UMA COLEÇÃO DE DEMONSTRAÇÕES DA EXISTÊNCIA DE INFINITOS PRIMOS

Daniel Dunck Cintra
IFMT - Campus Pontes e Lacerda - Fronteira Oeste
danieldunck@gmail.com

RESUMO

Os números primos são fascinantes e despertam a curiosidade dos estudiosos há muitos séculos. Euclides, há mais de dois mil anos, mostrou que os números primos são infinitos. Neste artigo apresentaremos diversas demonstrações da infinitude dos primos.

ABSTRACT

The prime numbers are fascinating and cause the curiosity of scholars for many centuries. Euclid, more than two thousand years ago, showed that the prime numbers are infinite. In this article we will present several demonstrations of the infinity of primes.

Palavras-chave: Números primos, Infinitude.

1 INTRODUÇÃO

A ideia da construção deste artigo se deu durante o desenvolvimento de uma dissertação do PROFMAT que foi descontinuada, pois o autor mudou o objeto de pesquisa no decorrer do mestrado.

Um dos objetivos do trabalho que vinha sendo desenvolvido era reunir, em um capítulo, diversas demonstrações da infinitude dos números primos criadas ao longo dos séculos. Por meio de pesquisa bibliográfica, reunimos uma quantidade razoável de demonstrações, algumas mais simples e outras mais elaboradas. É interessante perceber que as demonstrações envolvem diversas áreas da matemática, fazendo com o que leitor possa relembrar alguns tópicos da matemática e se entreter na leitura.

No final do artigo, apresentamos uma demonstração da infinitude dos números primos que é um novo olhar sobre outras demonstrações já realizadas. Ela foi inspirada na demonstração realizada por Northshield (2015), pelo fato de conseguir ser escrita em somente uma linha.

2 DEMONSTRAÇÕES DA INFINITUDE DOS NÚMEROS PRIMOS

A partir daqui, apresentaremos as demonstrações que encontramos da infinitude dos números primos em diversas literaturas. Tomamos a liberdade de reescrever alguns passos das demonstrações, mas mantendo sua ideia original, de modo que fique bem didático para quem está lendo. Começaremos com a demonstração mais tradicional que consta basicamente em todos os livros que envolvem teoria dos números. Essa demonstração foi feita por Euclides. Na sequência, trataremos de outras, algumas parcialmente similares à realizada por Euclides, e outras um tanto diferentes e intrigantes.

2.1 EUCLIDES (APROXIMADAMENTE 300 A.C).

Podemos encontrar a demonstração feita por Euclides em diversos livros, por exemplo, em [1].

Suponha, por absurdo, que $2, 3, 5, ..., p_r$ sejam todos os números primos, ou seja, existe uma quantidade finita de números primos. Considere $N = 2 \times 3 \times 5 \times 7 \times ... \times p_r + 1$, como esse número é maior que p_r, então N é um número composto. Entretanto, observe que ao dividir N por qualquer primo que vai 2 a p_r teremos resto 1, pois podemos escrever $N = p_i \cdot k + 1$ com i variando de 1 a r. Ou seja, N é primo ou é divisível por outro primo além de $2, 3, 5, 7, ..., p_r$, isso é uma contradição, pois supomos que $2, 3, 5, 7, ..., p_r$ são todos os primos.

É comum pensar que multiplicar a sequência de todos números primos até certo p primo e somar 1 resultaria em um número primo e isso nem sempre é verdade. Observe:

$2 + 1 = 3$, primo

$2 \times 3 + 1 = 7$, primo

$2 \times 3 \times 5 + 1 =$, primo

$2 \times 3 \times 5 \times 7 + 1 = 211$, primo

$2 \times 3 \times 5 \times 7 \times 11 + 1 = 2311$, primo

$2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$, composto

Observe que a demonstração realizada não garante que $2.3.5.7...p_r + 1$ será um número primo. Ela mostra apenas que que número $2.3.5.7...p_r + 1$ será divisível por um número primo maior que p_r, implicando que haja pelo menos um primo além desses.

2.2 KUMMER (1878)

Podemos encontrar a demonstração de Kummer, por exemplo, em [2].

O matemático alemão Ernst Kummer apresentou um novo olhar sobre a demonstração feita por Euclides.

Suponha, por aburdo, que a quantidade de números primos seja finita, ou seja, $2, 3, 5, 7, ..., p_r$ sejam todos os primos. Seja $N = 2 \times 3 \times 5 \times 7 \times ... \times p_r$, observe que $N - 1$ é composto pois é maior que o último primo p_r. Então existe p_i que divide $N - 1$, mas p_i também divide N, pois é um fator desse número. Então p_i divide $N - (N - 1) = 1$, ou seja p_i divide 1, isso acontece somente se p_i for 1, isso é uma contradição pois p_i é primo.

2.3 STIELTJES (1890)

Podemos encontrar a demonstrção de Stieltjes, por exemplo, em [2].

Suponha, por absurdo, que a quantidade de números primos seja finita, ou seja, $p_1, p_2, ..., p_r$ são todos os primos. Agora considere $N = p_1p_2.p_3...p_r = a.b$, com $a, b \geq 2$. Note que p_i divide a ou p_i divide b não podendo dividir a e b simultaneamente, pois é fator primo de apenas um deles. Logo, $a + b$, que é composto, por ser maior que p_r, não é divisível por p_i, o que é um absurdo.

2.4 GOLDBACH (1730)

Podemos encontrar a demonstração de Goldbach, por exemplo, em [2].

O matemático prussiano Christian Goldbach mostrou que os números de Fermat, que são da forma $F_n = 2^{2^n} + 1$ são relativamente primos dois a dois. A consequência disso é que existem infinitos números primos.

Para fazer essa demonstração primeiro será demonstrado que se $m < n$, então $F_m | F_n - 2$, para isso, vamos mostrar, usando o princípio da indução finita, que $F_m = F_0.F_1.F_2...F_{m-1}+2$.

(Observação: o símbolo | significa *divide*, ou seja se $a|b$, com a e b inteiros, temos que $b = ka$, com k número inteiro).

- Para $m = 1$, $F_1 = 2^{2^1} = 4 = 2^{2^0} + 2 = F_0 + 2$.
- Suponha válido para $m - 1$. Então $F_0F_1...F_{m-2}F_{m-1} + 2 = (F_{m-1} - 2)F_{m-1} + 2 = (2^{2^{m-1}} + 1 - 2)(2^{2^{m-1}} + 1) + 2 = (2^{2^{m-1}} - 1)(2^{2^{m-1}} + 1) + 2 = 2^{2^m} - 1 + 2 = 2^{2^m} + 1$

(Observação: usaremos a denotação $(a, b) = d$ ao longo do artigo que significa dizer que o máximo divisor comum de a e b é igual a d.)

Agora, temos que $F_m = F_0.F_1.F_2...F_{m-1} + 2$, ou seja, $F_m - 2 = F_0.F_1.F_2...F_{m-1}$, isso significa que dado $n < m$, então $F_n|(F_m - 2)$, ou seja, $F_m - 2 = F_n.t$, com $t \in \mathbb{N}$. Logo $(F_n, F_m) = (F_n, F_n.t + 2) = (F_n, F_n.t + 2 - F_n.t) = (F_n, 2) = 1$, pois F_n é ímpar. Assim, todos números de Fermat são relativamente primos entre si.

Um corolário desse resultado é que existem infinitos números primos, pois cada número de fermat terá primos distintos em sua decomposição, caso contrário não seriam primos entre si. Veja:

- $2^{2^0} = 3$
- $2^{2^1} = 5$
- $2^{2^2} = 17$
- $2^{2^3} = 257$
- $2^{2^4} = 65537$
- $2^{2^5} = 4294967297 = 641 \times 6700417$, e assim sucessivamente e infinitamente.

Como podemos variar n infinitamente em $2^{2^n} + 1$, serão "descobertos" infinitos números primos distintos. Portanto, a quantidade de números primos é infinita.

2.5 SAIDAK (2006)

Podemos encontrar a demonstração de Saidak em [3].

A ideia dessa demonstração é que para mostrarmos que existem infinitos números primos, basta criarmos uma sequência com infinitos números inteiros que tenham, cada um, pelo menos um número primo distinto em sua decomposição dos demais inteiros da sequência.

Considere $n \geq 2$, temos que $(n, n + 1) = 1$, ou seja, os números primos da decomposição de n são distintos dos de $n + 1$. Logo, $n(n + 1)$ é formado por pelo menos dois números primos distintos. Repetindo o processo, temos que $(n(n + 1), n(n + 1) + 1) = 1$, ou seja, os números primos da decomposição de $n(n + 1)$ são distintos dos de $n(n + 1) + 1$. Logo, como $n(n + 1)$ tem pelo menos dois números primos distintos em sua decomposição, então $n(n + 1)(n(n + 1) + 1)$ tem pelo menos três números distintos em sua decomposição. Note que esse processo pode ser repetido infinitas vezes, fazendo com que os números gerados tenham pelo menos um número primo em sua decomposição a mais que o número gerado anteriormente.

Desse modo, a sequência:

$$n, n(n + 1), n(n + 1)(n(n + 1) + 1), n(n + 1)(n(n + 1) + 1)(n(n + 1)(n(n + 1) + 1) + 1), ...$$

é composta por números em que o cada número da sequência tem pelo menos um número primo a mais em sua decomposição que seu antecessor.

Vamos fazer um exemplo com $n = 2$, teremos a seguinte sequência,

$$2, 2(2 + 1), 2(2 + 1)(2(2 + 1) + 1), 2(2 + 1)(2(2 + 1) + 1)(2(2 + 1)(2(2 + 1) + 1) + 1), ...$$

Escrevendo como multiplicação de potência de números primos fica

$$2, 2 \times 3, 2 \times 3 \times 7, 2 \times 3 \times 7 \times 43, ...$$

Observe que à medida que a sequência é construída de modo que cada novo termo tem pelo menos um número primo a mais em sua decomposição que o termo anterior, como deve acontecer. Logo, como essa sequência tem infinitos números, então existem infinitos números primos.

2.6 THUE (1897)

Podemos encontrar a demonstração, por exemplo, em [2].

Essa demonstração da infinitude dos números primos foi realizada pelo matemático norueguês Axel Thue.

Suponha, por absurdo, que existam k números primos e p seja o maior primo. Agora considere os inteiros que vão de 1 até 2^n, de modo que $2^n > p$. A quantidade de elementos desse conjunto é 2^n. Assim, todo inteiro de 1 até 2^n deve ser escrito na forma $2^{n_1} \times 3^{n_2} \times 5^{n_3} \times ... \times p^{n_k}$ onde $0 \leq n_1 \leq n, 0 \leq n_2 < n, 0 \leq n_3 < n, ..., 0 \leq n_k < n$, pois, caso contrário, o número seria maior que 2^n. A quantidade de elementos possíveis de serem formados pelos expoentes é de $(n+1)n^{k-1}$. Observe que temos que ter $2^n \leq (n+1)^k$, senão não é possível formar todos inteiros de 1 até 2^n, mas isso é falso para n grande, pois o número k, que é a quantidade de números primos, é fixa.

2.7 A. ENGEL (1998)

Podemos encontrar a demonstração de A. Engel em [4].

A ideia dessa demonstração é mostrar que para cada inteiro não negativo n, a expressão $f(n) = 2^{2^{n+1}} + 2^{2^n} + 1$ tem pelo menos $n+1$ fatores primos distintos, desse modo, a medida que aumentamos n, conseguimos fazer aparecer $n+1$ números primos distintos.

Para demonstrar, usaremos indução em n, para $n \geq 1$. Para isso, usaremos o seguinte fato: $x^4 + x^2 + 1 = (x^2 - x + 1)(x^2 + x + 1)$. Assim, se $g(x) = x^4 + x^2 + 1$, então $f(n) = g(2^{2^{n-1}})$. Pois $g(2^{2^{n-1}}) = ((2^{2^{n-1}})^2 - 2^{2^{n-1}} + 1)((2^{2^{n-1}})^2 + 2^{2^{n-1}} + 1) = (2^{2^n} - 2^{2^{n-1}} + 1)(2^{2^n} + 2^{2^{n-1}} + 1) = 2^{2^{n+1}} + 2^{2^n} + 1 = f(n)$.

Note também que $(2^{2^n} - 2^{2^{n-1}} + 1, 2^{2^n} + 2^{2^{n-1}} + 1) = 1$, pois a diferença entre esses dois números vale $2^{2^{n-1}+1}$ e isso só pode ser divisível por uma potência de 2, entretanto ambos números são ímpares.

Agora vamos a demonstração de fato, usando indução finita em n.

(i) para $n = 1$, $f(1) = 2^{2^2} + 2^{2^1} + 1 = 21 = 3.7$, um número com exatamente $1+1 = 2$ fatores.

(ii) Suponha válido para $n \geq 1$. Ou seja $f(n) = 2^{2^{n+1}} + 2^{2^n} + 1$ tem pelo menos $n+1$ fatores primos. Assim, usando o que foi mostrado anteriormente, temos que $f(n+1) = 2^{2^{n+2}} + 2^{2^{n+1}} + 1 = (2^{2^{n+1}} - 2^{2^n} + 1)(2^{2^{n+1}} + 2^{2^n} + 1) = f(n)(2^{2^{n+1}} - 2^{2^n} + 1)$. Note que, usando o que foi mostrado, $(f(n), 2^{2^{n+1}} - 2^{2^n} + 1) = (2^{2^{n+1}} - 2^{2^n} + 1, 2^{2^{n+1}} + 2^{2^n} + 1) = 1$, ou seja $2^{2^{n+1}} - 2^{2^n} + 1$ tem fatores primos distintos de $f(n)$ em sua decomposição. Como, por hipótese de indução $f(n)$ tem pelo menos $n+1$ fatores primos, então $f(n+1) = f(n)(2^{2^{n+1}} - 2^{2^n} + 1)$ tem pelo $n+2$ fatores primos, e a demonstração está completa.

Vamos elencar alguns números dessa forma

- $n = 1$, temos que $f(1) = 3.7$
- $n = 2$, temos que $f(2) = 3.7.13.241$
- $n = 3$, temos que $f(3) = 3.7.13.97.241.673$

Em que podemos verificar que à medida que aumentamos n, a quantidade de primos em sua decomposição de fato aumenta.

2.8 M. WUNDERLICH (1965)

Podemos encontrar a demonstração de Wunderlich em [5].

Nesta demonstração, usaremos os números de Fibonacci juntamente com princípio das gavetas para chegar em uma contradição, caso existam finitos números primos. Lembramos que os números de fibonacci são formados através da construção de uma sequência em que cada elemento é gerado pela soma dos dois anteriores, considerando que os dois primeiros números da sequência são 1 e 1, assim os primeiros termos dessa sequência são: $1, 1, 2, 3, 5, 8, 13, 21, 34, 55$ etc.

Suponha que os números primos sejam finitos, ou seja $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, ..., p_k$ são todos os primos. Observe que $(F_{p_i}, F_{p_j}) = F_{(p_i,p_j)} = F_1 = 1$, ou seja os números F_{p_i} são relativamente primos entre si. Descartamos a primeira gaveta $F_2 = 1$, pois 1 não é primo. Assim, nas $k - 1$ gavetas que sobraram, temos k primos para distribuir, isso significa que temos crédito de um primo a mais somente em uma delas. Mas $F_{19} = 4181 = 37.113$, aqui utilizamos dois primos em uma gaveta que podíamos gastar, ou seja, nas demais $k - 2$ gavetas, só podemos ter potência de um primo, entretanto, $f_{31} = 1346269 = 557.2417$, e isso é uma contradição, ou seja, existem mais que k números primos.

Veja os números de Fibonacci F_{p_i} até F_{37}

- $F_2 = 1$
- $F_3 = 2$
- $F_5 = 5$
- $F_7 = 13$
- $F_{11} = 89$
- $F_{13} = 233$
- $F_{17} = 1597$
- $F_{19} = 4181 = 37.113$
- $F_{23} = 28657$
- $F_{29} = 514229$
- $F_{31} = 1346269 = 557.2417$
- $F_{37} = 24157817 = 73.149.2221$

Desse modo, percebemos que, se fixarmos uma quantidade k de números primos, rapidamente a sequência de Fibonacci nos mostra que existe mais que k.

Outra maneira de pensar é parecida com a demonstração feita por Euclides, se $F_2, F_3, ..., F_{p_k}$ engloba todos os números primos, então $F_2F_3...F_{p_k} + 1$ não é divisível por nenhum desses números primos, e isso é uma contradição.

2.9 S. NORTHSHIELD (2015)

Podemos encontrar a demonstração de Northshield em [6].

Essa demonstração foi criada recentemente, é chamada de "Prova em uma linha", pois cabe somente em uma linha. Veja:

$$0 < \prod_p sen\left(\frac{\pi}{p}\right) = \prod_p sen\left(\pi \frac{1 + 2\prod_{p'} p'}{p}\right) = 0$$

Apesar de não estar escrito, nessa demonstração supõe que a quantidade de primos é finita, por isso chega em uma contradição.

Para clarificar, um passo intermediário entre as igualdades pode ser interessante.

$$0 < \prod_p sen\left(\frac{\pi}{p}\right) = \prod_p sen\left(\frac{\pi}{p} + \frac{2\prod_{p'} p'}{p}\pi\right) = \prod_p sen\left(\pi\frac{1+2\prod_{p'} p'}{p}\right) = 0$$

Observe que $sen\left(\frac{\pi}{p}\right) = sen\left(\frac{\pi}{p} + 2k\pi\right)$, com $k \in \mathbb{Z}$, ou seja,

$$\prod_p sen\left(\frac{\pi}{p}\right) = \prod_p sen\left(\frac{\pi}{p} + \frac{2\prod_{p'} p'}{p}\pi\right)$$

pois o produtório sempre resultará em um inteiro divisível pelo p em questão. Mas ao somarmos essas frações, chegamos que $\prod_p sen\left(\pi\frac{1+2\prod_{p'} p'}{p}\right)$ deve ser divisível por algum p_i, pois supomos que a quantidade de primos é finita e esse número, com certeza, é maior que o último primo. Com isso, o produto resulta zero pois $sen(k\pi) = 0 \; \forall \; k \in \mathbb{Z}$ e irá aparecer zero no produtório para algum p. Ou seja, concluiremos que $0 < 0$, e isso é uma contradição.

2.10 USANDO A FUNÇÃO ϕ DE EULER

Essa demonstração usa a função ϕ de Euler. Não foi possível conhecer seu surgimento, alguns dizem que o próprio Euler foi quem a produziu, mas não se tem certeza. Sabemos que $\phi(n)$ conta quantos números são primos entre si com n de 1 até n. Usaremos apenas duas propriedades dessa função na demonstração, que são, se a, b são primos entre si, então $\phi(ab) = \phi(a)\phi(b)$ e se p é primo, então $\phi(p) = p - 1$.

Suponha, por absurdo, que existam finitos números primos, ou seja $p_1, p_2, ..., p_k$ são todos os primos. Agora considere o número $N = p_1 p_2 ... p_k$, note que esse número contém todos os números primos, logo, somente o número 1 é relativamente primo com N. Assim temos que:

$$1 = \phi(N) = \phi(p_1.p_2...p_n) = \phi(p_1)\phi(p_2)...\phi(p_n) = (p_1 - 1)(p_2 - 1)...(p_n - 1) > 1$$

Isso é uma contradição, então a quantidade de números primos não pode ser finita, ou seja, tem que ser infinita.

2.11 P. ERDÖS (1938)

Essa demonstração de Erdös pode ser encontrada em [7].

Antes de começar, definimos a função $\pi(n)$ como a função que conta a quantidade de números primos menores ou iguais a n.

Seja $n \in \mathbb{N} = 1, 2, 3, 4, ...$ Considere o conjunto $S(n) = \{(k, l) \in \mathbb{N}^2$ onde l é um número livre de quadrado e $k^2 l \leq n\}$.

De fato, é fácil verificar que, pelo Teorema Fundamental da Aritmética, todo número natural tem representação única na forma $k^2 l$, em que k e l são números naturais e l é livre de quadrados. Como a representação é única, isso nos dá que $|S(n)| = n$. Ou seja, existem n elementos em $S(n)$.

Assim, se temos um par (k, l) com $k^2 l \leq n$, então temos que $k^2 \leq n$ e $l \leq n$. Note que isso resulta que $k \leq \sqrt{n}$. Como l é um número livre de quadrado, l pode ser escrito como o produto de números primos menores ou iguais a n, ou seja, como produto dos primos $p_1, p_2, ..., p_{\pi(n)}$. Desse modo, existem $2^{\pi(n)}$ combinações possíveis desse produto para l.

Como $(k, l) \in S(n)$, então existem no máximo $\sqrt{n}$ possibilidades para k e no máximo $2^{\pi(n)}$ possibilidades para l. Isso significa que $|S(n)| \leq 2^{\pi(n)}\sqrt{n} \implies n \leq 2^{\pi(n)}\sqrt{n} \implies \frac{n}{\sqrt{n}} \leq$

$2^{\pi(n)} \implies log(n^{\frac{1}{2}}) \leq \pi(n)log(2) \leq \pi(n) \implies log\left(\frac{n}{2}\right) \leq \pi(n)$.

Note que $log\left(\frac{n}{2}\right)$ é uma função crescente, assim, $\pi(n)$ também cresce, ou seja, a quantidade de números primos diferentes menores ou iguais a n cresce à medida que n cresce, e temos a garantia de que essa quantidade não fica "estagnada". Ou seja, existem infinitos números primos.

2.12 S. P. MOHANTY (1978)

As próximas duas demonstrações foram feitas por Mohanty e podem ser encontradas em [8].

Existem infinitos conjuntos de inteiros positivos com infinitos elementos tais que quaisquer elementos desses conjuntos são primos entre si, dois a dois. Consequentemente, existem infinitos números primos.

Demonstração: Escolha quaisquer inteiros a e m primos entre si e forme a seguinte sequência:

$$\begin{cases} A_0 = a + m \\ A_{n+1} = A_n^2 - mA_n + m, n > 0 \end{cases}$$

Vamos provar que $(A_i, A_j) = 1$ para $i \neq j$. O passo principal para isso é concluir que $A_n = \alpha A_0 A_1 A_2 ... A_{(n-1)} + m$, com α inteiro. Primeiramente, note que

$$\begin{cases} A_1 = A_0^2 - mA_0 + m \implies A_1 = (A_0 - m)A_0 + m \\ A_1 = \alpha A_0 + m \\ A_2 = A_1^2 - mA_1 + m = (A_1 - m)A_1 + m \\ A_2 = ((A_0 - m)A_0 + m - m)A_1 + m = A_2 \\ A_2 = (A_0 - m)A_0 A_1 + m \\ A_2 = \alpha A_0 A_1 + m \end{cases}$$

Assim, vamos assumir que $A_{k+1} = \alpha A_0 A_1 .... A_k + m$ e mostrar por indução que isso é verdade.

(i) para $n = 0$, $A_0 = \alpha$, ok.

(ii) Suponha válido para n, temos que $A_{n+1} = A_n^2 - mA_n + m = (\alpha A_0 A_1 ... A_{n-1} + m)^2 - m(\alpha A_0 A_1 ... A_{n-1} + m) + m$, logo, $A_{n+1} = (\alpha A_0 A_1 ... A_{n-1})^2 + m\alpha A_0 A_1 ... A_{n-1} + m$, então temos que $A_{n+1} = (\alpha A_0 A_1 ... A_{n-1})(A_0 A_1 ... A_{n-1} + m) + m$, assim concluímos que $A_{n+1} = \alpha A_0 A_1 ... A_{n-1} A_n + m$, como queríamos mostrar.

Com isso, note que $A_n \equiv a^{2^n} (\text{mod } m)$. Agora, suponha $(A_i, A_j) = d$ com $j > i$. Note que $d|m$, pois d divide $\alpha A_0 A_1 ... A_{j-1}$, pois A_i está nesse produto, mas $(a, m) = 1$, logo $d|1$, ou seja $d = 1$, como queríamos demonstrar.

Um corolário disso é que existem infinitos números primos. De fato, como $(A_i, A_j) = 1$ para todo $i \neq j$, temos que cada $A_1, A_2, A_3, ...$ é divisível por um primo que não é divide nenhum outro elemento da sequência, logo, há pelo menos n primos distintos menores ou iguais a A_n. Como n pode crescer infinitamente, existem infinitos números primos.

Vamos fazer um caso particular dessa sequência. Vamos pegar $a = 3$ e $m = 5$, note que $(3, 5) = 1$, a sequência fica definida da seguinte maneira:

$$\begin{cases} A_0 = 3 + 5 = 8 \\ A_{n+1} = A_n^2 - 5A_n + 5, n > 0 \end{cases}$$

Que resulta na seguinte sequência de números:

1 $A_0 = 2^3$

2 $A_1 = 29$

3 $A_2 = 701$

4 $A_3 = 19 \times 25679$

5 $A_4 = 1279 \times 186118019$

Note que realmente a medida que n aumenta, são gerados números com primos distintos em sua decomposição como queríamos.

2.13 S. P. MOHANTY (1978)

Agora uma demonstração também feita por Mohanty.

Todo divisor primo de $\frac{1}{3}(2^p + 1)$, em que p é primo maior que 3, é maior que p.

Demonstração: Primeiro, vamos mostrar que $\frac{1}{3}(2^p + 1)$ em que p é um primo maior que 3, não é divisível por 3.

Note que $\frac{1}{3}(2^p + 1) = \frac{2^p+1}{2+1} = 2^{p-1} - 2^{p-2} + 2^{p-3} - 2^{p-4} + ... - 2 + 1$, e isso é um inteiro. Logo, $\frac{1}{3}(2^p+1) = (2^{p-1}+2^{p-3}+...+1) - (2^{p-2}+2^{p-4}+...+2)$. Como $2^{2k} \equiv 1(\text{mod } 3)$ e $2^{2k+1} \equiv 2(\text{mod } 3)$. Assim $\frac{1}{3}(2^p + 1) \equiv \frac{p+1}{2} - \frac{2(p-1)}{2}(\text{mod } 3) \equiv \frac{-p+3}{2}(\text{mod } 3)$.

Como p é primo > 3, então $p = 6k + 1$ ou $p = 6k + 5$. Se $p = 6k + 1$, então temos $\frac{1}{3}(2^p + 1) \equiv \frac{-6k-1+3}{2} \equiv 1(\text{mod } 3)$ e se $p = 6k + 5$ temos $\frac{1}{3}(2^p + 1) \equiv \frac{-6k-5+3}{2} \equiv 2(\text{mod } 3)$. Ou seja, de fato $\frac{1}{3}(2^p + 1)$ não é divisível por 3.

Suponha, por absurdo, que $\frac{1}{3}(2^p + 1) \equiv 0(\text{mod } q)$ com q primo maior que 3. Note que não pode ser 3 pelo que já vimos e não pode ser 2, pois $\frac{1}{3}(2^p + 1) \equiv 1(\text{mod } 2)$.

Note que, pelo pequeno teorema de Fermat, temos que $2^{q-1} \equiv 1(\text{mod } q)$. Temos dois casos para analisar, o caso de $q = p > 3$ e o caso $q < p$.

(i) Se $q = p > 3$, temos que $2^{p-1} \equiv 1(\text{mod } q)$, daí $2^p \equiv 2(\text{mod } q)$, logo $2^p + 1 \equiv 3(\text{mod } q)(i)$, mas, por hipótese $\frac{1}{3}(2^p + 1) \equiv 0(\text{mod } q)$, então $(2^p + 1) \equiv 0(\text{mod } q)(ii)$, juntando as (i) e (ii) temos que $0 \equiv 3(\text{mod } q)$, o que é uma contradição, pois $q > 3$.

(ii) Agora, suponha $q < p$. Logo, temos que $(q - 1, p) = 1$, isso implica que existem inteiros a e b tais que $ap+b(q-1) = 1$. Então $2 = 2^{ap+b(q-1)} = (2^p)^a(2^{q-1})^b \equiv (-1)^a(1)^b \equiv -1(\text{mod } q)$ para a ímpar e $\equiv 1(\text{mod } q)$ para a par. Assim, chegamos que $2 \equiv \pm 1(\text{mod } q)$ e isso é uma contradição, pois q é primo maior que 3.

Portanto, todo divisor primo de $\frac{1}{3}(2^p + 1)$ é maior que p.

Como corolário, existem infinitos números primos.

Seguem alguns exemplos a partir do primo 5:

1) $\frac{1}{3}(2^5 + 1) = 11$

2) $\frac{1}{3}(2^7 + 1) = 43$

3) $\frac{1}{3}(2^{11} + 1) = 683$

4) $\frac{1}{3}(2^{13} + 1) = 2731$

5) $\frac{1}{3}(2^{17} + 1) = 43691$

6) $\frac{1}{3}(2^{19} + 1) = 174763$

7) $\frac{1}{3}(2^{23} + 1) = 2796203$

8) $\frac{1}{3}(2^{29} + 1) = 59 \times 3033169$

Interessante notar que nos sete primeiros exemplos, todos resultados são números primos. Vamos ter um número composto quando $p = 29$ e, de fato, os divisores primos desse número, que são 59 e 3033169, são maiores que 29, como deve acontecer.

2.14 M. AIGNER, G. M. ZIEGLER (1998)

Podemos encontrar a demonstração de Aigner e Ziegler em [7].

Assim como na demonstração de Mohanty, vamos mostrar que todo divisor primo de $2^p - 1$ é maior que p. Note que, $2^n > n$ para $n \in \mathbb{N}, n \geq 2$, logo, seja p um primo maior que 3, temos que $2^p - 1 > p$. Isso significa que existe q primo tal que $q|2^p - 1$, logo $2^p \equiv 1(\text{mod } q)$, como p é primo, $ord_q 2 = p$, então, temos que $p|\phi(q) = q - 1$, como $p \neq q - 1$, pois $q - 1$ é par, logo, $q > p$. Como corolário, existem infinitos números primos. (lembramos que a ordem de a módulo n, denotado por $ord_n a$ é o menor inteiro $t > 0$ tal que $\overline{a}^t = \overline{1}$.

Seguem alguns exemplos, vamos fazer do primo 3 em diante,

1) $2^3 - 1 = 7$

2) $2^5 - 1 = 31$

3) $2^7 - 1 = 63$

4) $2^{11} - 1 = 23 \times 89$

Os três primeiros números encontrados são primos, já o quarto número é um produto de primos maiores que 11, como deve acontecer.

2.15 EULER (1737)

Podemos encontrar essa demonstração de Euler em [9].

Para essa demonstração usaremos o fato que $\sum \frac{1}{n}$ é a série harmônica, logo, diverge. Primeiramente, note que

$$1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + ... = \frac{1}{1 - \frac{1}{p}}$$

Essa fração representa a soma dos termos de uma PG infinita em que a razão é maior que 0 e menor que 1.

Agora vamos calcular o produto dessa série com todas possibilidades possíveis para p primo.

$$\prod_p \frac{1}{1 - \frac{1}{p}} = \left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + ...\right) \cdot \left(1 + \frac{1}{p_2} + \frac{1}{p_2^2} + ...\right) + ...$$

Veja que essa multiplicação gera todos os números $\frac{1}{n}$ pois ocorre toda combinação possível ao multiplicarmos os números dentro de cada parênteses. Logo, usando o Teorema Fundamental da Aritmética temos que

$$\prod_p \frac{1}{1 - \frac{1}{p}} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + ... = \sum_n^{\infty} \frac{1}{n} = \infty$$

Logo, como cada parcela de parênteses representa $\frac{1}{1-\frac{1}{p}}$, a quantidade de números primos não pode ser finita, caso contrário teríamos a multiplicação de uma quantidade finita de números e sabemos que a série harmônica diverge. Portanto, por consequência, a quantidade de números primos deve ser infinita.

2.16 "NOVA" DEMONSTRAÇÃO REALIZADA PELO AUTOR DO ARTIGO E NÃO PUBLICADA (2017)

A fim de criar outra demonstração curta, inspirado na demonstração de Northshield, devido a possibilidade de escrever em uma linha, o autor deste trabalho teve a ideia da seguinte demonstração:

Suponha que p seja o maior primo, porém o $(p!, p! + 1) > 1$, absurdo.

A demonstração usa o fato conhecido de que o mdc de dois números inteiros consecutivos sempre será 1. Essa ideia, muitas vezes, é usada em outras demonstrações, porém de maneira não tão explícita. Entretanto, nessa demonstração em especial, usando esse fato, conseguiu-se concluir em apenas uma linha que a quantidade de primos é infinita, pois $p!+1$, que é maior que p, deve ser composto, logo, o mdc entre $p!$ e $p!+1$ deve ser maior que 1, já que $p!$ é múltiplo de todos os primos menores ou iguais a p, mas isso é uma contradição, pois, como foi dito, o mdc de dois números inteiros consecutivos sempre será 1. Salientamos que essa demonstração é uma pequena variação de outras já conhecidas, podendo até ter sido realizada antes. Porém, não foi possível encontrar demonstração semelhante por meio de buscas em bibliografias e sites de pesquisa tanto na língua portuguesa quanto na língua inglesa.

2.17 RECOMENDAÇÕES E CONCLUSÕES

Podemos encontrar diversas demonstrações da infinitude dos números primos. Quase sempre encontramos em inglês, entretanto, cada vez mais vem surgindo artigos e livros que apresentam demonstrações também em português. Uma literatura em português que recomendamos é o livro "Números Primos" de Paulo Ribenboim [10], publicada pelo IMPA. Nele, encontramos algumas demonstrações interessantes sobre a infinitude dos números primos além de diversas curiosidades sobre esses números.

Existem outras demonstrações da existência de infinitos primos que requerem alguns conhecimentos mais avançados de conteúdos matemáticos. Optamos por deixar essas demonstrações fora do artigo. Nossa ideia foi construir um texto para provocar a curiosidade do leitor em busca de novos meios de mostrar a infinitude dos primos, e, ao mesmo tempo, que ele não encontrasse tanta dificuldade em acompanhar as demonstrações aqui apresentadas.

REFERÊNCIAS

[1] W. Narkiewicz, *The development of prime number theory: from Euclid to Hardy and Littlewood*. Springer Science & Business Media, 2013.

[2] P. Ribenboim, *The new book of prime number records*. Springer Science & Business Media, 2012.

[3] F. Saidak, "A new proof of Euclid's theorem," *Biscuits of Number Theory*, no. 34, p. 61, 2009.

[4] A. Engel, *Problem-solving strategies, Problem books in mathematics*. Springer-Verlag, 1998.

[5] M. Wunderlich, "Another proof of the infinite primes theorem," *The American Mathematical Monthly*, vol. 72, no. 3, pp. 305–305, 1965.

[6] S. Northshield, "A one-line proof of the infinitude of primes," vol. 122, 05 2015.

[7] M. Aigner, G. M. Ziegler, and A. Quarteroni, *Proofs from the Book*, vol. 274. Springer, 2010.

[8] S. Mohanty, "The number of primes is infinite," *Fibonacci Quart*, vol. 16, no. 4, pp. 381–384, 1978.

[9] M. C. Motta, "Existência de infinitos números primos e a série dos inversos dos primos, qual a relação?,"

[10] P. Ribenboim, *Números primos: velhos mistérios e novos recordes*. IMPA, 2012.