Sequências de P.A.s Contendo Infinitos Números Primos – Parte II

Fábio Lima de Oliveira[1] **- fabiolimaoliveira99@gmail.com**
Gabriel Pereira de Figueiredo[1] **- gabrielpdf97@gmail.com**
Daniel Cordeiro de Morais Filho[1] **- daniel@mat.ufcg.edu.br**

[1]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil - Parcialmente financiado pelo MEC/FNDE/PET

Resumo: *A descoberta de grandes números primos contribui para a melhoria do método usado pela Criptografia RSA, que é uma ferramenta importante na segurança da comunicação nas mídias digitais. O estudo dos números primos não é tão atual quanto a Criptografia, séculos atrás, Euclides de Alexandria (360-295 a.C) já havia dado uma demonstração da infinidade dos números primos. O matemático Johann Peter Gustav Lejeune Dirichlet (1805-1859) relacionou o estudo sobre a infinidade de números primos com progressões aritméticas (P.A.s) provando que qualquer progressão aritmética de termo geral* $a+nq$*, com* $n \in \mathbb{N}$ *e* $a, q \in \mathbb{Z}$*, tais que* $mdc(a, q) = 1$*, possui infinitos números primos (SHIELDS, 1989). Esse é o conhecido Clássico Teorema de Dirichlet. Aqui, abordaremos alguns casos particulares de P.A.s associadas a esse teorema como continuação de um trabalho já publicado nessa direção (FIGUEIREDO et al., 2020). Para o desenvolvimento do trabalho, realizamos uma pesquisa bibliográfica sobre o tema, inclusive por meio de leituras em língua estrangeira. Após os estudos proveninetes dessas pesquisas, sob a orientação do Tutor Prof. Daniel Cordeiro, do Grupo PET-Matemática-UFCG, elaboramos uma apresentação para ser exposta na atividade Workshop didático-pedagógico desenvolvida pelo Grupo. Ao se debruçar sobre essa temática, é perceptível que mesmo com as dificuldades em trabalhar com números primos, as P.A.s surgem como uma forma de manter um certo controle sobre números primos, ainda que não se possa saber quais dos termos dessas P.A.s são números primos e onde estão.*
Palavras-chave*: Infinidade dos Números Primos; Progressões Aritméticas; Teorema de Dirichlet.*

1. Introdução

É possível que em algum momento se ouça a notícia da descoberta de um grande número primo, até então desconhecido, fato que é considerado como um novo recorde no campo de pesquisa por grandes números primos. Muitos pesquisadores dedicam grande parte de seu tempo e de seu esforço na busca por quebrar esses recordes, seja por curiosidade ou até mesmo por motivações financeiras. Um exemplo é o GIMPS (Great Internet Mersenne Prime Search), um grupo que reúne pesquisadores na busca por grandes números primos de Mersenne (WOLTMAN; KUROWSKI, 2021).

Independentemente do que os move, esses feitos tem ajudado, por exemplo, no aprimoramento da Criptografia RSA, que é uma ferramenta muito importante para o envio de mensagens seguras. De forma geral, a Criptografia consiste no conjunto de regras que visa codificar a informação de forma que só o emissor e o receptor conheçam a mensagem (COUTINHO, 2000).

A principal relação entre a Criptografia RSA e a obtenção de grandes números primos está justamente no fato de que, quanto maior for um número primo, maior é a segurança dos códigos estabelecidos na criptografia. No entanto, encontrar esses números grandes é uma tarefa difícil, pois nunca foi encontrado e, certamente, não existe um padrão na sequência infinita dos números primos.

Desde a antiguidade, já se sabia da infinidade dos números primos com a demonstração dada por *Euclides de Alexandria* (360-295 a.C). Posterior à demonstração dada por Euclides, tiveram muitas outras, cada uma com sua forma peculiar de observar o mesmo fato. Um pesquisador de muito prestígio, *Pierre de Fermat* (1601-1665) também se debruçou sobre o tema e tentou uma fórmula de gerar números primos, a qual nem todos os números dessa sequência são primos, porém ficaram conhecidos como *Números de Fermat* (EVES, 2004).

Já no século XIX, o matemático *Johann Peter Gustav Lejeune Dirichlet* (1805-1859) apresentou uma nova forma de olhar para a infinidade dos números primos, quando exibiu um vínculo entre a infinidade desses números e as Progressões Aritméticas (P.A.s) (SHIELDS, 1989). O resultado de Dirichlet é o *Clássico Teorema de Dirichlet* (RIBENBOIM, 2001), que pode ser enunciado da seguinte forma:

Teorema 1. *Sejam $r \geq 2$ e $a \neq 0$ inteiros primos entre si, então a progressão aritmética*

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

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

A demonstração para esse teorema é extremamente técnica e pode ser encontrada em Selberg (1949). Diante disso, o presente trabalho é a continuação de um estudo inicial que pode ser lido em Figueiredo et al. (2020), no qual pretende-se abordar mais alguns casos particulares do Teorema de Dirichlet. Diferente do primeiro, nessa continuação as P.A.s exigem alguns resultados preliminares, para só então seguirmos para o modelo de demonstração, cujas ideias germinais, já se encontram no Teorema da Infinitude dos Números Primos de Euclides.

2. Metodologia

Este trabalho é proveniente de duas das atividades realizadas pelo Grupo PET-Matemática-UFCG, intituladas "Pesquisa em competências básicas no uso da linguagem escrita e oral, em idioma estrangeiro e na área de tecnologias de informação e comunicação" e "Workshop didático-pedagógico de prática de ensino em Matemática". Para o desenvolvimento do trabalho, realizamos uma pesquisa bibliográfica sobre o tema, por meio da leitura de livros, artigos e pesquisa em sites. Após os estudos provenientes da pesquisa, sob a orientação do Tutor do Grupo, Prof. Daniel Cordeiro, partimos para a fase de elaboração de uma apresentação em slides para ser exposta no Workshop didático-pedagógico.

3. Resultado e discussão

Em um trabalho já publicado demonstramos alguns casos particulares de P.A.s contendo uma infinidade de números primos (FIGUEIREDO et al., 2020). Nele podemos perceber um certo "padrão" de demonstração, também encontrado na demonstração do Teorema da Infinidade de Números Primos dada por Euclides. Nesse sentido, apresentaremos agora mais dois casos de progressões aritméticas com uma infinidade de números primos, cujas demonstrações desse fato apresentam algumas peculiaridades.

Ademais, para nossa abordagem utilizaremos alguns resultados preliminares que apresentaremos a seguir.

Teorema 2 (Teorema Fundamental da Aritmética)**.** *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*

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

Essa decomposição é única, a menos de ordem (VIEIRA, 2015).

Teorema 3 (O Pequeno Teorema de Fermat)**.** *Se q é primo e $s \in \mathbb{N}$, então $q \mid s^q - s$. Ou ainda em termos de congruência*

$$s^q \equiv s \ (mod\ q)$$

(VIEIRA, 2015).

3.1 A P.A. $(1, 5, \ldots, 4k+1, \ldots)$

Para demonstrarmos a infinitude de números primos na P.A. $(1, 5, \ldots, 4k+1, \ldots)$ necessitamos do seguinte lema:

Lema 3.1. *Todo número da forma s^2+1, com $s \in \mathbb{N}$ e $s > 1$, tem algum divisor primo da P.A. $(5, 9, \ldots, 4k+1, \ldots)$ e não pode ter divisores primos na P.A. $(7, 11, \ldots, 4k+3, \ldots)$ (RIBENBOIM, 2001).*

Demonstração: Observemos que $s^2 + 1 \neq 2^r$, com $r \in \mathbb{N}$ e $r > 2$. De fato, se s for par, então $s^2 + 1$ é ímpar e não há o que discutir. Por outro lado, se s for ímpar, isto é, $s = 2m + 1$, então $s^2 + 1$ é um número da forma $4k + 2$, com $k \in \mathbb{N}$, donde segue que $4 \nmid s^2 + 1$, mas $4 \mid 2^r$, pois $r > 2$.

Além disso, o Teorema 2 garante que existe p primo tal que $p \mid s^2 + 1$. Desse modo, como $p \neq 2$ teremos p da forma $4k + 1$ ou $4k + 3$, para algum $k \in \mathbb{N}$. Mostraremos que p só pode ser da forma $4k + 1$. Com efeito, suponha por contradição que $p = 4k + 3$, para algum $k \in \mathbb{N}$. Assim, podemos observar que

$$p = 4k + 3 = 4m - 1, \text{ onde } m = k + 1 \text{ para algum } k \in \mathbb{N}.$$

Ademais, como $p \mid s^2 + 1$, da definição de congruência, segue que

$$s^2 \equiv -1(mod\ p). \tag{1}$$

Das propriedades de congruência, podemos elevar ambos os lados de (1) pela potência $\frac{p-1}{2} \in \mathbb{N}$, e assim, temos

$$\begin{aligned}(s^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}}(mod\ p) &= (-1)^{\frac{4m-2}{2}}(mod\ p)\\ &= (-1)^{2m-1}(mod\ p)\\ &= -1(mod\ p).\end{aligned}$$

Daí, segue que

$$s^{p-1} \equiv -1(mod\ p) \Rightarrow p \mid s^{p-1} + 1.$$

Logo, $p \mid s^p + s$. Além disso, pelo Teorema 3, $p \mid s^p - s$. Assim, tem-se

$$p \mid (s^p + s) - (s^p - s) = 2s.$$

Dessa forma, sendo p um primo ímpar segue que $p \mid s$ e, consequentemente, $p \mid s^2$. Como $p \mid s^2 + 1$, obtemos

$$p \mid s^2 + 1 - s^2 = 1,$$

o que é um absurdo. Portanto, $p = 4k + 1$ para algum $k \in \mathbb{N}$. ■

Com isso, partiremos para a demonstração do Teorema.

Teorema 4. *Na P.A.* $(1, 5, \ldots, 4k + 1, \ldots)$ *há uma infinidade de números primos.*

Demonstração: Suponhamos, por contradição, que exista uma quantidade finita de números primos na P.A. $(5, 9, \ldots, 4k + 1, \ldots)$, com $k \in \mathbb{N}$, digamos

$$P := \{5, 13, \ldots, 4k_0 + 1\}.\ (1^{\underline{a}}\ Etapa)$$

Considere o número $n = (2 \cdot 5 \cdot \ \ldots \ \cdot (4k_0 + 1))^2 + 1 > 1$ ($2^{\underline{a}}$ *Etapa*). Temos $n > p$ para qualquer $p \in P$ e daí, como $(2 \cdot 5 \cdot \ \ldots \ \cdot (4k_0 + 1))^2 > 1$, pelo Lema 3.1, existe $q = 4k+1$ primo, para algum $k \in \mathbb{N}$, tal que $q \mid n$ ($3^{\underline{a}}$ *Etapa*).

Ora, $q \notin P$, pois caso contrário $q \mid (2 \cdot 5 \cdot \ \ldots \ \cdot (4k_0 + 1))^2$ e como $q \mid n$, teríamos

$$q \mid [n - (2 \cdot 5 \cdot \ \ldots \ \cdot (4k_0 + 1))^2] = 1,$$

o que é um absurdo ($4^{\underline{a}}$ *Etapa*).

Portanto, deve existir uma infinidade de números primos na P.A. $(1, 5, \ldots, 4k + 1, \ldots)$. ■

Observe que o número n foi tomado como um número da PA, pois $n = 4(5 \cdot 13 \cdot \ \ldots \ \cdot (4k_0 + 1))^2$. Daí, na demonstração anterior, podemos notar algumas etapas semelhantes as encontradas em Figueiredo et al. (2020), apenas diferenciando-se por informações adicionais. Agora, veremos um caso mais geral.

3.2 P.A. $(1, 1+2^r, 1+2\cdot 2^r, \ldots, 1+k\cdot 2^r, \ldots)$, com $r>2$ e $k\in\mathbb{N}$

Para demonstrarmos a infinitude de números primos na P.A. $(1, 1+2^r, 1+2\cdot 2^r, \ldots, 1+k\cdot 2^r, \ldots)$ precisaremos do seguinte lema:

Lema 4.1. *Sejam p um número primo e $M, n\in\mathbb{N}$, com $mdc(M,n)=1$, tais que $p \mid M^n-1$. Seja $b\geq 1$ o menor natural tal que $p\mid M^b-1$. Então $b\mid n$.*

Demonstração: Inicialmente, observe que a existência de b é garantida pelo Teorema 3 e pelo Princípio da Boa ordenação.

Ademais, nas condições dadas, temos

$$M^n \equiv 1 (mod\ p) \tag{2}$$

e

$$M^b \equiv 1 (mod\ p). \tag{3}$$

Daí, pelo Algoritmo da Divisão, segue que $n=qb+r$, onde $q>0$ e $0\leq r<b$.

Suponha que $r>0$, ou seja, $r\geq 1$. Segue de 3 e das propriedades de congruência que

$$\begin{aligned}(M^b)^q \equiv 1^q\ (mod\ p) &\Rightarrow (M^b)^q M^r \equiv 1^q\cdot M^r\ (mod\ p)\\ &\Rightarrow M^n = M^{(qb+r)} \equiv M^r\ (mod\ p)\end{aligned}$$

Daí, observando 2 tem-se $M^r\equiv 1\ (mod\ p)$, o que contraria a minimalidade de b, pois $1\leq r<b$. Portanto, $r=0$ e $b\mid n$. ■

Teorema 5. *A progressão aritmética $(1, 1+2^r, 1+2\cdot 2^r, \ldots, 1+k\cdot 2^r, \ldots)$, com $r>2$ fixo e $k\in\mathbb{N}$, contém uma infinidade de números primos.*

Demonstração: Suponhamos que exista uma quantidade finita de números primos na P.A. $(1, 1+2^r, 1+2\cdot 2^r, \ldots, 1+k\cdot 2^r, \ldots)$, digamos

$$\mathcal{P} := \{p_1, p_2, \ldots, p_n\}, n\in\mathbb{N}.$$

Desse modo, os elementos de $\mathcal{P}$ são os únicos primos tais que $2^r | p_i-1$, para $1\leq i\leq n$.

Considere o número $N = 2\cdot p_1\cdot p_2\cdot\ \ldots\ \cdot p_n$ e $M = N^{2^{r-1}}$. Desse modo, mostraremos que existe p primo tal que $2^r | p-1$ e $p\neq p_i$ para $1\leq i\leq n$.

Com efeito, nas condições dadas tem-se $M-1>1$ e, além disso, observe que $M^2-1=(M-1)(M+1)$, ou seja, $M-1\mid M^2-1$. Ademais, como $1<M-1<M^2-1$, pelo Teorema 2, segue que existe p primo tal que

$$p \mid \frac{M^2-1}{M-1} = \frac{(M-1)(M+1)}{M-1}.$$

isto é, $p\mid M+1$.

Assim, se $p\mid M-1$, como $p\mid M+1$ então $p\mid M+1-(M-1)=2$. Daí, sendo p primo tem-se $p=2$, donde segue que

$$p \mid M = N^{2^{r-1}} = (2\cdot p_1\cdot p_2\cdot\ \ldots\ \cdot p_n)^{2^{r-1}}$$

e, consequentemente, $p\mid M-(M-1)=1$, o que nos leva a um absurdo. Logo,

$$p \nmid M-1 = N^{2^{r-1}}-1 \tag{4}$$

Por outro lado, sabendo que $p\mid M+1$, tem-se

$$p \mid (M+1)(M-1) = M^2-1 = N^{2^r}-1. \tag{5}$$

Observe que se $p\in\mathcal{P}$, então $p\mid N$ e, por conseguinte, $P\mid M$ donde teríamos $p\mid M+1-M=1$, o que é um absurdo. Logo, $mdc(p,N)=1$ e assim, pelo Teorema 3 obtemos

$$p \mid N^{p-1}-1. \tag{6}$$

Sabendo que $p \notin \mathcal{P}$, para concluírmos a demonstração, basta mostrarmos que $2^r \mid p-1$, chegando a uma contradição.

De fato, de 5 e 6, sendo $t \geq 1$ o menor natural tal que $p \mid N^t - 1$, segue pelo Lema 4.1 que $t \mid 2^r$ e $t \mid p-1$, respectivamente. Ademais, de 4 tem-se que $t \nmid 2^{r-1}$, isto é, $t \neq 2^s$ para $1 \leq s < r$. Logo, $t = 2^r$, donde obtém-se $2^r \mid p-1$, o que é uma contradição.

Portanto, existe uma infinidade de números primos na P.A. $(1, 1+2^r, 1+2\cdot 2^r, \ldots, 1+k\cdot 2^r, \ldots)$. ■

Com isso, encontramos uma forma para obter alguns dos números primos, o que nos dá um certo controle, no entanto, não conhecemos esses números primos e nem sabemos onde estão.

4. Conclusões

De acordo com o apresentado, pode-se perceber a dificuldade em trabalhar com os números primos, uma vez que não conhecemos todos, ou seja, não temos uma fórmula que descreva todo o conjunto dos números primos. Entretanto, ao trabalhar com certos tipos de progressões aritméticas, temos um "controle" sobre uma infinidade de números primos mesmo sem saber quem são e onde estão.

As P.A.s vistas neste trabalho remetem à demonstração de Euclides, porém fornecendo uma nova forma de observar a infinidade de números primos, trabalhando com outros resultados importantes da Teoria dos números.

Agradecimentos

Agradecemos ao FNDE, Fundo Nacional de Desenvolvimento da Educação Brasil, pelo financiamento e aos demais integrantes do Grupo PET-Matemática-UFCG, pela colaboração.

Referências

COUTINHO, S. C. *Números Inteiros e Criptografia RSA*. 2. ed. IMPA: SBM, 2000. Citado na página 1.

EVES, H. *Introdução a história da matemática*. Campinas: Unicamp, 2004. Tradução: Hygino H. Domingues. Citado na página 1.

FIGUEIREDO, G. P. de; OLIVEIRA, F. L. de; GUEDES, P. H. A.; DE MORAIS FILHO, D. C. P.a.s com infinitos números primos que ninguém sabe onde estão. *VII ECMAT*, 2020. 10 p. Citado 3 vezes nas páginas 1, 2 e 3.

RIBENBOIM, P. *Números Primos: mistérios e recordes*. 1. ed. IMPA: SBM, 2001. Citado 2 vezes nas páginas 1 e 2.

SELBERG, A. An elementary proof of dirichlet's theorem about primes in an arithmetic progression. *Annals of Mathematics*, v. 50, n. 2, 1949. 297-304 p. Disponível em: ⟨https://www.jstor.org/stable/1969454⟩. Citado na página 2.

SHIELDS, A. Lejeune dirichlet and the birth of analytic number theory: 1837-1839. *The Mathematical Intelligencer*, v. 11, n. 4, p. 07–11, 1989. Citado na página 1.

SILVA JUNIOR, J. C. *O teorema de Dirichlet: primos em progressão aritmética*. Dissertação (Mestrado), João Pessoa, 2017. Citado na página 2.

VIEIRA, V. L. *Um curso básico em Teoria dos números*. Campina Grande: EDUEPB, 2015. 560 p. Citado na página 2.

WOLTMAN, G.; KUROWSKI, S. Great internet mersenne prime search (gimps). PrimeNet, 2021. Disponível em: ⟨https://www.mersenne.org/primes/⟩. Citado na página 1.