



SEQUÊNCIAS QUE REVELAM A INFINITUDE DOS NÚMEROS PRIMOS.

CRIE A SUA!

Amanda de Araújo Queiroz ¹

Fábio Lima de Oliveira ²

Rodrigo Marques Faustino da Silva ³

Daniel Cordeiro de Moraes Filho ⁴

RESUMO

Os números primos encantam a humanidade desde os tempos mais remotos e hoje são bastante utilizados. Aparecem desde a Educação Básica e seu uso consta em diversas áreas da Matemática. Surpreendentemente, depois de séculos de estudo, por causa da sua infinitude e da aleatoriedade de seu comportamento, os números primos aparecem em diversas aplicações tecnológicas. Atualmente, assumem papel central na criptografia *Rivest-Shamir-Adleman* (RSA) para a transmissão de mensagens codificadas, tão imprescindíveis em nossos tempos de desenvolvida tecnologia. Neste trabalho ensinamos a construir sequências de números naturais que revelam a infinitude dos números primos, propriedade indispensável para fazer com que a criptografia RSA funcione. Ademais, sugerimos uma proposta metodológica-didática objetivando suscitar a importância da pesquisa matemática em Ensino, ao tempo que exibimos um tipo de demonstração da infinitude dos números primos, focando na independência cognitiva de cada aluno. Este trabalho é oriundo de uma atividade do Grupo PET-Matemática-UFCG, orientada sob os auspícios do Tutor Daniel Cordeiro de Moraes Filho. O objetivo principal é promover discussões sobre algumas demonstrações da infinitude de números primos, inteligíveis para professores e alunos de Matemática. Para exemplificar e instigar a curiosidade, os autores elaboraram três tipos de demonstrações da infinitude dos números primos, baseando-se nas ideias da demonstração do matemático alemão Christian Goldbach (1690-1764) e produziram atividades didáticas para sala de aula, conforme os direcionamentos da Base Nacional Comum Curricular (BNCC). Esperamos que professores se utilizem e aperfeiçoem essa proposta metodológica, promovendo debates sobre a importância de pesquisar matemática.

Palavras-chave: Proposta metodológica de demonstrações de infinitude dos números primos, Investigação matemática, Sequências numéricas.

¹ Graduanda do Curso de Licenciatura em Matemática da Universidade Federal de Campina Grande – UFCG, amanda.araujoqueiroz91@gmail.com; parcialmente financiada pelo PET/FNDE/MEC.

² Graduando do Curso de Licenciatura em Matemática da Universidade Federal de Campina Grande – UFCG, fabiolimaoliveira99@gmail.com; parcialmente financiado pelo PET/FNDE/MEC.

³ Graduando do Curso de Licenciatura em Matemática da Universidade Federal de Campina Grande – UFCG, rodriigosilv@gmail.com; parcialmente financiad pelo PET/FNDE/MEC.

⁴ Professor Orientador: Pós-doutor, Universidade Federal de Campina Grande – UFCG, demoraisfilho@gmail.com; parcialmente financiado pelo PET/FNDE/MEC.



INTRODUÇÃO

O Ensino em Matemática, na atualidade brasileira, visa desenvolver diversas competências e habilidades preconizadas na Base Nacional Comum Curricular (BNCC, 2017). O objetivo é que os alunos tenham mais autonomia, uma aprendizagem mais eficaz e significativa e não encarem o conhecimento matemático como pronto e inalterado. Neste trabalho, procuramos desenvolver a seguinte competência enunciada na BNCC:

Investigar e estabelecer conjecturas a respeito de diferentes conceitos e propriedades matemáticas, empregando recursos e estratégias como observação de padrões, experimentações e tecnologias digitais, identificando a necessidade, ou não, de uma demonstração cada vez mais formal na validação das referidas conjecturas (BNCC, 2017).

Um tema sempre trabalhado no Ensino Básico é o conceito de números primos e, veladamente, o Teorema Fundamental da Aritmética, quando se ensina nas escolas fatoração de números. Entretanto, pouco é discutido sobre a importância dos números primos na atualidade e, menos comum ainda, é ressaltada alguma demonstração da infinitude desses números, um fato que pode aparentar apenas importância matemática, mas, pelo contrário, tem significativa utilidade atualmente.

Além disso, mesmo vários professores de matemática, quando conhecem a demonstração da infinitude dos números primos, geralmente, conhecem apenas a clássica demonstração dada por Euclides de Alexandria (300 a.C), encontrada no livro *Os Elementos* (BICUDO, 2009). No presente trabalho, além de discutir a importância da infinidade dos números primos na criptografia de transmissão de mensagens em nosso mundo atual, apresentamos uma maneira pela qual cada aluno possa compreender facilmente a demonstração da infinitude dos números primos, e possam sentir-se estimulados e serem capazes de criar suas próprias demonstrações! Uma ocasião rara na Matemática.

METODOLOGIA

O trabalho foi elaborado como atividade do Grupo PET-Matemática-UFCG sob orientação do Professor Tutor Daniel Cordeiro de Moraes Filho. Além de um estudo bibliográfico mais abrangente do tema, foi instigado desenvolvermos demonstrações próprias da infinitude dos números primos e criarmos uma metodologia de forma que alunos do ensino básico sintam-se estimulados e consigam desenvolver, também, suas próprias demonstrações.



REFERENCIAL TEÓRICO

Segundo (COUTINHO, 2000), a Criptografia é o estudo dos métodos de envio de mensagens ininteligíveis, em forma “disfarçada”, de modo a apenas o seu destinatário legítimo consiga interpretá-la. Um exemplo de Criptografia é a *Rivest-Shamir-Adleman* (RSA) e a forma de deixar essas mensagens ainda mais difíceis de serem codificadas é usando números primos. O suporte matemático do processo vem da Teoria dos Números e essa criptografia só é possível porque eles são infinitos e não seguem um padrão definido! Pelo importante fato de serem infinitos, podemos sempre tentar conseguir novos números primos, cada vez maiores, e, conseqüentemente, dificultar cada vez mais os métodos criptográficos.

A demonstração da infinitude dos números primos mais conhecida e antiga é a demonstração de Euclides de Alexandria (300 a.C), presente no notável livro *Os Elementos*. Daremos a seguir uma demonstração desse fato, usando divisibilidade, de fácil compreensão até para alunos do Ensino Fundamental II.

Definição 1: Sejam a e b números inteiros. Dizemos que a **divide** b quando b é múltiplo de a e denotamos por $a \mid b$. Ou seja, a divide b , quando existe um inteiro c tal que $b = c \cdot a$. Quando a não divide b simbolizamos por $a \nmid b$.

Exemplos: $3 \mid 6$ e $6 \mid 18$, pois 6 é múltiplo de 3 e 18 é múltiplo de 6; $5 \mid -25$, pois $-25 = (-5) \cdot 5$; $-2 \mid 0$, pois $0 = 0 \cdot (-2)$.

Definição 2: Define-se **número primo** como um número inteiro positivo $p > 1$ tal que seus divisores naturais sejam apenas ele mesmo e a unidade.

Exemplos: 3 é um número primo, pois 1 e 3 são os únicos divisores naturais de 3; 449 é um número primo, pois 1 e 449 são os únicos divisores naturais de 449; 16 não é um número primo, pois 4 é um divisor de 16.

Definição 3: Sejam a e b números inteiros. Dizemos que a e b são **primos entre si**, quando o máximo divisor comum (mdc) de a e b é 1.

Exemplos: os números 5 e 8 são primos entre si, pois $mdc(5,8) = 1$; 35 e 44 são primos entre si, pois $mdc(35,44) = 1$; 12 e 20 não são primos entre si, pois $mdc(12,20) = 4 \neq 1$.

Note que dois números podem ser primos entre si sem serem primos, como é o caso de 4 e de 15.



O seguinte Teorema é bastante utilizado no Ensino Básico, quando se estuda fatoração de números, apesar de aparecer nessa fase do ensino apenas de forma velada e não ser citado.

Teorema Fundamental da Aritmética: Todo número inteiro maior do que 1 pode ser representado de maneira única, a menos da ordem, como um produto de fatores primos. (VIEIRA, 2015).

Demonstremos o Teorema da infinitude de primos de Euclides.

Teorema 1: Existe uma infinitude de números primos.

Demonstração de Euclides: Suponha que exista uma quantidade finita de números primos. Sejam p_1, p_2, \dots, p_n os números primos com $n \in \mathbb{N}$. Considere o número

$$p = (p_1 \cdot p_2 \cdot \dots \cdot p_n) + 1.$$

Temos duas opções para p : ele pode ser um número primo, e daí p será um primo maior do que todos os $p_i, i \in \{1, \dots, n\}$, o que é um absurdo. No caso de p ser composto, pelo Teorema Fundamental da Aritmética, sabemos que p pode ser decomposto em fatores primos. Desse modo, existe algum primo q que divide p .

Mas como só existem n primos, então o primo q deve ser igual a algum dos primos p_1, p_2, \dots, p_n e, daí, $q = p_i$. Dessa forma

$$p_i | (p_1 \cdot p_2 \cdot \dots \cdot p_n).$$

Como

$$p_i | p = (p_1 \cdot p_2 \cdot \dots \cdot p_n) + 1 \text{ e } p_i | (p_1 \cdot p_2 \cdot \dots \cdot p_n)$$

temos

$$p_i | (p - (p_1 \cdot p_2 \cdot \dots \cdot p_n)) = 1.$$

Um absurdo! Logo, concluímos que existem infinitos números primos. ■

Existem várias outras demonstrações desse teorema (no entanto, diferente dos números primos, são um número finito!) (RIBENBOIM, 2001). Um tipo dessas demonstrações funciona se conseguirmos uma determinada sequência de números, com certas propriedades, a qual apresentaremos a seguir.



Uma demonstração diferente da anterior que, a partir dela, podemos gerar sequências que revelam a infinitude dos números primos é a demonstração de Christian Goldbach (1690-1764):

Teorema 1: Existe uma infinitude de números primos.

Demonstração de Goldbach: Esta demonstração utiliza a seguinte ideia: encontrar uma sequência $a_1 < a_2 < a_3 < \dots < a_n < \dots$ de números naturais, dois a dois primos entre si, isto é, sem fator primo em comum. Se p_1 é fator primo de a_1 , se p_2 é fator primo de a_2 , ..., se p_n é fator primo de a_n , ..., então a sequência de números primos $p_1, p_2, \dots, p_n, \dots$ são todos distintos. Observe que não exibimos os números primos, mas sabemos que existem infinitos.

Há várias sequências de números naturais que cumprem essa propriedade. A demonstração encerra ao exibirmos uma sequência infinita de termos dois a dois primos entre si. Faremos isso a seguir.



RESULTADOS E DISCUSSÃO

No contexto da demonstração de Goldbach, instiga-se os leitores e alunos a procura por sequências dos números naturais dois a dois primos entre si. Assim, há a possibilidade de que cada um desvende uma sequência diferente que possa revelar a infinitude dos números primos!

Indicaremos um caminho a ser trilhado para que o aluno e o leitor consigam desenvolver a própria sequência de números naturais dois a dois primos entre si. Sem perder o ponto de partida, o tipo de sequência que desejamos encontrar está descrita a seguir:

“As sequências que revelam números primos são sequências crescentes em que os termos são dois a dois primos entre si.”

Como, na investigação, a experimentação é um fator imprescindível para compreender o contexto do problema, a seguir exporemos alguns questionamentos norteadores:

1º) Nessa sequência pode ter mais de um número par?

Não, porque esses números pares teriam dois como divisor comum e não seriam primos entre si. Logo, não podem existir mais de um número par!

2º) Podemos colocar diversas potências de um número na sequência?



Também não! Pensemos nas potências mais simples que não sejam pares, as potências de 3. Em quaisquer duas potências distintas de 3, teremos o 3 como divisor e, assim, não serão dois a dois primos entre si.

3º) Tentemos um caso particular. Como conseguir dois números primos entre si?

Uma forma de começar seria escolhendo aleatoriamente dois números naturais e comparar os divisores comuns para verificar se o máximo divisor comum é o 1. Uma maneira interessante e recursiva de fazer isso seria construir dois números (futuros termos consecutivos da sequência), de tal forma que na expressão numérica de um apareça o outro e que sejam primos entre si. Assim, possibilitaria repetir o procedimento padrão para tentar gerar novos números que são primos entre si com os anteriores.

Vejamos alguns exemplos:

Exemplo 1: Os números 3 e 16 são primos entre si.

Tentemos desenvolver uma expressão para o 16 em que o 3 esteja presente. Uma delas é $16 = 3 \cdot 5 + 1$. Essa representação é boa!

Suponhamos que d é um divisor de 3 e $16 = 3 \cdot 5 + 1$. Note que, como d é um divisor de 3, segue que d divide $3 \cdot 5$. Assim, d também divide a diferença entre 16 e $3 \cdot 5$ que é o 1. Recordando que o único divisor natural do 1 é o próprio 1, segue que $d = 1$. Logo, o único divisor comum de 3 e 16 é o 1, ou seja, 3 e 16 são primos entre si.

Nesse caso particular, é importante observar o fato essencial de que o 16 foi escrito como um múltiplo de 3 somado com 1.

Observe que esse raciocínio é bem mais eficiente no caso de números com muitos divisores, pois não foi necessário discriminar todos os divisores para poder constatar que são primos entre si! Vejamos que o mesmo argumento em outro exemplo.

Exemplo 2: Os números 4 e 9 são primos entre si.

Na expressão de 9, procuremos utilizar o mesmo raciocínio do exemplo 1, ou seja, reescrever o 9 como um produto que envolva o 4 e some 1. Assim, reescrevamos o 9 da seguinte maneira $9 = 4 \cdot 2 + 1$. Seja d um divisor comum do 4 e do 9 e verifiquemos, utilizando a mesma ideia do exemplo 1, que d é 1.



Ora, d divide o $9 = 4 \cdot 2 + 1$. Como d divide 4, segue que d divide $4 \cdot 2$ e assim, vai dividir a diferença entre 9 e $4 \cdot 2$ que é o 1. Logo, $d = 1$. Dessa forma, 4 e 9 são primos entre si.

Vejamos outro caso em que envolva números grandes:

Exemplo 3: Os números 10 e 131 são primos entre si.

Reescrevamos o 131 como um múltiplo de 10 somado com 1. Ou seja, $131 = 13 \cdot 10 + 1$. Seguindo o mesmo raciocínio do exemplo anterior, consideremos d como sendo um divisor comum do 10 e do 131. Como d divide 10, segue que d divide $10 \cdot 13$. Ora, sendo d divisor de $131 = 13 \cdot 10 + 1$ e de $10 \cdot 13$, temos d também divisor da diferença entre eles que é o 1. Logo, d é 1 e, assim, 10 e 131 são primos entre si.

Esses exemplos nos auxiliaram a verificar a validação do caso geral abaixo.

Propriedade 1: Dado um número n natural, ao multiplicarmos por outro número natural e somarmos 1, obteremos um novo número em que ele e n são primos entre si!

Exemplos:

- Considere $n = 5$ e o multipliquemos por 8. Note que 5 e $41 = 5 \cdot 8 + 1$ são primos entre si;
- Considere $n = 6$ e o multipliquemos por 2. Note que 6 e $13 = 6 \cdot 2 + 1$ são primos entre si;
- Considere $n = 10$ e o multipliquemos por 12. Note que 10 e $121 = 10 \cdot 12 + 1$ são primos entre si.

A partir desses exemplos, conseguimos aprender como gerar diversas quantidades de pares de naturais primos entre si. Será que conseguimos utilizar essa ideia para, não mais pares, mas gerar ternas de números naturais dois a dois primos entre si? E depois quatro números dois a dois primos entre si? Depois uma quantidade finita qualquer? Depois uma infinidade de números primos dois a dois primos entre si?

Observemos que na ideia de gerar três números naturais dois a dois primos entre si, conseguiremos já partir para o caso geral! Vejamos no seguinte exemplo:

Exemplo 4: Maria escolheu o número 4 para começar a sequência. Graças a Propriedade 1, ela escolheu o 6 para formar o segundo número da sequência e gerou o número $4 \cdot 6 + 1 = 25$.



Para o terceiro número, Maria pensou em usar a Propriedade 1 de novo. Mas para que o novo número da sequência seja primo entre si tanto com o 4, como com o $25 = 4 \cdot 6 + 1$, ela descobriu que na parcela que aparece o produto deve ter 4 e 25 como fatores, por isso o terceiro número da sequência será dado por $4 \cdot (4 \cdot 6 + 1) + 1 = 4 \cdot 25 + 1 = 101$, onde que a parcela que aparece o produto é a multiplicação dos dois anteriores!

Exemplo 5: João, vislumbrado pela ideia de Maria, pensou consigo que conseguiria formar uma sequência com 4 números, dois a dois primos entre si. Ele queria gerar um novo número que é primo entre si com os três anteriores e, usando a Propriedade 1, pensou em considerar o novo número como o produto dos três anteriores somado 1:

$$4 \cdot (4 \cdot 6 + 1) \cdot (4 \cdot (4 \cdot 6 + 1) + 1) + 1 = 4 \cdot 25 \cdot 101 + 1 = 2757.$$

Observando as ideias de Maria e João, Emília pensou que poderia formar uma sequência infinita de números naturais dois a dois primos entre si! Da seguinte maneira:

Representemos o n -ésimo termo da sequência por a_n . Seguindo a ideia de Maria, temos $a_1 = 4$, $a_2 = 4 \cdot 6 + 1$ e $a_3 = 4 \cdot (4 \cdot 6 + 1) + 1$. Agora, usando a ideia de João, reescrevamos o terceiro termo como $a_3 = a_1 \cdot a_2 + 1$ e o quarto seria $a_4 = a_1 \cdot a_2 \cdot a_3 + 1$. Vendo essa forma, Emília propõe a seguinte sequência:

$$\begin{aligned} a_1 &= 4; \\ a_2 &= 4 \cdot 6 + 1 = 25; \\ a_3 &= 4 \cdot (4 \cdot 6 + 1) + 1 = 4 \cdot 25 + 1 = 101; \\ &\vdots \\ a_n &= a_1 \cdot a_2 \cdot \cdots \cdot a_{n-1} + 1, \\ &\vdots \end{aligned}$$

que é formada de números dois a dois primos entre si!

O diálogo anterior resultou na seguinte proposição:

Sequências do PET 1: Seja (a_n) uma sequência de números naturais onde a_1 é um número natural e $a_n = a_1 \cdot a_2 \cdot \cdots \cdot a_{n-1} + 1$, para $n \geq 2$. Então, (a_n) é uma sequência de números dois a dois primos entre si.

Demonstração: Sejam n e m naturais quaisquer. Suponhamos, sem perda de generalidade, que $n > m$. Assim,



$$a_n = a_1 \cdots a_m \cdots a_{n-1} + 1.$$

Seja $d = \text{mdc}(a_m, a_n)$. Então $d|a_n$ e

$$d|a_1 \cdots a_m \cdots a_{n-1}.$$

Logo,

$$d|a_n - a_1 \cdots a_n \Rightarrow d|1 \Rightarrow d = 1.$$

Portanto, os termos da sequência são dois a dois primos entre si.

■

Assim, conseguimos formar diversas sequências que revelam a infinitude dos números primos! Os alunos podem, nesse momento, construir suas próprias sequências.

Um fato curioso é que esse jeito não é a única forma de gerar uma sequência de números dois a dois primos entre si.

Repensando na estratégia utilizada na Sequência PET 1, decidimos formar o novo número da sequência multiplicando todos os anteriores e somando 1, mas, pela Propriedade 1, nada nos impede de poder multiplicar por outro inteiro não-nulo que desejasse também além dos anteriores.

Sendo assim, outra forma de gerar números dois a dois primos entre si é a partir de um resultado análogo à Propriedade 1:

Propriedade 2: Sejam m e n números naturais tais que m é menor do que n . Então, m e $n! + 1$ são primos entre si.

Demonstração: Basta perceber que o m aparece no número $n!$ (fatorial de n) e a partir da Propriedade 1, segue que m e $n!+1$ são primos entre si.

■

A partir dessa Propriedade 2, consegue-se outro tipo de sequência de números dois a dois primos entre si:

Sequência do PET 2: Seja (a_n) uma sequência de números naturais onde a_1 é um número natural e $a_n = a_{n-1}! + 1$. Então a sequência (a_n) é formada por termos dois a dois primos entre si.



Demonstração: Sejam a_i e a_j termos da sequência (a_n) tais que $i > j$. Observando que (a_n) é crescente, segue que $a_{i-1} \geq a_j$, pois $i - 1 \geq j$. Logo, pela Propriedade 2, segue que a_j e $a_{i-1}! + 1 = a_i$ são primos entre si.

Portanto, os termos da sequência (a_n) são dois a dois primos entre si.



Por exemplo, José escolheu para dar início a sua sequência $a_1 = 3$. Assim, obteve:

$$\begin{aligned}a_1 &= 3 \\a_2 &= 3! + 1 = 7 \\a_3 &= 7! + 1 = 5041 \\&\vdots \\a_n &= a_{n-1}! + 1, n \geq 3 \\&\vdots\end{aligned}$$

que é um caso particular da Sequência do PET 2.

Agora que construímos diferentes modos de gerar novas sequências de números dois a dois primos entre si, escolha a sua! É simples, basta escolher a sequências PET 1 ou 2 e atribuir os valores fixos que você deseje.

Essa é uma abordagem que pode ser utilizada por professores tanto do Ensino Fundamental como no Médio instigando os alunos a pesquisarem e a desenvolverem o espírito investigativo matemático. Ainda mais, promoverá ao aluno a alegria de possuir a própria demonstração da infinitude dos números primos reconhecendo que, apesar dos resultados matemáticos apresentados no Ensino Básico serem bem antigos, eles possam ter a alegria da redescoberta e colocar a própria característica neles.

CONSIDERAÇÕES FINAIS

Como foi apresentado na proposta metodológica da construção da demonstração da infinitude dos números primos, os alunos podem investigar e estabelecer conjecturas a respeito dos números naturais. Para isso, foi proposta a estratégia de observação de padrões por meio da experimentação e, após cada experimentação, fez-se o registro das novas informações obtidas.



A partir daí, foi sugerido uma generalização das propriedades conjecturadas e foi apresentada uma forma de validar essa conjectura por meio de uma demonstração. Ademais, as demonstrações das generalizações seguiram as mesmas ideias dos casos particulares o que evidencia como a experimentação foi positiva tanto para a conjecturação como para a validação desta.

Dessa forma, acredita-se que a proposta metodológica apresentada está conforme os direcionamentos da Base Nacional Comum Curricular. Outro fato interessante é que, historicamente, a pesquisa matemática sobre os números primos não tinha clara a importância e aplicabilidade desses estudos, os antigos matemáticos estudavam pelo prazer de aprender e descobrir novas propriedades. Neste contexto, esperamos que os professores se utilizem e aperfeiçoem essa proposta metodológica acrescentando dinâmicas que envolvem a criptografia e ofertando debates sobre a importância de pesquisar matemática mesmo que a aplicabilidade não esteja tão evidente.

AGRADECIMENTOS

Somos gratos a Deus e a todos os integrantes do grupo PET-Matemática-UFCG que contribuíram direta ou indiretamente na construção e aprimoramento deste trabalho.

REFERÊNCIAS

BNCC. Ministério da Educação. Secretaria da Educação Básica. **Base Nacional Comum Curricular.** Brasília, DF, 2017. Disponível em: <http://basenacionalcomum.mec.gov.br/#/site/inicio>. Acesso em: 01 set. 2020.



COUTINHO, Severino Collier. **Números Inteiros e Critografia RSA**. 2. ed. IMPA: SBM, 2000. ISBN 85-244-0124-9.

EUCLIDES. **Os Elementos**. Editora da Unesp. Tradução de Irineu Bicudo. 2009.

FRAZÃO, Dilva. **Euclides Matemático de Alexandria**. 2019. Disponível em: <https://www.ebiografia.com/euclides/>. Acesso em: 01 set. 2020.

MORENO, Víctor *et al.* **Biografía de Christian Goldbach**. 2015. Disponível em: <https://www.buscabiografias.com/biografia/verDetalle/8558/Christian%20Goldbach>. Acesso em: 01 set. 2020.

RIBENBOIM, Paulo. **Números Primos: mistérios e recordes**. 1. ed. IMPA: SBM, 2001. ISBN 978-85-244-0168-8.

TIPOS de criptografia: conheça os 10 mais usados e como funciona cada um. 2019. Disponível em: <https://cryptoid.com.br/valid/tipos-de-criptografia-conheca-os-10-mais-usados-e-como-funciona-cada-um/>. Acesso em: 01 set. 2020.

VIEIRA, Vandenberg Lopes. **Um Curso Básico em Teoria dos Números**. 1. ed. São Paulo: EDUEPB, 2015. ISBN 978-85-7879-275-6.