



UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA
Mestrado Profissional em Matemática em Rede Nacional



BRIANNE MOURÃO LOPES

**NÚMEROS PRIMOS: A ENGENHARIA ALGÉBRICA DA
FÓRMULA DE C.P. WILLIANS**

RECIFE
2024



UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA
Mestrado Profissional em Matemática em Rede Nacional



BRIANNE MOURÃO LOPES

**NÚMEROS PRIMOS: A ENGENHARIA ALGÉBRICA DA
FÓRMULA DE C.P. WILLIAMS**

Dissertação de mestrado apresentada ao Departamento de Matemática da Universidade Federal Rural de Pernambuco como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Rodrigo José Gondim Neves

RECIFE
2024

Dados Internacionais de Catalogação na Publicação
Universidade Federal Rural de Pernambuco
Sistema Integrado de Bibliotecas
Gerada automaticamente, mediante os dados fornecidos pelo(a) autor(a)

- L864n Lopes, Brianne
 Números primos: A engenharia algébrica da fórmula de C. P. Willians. / Brianne Lopes. - 2024.
 60 f. : il.
- Orientador: RODRIGO JOSE GONDIM NEVES.
 Inclui referências e apêndice(s).
- Dissertação (Mestrado) - Universidade Federal Rural de Pernambuco, Programa de Mestrado
 Profissional em Matemática (PROFMAT), Recife, 2024.
1. Números Primos. 2. Aritmética. 3. C. P. Willians. I. NEVES, RODRIGO JOSE GONDIM, orient. II.
Título

CDD 510


BRIANNE MOURÃO LOPES

"Números primos: A engenharia algébrica da fórmula de C. P. Willians"

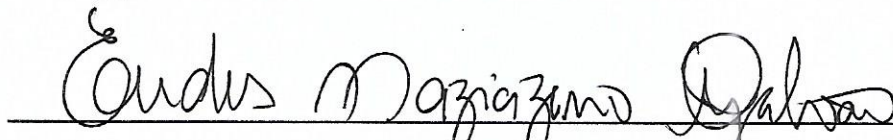
Trabalho apresentado ao Programa de Mestrado Profissional em Matemática – PROFMAT do Departamento de Matemática da UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO, como requisito parcial para obtenção do grau de Mestre em Matemática.

Aprovado em 08/04/2024

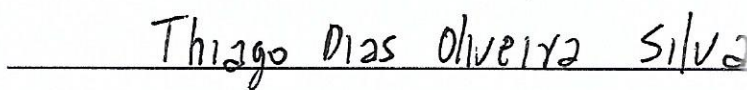
BANCA EXAMINADORA



Prof. Dr. Rodrigo José Gondim Neves (Orientador) – UFRPE



Prof. Dr. Eudes Naziazeno Galvão - UFPE



Prof. Dr. Thiago Dias Oliveira Silva – PROFMAT/UFRPE

Ao criador e à minha família

Agradecimentos

Agradeço ao Criador por me conceder o dom do aprender e ensinar, por sua presença e proteção em minha vida.

À minha família como todo, especialmente as mulheres mais fortes e inspiradoras que conheço: minha mãe, Diva, e minha avó, Rosa, que sempre estiveram ao meu lado, me educando, me amando e me incentivando aos estudos; ao meu avô Chico, que não está neste plano neste momento, mas eu sinto a sua presença e sei que estará feliz por mim onde estiver; ao meu tio Carlão por todo carinho, dedicação e todas as conversas encorajadoras; ao meu esposo, Eduardo, e minha filha, Lila, por tornar a minha vida mais leve, por nosso maravilhoso humor, por seus carinhos diários e compreensão diante da minha dedicação ao mestrado. A minha amiga, irmã do coração e madrinha, Laís por me acompanhar e me apoiar ao longo da minha vida inteira e seguirmos juntas. Aos meus amigos e companheiros de profissão Antônio e Jamille; ele me acolheu, me ensinou a ensinar e me adotou como irmã; com ela nasceu uma parceria incrível e um apoio mútuo, uma inspiração de inteligência, força e ousadia; aos dois agradeço pela força de sempre e suporte na confecção deste texto. Amo todos vocês!

Aos meus professores da escola básica, em especial os de matemática que foram inspiração pra mim: Joana D'Arc, com seu jeito grande, imponente, exigente e amorosa de ser, e Anselmo Guerra, com a calma e devoção que falava e ensinava matemática; e Levi Bispo, professor de física do pré-militar, que me deu uma bolsa num pré-vestibular por acreditar em mim, me encorajando e apoiando. Jamais esquecerei de vocês.

Aos Professores do PROFMAT-UFRPE pela dedicação e empenho, em especial a três queridos que me acompanham desde a graduação: ao meu orientador (pela segunda vez consecutiva) Rodrigo Gondim, por acreditar em mim, ser compreensivo com minhas demandas e ainda assim, me forçar a ir mais longe do que eu achava que conseguia, a Adriano Regis, que seguiu me prestando o seu carinho e amizade, me apoiando e motivando a permanecer firme no curso, e a Anete Soares, professora maravilhosa, inteligentíssima, gente da gente, forte e inspiradora para todas nós, mulheres na matemática.

Aos colegas de turma, por todo carinho, amizade, estudos juntos e momentos de suporte.

*"A matemática é o alfabeto com o qual
Deus escreveu o universo."
Galileu Galilei (1564-1642)*

Resumo

Os números primos intrigam as pessoas há muito tempo; seja por sua ausência de padrões, por suas aparições em várias áreas da matemática, pelas aplicações no cotidiano ou até mesmo a associação com situações místicas.

Com as ferramentas tecnológicas que possuímos atualmente, é possível realizar testes com algumas fórmulas para encontrar números primos. Atualmente, calculado em janeiro de 2019, o maior é $2^{82589933} - 1$ (com 24,8 milhões de dígitos) descoberto através de um computador, usando a fórmula dos números de Mersenne ($2^p - 1$).

Ao longo da história vários matemáticos desenvolveram conjecturas e fórmulas na tentativa de achar um padrão de comportamento nesses números tão intrigantes e peculiares.

Este texto tem a intenção de fazer um breve “passeio” histórico sobre as investidas nos estudos dos números primos e mostrar algumas ferramentas para trazer a luz a fórmula de C.P. Willians, matemático que usou de uma “engenharia algébrica” para confeccionar uma fórmula que calcula o n -ésimo número primo.

Palavras-chave: Números Primos, Aritmética, C.P. Willians.

Abstract

Prime numbers intrigue humans for a long time; for the lack of patterns, for their show up in various areas of mathematics, for the possible applications and for the mysticism associated to them.

Using the technologic tools that we have nowadays, it is possible to perform tests using known formulae to find prime numbers. The biggest known prime number is $2^{82589933} - 1$. It was found by a computer using Mersene's formulae.

Over the history, several mathematicians developed conjectures and formulae trying to find a pattern to understand these intriguing and peculiar numbers.

This text is a historic walk on the study of prime numbers. We give the necessary tools to understand the C.P. Willians formulae to compute the n -th prime number.

Keywords: Prime numbers, arithmetic, C. P. Willians

Lista de ilustrações

Figura 1 – “Peneira” ou Crivo de Eratóstenes	22
Figura 2 – Recorte da Linha do Tempo - Números Primos	23
Figura 3 – Gráfico da Função Piso	26
Figura 4 – Gráfico da Função Teto	27
Figura 5 – Triângulo de Pascal	28
Figura 6 – Consequências da Definição do Número Binomial do Triângulo de Pascal	29
Figura 7 – Relação de Stifel	29
Figura 8 – Gráfico da função cosseno	42
Figura 9 – Gráfico da função cosseno elevado ao quadrado	42
Figura 10 – Gráfico do comportamento da curva	44
Figura 11 – Exercício 1	49
Figura 12 – Exercício 2	49
Figura 13 – Exercício 3	50

Sumário

	Introdução	19
1	UM POUCO DE HISTÓRIA	21
2	RESULTADOS PRELIMINARES	25
2.1	Somatórios	25
2.1.1	Propriedades	25
2.2	Função Piso e Função Teto	26
2.2.1	Função Piso	26
2.2.2	Função Teto	26
2.2.3	Propriedades	27
2.3	Números Binomiais	28
2.3.1	O Triângulo de Pascal	28
2.3.2	Propriedades	29
3	NÚMEROS PRIMOS	31
3.1	Definições	31
3.2	Teorema Fundamental da Aritmética	31
3.3	Teorema de Wilson	32
3.4	Teorema de Legendre	34
3.5	Postulado de Bertrand	35
4	A FÓRMULA DE C. P. WILLIANS	41
5	PROPOSTA DE SEQUÊNCIA DIDÁTICA	47
5.1	Habilidades BNCC	47
5.2	Cronograma	48
5.3	Atividades	49
	REFERÊNCIAS	51
A	NÚMEROS PRIMOS ATÉ 1000	53
B	A FÓRMULA DE WILLIANS CALCULANDO O 100º NÚ- MERO PRIMO	55
C	COMPORTAMENTO DE $f(x) = \left(\frac{x}{n+1}\right)^{\frac{1}{x}}$	57

Introdução

“Matemáticos tem tentado em vão, até o dia de hoje, descobrir alguma ordem na sequência de números primos, e nós temos razões para acreditar que é um mistério no qual a mente humana jamais penetrará. ”

(Frase atribuída a Leonhard Euler)

Quando estudamos aritmética, na educação básica, aceitamos o Teorema Fundamental da Aritmética, assim como outras ferramentas oferecidas ao estudante para que chegue em suas respostas, como algo muito simples e natural. Tome um número natural e se ele for divisível apenas por 1 e por ele próprio, é um número primo; caso possua mais de dois divisores, é composto, e sendo este, pode ser escrito como produto de fatores primos.

Por trás desta simples atitude de executar a técnica da decomposição existem anos de curiosidade, pesquisa, tentativas, acertos e muitos, muitos erros. Todos com o propósito matemático, e porque não dizer filosófico, de desvendar o mistério e a beleza dos números primos, base da nossa composição numérica.

Inicialmente vamos realizar uma breve visita cronológica a alguns momentos em que esta simples classificação de números primos, traz em si dilemas imensos para os matemáticos, e para a humanidade.

Em seguida, veremos algumas ferramentas que são pré-requisitos para o acompanhamento da fórmula que é tema central deste trabalho.

Então, serão explicadas as etapas de execução da fórmula de C.P. Willians, que através de um raciocínio engenhoso realizou uma composição de várias funções e teoremas que aparentemente não possuíam ligação direta com números primos, e gerou uma fórmula que calcula o n-ésimo número primo.

1 Um pouco de história

Há muito tempo, os números primos, suas aparições, problemáticas e propriedades, encantam e desafiam os que se propõem a estudá-los.

Atribui-se que, inicialmente, Pitágoras (Grécia, 530 a. C.) tenha levado a sério os estudos sobre os números primos. A escola pitagórica dava grande importância ao número um, que era chamada de unidade. Os demais números inteiros naturais (2, 3, 4, ...) tinham "menos relevância", sendo vistos como meras multiplicações geradas pela unidade e por isso recebiam a denominação de número. Entre os pitagóricos a preocupação com a geração dos números não parava por aí. O próprio Pitágoras teria percebido que existem dois tipos de número:

- Os números primários ou primos, que são aqueles que não podem ser gerados – através da multiplicação – por outros números, como é o caso de 2, 3, 5, 7...
- Os números secundários, que podem ser gerados por outros números, por exemplo, $4 = 2 \cdot 2$, $6 = 3 \cdot 2$, etc.

Ainda por influência dos Pitagóricos, por muitos séculos houve polêmica a respeito da primalidade do número 2. Os primeiros pitagóricos atribuíam-lhe caráter especial – embora menos importante que a unidade – e alguns deles não o incluíam entre os números. Consequentemente, muitos pitagóricos não consideravam o 2 como primo.

É só pela época de Aristóteles, (Grécia, 350 a. C.), que o número 2 passou a ser considerado como primo, sendo que esta prática foi consagrada pela publicação de "Os Elementos" (um tratado matemático e geométrico consistindo de 13 livros) escrito por Euclides (Grécia, 330 a. C.), onde ainda ele prova que há infinitos números primos e entrega subsídios para provar o Teorema Fundamental da Aritmética.

Por volta de 200 a.C. Eratóstenes desenvolveu sua "peneira" como método para acelerar a descoberta de números primos. O método começa com uma tabela de números consecutivos e, inicialmente, o 1 é riscado pois não é primo e nem composto, Em seguida os múltiplos de 2 (exceto ele próprio) são riscados, depois os múltiplos de 3, 5, 7, e assim por diante.

Figura 1 – “Peneira” ou Crivo de Eratóstenes



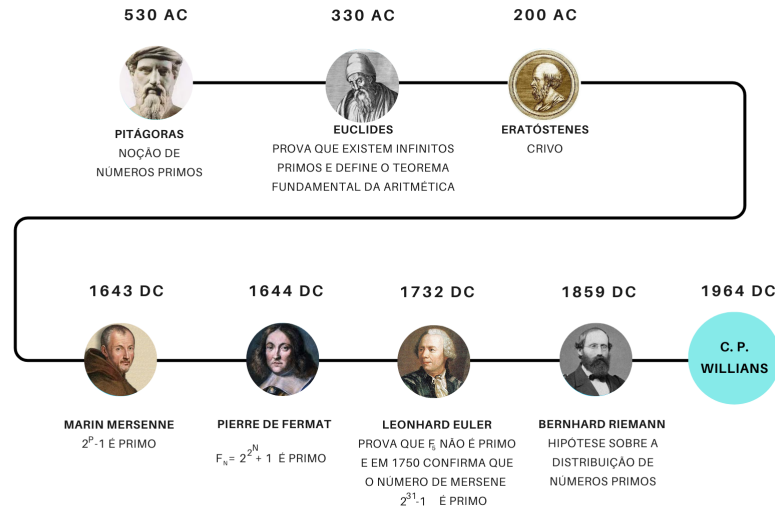
Fonte: Produção da Autora

Avançando pouco mais de um milênio, em meados de 1643, Marin Mersenne afirmou que $2^p - 1$ gerava números primos para $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ e 257 . Seu interesse reavivou o interesse pelo tema e hoje os números primos gerados por essa expressão são chamados Primos de Mersenne. Entretanto, convém observar desde logo que nem todo número de Mersenne é primo, assim como nem todo número primo é de Mersenne. Ainda assim, é uma das expressões usadas ainda hoje na busca de números primos, como mencionado na introdução.

Em seguida, Pierre Fermat (1644) conjecturou que os números calculados na forma $F_n = 2^{2^n} + 1$ eram primos para qualquer n natural. Ele verificou que $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65537$ eram de fato primos. A conjectura se revelou incorreta em 1732 quando Euler mostrou que $F_5 = 4294967297$ é divisível por 641 ($4294967297 = 641 \cdot 6700417$). Os únicos números de Fermat conhecidos que são primos são aqueles acima. Para $n \in \{5, \dots, 32\}$ bem como os gigantes F_{23288} e F_{23471} são comprovadamente compostos. Mas não se tem certeza se os únicos primos de Fermat são os cinco citados anteriormente.

A hipótese de Riemann foi proposta por Bernhard Riemann em 1859. A teoria afirma que a distribuição de números primos não é aleatória (como é classificada), mas pode seguir um padrão descrito por uma equação chamada "função zeta de Riemann", quando se coloca na equação alguns números complexos que dão zero na função.

Figura 2 – Recorte da Linha do Tempo - Números Primos



Fonte: Produção da Autora

Os momentos na história citados aqui tem a intenção de situar evoluções no campo de estudo dos números primos e algumas tentativas de reconhecer um padrão em sua distribuição e/ou gerar fórmulas que calculassem tais números.

Estacionaremos a nossa linha do tempo onde este texto se propõe a esmiuçar a ferramenta desenvolvida por C.P. Willians, cujas informações são escassas, exceto pelo artigo que enuncia sua fórmula e lista “ The University, Birmingham” para sua filiação.

2 Resultados Preliminares

Neste capítulo serão definidas as ferramentas utilizadas para realizar algumas provas dos capítulos seguintes.

2.1 Somatórios

Muitas quantidades importantes em matemática são definidas como a soma de uma quantidade variável de parcelas também variáveis. Para estas situações, uma notação muito prática é a somatória (também chamada somatório ou notação sigma), introduzida por Joseph Fourier em 1820.

Em geral, a notação sigma tem a forma

$$\sum_{k=n}^m f(k)$$

onde k é uma variável arbitrária, $f(k)$ é uma fórmula qualquer que depende de k (o termo geral da somatória), e m e n são inteiros que não dependem de k .

Exemplo:

$$\sum_{k=1}^5 2^k = 2^1 + 2^2 + 2^3 + 2^4 + 2^5$$

2.1.1 Propriedades

1. Produto por escalar: Seja X um conjunto de valores reais e a um escalar qualquer (valor usado para multiplicar). A propriedade afirma que:

$$\sum_{i=m}^n a \cdot x_i = a \cdot \sum_{i=m}^n x_i$$

2. Adição e subtração: Sejam $X = \{x_1, \dots, x_n\}$ e $Y = \{y_1, \dots, y_n\}$ dois conjuntos distintos de valores reais. A propriedade afirma que:

$$\sum_{i=m}^n x_i \pm y_i = \sum_{i=m}^n x_i \pm \sum_{i=m}^n y_i$$

2.2 Função Piso e Função Teto

2.2.1 Função Piso

A função piso (também chamada de chão ou solo) associa a cada número real x o maior número inteiro que é menor ou igual a x .

Este inteiro é denotado por $\lfloor x \rfloor$

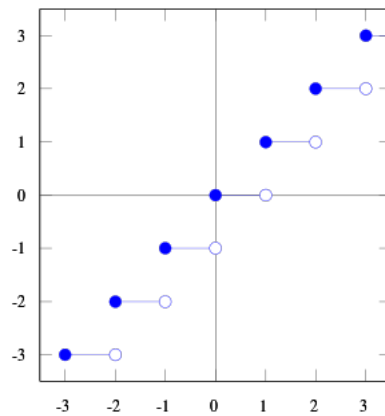
Observe:

$$\lfloor 1/3 \rfloor = \lfloor 2/3 \rfloor = 0$$

$$\lfloor -1/3 \rfloor = \lfloor -2/3 \rfloor = -1$$

$$\lfloor 5 \rfloor = 5$$

Figura 3 – Gráfico da Função Piso



Fonte: Wikipedia

2.2.2 Função Teto

A função teto associa a cada número real x o menor número inteiro que é maior ou igual a x .

Este inteiro é denotado por $\lceil x \rceil$.

Observe:

$$\lceil 5/4 \rceil = 2$$

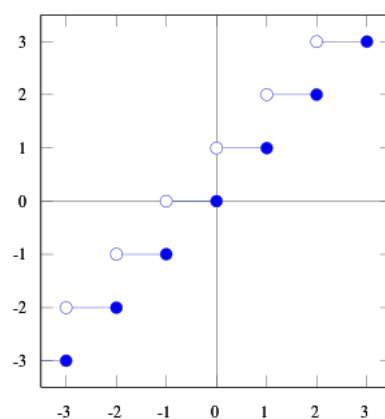
$$\lceil 7/4 \rceil = 2$$

$$\lceil -1/4 \rceil = 0$$

$$\lceil 1/4 \rceil = 1$$

$$\lceil 4 \rceil = 4$$

Figura 4 – Gráfico da Função Teto



Fonte:Wikipedia

Observando os gráficos das funções Piso e Teto percebemos que elas são descontínuas nos números inteiros e contínuas nos intervalos reais entre inteiros.

2.2.3 Propriedades

1. $\lfloor x \rfloor + z = \lfloor x + z \rfloor$, para todo $x \in \mathbb{R}$, $z \in \mathbb{Z}$.
2. $-\lceil x \rceil = \lfloor -x \rfloor$, para todo $x \in \mathbb{R}$.
3. $z - \lfloor x \rfloor = \lceil z - x \rceil$, para todo $x \in \mathbb{R}$, $z \in \mathbb{Z}$.
4. $0 \leq x - \lfloor x \rfloor < 1$, para todo $x \in \mathbb{R}$.

2.3 Números Binomiais

Por definição, para $n \in \mathbb{N}$ e $k \in \mathbb{N}$, com $n \geq k$, o número binomial n na classe k consiste em

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

Observe:

$$\binom{7}{2} = \frac{7!}{2! \cdot (7-2)!} = \frac{7!}{2! \cdot 5!} = \frac{7 \cdot 6 \cdot 5!}{2 \cdot 5!} = \frac{30}{2} = 15$$

Como consequência imediata da definição temos que

$$\binom{n}{0} = \binom{n}{n} = 1 \text{ e } \binom{n}{1} = \binom{n}{n-1} = n,$$

e ainda temos

$$\binom{n}{k} = \binom{n}{n-k}, \text{ denominados } \mathbf{binomiais complementares}.$$

2.3.1 O Triângulo de Pascal

Os números binomiais podem ser dispostos de tal forma, que geram o Triângulo de Pascal a seguir:

Figura 5 – Triângulo de Pascal

$$\begin{array}{cccccc}
 \binom{0}{0} & & & & & & 1 \\
 \binom{1}{0} \binom{1}{1} & & & & & & 1 & 1 \\
 \binom{2}{0} \binom{2}{1} \binom{2}{2} & & & & & & 1 & 2 & 1 \\
 \binom{3}{0} \binom{3}{1} \binom{3}{2} \binom{3}{3} & & & & & & 1 & 3 & 3 & 1 \\
 \binom{4}{0} \binom{4}{1} \binom{4}{2} \binom{4}{3} \binom{4}{4} & & & & & & 1 & 4 & 6 & 4 & 1 \\
 \binom{5}{0} \binom{5}{1} \binom{5}{2} \binom{5}{3} \binom{5}{4} \binom{5}{5} & & & & & & 1 & 5 & 10 & 10 & 5 & 1 \\
 \dots & & & & & & \dots & & & & & &
 \end{array}$$

Fonte:Produção da Autora

Essa disposição, facilita a visualização das consequências da definição citadas anteriormente:

Figura 6 – Consequências da Definição do Número Binomial do Triângulo de Pascal

$\binom{0}{0}$	1
$\binom{1}{0}\binom{1}{1}$	1 1
$\binom{2}{0}\binom{2}{1}\binom{2}{2}$	1 2 1
$\binom{3}{0}\binom{3}{1}\binom{3}{2}\binom{3}{3}$	1 3 3 1
$\binom{4}{0}\binom{4}{1}\binom{4}{2}\binom{4}{3}\binom{4}{4}$	1 4 6 4 1
$\binom{5}{0}\binom{5}{1}\binom{5}{2}\binom{5}{3}\binom{5}{4}\binom{5}{5}$	1 5 10 10 5 1
...	...

Fonte:Produção da Autora

2.3.2 Propriedades

1. **Relação de Stifel:** Cada número do triângulo de Pascal é igual à soma do número imediatamente acima e do antecessor do número de cima.

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$$

Figura 7 – Relação de Stifel

$\binom{0}{0}$	1
$\binom{1}{0}\binom{1}{1}$	1 1
$\binom{2}{0}\binom{2}{1}\binom{2}{2}$	1 2 1
$\binom{3}{0}\binom{3}{1}\binom{3}{2}\binom{3}{3}$	1 3 3 1
$\binom{4}{0}\binom{4}{1}\binom{4}{2}\binom{4}{3}\binom{4}{4}$	1 4 6 4 1
$\binom{5}{0}\binom{5}{1}\binom{5}{2}\binom{5}{3}\binom{5}{4}\binom{5}{5}$	1 5 10 10 5 1
...	...

Fonte:Produção da Autora

2. **Um Lema útil:** A partir dos números binomiais, surgem várias possibilidades de comparações. Neste texto usaremos o seguinte lema:

$$\frac{4^n}{2n+1} \leq \binom{2n}{n}$$

Prova:

Vamos provar a desigualdade por indução em n .

Para $n = 1$ temos

$$\frac{4^1}{2 \cdot 1 + 1} \leq \binom{2}{1}$$

$$\frac{4}{3} \leq 2$$

temos a desigualdade verdadeira.

Vamos supor que seja verdade para um certo $n \geq 1$, temos então

$$\frac{4^n}{2n + 1} \leq \binom{2n}{n}$$

$$\frac{4^n}{2n + 1} \leq \frac{(2n)!}{n! \cdot n!}$$

$$\frac{4^n \cdot (n!)^2}{(2n + 1) \cdot (2n)!} \leq 1.$$

Vamos provar que a desigualdade vale para $n + 1$, isto é:

$$\frac{4^{n+1} \cdot [(n + 1)!]^2}{(2n + 3) \cdot (2n + 2)!} \leq 1$$

temos que

$$\frac{4^{n+1} \cdot [(n + 1)!]^2}{(2n + 3) \cdot (2n + 2)!} = \frac{4 \cdot (n + 1)^2}{(2n + 3) \cdot (2n + 2)} \cdot \frac{4^n \cdot (n!)^2}{(2n + 1) \cdot (2n)!}$$

Por hipótese de indução, a segunda fração já possui valor menor ou igual a 1.

Queremos mostrar que

$$\frac{4 \cdot (n + 1)^2}{(2n + 3) \cdot (2n + 2)} \leq 1.$$

De fato, para $n \geq 1$, temos $0 \leq 2n + 2$, assim, somando $4n^2 + 8n + 4$, obtemos:

$$4n^2 + 8n + 4 \leq 4n^2 + 10n + 6$$

Portanto

$$\frac{4n^2 + 8n + 4}{4n^2 + 10n + 6} = \frac{4 \cdot (n + 1)^2}{(2n + 3) \cdot (2n + 2)} \leq 1$$

E o resultado segue por indução.

3 Números Primos

3.1 Definições

Por definição, um número natural $n > 1$ é dito **primo** se possui apenas dois divisores naturais, sendo 1 e o próprio número.

7 é um exemplo número primo, pois divide apenas por 1 e por 7 (dois divisores).

Já um número natural $n > 1$ que não é primo, é **composto**.

42 é um exemplo de número composto, pois além de possuir 1 e 42 como divisores, divide ainda por 2, 3, 6 e 7.

É importante observar que 1 não é primo e nem composto.

3.2 Teorema Fundamental da Aritmética

Sendo um número dito composto, podemos escrever como produto de dois fatores, através do processo de fatoração:

$$42 = 1 \cdot 42 = 2 \cdot 21 = 3 \cdot 14 = 6 \cdot 7$$

Teorema 3.1. *O Teorema fundamental da aritmética diz que todo o número natural ou é primo ou pode ser escrito como produto de números primos, e esse produto é único a menos da ordem dos fatores.*

$$17 \text{ é primo}$$

$$42 = 2 \cdot 3 \cdot 7$$

$$100 = 2 \cdot 2 \cdot 5 \cdot 5$$

Prova.

Para esta demonstração será usado o Princípio de Indução.

Nossa hipótese diz que qualquer a natural é primo ou pode ser escrito como produto de números primos.

Para $a = 2$ existe uma decomposição trivial em números primos, já que 2 é, ele próprio, um número primo; o mesmo ocorre para $a = 3$.

Sendo $a = 4$ podemos escrever 4 como $2 \cdot 2$, que são números primos.

Vamos supor que é válido para $a = \{1, 2, \dots, k\}$ e provar que vale para $a = k + 1$.

Pela nossa hipótese, ou $k + 1$ é primo, ou possui algum divisor cujo resultado é inteiro, $\frac{k+1}{p} = q$ onde p e q pertencem aos inteiros que devem estar entre $2 \leq q, p < k + 1$ ou ainda $2 \leq q, p \leq k$

E pela suposição anterior, p e q são primos ou podem ser escritos como produto de fatores primos.

3.3 Teorema de Wilson

O Teorema de Wilson diz que $(j - 1)! + 1$ é divisível por j precisamente quando j é um número primo ou j é o número 1.

$$\frac{(j - 1)! + 1}{j}$$

Vamos ver alguns exemplos a seguir:

j	$\frac{(j-1)!+1}{j}$
1	2
2	1
3	1
4	$\frac{7}{4}$
5	5
6	$\frac{121}{6}$
7	103
...	...

Teorema 3.2. *Seja p um número primo então $(p - 1)! \equiv -1 \pmod{p}$. Outra maneira de escrever esta afirmação é: Seja $p \in \mathbb{Z}_+$, p é primo, se e somente se, $p | (p - 1)! + 1$.*

Verificação de casos particulares

Para $p = 2$ temos $(2 - 1)! = 1! = 1 \equiv -1 \pmod{2}$

Para $p = 3$ temos $(3 - 1)! = 2! = 2 \equiv -1 \pmod{3}$

Para $p = 5$ temos $(5 - 1)! = 4! = 24 \equiv -1 \pmod{5}$

Para $p = 7$ temos $(7 - 1)! = 6! = 720 \equiv -1 \pmod{7}$

Demonstração: (\implies)

Lema 3.3. *Se p um número primo, então para todo $k \in \{2, \dots, p-2\}$, existe $s \in \{2, \dots, p-2\}$, $k \neq s$ tal que $p|k \cdot s - 1$ ou seja $k \cdot s = p \cdot q + 1$ (Consequência do Teorema de Bézout)*

Exemplo

$$p = 7$$

$$(p-1)! = (7-1)! = 6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$$

$$2 \cdot 4 = 8 = 7 \cdot 1 + 1$$

$$3 \cdot 5 = 15 = 7 \cdot 2 + 1$$

Sendo assim $(p-1)!$ pode ser escrito como

$$(p-1)! = (p \cdot q_1 + 1) \cdot (p \cdot q_2 + 1) \dots (p \cdot q_m + 1) \cdot (p-1)$$

Após as multiplicações, podemos escrever $(p-1)!$ da seguinte maneira

$$(p-1)! = (p \cdot Q + 1) \cdot (p-1) = p^2 \cdot Q + p - pQ - 1$$

Concluindo que $(p-1)! + 1 = p \cdot K$

 (\impliedby)

Se p é composto, existe $q < p$ tal que $q|p$.

Sendo q primo, temos que $q|(p-1)!$.

Se $p|(p-1)! + 1$, então $q|(p-1)! + 1$,

logo $q|1$, o que é absurdo.

Então p é primo.

3.4 Teorema de Legendre

Teorema 3.4. *O número $n!$ contém o fator primo p exatamente $\sum_{k=1} \left\lfloor \frac{n}{p^k} \right\rfloor$ vezes.*

Exemplo

$$6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720 = 2^4 \cdot 3^2 \cdot 5^1$$

Quantidade de fatores 2 em $6!$ será dado por

$$\sum_{k=1} \left\lfloor \frac{6}{2^k} \right\rfloor = \left\lfloor \frac{6}{2^1} \right\rfloor + \left\lfloor \frac{6}{2^2} \right\rfloor + \left\lfloor \frac{6}{2^3} \right\rfloor + \dots = 3 + 1 + 0 + 0 + 0 + 0 + \dots = 4$$

Quantidade de fatores 3 em $6!$ será dado por

$$\sum_{k=1} \left\lfloor \frac{6}{3^k} \right\rfloor = \left\lfloor \frac{6}{3^1} \right\rfloor + \left\lfloor \frac{6}{3^2} \right\rfloor + \dots = 2 + 0 + 0 + 0 + 0 + \dots = 2$$

Prova.

Os números compreendidos entre 1 e n que são divisíveis por p^i são da forma $p^i m$, em que m é um inteiro positivo e $p^i m \leq n$.

Note que exatamente $\left\lfloor \frac{n}{p} \right\rfloor$ dos fatores de $n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n$ são divisíveis por p , o que fornece $\left\lfloor \frac{n}{p} \right\rfloor$ fatores p .

Em seguida, $\left\lfloor \frac{n}{p^2} \right\rfloor$ desses fatores são divisíveis por p^2 , o que acrescenta $\left\lfloor \frac{n}{p^2} \right\rfloor$ fatores primos p em $n!$.

Continuando o processo podemos prosseguir calculando as quantidades de fatores primos divisíveis por p^3 ou qualquer outra potência inteira de p . Para cada uma das quantidades $\left\lfloor \frac{n}{p^k} \right\rfloor$, acrescentamos mais $\left\lfloor \frac{n}{p^k} \right\rfloor$ fatores p em $n!$; o que resulta na fórmula do teorema.

Note que, para $p^i > n$, temos $\left\lfloor \frac{n}{p^i} \right\rfloor = 0$, e a soma, formalmente infinita, termina a partir de um i tal que $i > \frac{\log n}{\log p}$.

3.5 Postulado de Bertrand

Para cada $n \geq 1$, existe algum número primo p com $n < p \leq 2n$.

Observe:

Para $n = 1$ temos $1 < p \leq 2$, ou seja $p = 2$

Para $n = 2$ temos $2 < p \leq 4$, ou seja $p = 3$

Para $n = 3$ temos $3 < p \leq 6$, ou seja $p = 5$

Para $n = 4$ temos $4 < p \leq 8$, ou seja $p = 5$ ou $p = 7$

...

Para n temos $n < p \leq 2n$.

Para provar o Postulado de Bertrand, vamos observar o seguinte Lema:

Lema 3.5. *Para todo $n \geq 2$ temos que o produto de todos os números primos p menores ou iguais a n resulta num valor menor ou igual a 4^n .*

$$\prod_{p \leq n} p \leq 4^n$$

Observe:

Para $n = 2$ temos

$$\prod_{p \leq 2} p = 2 \leq 16 = 4^2$$

Para $n = 3$ temos

$$\prod_{p \leq 3} p = 2 \cdot 3 = 6 \leq 64 = 4^3$$

Para $n = 5$ temos

$$\prod_{p \leq 5} p = 2 \cdot 3 \cdot 5 = 30 \leq 1024 = 4^5$$

Para $n = 7$ temos

$$\prod_{p \leq 7} p = 2 \cdot 3 \cdot 5 \cdot 7 = 210 \leq 16384 = 4^7$$

...

Para provar o lema, usaremos o Princípio da Indução forte dividida em dois casos:

- (1) Vamos provar que se vale para $2k - 1$ vale também para $2k$.
- (2) E que se vale para $2k$ vale também para $2k + 1$.

Prova do Lema

Suponha que para algum $k \geq 1$, temos

$$\prod_{p \leq 2k-1} p \leq 4^{2k-1}$$

Note que se tomarmos apenas $2k$ (um número par, conseqüentemente não é primo) o fator $2k$ já não aparece como fator do seu produtório, sendo assim

$$\prod_{p \leq 2k} p = \prod_{p \leq 2k-1} p \leq 4^{2k-1} < 4^{2k}$$

O que prova o passo (1) da indução.

Agora, vamos verificar o caso (2) da indução.

Suponha, que para todo m , $1 \leq m \leq 2k$, temos

$$\prod_{p \leq m} p \leq 4^m$$

Queremos provar que vale para $2k+1$; e para isso vamos analisar esse produtório como o produto de dois produtórios:

1. dos números primos menores ou iguais a $k+1$
2. dos números primos maiores que $k+1$ e menores ou igual a $2k+1$

$$\prod_{p \leq 2k+1} p = \left(\prod_{p \leq k+1} p \right) \cdot \left(\prod_{k+1 < p \leq 2k+1} p \right)$$

Na primeira etapa do produtório podemos aplicar o primeiro passo da indução, pois o produtório para $p \leq k+1$ é definitivamente menor que o produtório para $p \leq 2k$, ou seja, o resultado dessa primeira etapa do produtório é menor ou igual a 4^{k+1}

$$\left(\prod_{p \leq k+1} p \right) \leq 4^{k+1}$$

Para verificar a segunda etapa do produtório, usaremos o seguinte artifício:

Vamos supor que há um número primo q tal que $k+1 < q \leq 2k$. Isso implica que esse mesmo q divide o coeficiente binomial $\binom{2k+1}{k}$.

$$q \mid \binom{2k+1}{k} \text{ onde } \binom{2k+1}{k} = \frac{(2k+1)!}{k!(k+1)!}$$

Observe que, como q é um número primo estritamente maior que $k + 1$, ele não aparece em nenhum dos produtos do denominador, o que significa que q deve ser um fator que aparece no produto do numerador.

Mais ainda, vemos que isso funciona para qualquer q entre $k + 1$ e $(2k + 1)$.

Daí podemos substituir a segunda parte do produtório por aquele coeficiente binomial.

$$\prod_{p \leq 2k+1} p \leq 4^{k+1} \cdot \binom{2k+1}{k}$$

Como

$$\sum_{i \geq 1} \binom{n}{2i+1} = \sum_{i \geq 1} \binom{n}{2i} = 2^{n-1} \Rightarrow \binom{2k-1}{k} \leq 2^{2k} = 4^k$$

sendo assim, conseguimos

$$\prod_{p \leq 2k+1} p = \left(\prod_{p \leq k+1} p \right) \cdot \left(\prod_{k+1 < p \leq 2k+1} p \right) \leq (4^{k+1}) \cdot (4^k)$$

segue-se que

$$\prod_{p \leq 2k+1} p \leq 4^{2k+1}$$

O que prova o caso (2) da indução, encerrando aqui a prova do lema.

Vamos voltar à demonstração do Postulado de Bertrand.

Prova do Postulado de Bertrand:

Suponha que não haja nenhum número primo entre n e $2n$, sem incluir n e $2n$ (que obviamente não é primo).

Considere p um fator primo do binomial

$$\binom{2n}{n} = \frac{(2n)!}{n!n!} \Rightarrow 2 \leq p \leq 2n$$

Mas como supomos que não existe nenhum número primo entre n e $2n$, p tem que estar entre 2 e n .

$$2 \leq p \leq n$$

Para continuar o raciocínio, vejamos a sub afirmação a seguir

Sub afirmação

$$p \leq \frac{2n}{3}$$

Prova da Sub afirmação

Se supomos, que $p > \frac{2n}{3}$, então p é maior que $\frac{2n}{3}$ e menor que n .

$$\frac{2n}{3} < p < n$$

Temos então que a função piso indica que

$$(*) \left\lfloor \frac{2n}{p} \right\rfloor = 2 \text{ e } \left\lfloor \frac{n}{p} \right\rfloor = 1$$

devido ao intervalo

$$\frac{2n}{3} < p < n$$

mas também o piso de

$$(**) \left\lfloor \frac{2n}{p^k} \right\rfloor = 0 = \left\lfloor \frac{n}{p^k} \right\rfloor, \forall k \geq 2$$

Vemos agora que o expoente de p na fatoraçaõ do coeficiente binomial $\binom{2n}{n}$, pelo Teorema de Legendre, é exatamente igual a

$$\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \cdot \left\lfloor \frac{n}{p^k} \right\rfloor$$

Por causa da expressãõ em (*) vemos que conseguimos simplificar o resultado

$$\left\lfloor \frac{2n}{p} \right\rfloor - 2 \cdot \left\lfloor \frac{n}{p} \right\rfloor = 2 - 2 \cdot 1 = 0$$

o que significa que se $p \in]\frac{2n}{3}, n[$, então o expoente de p na fatoraçaõ de $\binom{2n}{n}$ é de fato zero, ou seja, p não pode ser um fator deste coeficiente binomial.

Daí, além de reduzir o intervalo de $2 \leq p \leq 2n$ para $2 \leq p \leq n$ temos $2 \leq p \leq \frac{2n}{3}$.

Até agora provamos que se p é um divisor primo de $\binom{2n}{n}$, então $2 \leq p \leq \frac{2n}{3}$.

Esta conclusão veio de duas situações:

1. Supondo que não existe primos entre n e $2n$.
2. Usando a fórmula de Legendre.

Para continuar, usaremos a seguinte fatoração do coeficiente binomial:

$$\binom{2n}{n} = \prod_{p \leq \frac{2n}{3}} p^{k_p}$$

O coeficiente binomial é igual ao produtório de todos os números primos que dividam $\binom{2n}{n}$, com expoente k_p , mas esses primos são menores ou iguais a $\frac{2n}{3}$.

Consequimos dividir este produtório em duas partes

$$\prod_{p \leq \frac{2n}{3}} p^{k_p} = \prod_{p \leq \sqrt{2n}} p^{k_p} \cdot \prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p^{k_p}$$

Para cada produtório conseguimos aplicar uma desigualdade:

No primeiro produtório, temos $\prod_{p \leq \sqrt{2n}} p^{k_p}$ em que $k_p = \sum_{j \geq 1} \left(\left\lfloor \frac{2n}{p^j} \right\rfloor - 2 \cdot \left\lfloor \frac{n}{p^j} \right\rfloor \right)$. Por outro lado, sabemos que $\left\lfloor \frac{2n}{p^j} \right\rfloor - 2 \cdot \left\lfloor \frac{n}{p^j} \right\rfloor \in \{0, 1\}$, logo $\left\lfloor \frac{2n}{p^j} \right\rfloor - 2 \cdot \left\lfloor \frac{n}{p^j} \right\rfloor \leq 1$ para cada j , além disso, será zero quando $p^j > 2n$. Daí, $k_p \leq 1 + \dots + 1 \leq \log_p 2n$ e portanto, $p^{k_p} \leq 2n$. Agora temos $\prod_{p \leq \sqrt{2n}} p^{k_p} \leq \prod_{p \leq \sqrt{2n}} 2n \leq (2n)^{\sqrt{2n}}$.

No segundo produtório vale observar que todos os expoentes $k_p = 1$. De fato, se algum desses primos ocorresse com expoente maior que 1, teríamos $p^2 > 2n$. Assim, o produtório inteiro é menor ou igual ao produto de todos os números primos menores ou iguais a $\frac{2n}{3}$, que pelo Lema anterior temos

$$\prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p^{k_p} = \prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p \leq 4^{2n/3}.$$

Então, podemos observar

$$\binom{2n}{n} = \prod_{p \leq \frac{2n}{3}} p^{k_p} = \prod_{p \leq \sqrt{2n}} p^{k_p} \cdot \prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p \leq (2n)^{\sqrt{2n}} \cdot 4^{2n/3}$$

Usaremos aqui um Lema provado na seção de resultados preliminares:

$$\frac{4^n}{2n+1} \leq \binom{2n}{n}$$

Daí, agora podemos agrupar essas duas desigualdades

$$\frac{4^n}{2n+1} \leq \binom{2n}{n} = \prod_{p \leq \frac{2n}{3}} p^{k_p} \leq (2n)^{\sqrt{2n}} \cdot 4^{\frac{2n}{3}}$$

Reduzindo a expressão acima para

$$\frac{4^n}{2n+1} \leq (2n)^{\sqrt{2n}} \cdot 4^{\frac{2n}{3}}$$

Reorganizando temos

$$4^{\frac{n}{3}} \leq (2n+1) \cdot (2n)^{\sqrt{2n}}.$$

Observamos que essa desigualdade é falsa para $n \geq 2048$. Isso nos diz que existe ao menos um número primo p tal que $n < p < 2n$, para todo $n \geq 2048$.

Para concluir, só precisamos verificar os casos entre 2 e 2048, já que conseguimos mostrar que para valores maiores ou iguais a 2048 existe um primo p tal que $n < p < 2n$.

Os números primos nesta condição são 2, 3, 5, 7, 23, 23, 43, 83, 163, 317, 631, 1259, 2503; pois em todos esse números temos que o número primo sucessivo é menor que o dobro do antecessor, de modo que serve para preencher todas as lacunas para valores de $n < 2048$.

Exemplo

Para $n = 500$ temos vários números primos tais que $500 < p < 1000$, mas a lista do parágrafo anterior entrega rapidamente o 631.

E esta é a estratégia para finalizar a prova do **Postulado de Bertrand**:

Para cada $n \geq 1$, existe algum número primo p com $n < p \leq 2n$.

4 A Fórmula de C. P. Willians

Em 1964 C.P. Willians encontrou esta fórmula para o enésimo número primo, denotado aqui por P_n

$$P_n = 1 + \sum_{i=1}^{2^n} \left[\left(\frac{n}{\sum_{j=1}^i [\cos^2(\pi \frac{(j-1)!+1}{j})]} \right)^{\frac{1}{n}} \right]$$

A fórmula de Willians foi gerada por uma série de etapas através da composição de funções algébricas e trigonométrica, além da utilização do Teorema de Wilson e do Postulado de Bertrand, entrega em seu resultado, o valor do n-ésimo número primo.

A seguir vamos abordar cada parte desta fórmula, acompanhando e justificando as etapas de cálculos realizadas.

Sendo 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,... a sequência de números primos, esperamos que a fórmula aqui estudada calcule 2 para $n=1$, já que 2 é o primeiro número primo; calcule 3 para $n=2$, e assim sucessivamente. E é exatamente isto que ela faz.

Vamos ver então como a fórmula funciona trabalhando de dentro para fora.

A peça mais interna usa o Teorema de Wilson, que diz que se $(j-1)!+1$ é divisível por j precisamente quando o j é um número primo ou j é o número 1.

$$\frac{(j-1)!+1}{j}$$

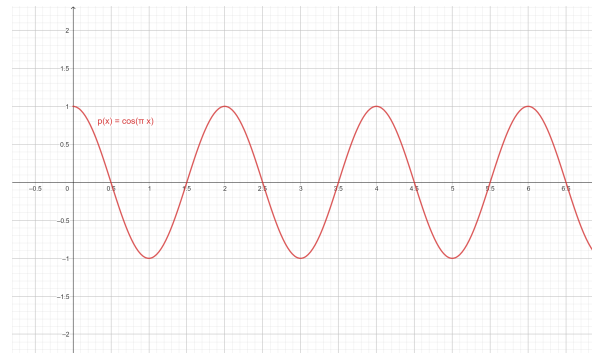
Isso implica dizer que quando usamos o teorema de Wilson obtemos um número inteiro quando o j é um número primo ou 1, e número não inteiro quando o j é um número composto, funcionando como um detector de números primos; como visto no item 3.2.

A próxima etapa da fórmula usa a função $\cos(\pi x)$, onde o x será substituído pelo Teorema de Wilson, ficando da seguinte maneira

$$\cos\left(\pi \frac{(j-1)!+1}{j}\right)$$

, e fazendo com que obtenhamos -1 ou 1 quando tivermos um número inteiro, e quando o x não é o número inteiro o $\cos(x\pi)$ está estritamente entre -1 e 1 .

Figura 8 – Gráfico da função cosseno



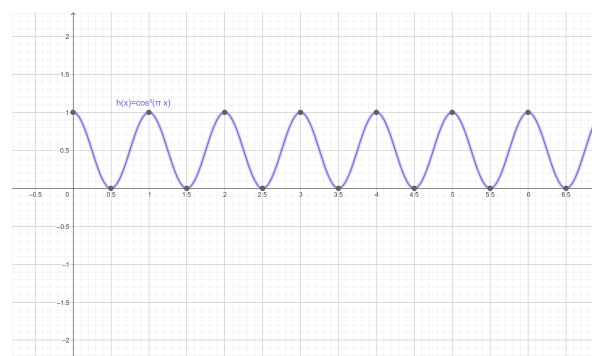
Fonte: Produção da Autora

Isso significa que o cosseno na fórmula de Willians gera +1 ou -1 se j for número 1 ou um número primo, e informa o número entre -1 e 1 se j for um número composto.

Elevando a função cosseno ao quadrado, os números -1 se tornam +1, o que faz com que essa operação entregue +1 quando o j é primo ou igual ao número 1; e é um número não negativo que é estritamente menor do que 1 quando o j for um número composto.

$$\cos^2 \left(\pi \frac{(j-1)! + 1}{j} \right)$$

Figura 9 – Gráfico da função cosseno elevado ao quadrado



Fonte: Produção da Autora

Nesta etapa, tomaremos o piso da função cosseno elevado ao quadrado, o que nos devolve 1 se j for um número primo ou 1, e reduz todo o resto para 0 (o intervalo entre 0 e os números estritamente menores do que 1), quando j for um número composto.

$$\left\lfloor \cos^2 \left(\pi \frac{(j-1)! + 1}{j} \right) \right\rfloor$$

Com esse detector de primos conseguimos começar a contar os números primos somando um intervalo de valores para j .

Para exemplificar, aqui está a soma quando i é 10

$$\sum_{j=1}^{10} \left\lfloor \cos^2 \left(\pi \frac{(j-1)! + 1}{j} \right) \right\rfloor = 1 + 1 + 1 + 0 + 1 + 0 + 1 + 0 + 0 + 0 = 4 + 1 = 5$$

Neste somatório j assume cada valor de 1 a 10 e o somatório contribui com 1 para a soma toda vez que j é primo ou 1; e com 0 quando j é composto.

Existem 4 primos nesse intervalo, então a soma é 5 porque adiciona o número 1, quando $j = 1$, onde 1 não é um número primo.

Em geral, se executados a soma para i , obtemos a quantidade de o número de primos até o valor de i mais 1 unidade. Assim sendo, nossa discussão até agora, demonstrou a seguinte:

Proposição 4.1. *Seja $p(n) = \#\{p \text{ primo} | 0 < p \leq n\}$ a quantidade de números primos positivos menores ou iguais a n , então:*

$$1 + p(n) = \sum_{j=1}^n \left\lfloor \cos^2 \left(\pi \frac{(j-1)! + 1}{j} \right) \right\rfloor$$

Mas se a fórmula de Willians deve calcular o enésimo primo, como sair da contagem desta quantidade e entregar o valor do número primo nesta posição?

No exemplo, determinamos que existem quatro números primos até 10. Mas queremos determinar o quarto número primo.

Nesta etapa, basicamente, faremos a função inversa do que temos atualmente.

A ideia principal é, se quisermos saber o quarto número primo, perguntamos:

A quantidade de números de primos até 1 é menor que 4?

A quantidade de números de primos até 2 é menor que 4?

A quantidade de números de primos até 3 é menor que 4?

Eventualmente a resposta será “não”. E a primeira vez que for não, será quando se localiza no quarto número primo.

Portanto, os próximos passos da fórmula percorrem esta questão: “o número de primos até i é menor do que n ?” para vários i 's, e isso nos dirá quando atingimos o enésimo primo.

Nesta etapa, ele divide n pelo número de primos até i adicionado de um e em seguida eleva todo o quociente a potência $\frac{1}{n}$.

$$\left(\frac{n}{\sum_{j=1}^i \left[\cos^2 \left(\pi \frac{(j-1)!+1}{j} \right) \right] \right)^{\frac{1}{n}}$$

Para avaliar o comportamento desta nova equação, vamos fixar o n e variar i .

Mantendo o exemplo, tome i como 10 novamente; e vimos que há quatro primos até o número 10.

Observe como se comporta a curva

$$\left(\frac{x}{4+1} \right)^{\frac{1}{x}}$$

Verificamos que o piso desta função é igual a 1, atingido pela primeira vez quando $x = 5$, isso porque quando o $x = 5$, o quociente é 1. Ainda que os valores de x continuem subindo, se aumentarmos o alcance vemos que atinge o máximo e depois começa a "estabilizar".

Figura 10 – Gráfico do comportamento da curva



Fonte: Produção da Autora

Para verificar uma prova deste comportamento de forma generalizada, ver o Apêndice C.

Isso significa que, quando tomarmos o piso desta função, obtemos 0 para valores inteiros de x até 4, e 1 para valores inteiros de x maiores que 4.

$$\left\lfloor \left(\frac{x}{4+1} \right)^{\frac{1}{x}} \right\rfloor$$

O piso desta função retornará 0 se $x \leq 4$ e 1 se $x > 4$, tornando uma maneira de identificar números maiores que 4.

$$\left\lfloor \left(\frac{n}{4+1} \right)^{\frac{1}{n}} \right\rfloor = \begin{cases} 1 & \text{se } n > 4 \\ 0 & \text{se } n \leq 4 \end{cases}$$

Podemos verificar que, ao alterar esse número 4 para outros valores essa equação ainda é válida.

Em nosso exemplo atual, temos 4 números de primos até 10.

$$\left\lfloor \left(\frac{n}{(\text{quantidade de primos} \leq 10) + 1} \right)^{\frac{1}{n}} \right\rfloor = \begin{cases} 1 & \text{se } n > \text{quantidade de primos} \leq 10 \\ 0 & \text{se } n \leq \text{quantidade de primos} \leq 10 \end{cases}$$

Em geral será substituído pelo número de primos até i .

$$\left\lfloor \left(\frac{n}{(\text{quantidade de primos} \leq i) + 1} \right)^{\frac{1}{n}} \right\rfloor = \begin{cases} 1 & \text{se } n > \text{quantidade de primos} \leq i \\ 0 & \text{se } n \leq \text{quantidade de primos} \leq i \end{cases}$$

Isso nos permite responder à pergunta: “o número de primos até i é menor que n ?”

Na fórmula de Willians para calcular o n ésimo primo, não é O valor do n que vai variar; é o valor de i , devido ao somatório a que estamos prestes a chegar.

Reescrevendo as condições nesta equação para a dependência da variação de i temos que a condição “ n é maior que o número de primos menores ou iguais a i ” é equivalente a condição de que “o n ésimo primo é maior que i ”.

Por exemplo: n é maior que 4 exatamente quando o n ésimo primo é maior do que 10.

$$\left\lfloor \left(\frac{n}{(\text{quantidade de primos} \leq i) + 1} \right)^{\frac{1}{n}} \right\rfloor = \begin{cases} 1 & \text{se o } n\text{ésimo primo} > i \\ 0 & \text{se o } n\text{ésimo primo} \leq i \end{cases}$$

Reordenando cada desigualdade para observamos a partir de i temos:

$$\left\lfloor \left(\frac{n}{(\text{quantidade de primos} \leq i) + 1} \right)^{\frac{1}{n}} \right\rfloor = \begin{cases} 1 & \text{se } i < \text{o } n\text{ésimo primo} \\ 0 & \text{se } i \geq \text{o } n\text{ésimo primo} \end{cases}$$

Daí temos um detector para números i s menores que o n ésimo primo.

Para a próxima etapa, faz-se o somatório de todos os resultados dos pisos variando os i s de 1 até 2^n

$$\sum_{i=1}^{2^n} \left[\left(\frac{n}{\sum_{j=1}^i [\cos^2(\pi \frac{(j-1)!+1}{j})]} \right)^{\frac{1}{n}} \right]$$

Retomando o exemplo temos que, o n for iguais a 4, estamos variando i de 1 até 16.

$$\sum_{i=1}^{2^4} \left[\left(\frac{4}{(\text{quantidade de primos} \leq i) + 1} \right)^{\frac{1}{4}} \right] = 1+1+1+1+1+1+0+0+0+0+0+0+0+0+0+0$$

Para cada valor de i menor que o quarto primo obtemos 1 e para cada valor de i maior ou igual que o quarto primo obtemos 0.

Neste exemplo, para $n = 4$ obtemos o valor 6, que é uma unidade a menos que o quarto primo (7)

Mas qual a justificativa para parar a soma em 16? Para garantir que iremos acima do enésimo primo.

Uma estimativa muito aproximada é fornecida pelo postulado de Bertrand, que foi conjecturado por Bertrand em 1845 e provado alguns anos depois por Chebyshev (enunciado e provado no tópico 3.3).

Portanto, é garantido que a soma até 2^n inclui todos os valores do número i que são menores que o enésimo primo.

Generalizando, essa soma é 1 a menos que a enésima linha, sendo assim, o último passo é adicionar 1, chegando assim a **Fórmula de Willians**.

$$P_n = 1 + \sum_{i=1}^{2^n} \left[\left(\frac{n}{\sum_{j=1}^i [\cos^2(\pi \frac{(j-1)!+1}{j})]} \right)^{\frac{1}{n}} \right]$$

5 Proposta de Sequência Didática

Os tópicos contemplados neste texto não possuem citação direta na BNCC nem abordagem realizada na educação básica, mas frequentemente são cobrados nos Conteúdos Programáticos de Olimpíadas de Matemática, exemplo: OPEMAT-UFRPE; que cita explicitamente o Teorema de Wilson.

Direcionando para uma turma de preparação olímpica de matemática, apresento aqui uma Proposta de Sequência Didática pautada na matemática experimental para explorar este tema. Além de trazer também, uma exploração sobre o Postulado de Bertrand.

A sugestão é que as atividades ocorram de forma gradativa, para que o estudante descubra através da experimentação de valores, propriedades e/ou padrões atribuídas às expressões sugeridas, registrando através de textos suas conclusões, e daí então, conheça e formalize o que aprendeu.

5.1 Habilidades BNCC

Embora a BNCC não cite expressamente o Teorema de Bertrand, Wilson e outros tópicos deste texto, para compreendê-los, é necessário que algumas habilidades contidas neste documentos estejam bem desenvolvidas pelo estudante. As principais são:

- (EF06MA05) 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.
- (EM13MAT310) Resolver e elaborar problemas de contagem envolvendo agrupamentos ordenáveis ou não de elementos, por meio dos princípios multiplicativo e aditivo, recorrendo a estratégias diversas, como o diagrama de árvore.
- (EM13MAT306) Resolver e elaborar problemas em contextos que envolvem fenômenos periódicos reais (ondas sonoras, fases da lua, movimentos cíclicos, entre outros) e comparar suas representações com as funções seno e cosseno, no plano cartesiano, com ou sem apoio de aplicativos de álgebra e geometria.
- (EM13MAT308) Aplicar as relações métricas, incluindo as leis do seno e do cosseno ou as noções de congruência e semelhança, para resolver e elaborar problemas que envolvem triângulos, em variados contextos.

5.2 Cronograma

A sugestão é que, durante duas aulas consecutivas (100 minutos), o professor conduza a atividade, oferecendo 15 minutos para a execução de cada exercício e levando 10 minutos para intervenção/formalização.

Situação	Tempo Estimado
Introdução/ Abertura da Aula	10 min
Execução do Exercício 1	15 min
Intervenção e Formalização Exercício 1	10 min
Execução do Exercício 2	15 min
Intervenção e Formalização Exercício 2	10 min
Execução do Exercício 3	15 min
Intervenção e Formalização Exercício 3	10 min
Conclusão da Aula e Indicação de Atividades	15 min

5.3 Atividades

Para construir o conhecimento, seguem as 3 atividades indicadas:

Exercício 1:

Neste exercício, o propósito é que os estudantes, por meio de substituição dos valores e análise dos resultados, percebam que a expressão oferecida só resulta em um número natural (divisão exata) quando o valor inserido é 1 ou primo.

Figura 11 – Exercício 1

Exercício 1.

Utilizando a expressão a seguir, substitua valores naturais e verifique se consegue perceber algum padrão de comportamento diante de seus resultados.

j	$\frac{(j-1)! + 1}{j}$

Fonte: Produção da Autora

Exercício 2:

O Exercício 2 traz uma expressão na qual a substituição já será feita utilizando os números primos e os restos da divisão serão analisados, tendo como objetivo que os estudantes concluam que sempre terão como resto $p - 1$.

Figura 12 – Exercício 2

Na atividade 1, você conheceu o **Teorema de Wilson**, que diz que $(j-1)! + 1$ é divisível por j quando j é um número **primo** ou j é o número **1**.

Nesta atividade, vamos explorar um outro Teorema.

Exercício 2.

Utilizando a fórmula a seguir, substitua valores naturais primos e verifique se consegue perceber algum padrão de comportamento diante dos restos da divisão.

p	$\frac{(p-1)!}{p}$

Fonte: Produção da Autora

Exercício 3:

Para finalizar, o Exercício 3 solicitará a verificação do Postulado de Bertrand e a identificação dos números primos nos intervalos mencionados.

Figura 13 – Exercício 3

Nas atividades 1 e 2, você conheceu o **Teorema de Wilson**, que diz que $(j - 1)! + 1$ é divisível por j precisamente quando j é um número **primo** ou j é o número **1**; e verificou outro teorema que é consequência do primeiro.

Nesta última atividade apresento a você o Postulado de Bertrand, que diz:

Para cada $n \geq 1$, existe algum número primo p tais que $n < p \leq 2n$.

Exercício 3.

Verifique o postulado na tabela a seguir:

n	$2n$	Número(s) primo(s) p tal(is) que $n < p \leq 2n$

Fonte: Produção da Autora

Referências

- WILLIAMS, C.P. On Formulae for the Nth Prime Number. The Mathematical Gazette. Volume 48 , Edição 366 , dezembro de 1964 , pp . 413 - 415.
- ROWLAND, E. Formulas for the Primes. Laboratoire de Combinatoire et d'Informatique Mathématique, Université du Québec à Montréal. 5 de dezembro de 2012. Disponível em: <https://ericrowland.github.io/talks/Formulas_for_primes.pdf>. Acesso em: 10 de julho de 2023.
- ROWLAND, E. An Exact Formula for the Primes: Willans' Formula. YouTube, 22 de setembro de 2022. Disponível em: <https://www.youtube.com/watch?v=j5s0h42GfvM&t=21s&ab_channel=EricRowland> . Acesso em: 10 de julho de 2023.
- PENN, Michael. You should know this number theory result – Bertrand's Postulate. YouTube, 17 de outubro de 2022. Disponível em: <<https://www.youtube.com/watch?v=X41dbvYGZzo&list=PLu9Ke99s4FTqhlpHhSFreUI8mB3JR1AGb&index=6>> . Acesso em: 11 de fevereiro de 2024.
- FONSECA, R.V. Números Primos. UEPA, 2011. Disponível em: <https://ccse.uepa.br/downloads/material_2011/NUMEROS_PRIMOS.pdf> Acesso em: 11 de fevereiro de 2024.
- HEFEZ, Abramo. Aritmética. 1. Ed. Rio de Janeiro: SBM, 2016.
- WATANABE, R. G. Uma fórmula para números primos. RPM37. Disponível em: <<http://www.rpm.org.br/cdrpm/11/2.htm>> Acesso em: 10 de julho de 2023.
- WARSI, Karl. O Livro da Matemática. 1. Ed. Globo Livros, 2020
- VAIANO, Bruno. A hipótese de Riemann: o mistério matemático de US 1 mi que explica os números primos. Revista Superinteressante Janeiro, 2023. Disponível em: URL. <<https://super.abril.com.br/ciencia/a-hipotese-de-riemann-o-misterio-matematico-de-us-1-mi-que-explica-os-numeros-primos/>> Acesso em: 19 de fevereiro de 2024.

A Números Primos até 1000

2, 3, 5, 7

11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97,

101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181,
191, 193, 197, 199,

211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293

307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397

401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499

503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599

601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691,

701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797,

809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887,

907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997.

C Comportamento de $f(x) = \left(\frac{x}{n+1}\right)^{\frac{1}{x}}$

Vamos agora fazer uma análise do comportamento da função $f : \mathbb{R}_+^* \rightarrow \mathbb{R}_+$ dada por $f(x) = \left(\frac{x}{n+1}\right)^{\frac{1}{x}}$ em que $n \in \mathbb{N}$ é um natural. Queremos mostrar que $0 < f(x) < 1$ para $x < n+1$ e que $1 < f(x) < 2$ para $x > n+1$, claramente $f(n+1) = 1$. Usaremos o fato que f é infinitamente derivável em todo o seu domínio.

1. **Derivada** Sendo $f(x) = \left(\frac{x}{n+1}\right)^{\frac{1}{x}}$, temos

$$f(x) = \left(\frac{x}{n+1}\right)^{\frac{1}{x}} = e^{\ln\left(\frac{x}{n+1}\right)^{\frac{1}{x}}}$$

$$f(x) = e^{\frac{1}{x} \ln\left(\frac{x}{n+1}\right)}$$

$$\frac{d}{dx} f(x) = e^{\frac{1}{x} \ln\left(\frac{x}{n+1}\right)} \cdot \frac{d}{dx} \left[\frac{1}{x} \cdot \ln\left(\frac{x}{n+1}\right) \right]$$

$$\frac{d}{dx} f(x) = \left(\frac{x}{n+1}\right)^{\frac{1}{x}} \cdot \left[\frac{1}{x} \cdot \frac{d}{dx} \ln\left(\frac{x}{n+1}\right) + \frac{d}{dx} \frac{1}{x} \cdot \ln\left(\frac{x}{n+1}\right) \right]$$

$$\frac{d}{dx} f(x) = \left(\frac{x}{n+1}\right)^{\frac{1}{x}} \cdot \left[\frac{1}{x} \cdot \frac{n+1}{x} \cdot \frac{1}{n+1} + (-1) \cdot x^{-2} \cdot \ln\left(\frac{x}{n+1}\right) \right]$$

$$\frac{d}{dx} f(x) = \left(\frac{x}{n+1}\right)^{\frac{1}{x}} \cdot \left[\frac{1}{x^2} - \frac{1}{x^2} \cdot \ln\left(\frac{x}{n+1}\right) \right]$$

$$\frac{d}{dx} f(x) = (n+1)^{\frac{-1}{x}} \cdot x^{\frac{1}{x}-2} \cdot [1 - \ln\left(\frac{x}{n+1}\right)]$$

2. **Monotonicidade**

O sinal de $\frac{d}{dx} f(x)$ fica determinado pelo sinal de $g(x) = 1 - \ln\left(\frac{x}{n+1}\right)$.

Note que $g(x) = 1 - \ln\left(\frac{x}{n+1}\right) > 0$ se e somente se $\ln\left(\frac{x}{n+1}\right) < 1 = \ln(e)$ ou seja, $\frac{x}{n+1} < e$. Analogamente, $g(x) = 1 - \ln\left(\frac{x}{n+1}\right) < 0$ se e somente se $\frac{x}{n+1} > e$.

Portanto f é crescente se $x \leq e(n+1)$ e decrescente se $x \geq e(n+1)$

Assim sendo, f possui um máximo quando $x = e(n+1)$. Note que $1 < f(e(n+1)) < 2$

3. **Valor assintótico para $x \mapsto +\infty$**

Vamos calcular o limite da função

$$f(x) = \left(\frac{x}{n+1}\right)^{\frac{1}{x}}$$

$$L = \lim_{x \rightarrow \infty} f(x) = \lim_{x \rightarrow \infty} \left(\frac{x}{n+1}\right)^{\frac{1}{x}}$$

$$L = \lim_{x \rightarrow \infty} \left(\frac{x}{n+1}\right)^{\frac{1}{x}} = \lim_{x \rightarrow \infty} e^{\ln\left(\frac{x}{n+1}\right)^{\frac{1}{x}}} = \lim_{x \rightarrow \infty} e^{\frac{\ln\left(\frac{x}{n+1}\right)}{x}}$$

Pela continuidade da função exponencial, temos:

$$L = e^{\lim_{x \rightarrow \infty} \frac{\ln\left(\frac{x}{n+1}\right)}{x}}$$

Pela regra de L'Hospital, temos

$$L = e^{\lim_{x \rightarrow \infty} \frac{1}{x}} = e^0 = 1.$$

Assim, para todo $x > n + 1$, temos $1 < f(x) < 2$.