENGAN, e. a. E. *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*. Rio de Janeiro, RJ: 5. edição, Projeto Euclides, IMPA, 2018. [13](#)
- VIDIGAL, e. a. A. *Fundamentos de Álgebra*. Belo Horizonte, MG: Editora UFMG, 2005. [13](#)