VII Encontro Cajazeirense de Matemática
A INOVAÇÃO E A CRIATIVIDADE TECENDO NOVOS CAMINHOS NA MATEMÁTICA
28 A 30 DE OUTUBRO DE 2020

P.A.S COM INFINITOS NÚMEROS PRIMOS QUE NINGUÉM SABE ONDE ESTÃO

Gabriel Pereira de Figueiredo
Universidade Federal de Campina Grande
gabrielpdf97@gmail.com
Parcialmente financiado pelo PET/FNDE/MEC

Fábio Lima de Oliveira
Universidade Federal de Campina Grande
fabiolimaoliveira99@gmail.com
Parcialmente financiado pelo PET/FNDE/MEC

Pedro Henrique Alves Guedes
Universidade Federal de Campina Grande
pedrohenrique.alvesguedes@gmail.com
Parcialmente financiado pelo PET/FNDE/MEC

Daniel Cordeiro de Morais Filho
Universidade Federal de Campina Grande
demoraisfilho@gmail.com
Parcialmente financiado pelo PET/FNDE/MEC

Resumo
Na História da Matemática existem vários problemas aparentemente simples, mas, de modo incrível, com grande aplicação prática. Um desses casos é a infinidade dos números primos, da qual dependem imensamente alguns atuais métodos de segurança de transmissão de mensagens. A primeira demonstração desse fato foi registrada por Euclides de Alexandria (323 a.C. - 283 a.C.) em *Os Elementos* (BICUDO, 2009). É sabido que não existe uma fórmula polinomial a coeficientes inteiros fornecendo somente números primos quando aplicada para números naturais (MOURA, 2018). Porém, podem-se encontrar Progressões Aritméticas (P.A.s) contendo uma infinidade de números primos! Com relação às P.A.s, "Um teorema clássico e de grande importância foi demonstrado por Dirichlet" (RIBENBOIM, 2001, p.168). Este teorema garante a infinidade de números primos em uma Progressão Aritmética, cujo termo geral é um polinômio de primeiro grau a coeficientes inteiros, mas não sabe-se onde estão nessa sequência. A demonstração do Teorema de Dirichlet requer conhecimentos matemáticos além dos objetivos desse artigo, entretanto, a mesma demonstração dada por Euclides, 21 séculos antes da de Dirichlet, pode ser usada para demonstrar alguns casos particulares do teorema geral dado pelo matemático alemão. Objetivamos fazer uma releitura dessa demonstração dada por Euclides, focando em seus métodos e trazer uma nova óptica para demonstrar casos particulares do Teorema de Dirichlet. Tudo factível de ser inteligível para quem tem formação básica mínima em Matemática, como é o caso de alunos do Ensino Médio e ingressantes nas universidades, dessa forma, a infinitude dos primos pode ser trazida para sala de aula.

Palavras-chave: Números Primos; Progressões Aritméticas; Euclides; Dirichlet.

1 Introdução

A distribuição dos números primos no conjunto dos Números Naturais é surpreendentemente caótica, uma fonte de mistérios, desafios e questionamentos. Há muita pesquisa científica sobre os números primos, objetivando encontrar propriedades interessantes que possam classificar esses números, saber onde localizá-los no conjunto dos Números Naturais.

Talvez a questão primordial, que iniciou as pesquisas sobre os números primos é: o conjunto dos Números Primos é infinito?

A resposta para essa pergunta foi dada por vários matemáticos, em diferentes épocas, ao longo dos séculos. Dentre eles destacamos: Euclides de Alexandria (323 a.C. - 283 a.C.), Leonhard Euler (1707-1783), Christian Goldbach (1690-1764) e Paul Erdös (1913-1996) (RIBENBOIM, 2001) (AIGNER e ZIEGLER, 2010) (EVES, 2004). O primeiro a responder a pergunta acima foi Euclides de Alexandria nos seus sapienciais *Elementos* (BICUDO, 2009): o conjunto dos números primos é infinito! A resposta de Euclides tornou-se o, hoje conhecido, Teorema da infinidade de números primos de Euclides (VIEIRA, 2015), cuja demonstração é vista em cursos básicos de Teoria dos números.

Procurando alguma "ordem" para o comportamento dos números primos, e, relacionando-se à resposta acima, poderíamos nos perguntar o que a demonstração de Euclides teria a ver com o aparecimento de números primos em uma Progressão Aritmética (P.A.). Esse questionamento motivou a realização da pesquisa na busca por essa relação, cujos resultados apresentaremos mais adiante neste trabalho.

Sabemos da infinidade dos números primos e que não existe fórmula polinomial, a coeficientes inteiros, que forneça somente números primos (MOURA, 2018). Porém, em algumas situações, podemos encontrar P.A.s, cujos termos gerais são polinômios a coeficientes inteiros, contendo infinitos números primos, mesmo sem saber quais são e onde estão.

Instituto Federal de Educação, Ciência e Tecnologia da Paraíba – Campus Cajazeiras ISSN: 2525-3727

Tanto os números primos quanto as P.A.s são conteúdos vistos no Ensino Básico. Ao conhecer esse tipo de sequência contendo infinitos números primos, os alunos podem despertar o interesse pela Matemática, tornando-a, mais atrativa. Com isso o professor tem uma oportunidade de abordar dois conteúdos de forma simultânea, reforçando o processo de ensino-aprendizagem.

Além disso, a infinidade dos números primos é essencial para um tipo de Criptografia (um conjunto de regras que visa codificar a informação de forma que só o emissor e o receptor consiga decifrá-la), que é uma ferramenta muito importante para a sociedade, nessa era digital em que vivemos. A Criptografia facilita o envio de mensagens de forma segura, e isso também é um fato curioso que pode chamar a atenção do aluno (COUTINHO, 2000).

Ao trabalhar com as P.A.s, tínhamos como objetivo encontrar algumas contendo uma infinidade de números primos, sem necessariamente exibí-los, para, então, apresentarmos o clássico Teorema de Dirichlet (RIBENBOIM, 2001). Porém, nos deparamos com o questionamento que surgiu a partir do estudo da demonstração feita por Euclides, e decidimos procurar uma relação entre essa demonstração e as Progressões Aritméticas que contém infinitos primos.

Com isso, temos o objetivo de mostrar essa relação de uma forma construtiva e interativa. Esse trabalho é um dos resultados da atividade de Leitura de Textos em Língua Estrangeira e da atividada Workshop Didático-Pedagógico, realizadas no PET-Matemática-UFCG.

2 Resultados Preliminares

Ao longo das demonstrações em nosso trabalho, utilizaremos alguns resultados que servirão de base e que não demonstraremos, pois nosso objetivo é outro. Seguem abaixo esses resultados.

Teorema Fundamental da Aritmética (T.F.A.): Seja $n \in \mathbb{N}$ e $n > 1$. Existem números primos $p_1 < p_2 < \cdots < p_k$ e $\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_k \in \mathbb{N}$ com $k \in \mathbb{N}$, tais que

$$n = p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_k^{\alpha_k}.$$

Instituto Federal de Educação, Ciência e Tecnologia da Paraíba – Campus Cajazeiras ISSN: 2525-3727

Essa decomposição é única, a menos da ordem dos fatores (VIEIRA, 2015).

Algoritmo da Divisão de Euclides: Sejam $a, b \in \mathbb{N}$. Então existem únicos $q, r \in \mathbb{Z}$ tais que

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

(VIEIRA, 2015)

Lema 1: Dado $k \in \mathbb{N}$, o conjunto $N_k = \{km + 1; m \in \mathbb{N}\}$ é fechado em relação a operação de multiplicação.

A demonstração desse lema é deixada como exercício, pelo fato de ser simples.

3 A relação entre a existência de infinitos números primos e a infinidade deles em uma Progressão Aritmética

3.1 Teorema da Infinidade dos Números Primos de Euclides

Em nossas investigações há uma questão de muita relevância no desenvolvimento de nossa proposta, que é o conhecimento da demonstração da infinidade dos números primos contida no famoso teorema:

Teorema 1: Existem infinitos números primos.

Demonstração: Suponha, por contradição, que exista uma quantidade finita de números primos $p_1, p_2, \dots, p_i, \dots, p_k$. Agora, considere o seguinte número

$$q = p_1 \cdot p_2 \cdot \cdots \cdot p_i \cdot \cdots \cdot p_k + 1.$$

Note que temos dois casos a considerar: q é um número primo ou q é composto.

Se q é primo, como $q > p_i$, para todo $i = 1, 2, \dots k$, então chegamos a uma contradição, pois, dessa maneira, existiria um número primo diferente de todos os primos $p_1, p_2, \dots, p_i, \dots, p_k$, listados inicialmente. Por outro lado, se q é composto, pelo T.F.A., existe p_i, com $1 \leq i \leq k$, tal que $p_i | q$. Assim, como $p_i | (p_1 \cdot p_2 \cdot \cdots \cdot p_i \cdot \cdots \cdot p_k)$, segue-se que

$$p_i | (q - p_1 \cdot p_2 \cdot \cdots \cdot p_i \cdot \cdots \cdot p_k) = 1,$$

Instituto Federal de Educação, Ciência e Tecnologia da Paraíba – Campus Cajazeiras ISSN: 2525-3727

o que é um absurdo, pois nenhum número natural primo divide 1. Logo, existe uma infinidade de números primos. ■

Sigamos agora para fazer uma análise mais detalhada desse teorema, sob um novo ponto de vista, extremamente útil para o que vamos fazer a seguir. Em seguida, partamos para nossos objetivos.

Podemos dividir essa demonstração em 4 etapas:

1ª Etapa: Supor, por contradição, que exista uma quantidade finita de números primos: $p_1, p_2, \dots, p_i, \dots, p_k$;
2ª Etapa: Construir um número especial que faz a demonstração funcionar. No caso, o número $q = p_1 \cdot p_2 \cdot \dots \cdot p_i \cdot \dots \cdot p_k + 1$;
3ª Etapa: Garantir que exista um número primo p_i, com $1 \leq i \leq k$, tal que $p_i | q$ (T.F.A.);
4ª Etapa: Usar a 3ª Etapa para chegar a um absurdo e concluir que existe uma infinidade de números primos.

3.2 Nova interpretação do Teorema da Infinidade dos Números Primos de Euclides

Observe um caso bem interessante: quando garantimos que existem infinitos números primos, já temos um primeiro caso de P.A. contendo infinitos números primos, a progressão dos números ímpares. De fato, observemos que dado $n \in \mathbb{N}$, os possíveis restos de sua divisão por 2 são 0 e 1. Assim, pelo Algoritmo da Divisão de Euclides, temos $n = 2k + r$, onde $k \in \mathbb{N}$ e $r \in \{0,1\}$. Desse modo, garantida a existência da infinidade dos números primos, a P.A. $(3, 5, 7, \dots, 2k + 1, \dots)$ contém uma infinidade de números primos, pois os números primos maiores do que 2 são todos ímpares. Esse é justamente o Teorema da Infinitude dos Números Primos de Euclides, visto de outra maneira!

Diante das discussões anteriores, como um primeiro caso da infinidade dos números primos em uma Progressão Aritmética (Teorema da Infinitude dos Números Primos de Euclides), já temos:

Teorema 2: Na P.A. $(3, 5, 7, \dots, 2k + 1, \dots)$ há uma infinidade de números primos.
(Uma observação crucial: "ninguém sabe quem são e nem onde estão" esses primos.)

Ao nos depararmos com a demonstração do *Teorema 1* surge, geralmente, a seguinte pergunta: *por que, na 2ª Etapa da demonstração, é escolhido o número* $q = p_1 \cdot \cdots \cdot p_k + 1$? A fim de responder essa pergunta, podemos então, fazer uma releitura da demonstração do *Teorema 1*, por meio de P.A.s com infinitos números primos.

Teorema 1: Existem infinitos números primos.
Demonstração sob uma nova óptica:

1ª Etapa: Suponha, por contradição, que exista uma quantidade finita de números primos $p_1, p_2, \dots, p_k$. Como qualquer primo $p_i > 2$ é da forma $2k + 1$, teremos uma quantidade finita de primos na P.A. $(3, 5, 7, \dots, 2k + 1, \dots)$, com os quais formamos o seguinte conjunto de números primos

$$P = \{3, 5, 7, 11, \dots, (2k + 1)\}.$$

2ª Etapa: Considere o número $q = 2\big(3 \cdot 5 \cdot \dots \cdot (2k + 1)\big) + 1$. Observe que, q é um número da P.A. $(3, 5, 7, \dots, 2k + 1, \dots)$, pois $q = 2k' + 1$, com $k' = 3 \cdot 5 \cdot \dots \cdot (2k + 1)$.

3ª Etapa: Se q é primo**,** então a demonstração encerra, pois $q > p_i$, para qualquer $p_i \in P$, o que é um absurdo. Caso contrário, q é composto e é da forma $2k + 1$, daí, pelo T.F.A., deve existir um número primo $p_i \in P$ tal que $p_i | q$. Assim, prosseguimos para a última etapa.

4ª Etapa: Como $p_i \in P$, consequentemente $p_i | 2\big(3 \cdot 5 \cdot \dots \cdot (2k + 1)\big)$, e $p_i | q$, segue que

$$p_i | [q - 2\big(3 \cdot 5 \cdot \dots \cdot (2k + 1)\big)] = 1.$$

Dessa forma, da *3ª Etapa* chegamos a um absurdo, pois um número primo não pode dividir a unidade. Portanto, o conjunto dos números primos na P.A. $(3, 5, \dots, 2k + 1, \dots)$ é infinito.

Note que, na *2ª Etapa*, foi essencial considerarmos o número $q = 2k' + 1$ como um termo da P.A. $(3, 5, \dots, 2k + 1, \dots)$, onde $k' = 3 \cdot 5 \cdot \dots \cdot (2k + 1)$. Isso explica o fato de escolhermos o número q da forma $q = p_1 \cdot p_2 \cdot \cdots \cdot p_k + 1$, na primeira demonstração, onde, lá, o p_1 faz o papel do número 2. Perceba, também, que o fato de não escolhermos o 2 para estar no conjunto P, pois esse número não é ímpar, não interfere na demonstração.

Vale destacar que essa ideia, utilizada na releitura da demonstração de Euclides, segue um modelo geral para a demonstração de alguns outros casos de P.A.s que possuem infinitos primos. Apresentaremos alguns desses casos na próxima seção:

4 Infinidade de números primos na Progressão Aritmética $(\mathbf{5}, \mathbf{8}, \mathbf{11}, \mathbf{14}, \ldots, \mathbf{3}\boldsymbol{k} + \mathbf{2}, \ldots)$

Como vimos, a releitura da demonstração da infinidade dos números primos realizada por Euclides de Alexandria nos dá a infinidade dos números primos na P.A. $(3, 5, 7, \ldots, 2k + 1, \ldots)$. Com isso, temos um primeiro caso de Progressão Aritmética contendo infinitos números primos.

Agora, observemos que dado $n \in \mathbb{N}$, os possíveis restos de sua divisão por 3 são 0, 1 e 2. Desse modo, pelo Algoritimo da Divisão de Euclides, enunciado nos resultados preliminares, obtemos as seguintes formas para n,

$$n = 3k \text{ ou } n = 3k + 1 \text{ ou } n = 3k + 2. \quad (1)$$

Sabemos que o conjunto dos números primos é infinito (Teorema da Infinitude dos Números Primos de Euclides), ou seja, deve existir uma quantidade infinita deles na P.A. de termo geral $3k + 2$, ou na P.A. de termo geral $3k + 1$, ou em ambas. Isso ocorre, pois a P.A. de termo geral $3k$ é formada por múltiplos de 3 e, consequentemente, nenhum deles, maior do que 3, é um número primo. Com isso, é natural nos questionarmos em qual das progressões acima há uma infinidade de números primos. Será que teremos apenas em uma das P.A.s citadas ou em ambas?

Adiantamos a resposta: ambas as P.A.s contém uma infinidade de números primos. Não abordaremos o caso da P.A. $(4, 7, \ldots, 3k + 1, \ldots)$ mas demonstraremos, seguindo o padrão de demonstração da Seção 3, que há uma infinidade de primos na P.A.:
$(5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 38, 41, 44, 47, 50, 53, 56, 59, 62, 65, 68, \ldots)$.

Teorema 3: Na P.A. $(5, 8, 11, 14, \ldots, 3k + 2, \ldots)$ há uma infinidade de números primos.

(Uma observação crucial: mais uma vez, "ninguém sabe quem são e nem onde estão" esses primos.)

Demonstração: Inicialmente, note por (1) que, se $p > 3$ é um número primo, então ele é da forma ou $3k + 1$ ou $3k + 2$, com $k \in \mathbb{N}$, pois um número da forma $3k$ não é primo, para $k > 1$. Portanto, analisaremos os casos em que o número primo é da forma $3k + 1$ ou $3k + 2$.

Suponhamos que exista uma quantidade finita de números primos na P.A. $(5, 8, 11, 14, \ldots, 3k + 2, \ldots)$, com os quais formamos o seguinte conjunto de todos os números primos da P.A.,

$$\mathcal{P} = \{5, 11, \ldots, 3k_0 + 2\}, \text{ com } k_0 \in \mathbb{N}. \ (1^{\text{a}} \text{ Etapa})$$

Considere o número

$$q = 3(5.11.\cdots.(3k_0 + 2)) + 2. \ (2^{\text{a}} \text{ Etapa})$$

Temos duas opções para q: ou ele é um número primo, ou ele é um número composto. Nosso objetivo é mostrar que essas duas situações não podem ocorrer, donde concluiremos que existe uma infinidade de números primos na P.A. em questão.

Se q for primo**,** então a demonstração encerra-se, pois $q > p_i$, para qualquer $p_i \in \mathcal{P}$, o que é um absurdo. Caso contrário, q é um número composto e, pelo T.F.A., existe um número primo p tal que $p|q$ (3^{a} Etapa). Pelo fato de p ser um número primo, então $p = 3k + 1$ ou $p = 3k + 2$, com $k \in \mathbb{N}$.

No caso em que $p = 3k + 2$, então existe $p_i \in \mathcal{P}$, tal que $p = p_i$ e, consequentemente,

$$p\big|\big[q - 3\big(5.11.\cdots.p_i.\cdots.(3k_0 + 2)\big)\big] \Rightarrow p|2,$$

o que não pode ocorrer, pois $p > 2$. Portanto, todo divisor primo de q não pode ser da forma $3k + 2$.

Dessa forma, teríamos todos os números primos da decomposição de q da forma $3k + 1$. Mas isso também não pode ocorrer, pois, pelo Lema 1 (p. 4), o produto de números da forma $3k + 1$, ainda é um número da forma $3k + 1$, o que não é o caso, pois q é da forma $3k + 2$ (4^{a} Etapa). Portanto, na P.A. $(5, 8, 11, 14, \ldots, 3k + 2, \ldots)$ há uma infinidade de números primos que ninguém sabe quem são e nem onde estão! ■

Instituto Federal de Educação, Ciência e Tecnologia da Paraíba – Campus Cajazeiras ISSN: 2525-3727

5 O Clássico Teorema de Dirichlet

Vimos dois casos de P.A.s contendo uma infinidade de números primos. São elas, $(3, 5, \ldots, 2k + 1, \ldots)$, de razão $r = 2$ e primeiro termo $a = 3$, e $(5, 8, \ldots, 3k + 2, \ldots)$, de razão $r = 3$ e primeiro termo $a = 5$.

Note que no primeiro caso, $r = 2$ e $a = 3$ são primos entre si, ou seja, não existe um divisor, diferente de 1, que seja comum entre eles. Da mesma forma, no segundo caso, $r = 3$ e $a = 5$ são primos entre si. Outros exemplos de P.A.s que possuem infinitos números primos, que ninguém sabe quais são e nem onde estão, são $(7, 11, \ldots, 4k + 3, \ldots)$, de razão $r = 4$ e primeiro termo $a = 7$, e $(11, 17, \ldots, 6k + 5, \ldots)$, de razão $r = 6$ e primeiro termo $a = 11$.

A demonstração de que existem infinitos números primos nesses exemplos é semelhante às demonstrações dos Teoremas 1 e 2. Um fato curioso nessas P.A.s é que em todas elas, a razão r e o primeiro termo a são primos entre si. Isso não é uma mera coincidência, de maneira geral, podemos agora enunciar o seguinte teorema geral e muito interessante:

Teorema (Dirichlet): Se $r \geq 2$ e $a \neq 0$ são inteiros primos entre si, então a Progressão Aritmética

$$a,\ a + r,\ a + 2r,\ a + 3r,\ \ldots,\ a + nr, \ldots$$

contém uma infinidade de números primos (SILVA JÚNIOR, 2017).

A demonstração do Teorema de Dirichlet demanda resultados avançados de Teoria Analítica dos Números e não faremos aqui, pois foge ao objetivo deste trabalho. Como visto anteriormente**,** o Teorema da infinidade dos números primos de Euclides é o que podemos considerar como primeiro caso particular desse teorema**.**

6 Considerações Finais

A importância de seguir apresentando, consecutivamente, o modelo de demonstração dos casos particulares de P.A.s contendo infinitos números primos, favoreceu a percepção de

Instituto Federal de Educação, Ciência e Tecnologia da Paraíba – Campus Cajazeiras ISSN: 2525-3727

um esquema de demonstração que estava velado na demonstração dada por Euclides e funciona em outros casos, mais específicos.

Esse foi um resultado surpreendente para nós e ao mesmo tempo gratificante para a pesquisa realizada, principalmente por podermos trazer esses resultados para a comunidade de professores e alunos, de maneira simples e que pode ser apresentada em uma sala de aula. Pretendemos dar seguimento ao estudo do tema apresentado, e avançar nas demonstrações relacionadas com a infinidade dos números primos em outras P.A.s.

Referências

AIGNER, M.; ZIEGLER, G. M. **Proofs from the book**. Berlim: Springer-Verlag, 2010.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA.** 2. ed. IMPA: SBM, 2000.

EUCLIDES. **Os Elementos**. Tradução: Irineu Bicudo. São Paulo: UNESP, 2009.

EVES, H. **Introdução à história da matemática.** Tradução: Hygino H. Domingues. Campinas: Unicamp, 2004.

SILVA JÚNIOR, J. C. **O teorema de Dirichlet:** primos em progressão aritmética. Orientador: Bruno Henrique Carvalho Ribeiro. 2017. Dissertação (Mestrado Profissional em Matemática-PROFMAT) - Universidade Federal da Paraíba - UFPB, João Pessoa, 2017.

MOURA, F. T. de. **Números primos:** uma fórmula geradora. Orientador: Robson Martins de Mesquita. 2018. Dissertação (Mestrado Profissional em Matemática-PROFMAT) - Universidade Federal do Tocantins, Arraias -TO, 2018.

RIBENBOIM, P. **Números Primos:** mistérios e recordes. 1. ed. IMPA: SBM, 2001.

VIEIRA, V. L. **Um curso básico em teoria dos números.** São Paulo: EDUEPB, 2015.