Universidade Federal de São Paulo

Instituto de Ciência e Tecnologia

Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

Números primos, Espiral de Ulam e outros caminhos

Gabriel Silva Delgado

Orientador: Prof. Dr. Robson da Silva

São José dos Campos
Maio, 2021

PROFMAT

Título: *Números primos, Espiral de Ulam e outros caminhos*

Dissertação apresentada ao Instituto de Ciência e Tecnologia da UNIFESP, campus São José dos Campos/SP, como parte dos requisitos exigidos para a obtenção do título de Mestre pelo Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT.

São José dos Campos
Maio, 2021

Delgado, Gabriel Silva

Números primos, Espiral de Ulam e outros caminhos, Gabriel Silva Delgado – São José dos Campos, 2021.

viii, 62f.

Dissertação (Mestrado) – Universidade Federal de São Paulo. Instituto de Ciência e Tecnologia. Programa de Pós-Graduação em Matemática em Rede Nacional (PROFMAT).

Prime numbers, Ulam's Spiral and other ways

1. Números primos. 2. Espiral de Ulam. 3. Teoria dos números.

UNIVERSIDADE FEDERAL DE SÃO PAULO

INSTITUTO DE CIÊNCIA E TECNOLOGIA

Mestrado Profissional em Matemática em Rede Nacional
PROFMAT

Chefe de departamento:

Prof. Dr. Marcelo Cristino Gama

Coordenador do Programa de Pós-Graduação:

Prof. Dr. Angelo Calil Bianchi

Gabriel Silva Delgado

Números primos, Espiral de Ulam e outros caminhos.

Dissertação apresentada à Universidade Federal São Paulo como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Matemática

Aprovada em 14 de maio de 2021.

Presidente da Banca:

Prof. Dr. Robson da Silva 

Banca Examinadora:

Prof. Dr. Alessandro Bagatini

Prof. Dr. Kelvin Souza de Oliveira

Prof. Dr. Marcelo Cristino Gama

"O caminho da vida é aprender,
você pode aprender rápido ou devagar,
você pode aprender certo ou errado,
mas nunca aprenderá tudo ou nada."
- Delgado, Gabriel S.

AGRADECIMENTOS

Agradeço primeiramente aos professores do Programa de Mestrado Profissional em Rede Nacional - PROFMAT, pois dedicaram o seu tempo à louvável arte de ensinar.

Agradeço também a todos professores que tive o prazer de conhecer durante minha jornada pelo ramo da matemática, com menção honrosa ao professor Rodrigo Rodrigues, que ainda no ensino fundamental me mostrou que a matemática é muito mais do que apenas números.

Agradeço aos meus amigos com quem tive muitas discussões filosóficas e acadêmicas e que me permitiram ter novas visões sobre antigos conceitos, além de me incentivarem a prosseguir com a ideia deste trabalho.

Agradeço aos colegas de turma, pois sempre estiveram dispostos a ajudar o próximo, e em especial a todos que nunca me negaram uma carona.

Agradeço à minha família, aos meus pais que sempre se esforçaram para me guiar pelos bons caminhos da vida, e a meu irmão e sua esposa, que me permitiram ver uma nova vida surgir após o fim de outra que outrora me criara.

Além disso, agradeço às fontes de fomento à ciência e tecnologia no Brasil, pois possibilitam o avanço científico no país, e embora eu não tenha usufruído diretamente de auxílio financeiro, possa ser que alguma de minhas referências o tenha feito, e por isso esse trabalho é do jeito que é graças a isso.

RESUMO

O estudo dos números primos é algo que pode ser encontrado até mesmo nos primeiros registros matemáticos que se tem notícias. Euclides dedicou um tempo de sua vida para esse estudo, e desde então, diversos outros matemáticos proeminentes também o fizeram, descobrindo cada vez mais perguntas que ainda hoje encontram-se em aberto. No fim do século XX, Stein, Ulam e Wells [14] apresentaram uma importante representação pictórica dos números primos que revelou certos padrões entre eles, e nesse trabalho, o objetivo foi encontrar uma generalização dessa representação como forma de incentivo para o ensino dos números primos na educação básica.

Palavras-chave: 1. Números primos. 2. Espiral de Ulam. 3. Teoria dos números.

ABSTRACT

The study of prime numbers is something that can be found even in the first mathematical records that have news. Euclid dedicated a time of his life on it, and since then, several other prominent mathematicians have done so, discovering more and more questions that are still open. At the end of the 20th century, Stein, Ulam and Wells [14] presented an important pictorial representation of prime numbers that revealed certain patterns between them, and in this papper, the objective was to find a generalization of this representation as a way of encouraging the teaching of prime numbers in education basic.

Keywords: 1. Prime numbers. 2. Ulam's Spiral. 3. Number's theory.

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

Os inteiros maiores do que 1 que possuem exatamente dois divisores positivos são denominados *primos*. Graças ao Teorema Fundamental da Aritmética, sabe-se que os números primos são os tijolos fundamentais na construção de toda a Teoria dos Números, o ramo da matemática que se ocupa do estudo das propriedades dos números inteiros. É difícil precisar quando teve início o estudo sistemático das propriedades desses números, no entanto, pode-se dizer que foi Euclides (300 a.C.) quem formalizou os conceitos até então conhecidos sobre os primos e apresentou algumas importantes propriedades, incluindo uma demonstração de sua infinitude.

Existem muitos problemas relativos aos primos que, mesmo após muito esforço ao longo dos séculos, continuam sem solução. Um dos grandes mistérios envolvendo tais números e que tem desafiado os matemáticos é o estudo da distribuição dos primos entre os números naturais. Deseja-se, pois, explorar a seguinte questão: como os números primos estão distribuídos? Se por um lado existe a Conjectura dos primos gêmeos[1], segundo a qual existem infinitos pares de primos gêmeos, por outro lado, existem sequências tão grande quanto se queira de inteiros consecutivos, todos compostos, bastando tomar, para $k > 1$, a sequência de k inteiros compostos:

$$(k+1)! + 2, (k+1)! + 3, \ldots, (k+1)! + (k+1).$$

O ensino básico no Brasil promove um primeiro contato com os números primos no início dos anos finais do ensino fundamental, e este conhecimento normalmente é associado à operação de encontrar o mínimo múltiplo comum entre dois ou mais números, expressando assim a ideia de que com os primos pode-se construir todos os outros naturais.

Há também a possibilidade de introduzir os primos por meio de uma abordagem geométrica, observando as diversas representações retangulares dos números, evidenciando que os primos só têm uma representação retangular possível, na qual uma de suas dimensões equivale a exatamente uma única unidade de comprimento, quase que a definição de primos exposta por Roque (2012) em [13], nas palavras da autora, um número é primo quando não é medido por nenhum número, somente por 1 (essa é, aliás, a definição de Euclides em [4]).

Em alguns materiais didáticos, segundo [5], os autores costumam trazer testes de primalidade, sendo os mais comuns o Crivo de Eratóstenes e o método das divisões sucessivas. Insistem nisso para construir na mente do aluno a ideia de números primos, visto que eles acompanham toda trajetória matemática do educando. Esses números estão presentes no processo de fatoração e decomposição numérica, operações com frações, cálculos de radi-

[1] primos gêmeos são pares de primos que diferem por exatamente 2: 3 e 5, 17 e 19, 101 e 103, etc.

ciação entre outros. Assim, na escola, estes tijolos fundamentais se mostram realmente importantes.

O mistério por trás dos números primos pode ser uma frutífera fonte de conhecimento. É possível explorar tal mistério para ensinar os conceitos que os permeiam. A Espiral de Ulam é um bom exemplo, algo simples que permite verificar muitas propriedades, como: a densidade de primos $\frac{\pi(x)}{x}$, na qual $\pi(x)$ é a função contadora de primos, sendo então seu valor a quantidade de primos até x; polinômios do tipo $x^2 + x + q$ que são ricos em primos, isto é, polinômios que contém em suas imagens, valores primos; existência de primos gêmeos; grandes intervalos sem primo algum; entre outras propriedades que podem ser notadas simplesmente ao olhar tal representação pictórica.

O objetivo desse trabalho é apresentar uma generalização de representações pictóricas para números primos e, introduzir isso em sala de aula como uma forma de explorar os números primos e seus mistérios. No primeiro capítulo serão abordadas algumas demonstrações da infinitude do conjunto dos números primos. O segundo capítulo trata sobre alguns testes de primalidade e teoremas clássicos envolvendo primos. O terceiro capítulo nos traz um panorama sobre a distribuição dos primos e avanços importantes no último século. Esses três primeiros capítulos fornecem uma boa base para apreciar o quarto capítulo, que traz a Espiral de Ulam, discute sobre o assunto, e aborda ideias de generalização da mesma. Por último, há uma proposta didática destinada à apresentação dos números primos para os alunos do 6º ano do ensino fundamental. Finalizando o trabalho temos as conclusões dessa dissertação, referências para quem busca aprofundar-se no assunto e o apêndice, fornecendo um material complementar para a proposta didática.

1

EXISTEM INFINITOS PRIMOS....

"Ao infinito... e além!"
- Lightyear, B.

Esse capítulo é dedicado a mostrar que existem infinitos primos, algo conhecido desde a época de Euclides e que ao longo da história foi se refinando e ganhando novas demonstrações que serão mostradas aqui, todas foram interpretadas à luz de [12] que traz essas e outras demonstrações mais complexas.

Teorema 1.1 (Teorema Fundamental da Aritmética)**.** *Todo número natural maior do que 1 ou é primo ou pode ser escrito de forma única, a menos da ordem dos fatores, como produto de números primos.*

Demonstração. Seguiremos essa demonstração pelo princípio da indução finita. Seja $n \in \mathbb{N}$ e suponha como hipótese de indução que todo número natural menor que n possa ser decomposto como produto finito de fatores primos.

Dessa forma ou n é primo, e a nossa demonstração se encerra, ou então $n = m \cdot k$, com $m < n$ e $k < n$. Nesse segundo caso, segue da hipótese de indução que m e k são produtos de fatores primos e, portanto, n também o é. Assim, pelo princípio da Indução, concluímos que todo número natural é produto de números primos.

Mostremos, utilizando o princípio da indução finita, que tal decomposição é única. Considere $n \in \mathbb{N}$ e suponha como hipótese de indução que a decomposição em fatores primos de todo número natural menor que n seja única, exceto pela ordem dos fatores.

Se n for primo, não há o que provar. Caso contrário, como n se decompõe como produto de fatores primos, podemos escrever $n = p \cdot q$, em que p é primo. Como $q < n$, temos pela hipótese de indução que q admite uma única decomposição em fatores primos e, assim, a decomposição de $p \cdot q$ também é única. Mas como $n = p \cdot q$, segue que a decomposição de n é única. Portanto, pelo princípio da indução, conclui-se que todo número natural se decompõe de modo único como produto de fatores primos.

□

Teorema 1.2. *Existem infinitos números primos*

Muitos matemáticos célebres já demonstraram que existem infinitos primos, algumas provas são parecidas entre si, outras tomam uma abordagem totalmente diferente. Uma das mais difundidas é a elaborada por Euclides.

Demonstração de Euclides para o Teorema 1.2. Seguiremos nossa demonstração por absurdo. Para isso, consideremos que o conjunto $\mathcal{P}$ dos primos seja finito, com $\mathcal{P} =$

$\{p_1, p_2, \ldots, p_n\}$.
Agora, podemos construir um número $N \in \mathbb{N}$ tal que $N = p_1 \cdot p_2 \cdot \cdots \cdot p_n$, perceba que N é composto, e, a partir dele, tome o seu sucessor, isto é, $N + 1$. Note que, ao tentarmos dividir $N + 1$ por qualquer elemento de $\mathcal{P}$ teremos um resto 1, ou seja, $N + 1$ não pode ser decomposto em fatores primos. Pelo Teorema Fundamental da Aritmética isso é um absurdo, pois $N + 1$ deveria ser decomposto como produto de elementos de $\mathcal{P}$. Logo esse conjunto não pode ser finito. □

É um exercício válido checar o que acontece para cada valor de $n \in \mathbb{N}$ neste caso, isto é, se $n = 1$ teríamos $\mathcal{P} = p_1 = 2$, portanto $N = 2$ e $N + 1 = 3$, temos aqui então um primo fora do conjunto $\mathcal{P}$ descrito. Confira a Tabela 1, note que dado $\mathcal{P}$ com n elementos, chamaremos $P\#$ o produto de todos os elementos de $\mathcal{P}$ (este é definido como Primorial).

Definição 1.3. *Se $n \in \mathbb{N}$, então o primorial de n, denotado por $n\#$ será dado pelo seguinte produto $n\# = \prod_{k=1}^{p_k \leq n} p_k$, onde p_k é o k-ésimo primo. Por definição $0\# = 1$.*

Mais tarde ficará claro que podemos definir $n\#$ também como $n\# = \prod_{i=1}^{\pi(n)} p_i$, em que $\pi(n)$ é função contadora de primos.

Exemplo 1.4. $6\# = 2 \cdot 3 \cdot 5 = 30$; $5\# = 2 \cdot 3 \cdot 5 = 30$

Observação 1.5. *Se n for composto, então $n\# = (n-1)\#$*

Tabela 1: Valores de $P\# + 1$ fatorados.

n	$P\#$	$P\# + 1$	Fatoração prima de $P\# + 1$
1	2	3	3
2	$2 \cdot 3$	7	7
3	$2 \cdot 3 \cdot 5$	31	31
4	$2 \cdot 3 \cdot 5 \cdot 7$	211	211
5	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	2311	2311
6	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	30031	$59 \cdot 509$
7	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	510511	$19 \cdot 97 \cdot 277$
8	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	9699691	$347 \cdot 27953$

Sobre a demonstração de Euclides para o Teorema 1.2, existem alguns problemas em aberto, dois deles são os seguintes: Será que $P\# + 1$ é livre de quadrados? Isto é, ao decompor esse número, haverá algum elemento repetido duas vezes? E o outro problema é se existem infinitos primos da forma $P\# + 1$. Para esse segundo questionamento, é possível ver que $P\# + 1$ é primo para $n =$ 0,1, 2, 3, 4, 5, 11, 75, 171, 172, 384, 457, 616, 643, 1391, 1613, 2122, 2647, 2673, 4413, 13494, 31260, 33237.

Sobre o Teorema 1.2, em 1878, Kummer, analisando a demonstração proposta por Euclides, elaborou algo simples e elegante, confira a seguir

Demonstração de Kummer para o Teorema 1.2. Eleja o mesmo conjunto $\mathcal{P}$ finito proposto por Euclides em sua demonstração. Com ele tem-se $N = p_1 \cdot p_2 \cdot \cdots \cdot p_n$, além disso, o número $N-1$ que tem pelo menos um fator primo p_i em comum com N, então p_i divide N e $N-1$, logo divide a subtração desses dois valores, ou seja, $N-(N-1) = p_i \cdot \left(\frac{N}{p_i} - \frac{N-1}{p_i}\right) = p_i \cdot \frac{N-N+1}{p_i} = p_i \cdot \frac{1}{p_i} = 1$ o que é um absurdo pois isso implica que p_i divide 1. □

Goldbach, em 1730, também elaborou uma prova que consiste em encontrar uma sequência infinita de números primos entre si, isto é, que não tenham fatores primos em comum. Talvez a maior dificuldade dessa demonstração seja encontrar ou definir tal sequência. Goldbach, sagazmente, utilizou os números de Fermat. Demonstremos algumas afirmações antes de mostrar a demonstração elaborada para o Teorema 1.2.

Definição 1.6. *O n-ésimo número de Fermat é definido por* $F_n = 2^{2^n} + 1, n \geq 0$.

Lema 1.7. $F_n - 2 = F_0 \cdot F_1 \cdot \ldots \cdot F_{n-2} \cdot F_{n-1}$, *para* $n \geq 1$

Demonstração. A prova será feita por indução.

Para $n = 1$ temos

$$F_1 - 2 = 2^{2^1} + 1 - 2 = 4 - 1 = 3 = 2^{2^0} + 1 = F_0$$

Tome como hipótese de indução que para todo $k < n, k \in \mathbb{N}$ tem-se

$$F_k - 2 = F_0 \cdot F_1 \cdot \ldots \cdot F_{k-2} \cdot F_{k-1} \Rightarrow F_k = F_0 \cdot F_1 \cdot \ldots \cdot F_{k-1} + 2$$

Mostremos que vale para F_n:

$$\begin{aligned} F_0 \cdot F_1 \cdot \ldots \cdot F_{n-2} \cdot F_{n-1} + 2 &= (F_{n-1} - 2)F_{n-1} + 2 \\ &= (2^{2^{n-1}} + 1 - 2)(2^{2^{n-1}} + 1) + 2 \\ &= (2^{2^{n-1}} - 1)(2^{2^{n-1}} + 1) + 2 \\ &= (2^{2^{n-1}})^2 - 1 + 2 \\ &= 2^{2^n} + 1 \\ &= F_n, \end{aligned}$$

o que completa a demonstração.

□

Definição 1.8. *Dados dois inteiros a e b tais que* $mdc(a, b) = 1$, *isto é, em fatoração prima, eles não possuem nenhum fator primo em comum, dizemos que a e b são coprimos, ou primos entre si.*

Teorema 1.9. *Os números de Fermat* $F_n = 2^{2^n} + 1$ *são dois a dois coprimos.*

Demonstração. Suponha por Absurdo que $\exists p \in \mathbb{N}$ tal que $p|F_n$ e $p|F_m$, com $n < m$.

Usando o Lema 1.7 no qual $F_m - 2 = F_0 \cdot F_1 \cdot \ldots \cdot F_n \cdot \ldots \cdot F_{m-1}$, então tem-se $q_1, q_2 \in \mathbb{N}$ tais que $p \cdot q_1 - 2 = p \cdot q_2$, logo $p \cdot q_1 = F_m$ e $p \cdot q_2 = F_0 \cdot F_1 \cdot \ldots \cdot F_n \cdot \ldots \cdot F_{m-1}$. Dessa forma, pode-se isolar o natural 2 e colocar em evidência o primo em comum, ganhando a seguinte igualdade envolvendo um produto de inteiros, que resulta em um n natural:

$$p(q_1 - q_2) = 2$$

Como $p \geq 2$, mesmo que tivéssemos $(q_1 - q_2) = 1$, isso implicaria $p = 2$, o que é um absurdo, pois assumimos que $p|F_n$ e $p|F_m$. Mas F_i é ímpar $\forall i \in \mathbb{N}$, o que completa a demonstração. □

E agora podemos analisar a demonstração proposta por Goldbach.

Demonstração de Goldbach para o Teorema 1.2. Suponha que exista um número finito n de primos, tome a sequência de números de Fermat composta por $n+1$ números. Como, pelo Teorema 1.9, eles são dois a dois coprimos, existem pelo menos $n+1$ primos, o que é um absurdo. □

Euler realizou uma prova indireta da infinitude dos primos partindo de uma série geométrica.

Definição 1.10. *Uma progressão geométrica (P.G.) é uma aplicação $x : \mathbb{N}^* \to \mathbb{R}$ em que $x(n)$, escrito como x_n, é o n-ésimo termo da sequência (x_n) e é definido como $x_n = x_1 \cdot q^n$, onde q é chamada a razão da P.G.*

Exemplo 1.11. *Seja $x_1 = 1$ e $q = 1/2$ tem-se $(x_n) = (1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8} \ldots)$*

Teorema 1.12. *A soma finita dos n primeiros termos de uma P.G. é dada por S_n, onde*

$$S_n = \sum_{i=1}^{n} x_1 q^{i-1} = x_1 + x_1 q + x_1 q^2 + \ldots + x_1 q^{n-1} = \frac{x_1(1-q^n)}{1-q}.$$

Demonstração. Tome $S_n = x_0 + x_0 q + x_0 q^2 + \ldots + x_0 q^n$, multiplicando ambos os lados da igualdade por q tem-se $qS_n = x_0 q + x_0 q^2 + x_0 q^3 + \ldots + x_0 q^{n+1}$ de tal modo que $qS_n - S_n = x_0 q^{n+1} - x_0$ e, portanto, $S_n = \frac{x_0(1-q^{n+1})}{1-q}$. □

Teorema 1.13. *A soma infinita dos termos da P.G., definida como Série Geométrica, quando $-1 < q < 1$, é dada por*

$$S_\infty = \sum_{i=1}^{\infty} x_1 q^{i-1} = x_1 + x_1 q + x_1 q^2 + \ldots + x_1 q^n + \ldots = \frac{x_1}{1-q}$$

Demonstração. Tome o limite de S_n com $n \to \infty$:

$$\lim_{n\to\infty} S_n = \lim_{n\to\infty} \frac{x_1(1-q^n)}{1-q} = \lim_{n\to\infty} \frac{x_1}{1-q} - \lim_{n\to\infty} \frac{x_1 q^n}{1-q} = \lim_{n\to\infty} \frac{x_1}{1-q} = \frac{x_1}{1-q}$$

□

Agora, com estes teoremas e definições estabelecidos, podemos começar a avançar no argumento de Euler. Defina uma série geométrica S^p com $x_1 = 1$ e $q = 1/p$, sendo p um primo qualquer, teremos então $S^p = \sum_{i=1}^{\infty} \left(\frac{1}{p}\right)^{i-1} = \frac{1}{1-\frac{1}{p}}$ que nos permite observar que quanto maior for p, mais próximo de 1 a soma se aproxima pois $\frac{1}{1-\frac{1}{p}} = \frac{p}{p-1}$. Note que podemos realizar esse mesmo raciocínio para um primo r obtendo uma nova série S'_n e, ao multiplicar essas duas séries, obtém-se

$$\begin{aligned} S^p S'^p &= \sum_{i=1}^{\infty} \left(\frac{1}{p}\right)^{i-1} \cdot \sum_{i=1}^{\infty} \left(\frac{1}{r}\right)^{i-1} \\ &= 1 + \frac{1}{p} + \frac{1}{r} + \frac{1}{pr} + \frac{1}{p^2} + \frac{1}{r^2} + \frac{1}{pr^2} + \frac{1}{p^2 r} + \frac{1}{p^2 r^2} + \dots \\ &= \frac{1}{1-\frac{1}{p}} \cdot \frac{1}{1-\frac{1}{r}} = \frac{p}{p-1} \cdot \frac{r}{r-1} \end{aligned}$$

Observe que aqui temos a soma do inverso de todos os naturais n que quando decompostos exibem apenas fatores primos p, r ou ambos, de modo que $n = p^h r^k, h \geq 0, k \geq 0$.

Com todos esses parâmetros estabelecidos, observe a demonstração elaborada para o Teorema 1.2.

Demonstração de Euler para o Teorema 1.2. Suponha que existe um número finito n de primos. Para cada $j = 1, \dots, n$ tome a seguinte igualdade:

$$\sum_{i=1}^{\infty} \left(\frac{1}{p_j}\right)^{i-1} = \frac{1}{1-\frac{1}{p_j}}$$

Multiplicando todas essas igualdades tem-se

$$\prod_{j=1}^{n} \left(\sum_{i=1}^{\infty} \left(\frac{1}{p_j}\right)^{i-1} \right) = \prod_{j=1}^{n} \frac{1}{1-\frac{1}{p_j}}$$

O lado esquerdo da igualdade, gera a soma do inverso de cada um dos infinitos números naturais, que possuem fatoração prima de forma única. Logo, os números naturais que aqui surgem aparecem apenas uma única vez de forma que temos, portanto, o somatório do inverso de todos os números naturais. Obtém-se, dessa forma, nesse lado esquerdo da igualdade, o que é chamado de uma Série Harmônica, definida por $S = \sum_{n=1}^{\infty}(1/n)$, e a mesma diverge, e, portanto, é infinita, enquanto do lado direito, tem-se um produto finito de n termos, que é a quantidade de primos que havíamos suposto no início. Portanto o valor desse produto converge. Logo, um absurdo. □

2

VOCÊ VIU MEU PRIMO POR AÍ?

"Onde estão meus primos?"
- Calcanhotto, A.

Esse capítulo aborda teoremas clássicos referentes a números primos, como o Pequeno Teorema de Fermat e o Teorema de Wilson, além de trazer ferramentas importantes para concluir se um número é primo ou não. Esses testes foram extraídos do livro [12] que debate outros testes e mais referências sobre o assunto.

Os estudos dos números primos datam de séculos atrás, e a partir do momento em que a investigação desses números peculiares iniciou-se, muitas descobertas foram feitas e vários pensamentos tomaram forma, como o crivo de Eratóstenes por exemplo, que consiste numa maneira intuitiva de se encontrar números primos, e que pode revelar algumas propriedades interessantes, partindo desde premissas básicas, como, o número 2 ser o único primo par, a até conclusões mais técnicas como a de que existem 25 primos entre 2 e 100.

A construção de um crivo de Eratóstenes de 2 a 100 é simples: Escreve-se em forma de uma tabela 10×10 os números de 2 a 100, ignorando a primeira célula, de cima para baixo, da esquerda para direita, e então para cada p primo, risque todos os múltiplos dele que são maiores do que ele, faça isso enquanto $p^2 < 100$.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Algumas pessoas talvez se perguntarão o porquê de fazer essa iteração apenas até que $p^2 < 100$. Acontece que se n não for primo, então $n = a \cdot b$, tendo em mente que

$n = \sqrt{n} \cdot \sqrt{n}$, então, para $a \neq 1$ e $b \neq 1$, $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$, pois caso contrário, $a \cdot b > n$, então, caso n seja fatorável, pelo menos um de seus fatores será menor ou igual a $\sqrt{n}$. Nesse caso, como $\sqrt{100} = 10$, temos que para $p = 11, p^2 > 100$. Logo, só precisamos eliminar os múltiplos dos quatro primeiros primos $2, 3, 5, 7$.

A fim de verificar alguns teoremas fundamentais sobre números primos, trabalharemos a seguir com congruências.

Definição 2.1. *Para $a, b, n \in \mathbb{Z}$, dizemos que a e b são congruentes módulo n se $n|a-b$, e escreve-se $a \equiv b \bmod n$. Consequentemente, isso implica dizer que $\exists\ k \in \mathbb{Z}$ tal que $nk = a - b$, podendo-se associar essa igualdade à uma divisão com dividendo igual ao termo a, divisor com valor n, resto b e quociente k. Caso as condições de congruência não sejam satisfeitas, dizemos que a é incongruente a b módulo n, e denotamos como $a \not\equiv b \bmod n$.*

A notação módulo pode ser muito útil quando se quer identificar o resto da divisão de um número em relação a outro. Por exemplo, quando utilizamos um relógio que segue o modelo 24h, algumas pessoas tendem a calcular a hora atual módulo 12 para ter o mesmo horário no sistema AM/PM. Uma das formas de se fazer isso é dividindo o horário no formato 24h por 12, verificar o resto da divisão, associar o quociente 0 para AM e 1 para PM. Caso fosse 18 horas por exemplo, teríamos resto 6 e quociente 1 indicando 06h00 PM, com a notação de módulo obtém-se $18 \equiv 6 \bmod 12$.

Na programação de computadores, o módulo pode ser usado para criar um algoritmo simples que identifica se um número é par ou não, uma vez que dado $n \in \mathbb{N}$ tem-se $n \equiv 0 \bmod 2$ caso n seja par e $n \equiv 1 \bmod 2$ caso não. Como exemplo, tome $n = 8$, como pelo algoritmo da divisão euclidiana $8 = 2 \cdot 4 + 0$, isto é, deixa resto 0 na divisão por 2, dizemos que 8 é par, o mesmo não acontece com 63, pois $63 = 2 \cdot 31 + 1$, indicando que 63 deixa resto 1 na divisão por 2, logo 63 é ímpar.

Às vezes, quando se fala em equações envolvendo congruências valores desconhecidos sendo multiplicados, como $ax \equiv 1 \bmod b$, nem sempre haverá uma solução, uma vez que é possível enxergar a congruência como uma equação diofantina e verificar o teorema a seguir.

Teorema 2.2 (Teorema de Bézout)**.** *Dados inteiros a e b, não ambos nulos, existem inteiros m e n tais que*

$$am + bn = mdc(a, b).$$

Demonstração. Seja $B = \{am + bn | m, n \in \mathbb{Z}\}$, tome n_0 e m_0 tal que $c = am_0 + bn_0$ seja o menor elemento positivo de B, mostremos que $c|a$. Nosso objetivo é mostrar que o valor de m e n procurados são $m = m_0$ e $n = n_0$.

Suponha que $c \nmid a$. Logo $\exists\ r, q \in \mathbb{Z}$, com $0 < r < c$ tais que

$$\begin{aligned} qc + r &= a \\ r &= a - qc \\ &= a - q(am_0 + bn_0) \\ &= a - qam_0 - qnn_0 \\ &= a(1 - qm_0) + b(-qn_0) \end{aligned}$$

implicando em

$$0 < a(1 - qm_0) + b(-qn_0) < c = am_0 + bn_0.$$

Logo $r < c$ e $r \in B$, o que contraria a hipótese de que c é o menor elemento de B. Analogamente é possível mostrar que $c|b$, o que nos resulta em $c \leq mdc(a, b)$.

Seja $d = mdc(a, b)$ então pode-se escrever $a = dk_1$ e $b = dk_2$, então $c = (dk_1)m_0 + (dk_2)n_0 = dk$ com $k = k_1m_0 + k_2n_0$. Com isso, c é um múltiplo de $mdc(a, b)$ logo $mdc(a, b) \leq c$.

Pode-se então concluir que $c = mdc(a, b)$. □

Do Teorema 2.2 fica claro que dados números inteiros tais que $ax + by = c$, então c é um múltiplo de $mdc(a, b)$ e, portanto, pode-se obter $\frac{a}{mdc(a,b)}x + \frac{b}{mdc(a,b)}y = 1$. Com isso, e dados $p, q \in \mathbb{Z}$ tais que $px + qy = 1$ então $mdc(p, q) = 1$.

Teorema 2.3 (Pequeno Teorema de Fermat)**.** *Se p é primo e $a \in \mathbb{Z}$, então $a^p \equiv a \bmod p$. Em particular, se $p \nmid a$ então $a^{p-1} \equiv 1 \bmod p$.*

Demonstração. Para $p = 2$ o resultado é simples pois $a^2 - a = a(a - 1)$ e $2|a(a - 1)$ uma vez que $a \in \mathbb{Z}$ e a ou $a - 1$ é par. Para os outros casos, assumir-se-á p um primo ímpar e realizaremos uma indução para $a \geq 0$.

Para $a = 0$, o resultado é trivial, uma vez que $p|0, \forall p \in \mathbb{N}$. Assumindo como hipótese de indução que, para $a \leq k, k \in \mathbb{N}$, tem-se $a^p \equiv a \bmod p$ e verificar-se-á a validade para $a + 1$, ou seja, que $(a + 1)^p \equiv a + 1 \bmod p$.

Pelo binômio de Newton, tem-se $(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a^1 + 1$, mas no lado direito dessa igualdade, dado que $\binom{p}{i} = p \cdot \frac{(p-1)\ldots(p-i+1)}{i!}$, então, todas as parcelas acompanhadas de $\binom{p}{i}, 1 \leq i \leq p - 1$ são divisíveis por p, de modo que $(a + 1)^p$ quando dividido por p tem o mesmo resto que $a^p + 1$ na divisão, isto é, $p|(a+1)^p - (a^p + 1)$ ou seja, $(a + 1)^p \equiv a^p + 1 \bmod p$. Mas da hipótese de indução, tem-se $a^p \equiv a \bmod p$ e, portanto, pode-se concluir que $(a + 1)^p \equiv a + 1 \bmod p$.

Caso $p \nmid a$, sabemos que $p|a^p - a$, ou seja, $p|a(a^{p-1} - 1)$, e como $p \nmid a$ então $p|a^{p-1} - 1$, isto é, $a^{p-1} \equiv 1 \bmod p$. □

A recíproca deste teorema não é válida, isto é, dado $n \in \mathbb{N}$, se $b^{n-1} \equiv 1 \bmod n$, isso não garante que n seja primo. Os números que respeitam essa expressão são chamados de

números de Carmichael, sendo 561 um exemplo. Esses números podem aparecer também sob o nome de pseudoprimos.

Definição 2.4. *Dados os inteiros n e b, tais que eles sejam coprimos e n é composto, dizemos que n é um número de Carmichael se $b^{n-1} \equiv 1 \bmod n$.*

Note que, com o Teorema 2.3, pode-se ter uma boa noção de inverso multiplicativo na aritmética modular ao calcular o valor de X para que $aX \equiv 1 \bmod p$, dado que $p \nmid a$, com p primo e $a \in \mathbb{Z}$.

Seja $aX \equiv 1 \bmod p$. Do Teorema 2.3 temos que $a^{p-1} \equiv 1 \bmod p$ e, portanto, $aX \equiv a^{p-1} \bmod p$, ou seja, $aX - a^{p-1} \equiv 0 \bmod p$. Logo $a(X - a^{p-2}) \equiv 0 \bmod p$, mas como $p \nmid a$ então $X - a^{p-2} \equiv 0 \bmod p$, que implica $X \equiv a^{p-2} \bmod p$. Note que $a^{p-2} = a^p \cdot a^{-2}$ e como do Teorema 2.3 tem-se $a^p \equiv a \bmod p$, então $a^{p-2} = a^p \cdot a^{-2} \equiv a \cdot a^{-2} \bmod p \equiv a^{-1} \bmod p$, ou seja, $X \equiv a^{-1} \bmod p$.

Perceba que $a^{-1} \neq \frac{1}{a}$ uma vez que estamos tratando de aritmética modular aqui, devemos interpretar a^{-1} como o inverso multiplicativo de a dado um módulo n qualquer.

Definição 2.5. *Dado números inteiros tais que $a \cdot a^{-1} \equiv 1 \bmod n$ é dito que a^{-1} é o inverso multiplicativo de a módulo n ($a \bmod n$).*

Nesse contexto, nem sempre um número possui inverso multiplicativo modular. Por exemplo, dado $n = 8$, não existe $X \in \mathbb{Z}$ tal que, dado a um número par, tenha-se $aX \equiv 1 \bmod 8$. Suponha por absurdo que exista tal valor para X, teríamos então $aX - 1 = 8k, k \in \mathbb{Z}$ e como a é par, então $a = 2m \in \mathbb{Z}$, logo $2mX - 1 = 8k \Rightarrow 2(mX - 4k) = 1$, o que é um absurdo visto que do lado esquerdo da igualdade obtém-se um número par e do lado direito um número ímpar.

A partir do Teorema 2.3, se p é primo, temos que

$$1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \bmod p.$$

Segundo [12], em 1950, Giuga perguntou se a recíproca da afirmação acima é verdadeira, ou seja, se $n > 1$ satisfazer $1^{n-1} + 2^{n-1} + 3^{n-1} + \cdots + (n-1)^{n-1} + 1$ é múltiplo de n, então n é primo. Os números compostos que atendem a essa característica são *números de Carmichael*, pois se enquadram na Definição 2.4.

Definição 2.6. *Um conjunto de inteiros $\{r_1, r_2, \ldots, r_m\}$ é chamado de sistema completo de resíduos módulo n se $\forall k \in \mathbb{Z}\ \exists\ r_i$ tal que $k \equiv r_i \bmod n$, além disso, $r_i \neq r_j$ para todo $i = j$ e, mais do que isso, esses valores são todos dois a dois incongruentes módulo m.*

Definição 2.7. *Dado um sistema completo de resíduos $\mathcal{T}$ módulo n, define-se como sistema reduzido de resíduos todos os elementos de $\mathcal{T}$ que são coprimos com n.*

Note que se n for primo, o sistema completo de resíduos gera sempre um sistema reduzido de resíduos. Além disso, o número de elementos do sistema reduzido de resíduos módulo m será representado por $\varphi(m)$ e, portanto, por definição, $\varphi(m) \leq m - 1$ para

todo $m \geq 2$. Usualmente, $\varphi(n)$ conta o número de inteiros positivos menores do que ou iguais a n que são coprimos com n. Esta função é chamada *função fi de Euler*.

Exemplo 2.8. $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ *é um sistema completo de resíduos módulo* 12 *e* $\{1, 5, 7, 11\}$ *é o sistema reduzido de resíduos módulo 12. Observe que* $\varphi(12) = 4$ *pois* $\{1, 5, 7, 11\}$ *contém apenas 4 elementos.*

Dados os inteiros $r_1, r_2, \ldots, r_{\varphi(m)}$ elementos de um sistema reduzido de resíduo módulo m, então:

a) $mdc(r_i, m) = 1$ para todo $1 \leq i \leq \varphi(m)$;

b) $r_i \not\equiv r_j \bmod m$, se $i \neq j$;

c) Para cada $n \in \mathbb{Z}$ tal que $mdc(n, m) = 1$, $\exists i$ tal que $n \equiv r_i \bmod m$.

Proposição 2.9. *Sejam* $a > 0$ *e* m *inteiros tais que* $mdc(a, m) = 1$. *Se* $A = \{r_1, \ldots, r_{\varphi(m)}\}$ *é um sistema reduzido de resíduos módulo* m*, então o conjunto* $B = \{ar_1, \ldots, ar_{\varphi(m)}\}$ *também é um sistema reduzido de resíduos módulo* m.

Demonstração. Note inicialmente que em B há $\varphi(m)$ elementos. Em seguida, como $mdc(a, m) = 1$ e $mdc(r_i, m) = 1$, então $mdc(ar_i, m) = 1$, para $i = 1, \ldots, \varphi(m)$. Além disso, se $ar_i \equiv ar_j \bmod m$, como $mdc(a, m) = 1$, então $r_i \equiv r_j \bmod m$, o que implica $i = j$. □

Proposição 2.10. *Se* $A = \{a_1, \ldots, a_{\varphi(m)}\}$ *e* $B = \{b_1, \ldots, b_{\varphi(m)}\}$ *são dois sistemas reduzidos de resíduos módulo* m*, então cada elemento de* A *é congruente a exatamente um elemento de* B.

Demonstração. Inicialmente, completamos o conjunto B até obtermos um sistema completo de resíduos módulo m: $C = \{b_1, \ldots, b_{\varphi(m)}, b_{\varphi(m)+1}, \ldots, b_m\}$. Logo, cada $a_i \in A$ é congruente a exatamente um elemento de C. Suponhamos que $a_i \equiv b_j \bmod m$ com $j \in \{\varphi(m) + 1, \ldots, m\}$. Como $mdc(b_j, m) > 1$, então $mdc(a_i, m) > 1$, o que seria uma contradição. Portanto, a_i é congruente a algum $b_j \in C$ com $1 \leq j \leq \varphi(m)$, isto é, a_i é congruente a exatamente um elemento de B. □

Teorema 2.11 (Teorema de Euler)**.** *Se* m *é um inteiro positivo e* a *é um inteiro com* $mdc(a, m) = 1$*, então*

$$a^{\varphi(m)} \equiv 1 \bmod m.$$

Demonstração. Seja $\{r_1, \ldots, r_{\varphi(m)}\}$ um sistema reduzido de resíduos módulo m. Como $mdc(a, m) = 1$, então, pela Proposição 2.9, $\{ar_1, \ldots, ar_{\varphi(m)}\}$ é também um sistema reduzido de resíduos módulo m. Logo, pela Proposição 2.10, cada ar_i é congruente a exatamente um dos r_j. Então,

$$ar_1 ar_2 \cdot \ldots \cdot ar_{\varphi(m)} \equiv r_1 r_2 \cdot \ldots \cdot r_{\varphi(m)} \bmod m,$$

ou seja,

$$a^{\varphi(m)} r_1 r_2 \cdot \ldots \cdot r_{\varphi(m)} \equiv r_1 r_2 \cdot \ldots \cdot r_{\varphi(m)} \bmod m.$$

Como $mdc(r_1 \cdot \ldots \cdot r_{\varphi(m)}, m) = 1$, segue que $a^{\varphi(m)} \equiv 1 \bmod m$. □

Note que o Pequeno Teorema de Fermat (Teorema 2.3) é um corolário do Teorema de Euler que acabamos de provar, pois $\varphi(p) = p - 1$ se p é primo.

Definição 2.12. *Dados $a, m, k \in \mathbb{N}$ tais que $a > 1$ e $m > 1$, com $mdc(a, m) = 1$ e sendo k o menor inteiro positivo tal que $a^k \equiv 1 \bmod m$, dizemos então que a ordem de a módulo m é k, e denota-se isso por $ord_m(a) = k$.*

Exemplo 2.13. *$ord_{12}(5) = 2$ pois $5^2 = 25$ e $25 \equiv 1 \bmod 12$.*

Observação 2.14. *Seja $ord_m(a) = k$, então, pelo Teorema 2.11, $k \leq \varphi(m)$.*

Lema 2.15. *Dados inteiros a, m com $m > 1$ e $mdc(a, m) = 1$ então $a^n \equiv 1 \bmod m$ se, e somente se, $ord_m(a) | n$.*

Demonstração. Inicialmente, suponha que $n = r \cdot ord_m(a)$ então

$$a^n = a^{r \cdot ord_m(a)} = (a^{ord_m(a)})^r \equiv 1^r \bmod m \equiv 1 \bmod m.$$

Agora, supondo que $a^n \equiv 1 \bmod m$. Da divisão euclidiana sabe-se que $n = q \cdot ord_m(a) + r, 0 \leq r < ord_m(a)$. Suponha por absurdo que $r \neq 0$, então $a^n = a^{q \cdot ord_m(a) + r} = a^{q \cdot ord_m(a)} \cdot a^r = (a^{ord_m(a)})^q \cdot a^r \equiv a^r \bmod m$. Mas $a^n \equiv 1 \bmod m$ então, $a^r \equiv 1 \bmod m$, o que é um absurdo já que $0 < r < ord_m(a)$ e $ord_m(a)$ é o menor inteiro i tal que $a^i \equiv 1 \bmod m$. □

Corolário 2.16. *Dados inteiros a e m tais que $mdc(a, m) = 1$, então $ord_m(a) | \varphi(m)$.*

Teorema 2.17 (Teorema de Wilson)**.** *Se p é primo, então*

$$(p-1)! \equiv -1 \bmod p.$$

Demonstração. Como $(p-1)! = (p-1)(p-2)(p-3) \cdot \ldots \cdot 2 \cdot 1$, e os fatores dessa multiplicação formam um sistema completo e reduzido de resíduos módulo p. Isso garante que para cada $1 \leq i \leq p-1$ existe $1 \leq k \leq p-1$ tal que $(p-i)(p-k) \equiv 1 \bmod p$. Note que para $i = 1$ tem-se $k = 1$ e para $i = (p-1)$ obtém-se $k = (p-1)$.

Isso ocorre pois dado l inteiro tal que $l^2 \equiv 1 \bmod p$ então $l = 1$ ou $l = p - 1$, pois $p | l^2 - 1$, logo $l | l + 1$ ou $l | l - 1$, implicando $l = p + 1$ ou $l = 1$.

Omitindo os valores $i = 1$ e $i = p - 1$ tem-se $2 \cdot 3 \cdot \cdots \cdot (p-2) \equiv 1 \bmod p$, ou seja $(p-2)! \equiv 1 \bmod p$, multiplicando ambos os lados por $p - 1$ o resultado é $(p-1)! \equiv p - 1 \bmod p$, como $(p-1) \equiv -1 \bmod p$ então $(p-1)! \equiv -1 \bmod p$. □

Com o terreno já bem definido, conseguimos agora trabalhar em alguns testes de primalidade além do crivo apresentado no início dessa seção. O Teorema 2.17 nos dá uma boa caracterização dos primos, mas exige um demasiado processo computacional devido ao cálculo do fatorial. Em planilhas eletrônicas comuns, por exemplo, o teste costuma

falhar para $p > 17$. Mostremos que a recíproca do Teorema de Wilson garante ser um teste válido.

Teste 1 (Recíproca do Teorema de Wilson)**.** *Dado $n \in \mathbb{N}$ tal que*

$$(n-1)! \equiv -1 \bmod n$$

então n é primo.

Demonstração. Suponha que n não seja primo. Nesse caso, é possível escrever $n = a \cdot b$, sendo $a, b \in \mathbb{N}$ tais que $1 < a \leq b < n$ (se a pudesse ser 1, teríamos $b = n$, o que contraria a hipótese de n ser composto). Então tem-se $a|n$ e $b|n$. Dado que $a|n$ e $a < n$ obtém-se que $a|(n-1)!$.

Seja $(n-1)! = a \cdot q$ e $n = a \cdot b$. Como $(n-1)! \equiv -1 \bmod n$, então $(n-1)! + 1 = n \cdot t$. Pode-se escrever $a \cdot q + 1 = n \cdot t = a \cdot b \cdot t$ e, portanto, $a \cdot q - a \cdot b \cdot t = -1 \Rightarrow a(b \cdot t - q) = 1$ o que implica $a = (b \cdot t - q) = 1$. Um absurdo já que $a > 1$, logo n não pode ser composto. □

Exemplo 2.18. *Vamos verificar se o número 6 é primo utilizando o Teste 1:*

Seja $n = 6$. Calculemos $(n-1)! = (6-1)! = 5! = 120$, como $120 = 6 \cdot 20$ então $120 \equiv 0 \bmod 6$. Logo $(6-1)! \not\equiv -1 \bmod 6$ e portanto 6 não é primo.

No século XIX, Lucas nos forneceu um teste de primalidade que mais tarde foi aprimorado. Inicialmente o teste era o seguinte:

Teste 2. *Seja m inteiro. Se existir um inteiro a,$1 < a < m$, com $mdc(a, m) = 1$ tal que*

$$a^{m-1} \equiv 1 \bmod m$$

e

$$a^k \not\equiv 1 \bmod m, \forall 1 < k < m-1$$

então m é primo.

Demonstração. Sabemos da hipótese que $ord_m(a) = m - 1$. O Corolário 2.16 nos diz que $m - 1 \leq \varphi(m)$, mas da Definição 2.7, $\varphi(m) \leq m - 1$, ou seja, nesse caso tem-se $\varphi(m) = m - 1$, o que implica que m é primo. □

Exemplo 2.19. *Vamos verificar se o número 11 é primo utilizando o Teste 2:*

Primeiro, devemos definir um valor a inteiro tal que $mdc(a, 11) = 1$, seja $a = 2$, como não existe nenhum primo que divida tanto o 11 quanto o 2, sabemos que $mdc(2, 11) = 1$.

Calculemos a^{m-1}, nesse caso, $2^{11-1} = 2^{10}$, note que em módulo 11, uma vez que $2^2 = 4 \equiv 4 \bmod 11$ então $2^10 = (2^2)^5 \equiv 4^5 \bmod 11$. Dessa forma, sabendo que $4^5 = 1024$ e que $11 \cdot 93 = 1023$, podemos afirmar que $4^5 \equiv 1 \bmod 11$, e assim temos $2^{10} \equiv 1 \bmod 11$.

Agora resta verificar se $a^k \not\equiv 1 \bmod m, \forall 1 < k < m-1$.

$$2^2 \equiv 4 \bmod 11$$
$$2^3 \equiv 8 \bmod 11$$
$$2^4 \equiv 5 \bmod 11$$
$$2^5 \equiv 10 \bmod 11$$
$$2^6 \equiv 9 \bmod 11$$
$$2^7 \equiv 7 \bmod 11$$
$$2^8 \equiv 3 \bmod 11$$
$$2^9 \equiv 6 \bmod 11$$

Portanto, 11 é primo.

Observação 2.20. *No Teste 2, caso* $a^{m-1} \equiv 1 \bmod m$ *mas* $a^k \equiv 1 \bmod m$ *para algum* $1 < k < m-1$*, não implica que* m *é composto, indica apenas que devemos escolher outro candidato para* a*. Para* $a = 5$ *e* $m = 1$ *por exemplo,* $5^{11-1} \equiv 1 \bmod 1$*, mas* $5^5 \equiv 1 \bmod 11$*, sendo que* $1 < k = 5 < 10$*. Quanto mais candidatos testarmos, mais certeza teremos do resultado.*

Note que, a partir do Lema 2.15, podemos simplificar o Teste 2, de modo a não precisar mais analisar cada valor de $k < m-1$. Obtém-se então:

Teste 3. *Seja* m *inteiro. Se existir um inteiro* a*,*$1 < a < m$*, com* $mdc(a, m) = 1$ *tal que*

$$a^{m-1} \equiv 1 \bmod m$$

e

$$a^d \not\equiv 1 \bmod m, \text{ tal que } d|m-1$$

então m *é primo.*

Exemplo 2.21. *Vamos verificar se o número 23 é primo utilizando o Teste 3:*

Primeiro, devemos definir um valor a *inteiro tal que* $mdc(a, 23) = 1$*, seja* $a = 5$*, como não existe nenhum primo que divida tanto o* 5 *quanto o* 23*, sabemos que* $mdc(2, 11) = 1$*.*

Calculemos 5^{m-1}*, nesse caso,* $5^{23-1} = 5^{22}$*, note que em módulo* 23*, uma vez que* $5^2 = 25 \equiv 2 \bmod 23$ *então* $5^{22} = (5^2)^{11} \equiv 2^1 1 \bmod 23$*. Dessa forma, sabendo que* $2^{11} = 2048$ *e que* $23 \cdot 89 = 2047$*, podemos afirmar que* $2^{11} \equiv 1 \bmod 23$*, e assim temos* $5^{22} \equiv 1 \bmod 23$*.*

Agora resta verificar se $a^d \not\equiv 1 \bmod m$, *tal que* $d|m-1$. *Note que nesse caso* d *pode assumir os valores* $1, 2, 11, 22$.

$$5^1 \equiv 5 \bmod 23$$
$$5^2 \equiv 2 \bmod 23$$
$$5^{11} \equiv 22 \bmod 23$$

Portanto, 23 é primo.

Mas existe uma maneira de refinar ainda mais esse teste. De fato, em 1967, Brillhart e Selfridge flexibilizaram ainda mais o teste de Lucas:

Teste 4. *Seja n>1. Assuma que para cada fator primo* p *de* $n-1$ *exista um natural* $a = a_p > 1$ *e* $1 < a < n$ *tal que:*

$$a^{n-1} \equiv 1 \bmod n$$

e

$$a^{\frac{n-1}{p}} \not\equiv 1 \bmod n.$$

Então n *é primo.*

Demonstração. Vamos mostrar que $n-1|\varphi(n)$. Já que $\varphi(n) \leq n-1$, então uma das consequências será $\varphi(n) = n-1$.

Suponha por absurdo que $n-1 \nmid \varphi(n)$, isso implica que existe um p primo tal que $p^r|n-1$ e $p^r \nmid \varphi(n), r \in \mathbb{N}$. Seja $a_p \in \mathbb{N}$ com $a_p^{n-1} \equiv 1 \bmod n$ e $a_p^{\frac{n-1}{p}} \not\equiv 1 \bmod n$. Logo em $ord_n(a_p)|n-1$ e $ord_n(a_p) \nmid \frac{n-1}{p}$.

Note que se $a_p^{n-1} \equiv 1 \bmod n$, então $\exists q \in \mathbb{Z}$ tal que $a_p(a_p^{n-2}) - nq = 1$ e pelo Teorema 2.2 sabemos que $mdc(a_p, n) = 1$. Como $ord_n(a_p)|n-1$ então $n-1 = k \cdot ord_n(a_p)$ para algum k. Logo $p^r|k \cdot ord_n(a_p)$, o que implica em $p^{r-1}|\frac{k \cdot ord_n(a_p)}{p}$, e como $ord_n(a_p) \nmid \frac{k \cdot ord_n(a_p)}{p}$ então $p \nmid k$, consequentemente $p^r|ord_n(a_p)$. Do Teorema 2.11 temos $a_p^{\varphi(n)} \equiv 1 \bmod n$. Logo, $ord_n(a_p)|\varphi(n)$. O que implica que $p^r|\varphi(n)$, logo $n-1|\varphi(n)$, contrariando a hipótese inicial e, portanto, $\varphi(n) = n-1$, logo n é primo. □

Exemplo 2.22. *Mostremos que o 7 é primo utilizando o Teste 4. Tome* $a = 3$, *como* $3^6 = 729 \equiv 1 \bmod 7$ *basta verificar se a segunda condição será satisfeita também. Como os fatores primos de 6 são 2 e 3, então*

$$3^{\frac{6}{2}} = 3^3 = 27 \equiv 6 \bmod 7$$
$$3^{\frac{6}{3}} = 3^2 = 9 \equiv 2 \bmod 7$$

e portanto, 7 é primo.

O leitor atento deve ter reparado em um problema similar nos últimos três testes apresentados, algo tão incômodo quanto no crivo de Eratóstenes: Dado n qualquer, a

necessidade de saber fatorar $n-1$. E isso muitas vezes pode ser um problema. Existem testes feitos a partir de Sequências de Lucas, uma sequência que pode ser definida de maneira similar à sequência de Fibonacci, mas com termos iniciais 2 e 1 respectivamente, e esses testes exigirão em sua maioria a necessidade de saber fatorar $n+1$. Para o leitor curioso, o capítulo 2 de [12] aborda com detalhes esse tema.

Existem testes que testam se n é primo e outros que testam se n é composto, como, de acordo com [10], o teste probabilístico de Miller-Rabin a seguir.

Teste 5. *Dado n ímpar, tome $n-1=2^k q, q$ ímpar. Se*

$$a^q \not\equiv 1 \bmod n$$

e

$$a^{2^i q} \not\equiv -1 \bmod n \text{ para } i = 0, 1, \ldots, k-1,$$

para algum $a \in (1, n-1)$ tal que $mdc(a,n)=1$, então n é composto.

Demonstração. Seguiremos nossa demonstração por contrapositiva. Tome p um primo ímpar. Considere os seguintes elementos, todos em relação a módulo p:

$$a^q, a^{2q}, a^{2^2 q}, \ldots, a^{2^{k-1} q}, a^{2^k q} \bmod p.$$

Como $2^k q = p-1$ então o elemento $a^{2^k q}$ é congruente a 1 módulo p pelo Teorema 2.3, e todos outros valores, com exceção do primeiro, são o resultado do valor anterior elevado ao quadrado. Como essa sequência é finita e, a partir de determinado momento, seu valor é 1, temos duas possibilidades: ou $a^q \equiv 1 \bmod p$ ou $a^{2^i q} \equiv -1 \bmod p$ para algum $i < k$. Visto que dada a congruência $x^2 \equiv 1 \bmod p$ as únicas soluções são $x = 1, x = -1 \bmod p$, então, por contrapositiva, n é composto.

□

Exemplo 2.23. *Vamos verificar se $n = 53$ é composto. Tome $n-1 = 53-1 = 2^2 13$, então $k = 2$ e $q = 13$. Usaremos $a = 2$.*

Note que $a^q = 2^1 3 = 8192 \equiv 30 \bmod 53$. Verifiquemos agora a segunda condição. Para $i = 0$ temos $a^{2^i q} = 2^{2^0 13} = 2^{13} = 8192 \equiv 30 \bmod 53$ e para $i = k-1 = 2-1 = 1$ temos $a^{2^i q} = 2^{2^1 13} = 2^{26} = 67\ 108\ 864 \equiv -1 \bmod 53$, e portanto 53 não é composto.

Observação 2.24. *Nem todo valor n que falhar no Teste 5 é necessariamente primo, e esses valores que falham e não são primos são conhecidos como Pseudoprimos fortes.*

Exemplo 2.25. *Seja $n = 2047$, note que $2047 = 23 \cdot 89$, ou seja, ele é composto, mas falha na primeira condição do Teste 5, pois temos $q = 1023$, e $2^{1023} \equiv 1 \bmod 2047$.*

Existem ainda mais testes, e inclusive testes específicos para diferentes tipos de números, como números na forma $2^k \pm 1$, com k natural. Para mais testes, a leitura de [2], [12] e [10] pode trazer alento ao leitor. Em diversos trabalhos sobre testes de primalidades

não encontraremos um teste bom o suficiente para todo e qualquer número, e quando se define isso, toma-se como base o poder computacional que executará o algoritmo de teste de primalidade de um número, tomando como base a taxa de acertos e tempo de cálculo. Assim, para números pequenos, o crivo de Eratóstenes pode ser a melhor alternativa em mãos e conforme a quantidade de contas aumentar, precisa-se ter em mãos outros testes que usem menos cálculos e nos garantam um resultado em tempo hábil.

Para exemplificar o que é considerado um número grande, até o momento de publicação desse texto não se sabe se o número $2^{2^{127}-1} - 1$ é primo ou não.

3

O QUE SEU PRIMO ESTÁ FAZENDO?

"A resposta certa, não importa nada: o essencial é que as perguntas estejam certas."
- Quintana, M.

Esse capítulo trata sobre a distribuição dos números primos entre os naturais, além de trazer alguns avanços proeminentes alcançados no último século sobre algumas funções específicas e primos gêmeos. Os resultados mostrados aqui foram considerados de certa forma relevantes para este trabalho, que foram interpretados a partir de [12].

A esse ponto, já vimos que existem infinitos primos, como também formas de saber se estamos olhando para um primo ou não, mas o que mais podemos fazer com eles? Será que eles têm algum padrão de distribuição?

Os números pares, por exemplo, têm um padrão bem definido. No intervalo entre 1 e 100 temos exatamente 50 números pares. Entre 1 e 1 000, são 500. O padrão continua, mas e se não estivermos falando sobre números pares? Quantos primos existem entre 1 e 100? E entre 1 e 1 000? Vamos definir essa contagem como $\pi(n)$, que é a função contadora de primos até n.

Definição 3.1. *Dado $n \in \mathbb{N}$, define-se $\pi(n)$ como a quantidade de números primos no conjunto $\{i, 0 < i \leq n \ e \ i \in \mathbb{N}\}$.*

Dessa forma, uma vez que entre 1 e 100 há 25 primos então $\pi(100) = 25$, analogamente temos $\pi(1\ 000) = 168$ e $\pi(10\ 000) = 1\ 229$. Enfim, parece não haver um padrão bem definido, mas nos dá uma boa dimensão da densidade dos números primos em relação aos naturais.

É interessante discutir na densidade da distribuição dos primos, isto é, estudar o comportamento de $\pi(x)/x$. Por exemplo, 25% dos 100 primeiros naturais são primos, mas essa taxa cai quanto mais números naturais analisarmos. De fato, de acordo com [12],

$$\lim_{x\to\infty} \frac{\pi(x)}{x/ln(x)} = 1,$$

mas embora tenhamos essa igualdade, e com isso podemos pensar em maneiras de trabalhar aproximações para $\pi(x)$, existe outra função que aproxima bem o valor de $\pi(x)$, a função integral logarítmica, definida por $Li = \int_2^x \frac{dt}{log(t)}$. Temos, então

$$\lim_{x\to\infty} \frac{\pi(x)}{Li(x)} = 1.$$

A função $Li(x)$ é bem melhor para uma aproximação do número de primos até um certo x. Mais sobre o assunto pode ser encontrado em [1], assim como a tabela 2.

Ainda que essas duas igualdades estejam retratadas como limites, elas são em verdade aproximações assintóticas, isto é, as funções $\frac{\pi(x)}{x}$ e $\frac{1}{ln(x)}$ são de mesma ordem quando x tende ao infinito. O mesmo ocorre com as funções $\pi(x)$ e $Li(x)$.

Tabela 2: Comparativo entre funções iguais a $\pi(x)$ quando $x \to \infty$ e a razão com $\pi(x)$.

x	$\pi(x)$	Li(x)	$\frac{x}{ln(x)}$	$\pi(x)$/Li(x)	$\pi(x)/\left(\frac{x}{ln(x)}\right)$
10	4	5,12	4,34	0,78 118	0,92 103
10^2	25	29,08	21,71	0,85 967	1,15 129
10^3	168	176,56	144,76	0,95 149	1,16 050
10^4	1 229	1 245,09	1 085,74	0,98 708	1,13 195
10^5	9 592	9 628,76	8 685,89	0,99 618	1,10 432
10^6	78 498	78 626,50	72 382,41	0,99 837	1,08 449
10^7	664 579	664 918,00	620 420,69	0,99 949	1,07 117
10^8	5 761 455	5 762 209,03	5 428 681,02	0,99 987	1,06 130
10^9	50 847 534	50 849 234,70	48 254 942,43	0,99 997	1,05 373

Muitos matemáticos estudaram os primos ao longo da história. Muitos levantaram perguntas e, algumas, já inclusive foram respondidas, como o postulado de Bertrand, demonstrado posteriormente por Tschebycheff.

Teorema 3.2 (Bertrand-Tschebycheff)**.** *Entre todo inteiro $n \geq 2$ e $2n$, há sempre um número primo.*

Uma demonstração para esse teorema pode ser encontrada em [7].

Ou seja, sabe-se que $\pi(2x) - \pi(x) \geq 1$, um resultado proeminente na discussão sobre a distribuição dos primos entre os naturais. Uma situação peculiar e intrigante são os casos em que $\pi(x+2) - \pi(x) = 1$, que define os primos gêmeos ($x = 3$ ou $x = 5$ por exemplo). Esses primos foram caracterizados por Clement em 1949 [3].

Teorema 3.3. *Uma condição necessária e suficiente para que dois inteiros, n e $n+2, n > 1$, sejam ambos primos é que*

$$4[(n-1)! + 1] + n \equiv 0 \bmod n(n+2)$$

Demonstração. A suficiência é trivial, uma vez que as divisões por n e $n+2$ separadamente se reduzem ao teorema de Wilson:

$$4[(n-1)! + 1] + n \equiv 0 \bmod n$$
$$4[(n-1)! + 1] \equiv 0 \bmod n$$
$$\text{mdc}(n, 4) = 1, \text{ pois se } n = 2, n+2 \text{ não é primo, logo } n \neq 2.$$
$$(n-1)! + 1 \equiv 0 \bmod n$$
$$(n-1)! \equiv -1 \bmod n$$

De modo similar,

$$\begin{aligned} 4[(n-1)!+1]+n &\equiv 0 \mod n+2 \\ 2[2(n-1)!+1]+n+2 &\equiv 0 \mod n+2 \\ 2[2(n-1)!+1] &\equiv 0 \mod n+2 \end{aligned}$$

Note que $\text{mdc}(n,2)=1,$ pois se $n=2, n+2$ não é primo, logo $n \neq 2$.

$$\begin{aligned} 2(n-1)!+1 &\equiv 0 \mod n+2 \\ (n+2)(n-1)(n-1)!+2(n-1)!+1 &\equiv 0 \mod n+2 \\ (n^2+n)(n-1)!+1 &\equiv 0 \mod n+2 \\ (n+1)(n)(n-1)!+1 &\equiv 0 \mod n+2 \\ (n+1)!+1 &\equiv 0 \mod n+2 \\ (n+1)! &\equiv -1 \mod n+2 \end{aligned}$$

A recíproca do teorema parte diretamente do Teorema de Wilson, onde, dados n e $n+2$ primos, a partir de

$$\begin{aligned} (n-1)!+1 &\equiv 0 \bmod n \quad (1) \\ (n+1)!+1 &\equiv 0 \bmod n+2, \quad (2) \end{aligned}$$

usando (1) temos:

$$\begin{aligned} (n-1)!+1 &\equiv 0 \bmod n \\ 4[(n-1)!+1]+n &\equiv 0 \bmod n, \quad (3) \end{aligned}$$

agora, nos apoiando sobre o Teorema de Wilson, e focando na equação (2), note que

$$\begin{aligned} n+2 &\equiv 0 \bmod n+2 \\ n+1 &\equiv -1 \bmod n+2 \quad (4) \\ n &\equiv -2 \bmod n+2. \quad (5) \end{aligned}$$

A partir de (4) e (5) temos então

$$\begin{aligned} (n+1)! = (n+1)n(n-1)! &\equiv (-1)(-2)(n-1)! \bmod n+2 \\ &\equiv 2(n-1)! \bmod n+2. \quad (6) \end{aligned}$$

Note que

$$4[(n-1)!+1]+m = 2(n-1)!+2(n-1)!+2+m+2,$$

usando (6) é possível verificar que

$$\begin{aligned} 2(n-1)!+2(n-1)!+2+n+2 &\equiv (n+1)!+(n+1)!+2 \bmod n+2 \\ &\equiv (n+1)!+1+(n+1)!+1 \bmod n+2 \end{aligned}$$

e pelo Teorema de Wilson,

$$2(n-1)!+2(n-1)!+2+n+2 \equiv 0 \bmod n+2 \tag{7}$$

Como n é impar, $mdc(n, n+2) = 1$ e portanto de (3) e (7) temos:

$$4[(n-1)!+1]+n \equiv 0 \bmod n(n+2).$$

O que completa a nossa demonstração. □

Se por um lado existem os primos gêmeos, por outro é possível determinar um d natural qualquer de modo que $\pi(x+d)-\pi(x) = 0$, isto é, d naturais seguidos que são compostos.

Teorema 3.4. *O intervalo de números inteiros* $[(d+1)!+2, (d+1)!+(d+1)]$*, com* $d \in \mathbb{N}$*, não contém números primos.*

Demonstração. Seja $(d+1)!+i$ com $2 \leq i \leq d+1$ o i-ésimo elemento do intervalo definido. Note que $(d+1)!+i = i(\frac{(d+1)!}{i}+1)$, logo, $(d+1)!+i$ é composto $\forall i$ no intervalo definido. □

É interessante notar que esse teorema não nos mostra o primeiro intervalo com d números compostos consecutivos. Ele também não garante que o intervalo encontrado é limitado por primos. Não há, portanto, garantia de que $(d+1)!+1$ e $(d+1)!+(d+2)$ são primos.

Exemplo disso é para o caso $d = 3$, que entrega o intervalo $[26, 28]$, pertencente ao conjunto de compostos $[24, 28]$, com 5 compostos tangidos pelos primos 23 e 29. Se o que se quiser for um intervalo com exatamente 3 compostos, não é preciso ir muito longe, uma vez que $[8, 10]$ já satisfaz essa condição, mas essa é uma busca por força-bruta.

Para o leitor atento, já está claro que esses conjuntos de espaçamento possuem cardinalidade ímpar, uma vez que dados os primos p_n e p_{n+1}, o número de compostos entre eles será $p_{n+1}-p_n-1$, vamos chamar esse número de $g(p_n)$. Simplificando, temos:

Definição 3.5. $g(p)$ *é o número de inteiros compostos consecutivos de* p*.*

Isso é algo que pode levantar algumas questões como: será que para todo m natural ímpar existe p, tal que $g(p) = m$? Segundo [12], essa pergunta ainda está em aberto.

Euler, ao estudar o comportamento de $\pi(x)$, observou que a série $\sum_{n=1}^{\infty} \frac{1}{n^\sigma}$, para $\sigma > 1$ é convergente. Mais tarde esse somatório foi definido como a *função zeta* $\zeta(\sigma)$.

$$\zeta(\sigma) = \sum_{n=1}^{\infty} \frac{1}{n^\sigma}.$$

Euler mostrou que

$$\zeta(\sigma) = \sum_{n=1}^{\infty} \frac{1}{n^\sigma} = \prod_p \frac{1}{1 - \frac{1}{p^\sigma}}, \text{ para } \sigma > 1 \tag{8}$$

estabelecendo assim uma relação entre a função zeta e os números primos. Para mostrar (8) temos que

$$\zeta(\sigma) = \sum_{n=1}^{\infty} \frac{1}{n^\sigma} = 1 + \frac{1}{2^\sigma} + \frac{1}{3^\sigma} + \frac{1}{4^\sigma} + \dots \tag{9}$$

Multiplicando ambos os lados da igualdade (9) por $\frac{1}{2^\sigma}$ obtemos

$$\frac{1}{2^\sigma}\zeta(\sigma) = \frac{1}{2^\sigma} + \frac{1}{4^\sigma} + \frac{1}{6^\sigma} + \frac{1}{8^\sigma} + \dots \tag{10}$$

Efetuando (9) − (10) encontramos um resultado proeminente

$$\left(1 - \frac{1}{2^\sigma}\right)\zeta(\sigma) = 1 + \frac{1}{3^\sigma} + \frac{1}{5^\sigma} + \frac{1}{7^\sigma} + \dots \tag{11}$$

Note que, em (11) não há mais no lado direito da igualdade o inverso de quaisquer múltiplos de 2. Efetuando raciocínio análogo com o próximo valor primo, 3, de fato concluímos o que queríamos no início:

$$\left(1 - \frac{1}{3^\sigma}\right)\left(1 - \frac{1}{2^\sigma}\right)\zeta(\sigma) = 1 + \frac{1}{5^\sigma} + \frac{1}{7^\sigma} + \frac{1}{11^\sigma} + \dots$$

Estendendo esse raciocínio para todos os primos obtém-se

$$\begin{aligned} \dots \cdot \left(1 - \frac{1}{7^\sigma}\right)\left(1 - \frac{1}{5^\sigma}\right)\left(1 - \frac{1}{3^\sigma}\right)\left(1 - \frac{1}{2^\sigma}\right)\zeta(\sigma) &= 1 \\ \left(\prod_p 1 - \frac{1}{p^\sigma}\right)\zeta(\sigma) &= 1 \\ \zeta(\sigma) &= \prod_p \frac{1}{1 - \frac{1}{p^\sigma}}. \end{aligned} \tag{12}$$

Euler conseguiu calcular também que a soma do inverso dos primos é divergente. A demonstração a seguir seguirá à luz de [12].

Teorema 3.6. *A soma dos inversos dos números primos é divergente:* $\sum_p \frac{1}{p} = \infty$

Demonstração. Seja $N \in \mathbb{N}$ qualquer. Todo $n \in \mathbb{Z}, n \leq N$ pode ser escrito de forma única como um produto de números primos $p \leq n$. De mesma forma, para cada primo p considere a série geométrica $\sum_{k=0}^{\infty} \frac{1}{p^k}$ de razão $q = \frac{1}{p}$. Logo

$$\sum_{k=0}^{\infty} \frac{1}{p^k} = \frac{1}{1 - \frac{1}{p}}$$

Então

$$\sum_{n=1}^{N} \frac{1}{n} \leq \prod_{p \leq N} \left(\sum_{k=0}^{\infty} \frac{1}{p^k} \right) = \prod_{p \leq N} \frac{1}{1 - \frac{1}{p}}$$

Mas,

$$\log \prod_{p \leq N} \frac{1}{1 - \frac{1}{p}} = - \sum_{p \leq N} \log \left(1 - \frac{1}{p} \right).$$

Observe que, dada uma função $y = \log(1 - x)$, então $y' = \frac{-1}{1-x} = -\sum_{n=0}^{\infty} x^n$, para $|x| < 1$, e, portanto, $\log(1-x) = -\sum_{n=0}^{\infty} \frac{x^{n+1}}{n+1} = -\sum_{n=1}^{\infty} \frac{x^n}{n}$. Dessa forma, tome $x = \frac{1}{p}$ e para cada primo p,

$$\begin{aligned} -\log \left(1 - \frac{1}{p} \right) &= \sum_{m=1}^{\infty} \frac{1}{mp^m} \leq \frac{1}{p} + \frac{1}{p^2} \left(\sum_{h=0}^{\infty} \frac{1}{p^h} \right) \\ &= \frac{1}{p} + \frac{1}{p^2} \cdot \frac{1}{1 - \frac{1}{p}} = \frac{1}{p} + \frac{1}{p(p-1)} \\ &< \frac{1}{p} + \frac{1}{(p-1)^2}. \end{aligned}$$

Então,

$$\begin{aligned} \log \sum_{n=1}^{N} \frac{1}{n} &\leq \log \prod_{p \leq N} \frac{1}{1 - \frac{1}{p}} \leq \sum_{p \leq N} \frac{1}{p} + \sum_{p \leq N} \frac{1}{(p-1)^2} \\ &\leq \sum_{p} \frac{1}{p} + \sum_{n=1}^{\infty} \frac{1}{n^2}. \end{aligned}$$

Mas a série $\sum_{n=1}^{\infty} \frac{1}{n^2}$ é convergente. Como esses cálculos independem do valor de N e a série harmônica $\sum_{n=1}^{\infty} \frac{1}{n}$ é divergente, então $\log \sum_{n=1}^{\infty} \frac{1}{n} = \infty$ e, como consequência, a série $\sum_{p} \frac{1}{p}$ é divergente.

□

Dentre os vários resultados que Euler divulgou, um deles foi que $\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$, chegando também a uma solução mais geral para $\zeta(2k)$:

$$\zeta(2k) = \sum_{n=1}^{\infty} \frac{1}{n^{2k}} = (-1)^{k+1} \frac{(2\pi)^{2k} B_{2k}}{2(2k)!},$$

onde B_n é um número de Bernoulli, que de acordo com [8], pode ser definido como

$$B_n = \begin{cases} 1, \ se\ n = 0 \\ -\frac{1}{2}, \ se\ n = 1 \\ (-1)^{\frac{n}{2}+1} \cdot \frac{2(n)!}{(2\pi)^n} \zeta(n), \ se\ n \in \{2, 4, 6, 8, \dots\} \\ 0, \ se\ n \in \{3, 5, 7, 9, \dots\}. \end{cases}$$

Legendre também teve êxito em seus estudos com a função $\pi(x)$, em 1808, utilizando o crivo de Eratóstenes. Ele conseguiu mostrar que

$$\pi(N) = \pi(\sqrt{(}N)) - 1 + \sum \mu(d) \left[\frac{N}{d}\right]$$

onde o somatório se refere a todos os divisores d do produto de todos os primos $p \leq \sqrt{N}$ e $\mu(n)$ é função de Möbius, ela pode ser usada para encontrar naturais livres de quadrados. De acordo com [12], a função de Möbius pode ser definida a partir da decomposição em fatores primos de $n = \prod_{j=1}^{k} p_j^{a_j} \in \mathbb{N}$, de modo que

$$\mu(n) = \begin{cases} 1, & \text{se } n = 1 \\ (-1)^k, & \text{se } a_j = 1 \text{ para todo } j \\ 0, & \text{se } a_j > 1 \text{ para algum } j \end{cases}$$

Foi só Tschebycheff, no entanto, quem conseguiu determinar a ordem de grandeza $\pi(x)$. Em 1850, ele conseguiu mostrar que existem constantes C e C', com $0 < C' < 1 < C$, tais que

$$C' \frac{x}{\log x} < \pi(x) < C \frac{x}{\log x}, \text{ para } x \geq 2.$$

Tschebycheff, inclusive, calculou valores para essas constantes. Além disso, ele trabalhou com a função $\theta(x) = \sum_{p \leq x} \log p$. Função essa que recebeu seu nome e, que traz, em seu âmago, ferramentas para se trabalhar o mesmo propósito de $\pi(x)$. Esta função, porém, é mais simples de ser manipulada algebricamente.

A função $\pi(x)$ reserva ainda muitos mistérios. Até a data de publicação deste trabalho, as afirmações a seguir ainda não foram demonstradas:

1. $\pi(N^2 + N) > \pi(N^2) > \pi(N^2 - N), \forall N > 1$ (Conjectura de L. Opperman, 1882)
2. $\pi(p_{n+1}^2) - \pi(p_n^2) \geq 4, \forall n \geq 2$ (Conjectura de H. Brocard, 1904).

3. $\pi((N+1)^2) - \pi(N^2) \geq 2, \forall N \geq 1$

4. $\sqrt{p_{n+1}} - \sqrt{p_n} < 1, \forall n \geq 1$ (Conjectura de D. Andrica, 1986).

5. $\pi((N+1)^2) - \pi(N^2) \geq 1, \forall n \geq 1$

Mesmo sem demonstrações, em [12], é mostrado que as implicações (1) $\Rightarrow$ (2) e (1) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (5) são verdadeiras.

Por último, ainda por acrescentar informações relevantes nesta seção, Dirichlet provou um famoso teorema sobre números primos em progressões aritméticas:

Teorema 3.7 (Teorema de Dirichlet)**.** *Em uma Progressão Aritmética (P.A.) de números naturais, com primeiro termo e razão primos entre si, existem infinitos números primos.*

Existe uma bela demonstração para esse teorema que, infelizmente, não cabe aqui. Não por conta de seu tamanho, mas por sua complexibilidade algébrica e, dependência do uso da teoria analítica dos números. Mesmo assim, para alguns casos particulares essa demonstração se faz mais simples. Em [6] nos é apresentada uma demonstração para a P.A. $4n+3$, e a seguir encontra-se uma com argumentos análogos para $6n+5$.

Proposição 3.8. *Na progressão aritmética* $5, 11, 17, \ldots, 6n+5, \ldots$ *existem infinitos números primos*

Demonstração. Note que todo número primo diferente de 2 ou 3 pode ser escrito na forma $6n+1$ ou $6n+5$. Mostraremos que existem infinitos primos da forma $6n+5$. Observe que o conjunto $A = \{6n+1; n \in \mathbb{N}\}$ é fechado pela operação de multiplicação. Suponha, então, por absurdo que existam finitos primos $3 < p_1 < \cdots < p_k$ da forma $6n+5$. Desse modo, o número $a = 6(p_1 \cdot 2 \cdot \ldots \cdot p_k) + 5$ não é divisível por nenhum dos primos $3, p_1, p_2, \ldots, p_k$ e, por conta disso, só poderá ser decomposto em primos da forma $6n+1$, o que é um absurdo, pois a é da forma $6n+5$. □

Em [12] o autor cita que dada uma P.A. definida por $a+dn$, é fácil demonstrar que para os seguintes valores têm-se progressões com infinitos primos: $a = 1$ e $d = 4$; $a = 1$ e $d = 6$; $a = 1$ e $d = 3$; $a = 3, 5$ ou 7 e $d = 8$; $a = 5, 7$ ou 11 e $d = 12$.

Além de provar que existem infinitos primos, Goldbach também estabeleceu uma memorável conjectura que permanece em aberto até hoje.

Conjectura 3.9 (Conjectura de Goldbach)**.** *Todo número par maior do que 4 é a soma de dois números primos.*

Poucos avanços foram feitos na tentativa de demonstração dessa conjectura, que já foi até tema de filme[1], em que um dos personagens a teria supostamente provado. Embora sem demonstração, essa conjectura é um bom incentivo e ponto de partida para conversas sobre números primos e problemas matemáticos em aberto com o público da educação básica.

[1] La habitación de Fermat(2007); dirigido por Luis Piedrahita e Rodrigo Sopeña

Segundo [12], Goldbach havia escrito para Euler, em 1742, a seguinte afirmação: "Todo inteiro $n > 5$ é a soma de três números primos", da qual obteve a resposta de Euler, afirmando que tal afirmação era equivalente a dizer que "Todo inteiro par $2n \geq 4$ é a soma de dois números primos"

Note que assumindo a segunda afirmação verdadeira, para $n \geq 3$, $2n - 2 = p + q$, com p e q primos, logo $2n = 2 + p + q$ e $2n + 1 = 3 + p + q$, o que demonstra a primeira afirmação.

A recíproca é trivial, pois, assumindo a primeira afirmação como verdadeira, e tendo $2n > 4$, então $2n + 2 = p + q + r$, onde p, q e r são primos, implicando que um desses primos é par, tomando $r = 2$ temos $2n = p + q$.

Atualmente, a melhor maneira de explorar essa conjectura é por meio de métodos analíticos finos e da teoria dos crivos, esta última sendo uma área que buscar estudar o tamanho de conjuntos formados por números inteiros.

De acordo com [12], Ramaré foi quem encontrou o melhor resultado atual para essa conjectura, demonstrando que todo inteiro par pode ser escrito como a soma de no máximo 6 números primos.

4

A MANIFESTAÇÃO DOS PRIMOS

"Primzahlen aller klassen, vereinigt euch!"[1]

Este capítulo tem, como intuito, trazer uma das representações pictóricas mais conhecidas no estudo de números primos: a Espiral de Ulam. Além de discutir um pouco sobre ela e suas variações, pretende trazer, como sugestão, uma generalização mais abstrata dessa espiral, capaz de reproduzir qualquer outro padrão pictórico ou gerar novos. As referências aqui são diversas, mas tudo parte do artigo [14] escrito por M. L. Stein, S. M. Ulam, e M. B. Wells.

Em [14], é apresentado um dos mais belos padrões pictóricos com números primos, conhecido como Espiral de Ulam. Organizamos os números em uma disposição retangular bem definida, como num tabuleiro de xadrez infinito, e, a partir de seu centro $(0,0)$, estabelece-se uma bijeção entre cada casa do tabuleiro e um número natural. Seguindo o padrão em espiral, os primeiros valores são: $(0,0) \to 1, (1,0) \to 2, (1,1) \to 3, (0,1) \to 4, (-1,1) \to 5, (-1,0) \to 6, (-1,-1) \to 7, (0,-1) \to 8, (1,-1) \to 9, (2,-1) \to 10, (2,0) \to 11, (2,1) \to 12, (2,2) \to 13$, etc. Então coloca-se em destaque apenas os números primos.

100	99	98	97	96	95	94	93	92	91
65	64	63	62	61	60	59	58	57	90
66	37	36	35	34	33	32	31	56	89
67	38	17	16	15	14	13	30	55	88
68	39	18	5	4	3	12	29	54	87
69	40	19	6	1	2	11	28	53	86
70	41	20	7	8	9	10	27	52	85
71	42	21	22	23	24	25	26	51	84
72	43	44	45	46	47	48	49	50	83
73	74	75	76	77	78	79	80	81	82

Figura 1: Espiral de Ulam com 100 primeiros valores.

Fonte: Figura de autoria própria

[1] Do alemão: "Números primos de todas as classes, uni-vos!"

O interessante da espiral de Ulam é que para grandes tabuleiros, certos padrões começam a aparecer, veja a figura 2.

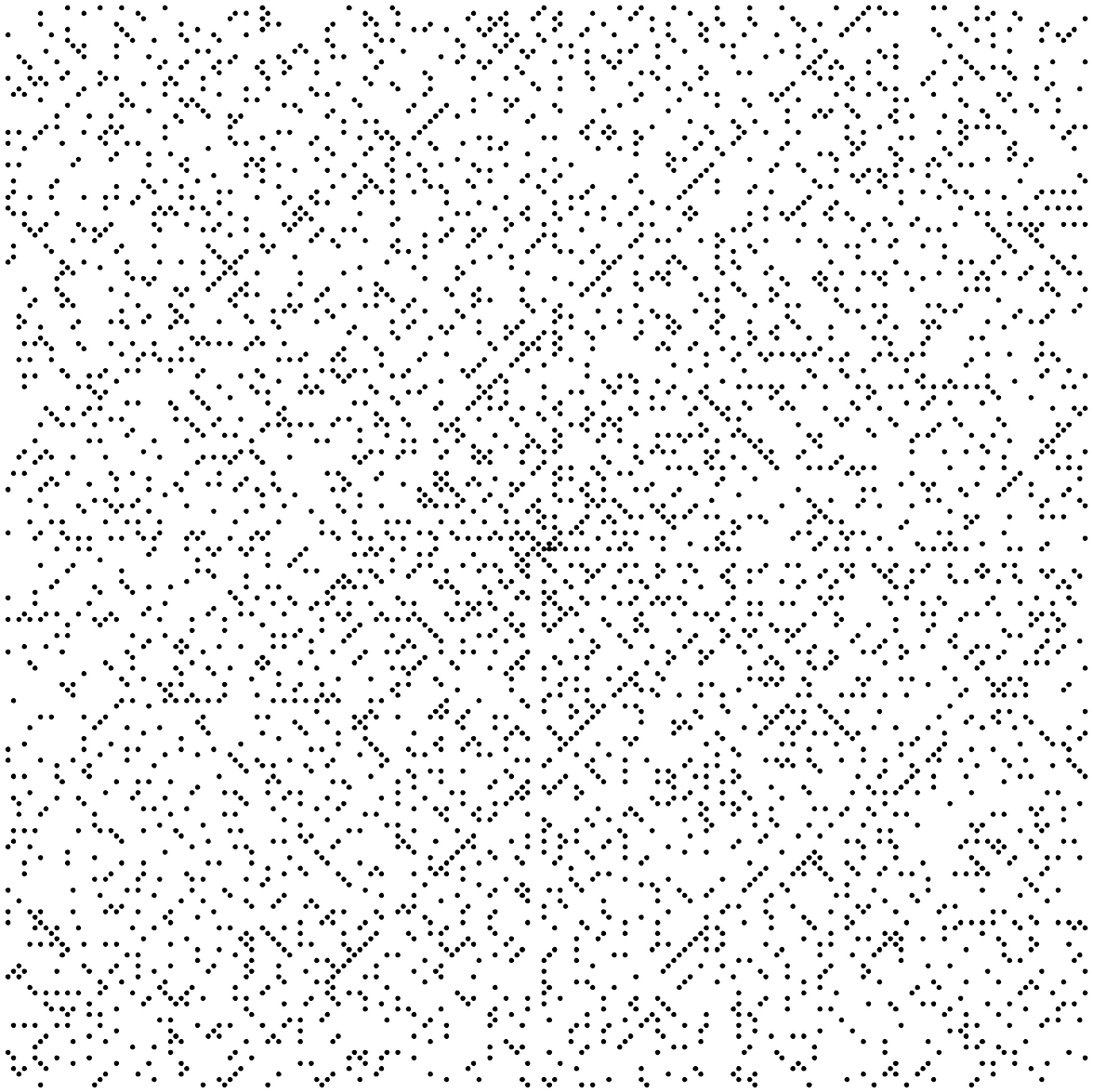

Figura 2: Espiral de Ulam com 40 000 números.

Fonte: Figura de autoria própria

Antes que se diga que quaisquer valores aleatórios apresentariam um padrão, eis uma espiral feita com as mesmas disposições da espiral de Ulam, porém, em destaque, temos apenas números ímpares aleatórios, respeitando a densidade $\frac{1}{ln(x)}$, de modo que fica evidente que não há padrões locais, diferente da espiral original, onde se evidenciam alguns primos em diagonais.

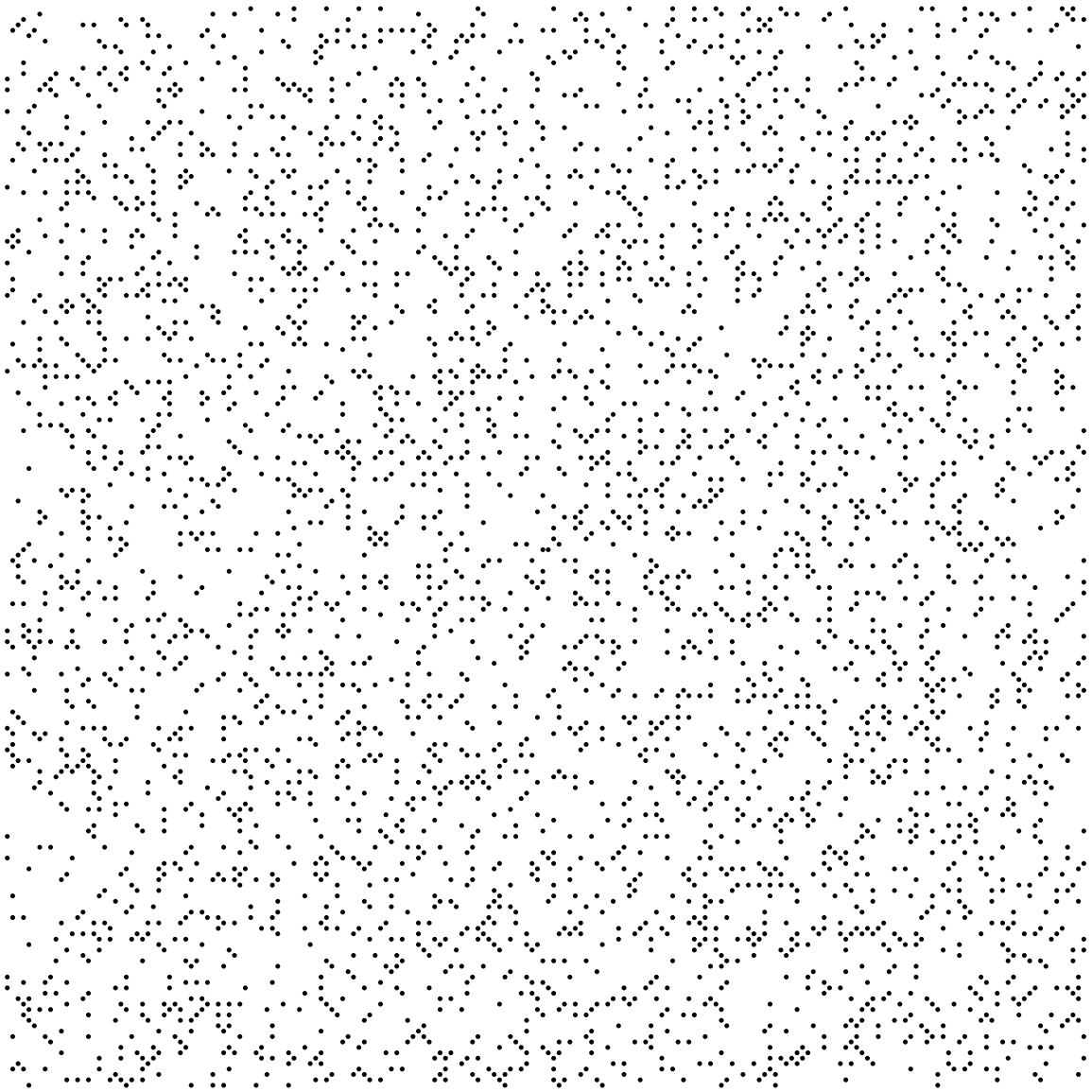

Figura 3: Espiral com 40 000 número, tendo ímpares aleatórios em evidência e densidade de pontos $\frac{1}{ln(x)}$.

Fonte: Figura de autoria própria

Definição 4.1. *Cada linha subjacente constitui um novo anel na espiral de Ulam, de tal forma que, sendo $A(n)$ o conjunto representando cada anel, tem-se: $A(1) = \{1\}, A(2) = \{2, 3, 4, 5, 6, 7, 8, 9\}, A(3) = \{10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25\}, \ldots$. Por conta da disposição poligonal do anel, é possível defini-lo pela quantidade de elementos em cada lado.*

Teorema 4.2. *Qualquer elemento de uma diagonal escolhida ao acaso da Espiral de Ulam pode ser definido por $y_t = 4t^2 + bt + c$, com constantes b e c inteiras.*

Demonstração. Seja $\#A(n)$ a quantidade de elementos em cada anel da Espiral de Ulam, esse valor é uma diferença de quadrados, em que para $n \neq 1, \#A(n) = (2n-1)^2 - (2n -$

$3)^2$. Logo $\#A(n) = (2n-1+2n-3)(2n-1-2n+3) = (4n-4)(2) = 8n-8$. É possível concluir, então, que $\#A(n+1) - \#A(n) = 8$, isto é, a cardinalidade do próximo anel será igual à do anterior acrescida de 8, com exceção de $A(2)$. Essa constante 8 é divisora da diferença de segunda ordem para quaisquer 3 termos que se encaixem em uma linha na espiral, seja essa linha horizontal, vertical ou diagonal. Seja então y_t um valor numa diagonal qualquer, temos a seguinte recorrência:

$$\begin{aligned}(y_{t+2} - y_{t+1}) - (y_{t+1} - y_t) &= 8 \\ y_{t+2} - 2y_{t+1} + y_t &= 8. \end{aligned} \tag{13}$$

Para resolver essa recorrência, tome como equação característica $r^2 - 2r + 1 = 0$, cujas raízes são $r_1 = r_2 = 1$, portanto a solução homogênea é dada por $h_n = bn + c, b, c \in \mathbb{N}$. Seja $t_n = kn^2$ solução particular da recorrência original. Substituindo em (13), obtemos $k(t+2)^2 - 2k(t+1)^2 + kt^2 = 8$ que implica $k[t^2 + 4t + 4 - 2t^2 - 4t - 2 + t^2] = 2k = 8$, dessa forma $k = 4$, portanto, a solução da recorrência original é $y_t = 4t^2 + bt + c$. □

Algumas diagonais na espiral de Ulam são ricas em números primos e, ao se alterar o valor inicial da espiral, as diagonais se deslocam. Para o valor inicial 41, tem-se em evidência, em uma das diagonais principais, os primos do polinômio de Euler, definido por $n^2 - n + 41$.

140	139	138	137	136	135	134	133	132	131
105	104	103	102	101	100	99	98	97	130
106	77	76	75	74	73	72	71	96	129
107	78	57	56	55	54	53	70	95	128
108	79	58	45	44	43	52	69	94	127
109	80	59	46	41	42	51	68	93	126
110	81	60	47	48	49	50	67	92	125
111	82	61	62	63	64	65	66	91	124
112	83	84	85	86	87	88	89	90	123
113	114	115	116	117	118	119	120	121	122

Figura 4: Espiral de Ulam com centro 41.

Fonte: Figura de autoria própria

Ao longo dos tempos foram estudados polinômios do tipo $x^2 + x + q$ que apresentam primos. Segundo [12], o polinômio citado acima foi descoberto em 1772 por Euler. Tal polinômio toma valores primos para $k = 0, 1, \ldots, 39$, estabelecendo um recorde de números primos sucessivos gerados a partir de um polinômio. Euler estudou outros tipos de polinômios que gerassem primos, mas nenhum foi tão eficiente quanto $n^2 - n + 41$. Outros recordes são o polinômio $36n^2 - 810n + 2753$ descoberto por R. Ruby, em 1990, e apresenta 44 números primos, se considerado valores absolutos. Há também, os polinômios $103n^2 - 3945n + 34381$, descobertos por R. Ruby; e $47n^2 - 1701n + 10181$, descoberto por G. Fung, que resultam em 43 valores absolutos primos iniciais. O polinômio $f(n) = n^2 - 79n + 1601$ não é mencionado em [12], pois embora apresente 80 primos para $n = 0, 1, \ldots, 78, 79$, eles se repetem, de modo que $f(n) = f(79 - n), 0 \leq n \leq 79$. Mais detalhes sobre isso podem ser encontrados em [12].

Há diversos fatores que podem modificar a Espiral de Ulam original, como mudar o valor inicial, mudar o sentido entre horário e anti-horário, basear-se em outras figuras além de quadrados, como heptágonos ou formato circular (Espiral de Sacks), deixar em evidência números compostos em vez de primos, ou mesmo pseudoprimos... Existem várias possibilidades. David Rainford estabelece em [11], parâmetros para se classificar quaisquer espirais baseadas na espiral de Ulam. As Figuras 5, 6 e 7 foram elaboradas por Rainford. Elas têm como características em comum o fato de terem incremento de 2 unidades de lado para cada anel sucessor, menor número de cada anel aparecendo em seu primeiro vértice, este é posicionado imediatamente à direita do ponto central e anel $A(2)$ de lado 3.

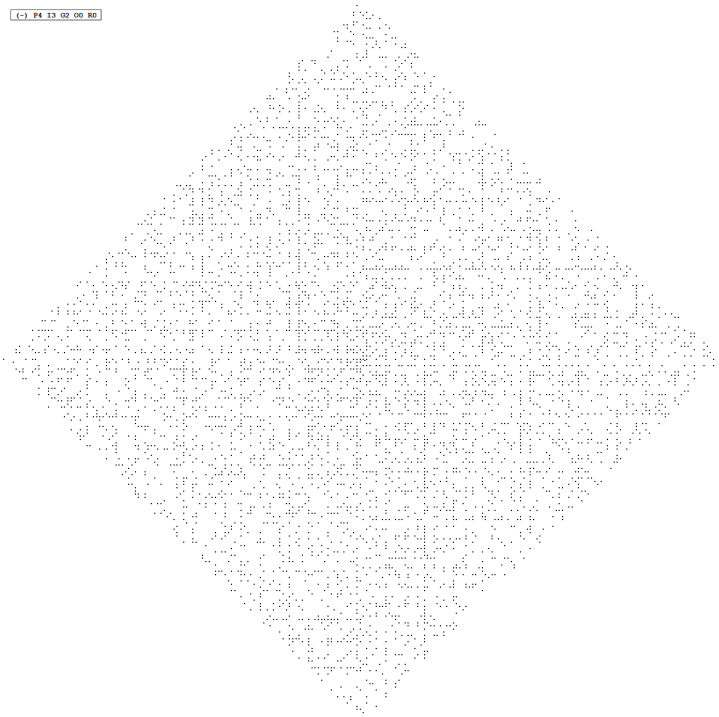

Figura 5: Espiral baseada em Polígono de 4 lados e 50 000 números.

Fonte: Disponível em [11]. Acesso em 18/05/2021.

Figura 6: Espiral baseada em Polígono de 5 lados e 165 000 números.

Fonte: Disponível em [11]. Acesso em 18/05/2021.

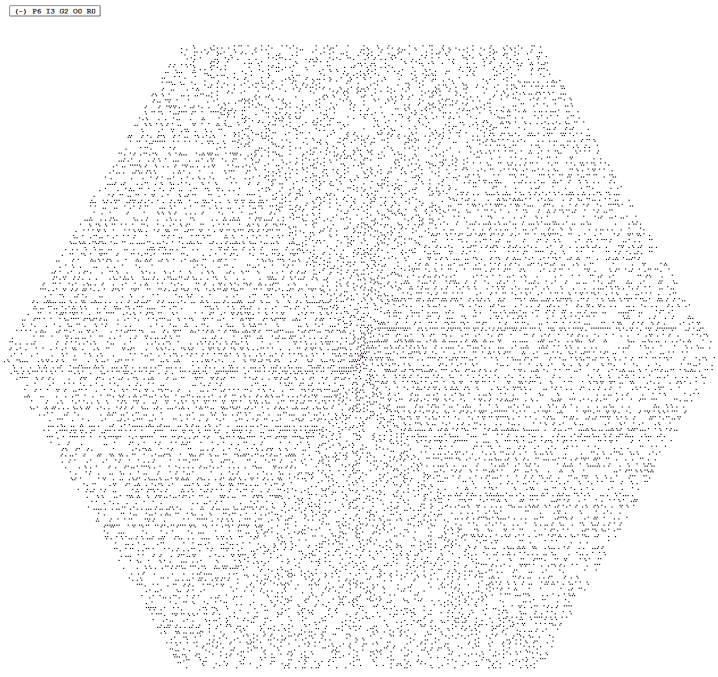

Figura 7: Espiral baseada em Polígono de 6 lados e 150 000 números.

Fonte: Disponível em [11]. Acesso em 18/05/2021.

O que será tratado nesse documento é uma outra forma de desenvolver essa espiral, generalizando a ideia original, promovendo uma ideia que reúne diversas possíveis espirais

em um único algoritmo, o Caminho. Seja um tabuleiro infinito com centro de coordenadas $(0, 0)$, estabelece-se:

1. uma bijeção entre cada coordenada desse tabuleiro e um número natural,
2. pontos de destaque,
3. uma direção de início,
4. um ângulo α de rotação,
5. se caminhos se cruzam ou não.

A imagem da bijeção é chamada de caminho. Sempre que a imagem da bijeção for um ponto de destaque, o caminho conterá uma curva com ângulo α. Caso o caminho encontre a si mesmo, de acordo com (5), há duas opções, uma de, na coordenada de encontro, adicionar uma unidade à cota para cada sobrescrição e, outra de ignorar o caminho à frente, avançando uma nova coordenada no tabuleiro até encontrar uma coordenada vazia até então. Cada coordenada com um valor definido é chamada de passo.

Por padrão, fica definido que a coordenada $(0, 0)$ recebe o valor 1. Os pontos de destaque são os números primos. A direção de início sendo logo à direita do primeiro ponto, ângulo $\alpha = 90°$ e o caminho não sobrescrevendo coordenadas que já contenham algum valor.

Na figura 8 encontra-se um exemplo de Caminho padrão com 50 passos.

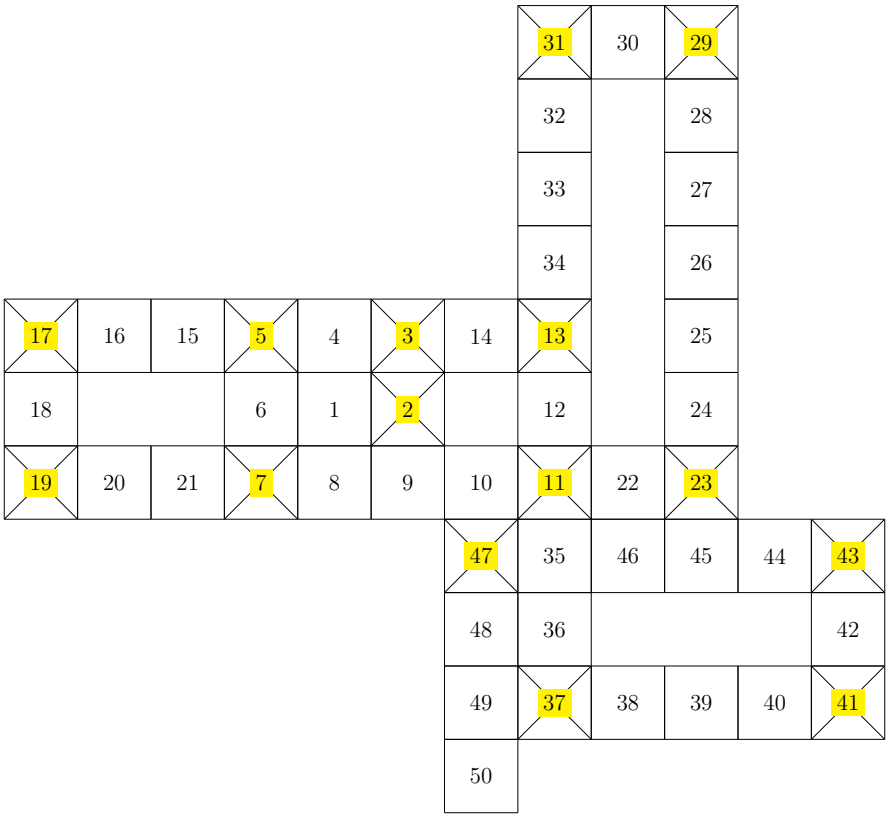

Figura 8: Caminho padrão com 50 passos.

Fonte: Figura de autoria própria

Na figura 9 há um caminho com as mesmas especificações da figura 8, porém, sobrescrevendo passos já dados.

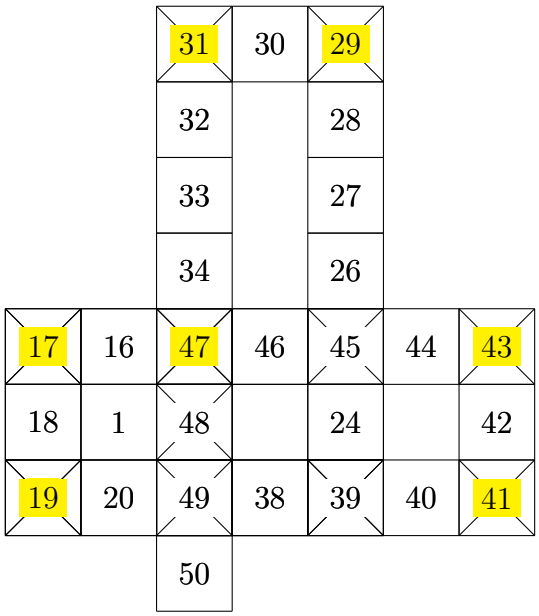

Figura 9: Caminho padrão de 50 passos com sobrescrição.

Fonte: Figura de autoria própria

A ideia do Caminho é produzir qualquer espiral. Caso os pontos de destaque sejam, por exemplo, o valor 2 em conjunto com as imagens de $a(n) = 4n^2 - 10n + 7$, $b(n) = 4n^2 + 1$, $c(n) = 4n^2 - 6n + 3$, $d(n) = 4n^2 + 4n + 1$, com parâmetros padrões, o resultado será a espiral de Ulam. Isso ocorre, pois $a(n), b(n), c(n)$ e $d(n)$, para $n \in \mathbb{N}$ representam as diagonais principais da espiral de Ulam.

Com o uso da programação de computadores, fica fácil construir grandes Caminhos com as características desejadas. O primeiro algoritmo para um Caminho padrão foi elaborado para a linguagem Virtual Basic for Applications (VBA), pois, por ser integrado à uma planilha eletrônica, o resultado visual ficava muito claro e fácil de ser trabalhado.

Essa é, inclusive, uma sugestão de como introduzir a espiral de Ulam ou outros padrões pictóricos para alunos da educação básica, pois necessita apenas que os alunos tenham acesso à uma planilha eletrônica com recurso integrado de programação. O desenvolvimento dessa aula pode ser feito inicialmente para que os alunos criem a Espiral de Ulam manualmente, e depois, que sejam introduzidas as noções de programação na planilha eletrônica, inicialmente como uma ferramenta para formatar as células e identificar automaticamente números primos e posteriormente, com um algoritmo para construir a Espiral de Ulam de maneira iterativa. A seguir o algoritmo original feito em VBA.

```
Public direcao As Integer
Sub Caminho_padrao()
Dim numero As Integer
direcao = 3 'Classifica em qual direcao o caminho deve ir
numero = 0 'numero inicial para as iteracoes
Do While numero < 5 'valor maximo de iteracoes
Call rotina 'funcao que determina para onde o caminho vai
numero = numero + 1 'acrescenta uma unidade a cada iteracao
Loop
End Sub
//
Sub rotina()
Dim valor_inicial As Integer, prim As Boolean
valor_inicial = ActiveCell.Value 'recebe o valor da celula ativa
Call primos(valor_inicial, prim) 'funcao para checar se um numero e primo ou nao
If prim = True Then direcao = direcao + 1 'Se for primo, a direcao muda
'Sao 4 direcoes possiveis
If direcao Mod 4 = 0 Then
Do While ActiveCell.Value <> ""
ActiveCell.Offset(0, 1).Select 'cima
Loop
ActiveCell.Value = valor_inicial + 1
End If
If direcao Mod 4 = 1 Then
Do While ActiveCell.Value <> ""
ActiveCell.Offset(-1, 0).Select 'esquerda
Loop
ActiveCell.Value = valor_inicial + 1
End If
If direcao Mod 4 = 2 Then
Do While ActiveCell.Value <> ""
ActiveCell.Offset(0, -1).Select 'baixo
Loop
ActiveCell.Value = valor_inicial + 1
End If
If direcao Mod 4 = 3 Then
Do While ActiveCell.Value <> ""
ActiveCell.Offset(1, 0).Select 'direita
Loop
ActiveCell.Value = valor_inicial + 1
End If
End Sub
//
Sub primos(num As Integer, primo As Boolean)
'algoritmo para checar se um numero e primo
'baseado no crivo de Eratostenes
primo = True
For div = 2 To Sqr(num)
If num Mod div = 0 Then
primo = False
End If
Next
If num = 1 Then primo = False
If primo = True Then ActiveCell.Interior.Color = vbGreen 'Verde se o numero for primo
If primo = False Then ActiveCell.Interior.Color = vbBlue 'Azul se o numero for composto
End Sub
```

Figura 10: Algoritmo em VBA para gerar um caminho padrão em uma planilha eletrônica.

Fonte: Autoria própria

Os resultados a seguir foram feitos com linguagem Python utilizando o software Sage-Math.

Figura 11: Caminho padrão de $10^5 - 1$ passos.

Fonte: Figura de autoria própria

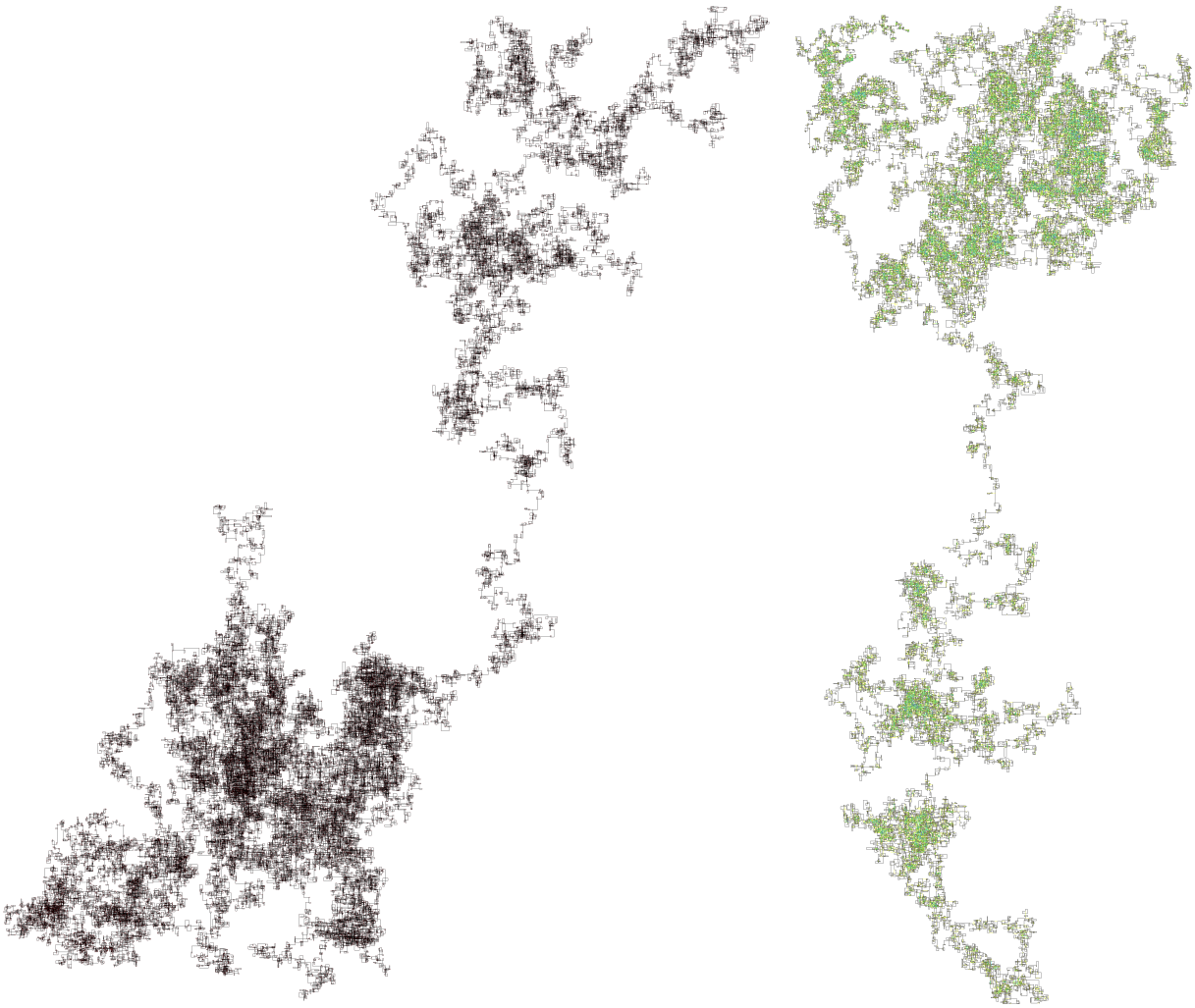

Figura 12: A esquerda um Caminho padrão de $10^6 - 1$ passos e a direita um Caminho com sobrescrição de 10^6 passos.

Fonte: Compilação do autor a partir de figura de autoria própria e figuras de [9]

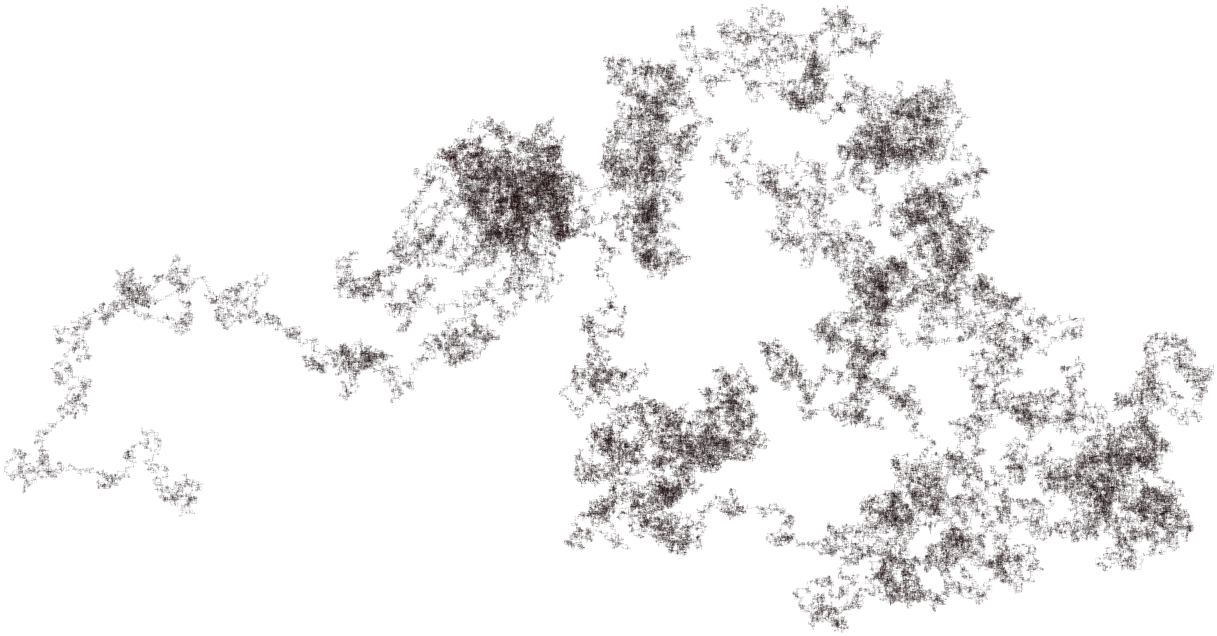

Figura 13: Caminho padrão de $10^7 - 1$ passos.

Fonte: Figura de autoria própria

Sobre o Caminho padrão, algumas perguntas podem ser feitas, como: Há algum padrão? Há coordenadas que nunca receberão passos? Qual é a maior distância sem curvas? Caso o caminho se sobrescreva, é possível determinar quantas vezes ele passará por uma mesma coordenada?

Encontrar um padrão no Caminho seria encontrar um padrão para os números primos. Essa questão, portanto, ainda está em aberto e, consequentemente, fica inviabilizado discutir se uma coordenada em específico será visitada ou não. Sobre a maior distância sem curvas, isso se deve à função $g(p)$ da Definição 3.5. Logo, fica evidente que a menor distância sem curvas tem comprimento 3 para primos gêmeos e a maior distância é algo tão grande quanto se queira, de acordo com o Teorema 3.4.

5

PROPOSTA DIDÁTICA

"Tenho apenas duas mãos e o sentimento do mundo "
- de Andrade, C. D.

Como proposta didática, foi pensado uma sequência didática de matemática do 6° ano do Ensino Fundamental, mas que pode ser aplicado a qualquer turma, visto que o objetivo é incentivar o estudo dos números primos.

Foi idealizada uma aula introdutória ao assunto, definindo os números primos e evidenciando as observações feitas por Euclides sobre isso, além de mostrar alguns dos matemáticos que provaram que existem infinitos números primos. Em seguida, apresentar "métodos práticos" para se encontrar números primos e métodos não tão práticos assim, apenas como curiosidade. Após essa introdução, trazer o uso cotidiano desses números, fechando com as espirais de Ulam e outros modelos pictóricos possíveis.

Os objetivos gerais da aula são de compreender a definição de números primos e sua importância, identificado suas características, e, abordando a complexabilidade do tema, exemplificando que até mesmo computadores superpotentes, caso não sejam bem programados, enfrentam dificuldades em cálculos envolvendo números primos.

Como objetivos específicos, espera-se que o aluno seja capaz de definir números primos (e consequentemente, números compostos), entender que existem infinitos deles, e, que existem também diversos testes de primalidade, além de conhecer o uso de números primos em tempos contemporâneos e explorar padrões pictóricos formados a partir de primos.

A habilidade BNCC (Base Nacional Curricular Comum) associada a essa aula é a EF06MA05:

> (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.

Para a aula, será necessário organizar uma apresentação. Um exemplo pode ser encontrado no apêndice desse trabalho, contendo 4 tópicos principais: números primos; identificação; uso cotidiano e representações pictóricas.

Para o primeiro tópico, sobre números primos, dever-se-á apresentar inicialmente as ideias de Euclides, mostrando principalmente que, ao tomar um quadrado como uma unidade e, ao tentar representar os números de forma retangular, de tal modo que esses retângulos sejam compostos pelo quadrado previamente definido, alguns números têm representação única. É importante definir esses retângulos únicos como os blocos fundamentais de todos os números, pois ou um número é representado por esse bloco fundamental,

e então ele é chamado de número primo, ou ele é formado por dois ou mais blocos, e então ele é chamado de número composto.

É interessante deixar claro para os alunos que Euclides percebeu essa interessante propriedade entre os números primos e compostos, e ainda em sua época, cerca de 300 a.C., conseguiu provar que existem infinitos números primos. A demonstração desse fato pode ser feita junta aos alunos, caso surja a necessidade, seguindo a primeira demonstração do Teorema 1.2, e frisar que, além de Euclides, ao longo dos tempos, outros matemáticos também estudaram o assunto e chegaram a mesma conclusão de Euclides, porém com argumentos diferentes. Vale citar os nomes de Kummer, Goldbach (e cabe aqui um comentário em aula sobre a Conjectura de Goldbach) e Euler, que usou um argumento tão relevante para a demonstração da infinitude dos primos que o mesmo argumento pode ser trabalhado para se transformar num problema que já tem 160 anos sem solução, a hipótese de Rienmann[1].

No segundo tópico, sobre a identificação de números primos, é importante começar o assunto com o crivo de Eratóstenes, e pedir para os alunos o construírem até determinado número. É comum a construção do crivo até o valor 100, mas dependendo do nível de atenção da turma sobre o assunto, é possível pedir a construção até 200, e introduzir, como curiosidade, a função $\pi(x)$, pedindo para os alunos calcularem $\pi(100)$ e $\pi(200)$. Depois, deve-se mostrar em forma de tabela, os valores de $\pi(x)$ para as centenas de 100 à 1000, mostrando que quanto maior os números, menos primos são encontrados a cada centena.

Frise com os alunos a importância do crivo de Eratóstenes, pois ele fornece uma tabela com todos números primos até determinado valor, e essa é uma das maneiras mais eficientes para saber se um número é primo ou não, e que outras maneiras podem ser demasiado complexas. Nesse momento vale a pena, com o uso de uma planilha eletrônica, que o professor programe o Teorema de Wilson, pois ele é um teste confiável de primalidade, mas que exige muitas contas. Por isso, mesmo computadores que podem fazer várias contas por segundo falham ao tentar apurar se um número é primo usando o Teorema de Wilson. Em planilhas eletrônicas comuns, o teste costuma falhar para $n \geq 17$. Vale aqui ressaltar que existem outros testes de primalidade, e que todos acabam recorrendo ao que se chama de força-bruta. Alguns, porém, são mais eficientes que outros para determinados números. Não necessariamente precisamos compreender esses testes, mas é interessante saber da existência deles, senão acaba até parecendo algo mágico: uma pessoa pergunta se um número é primo e um matemático dá o veredito.

No terceiro tópico, sobre usos cotidianos, não tem como não abordar criptografia. É claro que não cabe no 6° ano falar sobre métodos de criptografia avançada, mas cabe explicar o processo que a criptografia toma. Esse processo consiste em usar um número primo muito grande, com várias classes numéricas (mencione por exemplo o primo de Belfegor: 100 000 000 000 006 660 000 000 000 000 1, um nonilhão, sessenta e seis

[1] Despretensiosamente falando, essa hipótese teria contribuições sobre a possibilidade de a distribuição de números primos não ser aleatória.

quatrilhões, seiscentos trilhões e um), e na existência de diversos números primos enormes, que são a base da criptografia. Um bom exemplo é usar a operação de potenciação para exemplificar a situação. Escolha um número qualquer mostre-o para os alunos. Eleve, então, esse número a um certo expoente e divida o resultado dessa potência por algum valor conhecido. Então apresente o resto dessa divisão, explique que a criptografia consiste em descobrir qual era o expoente ao qual o número foi elevado, conhecendo apenas a base da potência, o valor pelo qual o resultado foi dividido e o resto da divisão. Isso pode ser uma tarefa extremamente difícil quando o expoente for um número primo, ainda mais um número primo muito grande.

Tratemos, então, do último tópico, em que serão abordadas representações pictóricas de números primos. Cabe ressaltar que o crivo de Eratóstenes pode ser encarado como tal, mas que o foco aqui será a espiral de Ulam. Incentive os alunos a construírem uma espiral de Ulam iniciando com o número 41 e tomando pelo menos 5 camadas (uma espiral iniciando em 41 e terminando em 104). Explique que o padrão visto se perpetua apenas até a vigésima camada e que tal padrão pode ser descrito pelo polinômio de Euler. Ainda que polinômios sejam um assunto aprendido apenas no 8° ano, vale a pena citar isso como incentivo. Para encerrar o assunto, mostre que existem outras possibilidades de representações pictóricas de números primos. Sugira, por exemplo, os Caminhos padrões apresentados nesse trabalho, e incentive os alunos a criarem um novo padrão pictórico usando números primos.

É ideal que o professor faça uma aula expositiva e dialogada, sempre trabalhando na contextualização de problemas. Nesse caso, haverá uma aula prática de construção dos números primos. É sugerido o uso de computador, projetor multimídia, pincel, quadro, folha quadriculada e lápis para essa aula que pode se estender conforme necessidade.

Uma sugestão de avaliação é a análise do comportamento individual de cada aluno assim como sua devida participação e desempenho nas atividades propostas.

6

CONCLUSÕES

A ideia principal desse trabalho surgiu em meados de setembro de 2017 e, por meio de uma programação simples de planilha eletrônica, o que era uma descomplicada ideia, tomou forma, como podemos ver na figura 14.

Figura 14: Postagem em rede social sobre os Caminhos padrões.

Fonte: Figura de autoria própria

Engraçado pensar que, como a história do desenvolvimento do Cálculo, que teve como protagonistas Leibniz e Newton, desenvolvendo ferramentas parecidas praticamente ao mesmo tempo, segundo [15], em meados de janeiro daquele 2017, um usuário de um fórum de matemática teve praticamente a mesma ideia (figura 15). No entanto, ele pensou com uma ínfima diferença: permitir que o caminho cruzasse a si próprio, algo que inicialmente os Caminhos não levavam em consideração. O interessante é que, com essa possibilidade, novas perguntas poderiam ser feitas, como, por exemplo: quantas vezes o Caminho se cruza numa mesma coordenada?

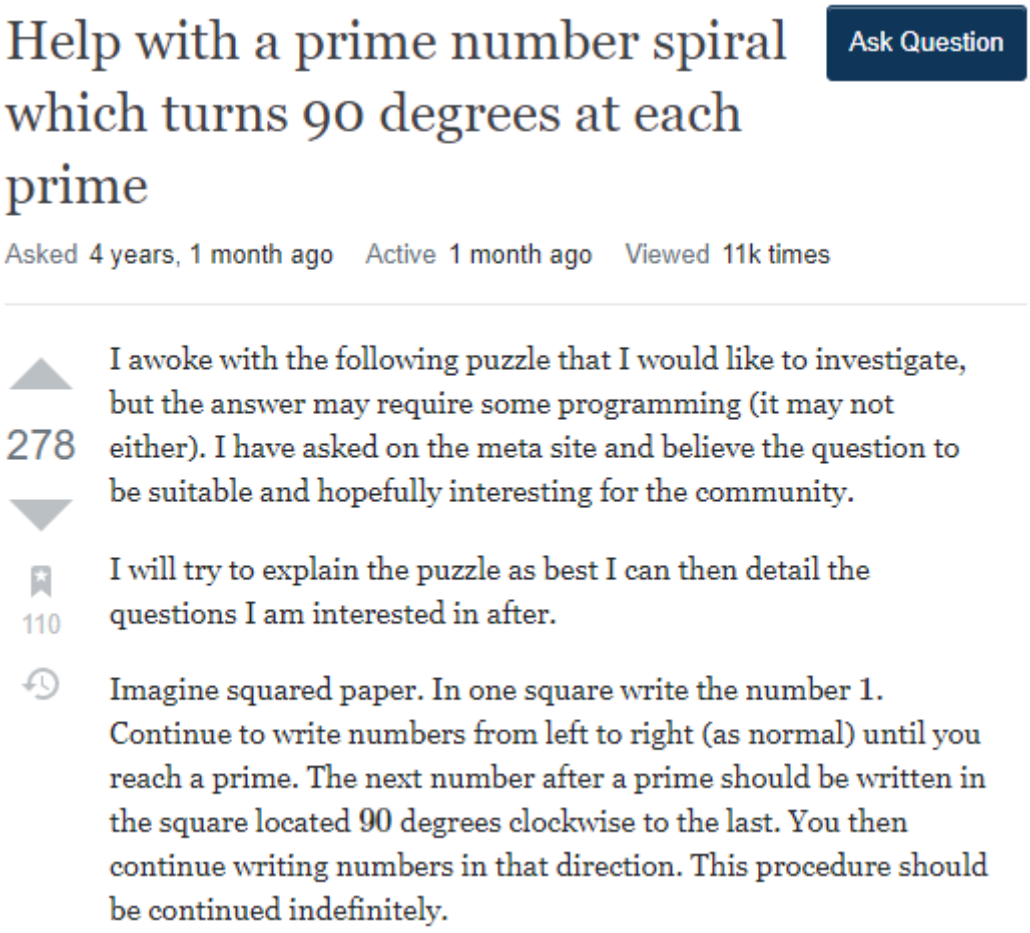

Figura 15: Postagem em fórum sobre os caminhos que se cruzam baseados em primos.

Fonte: Figura de autoria própria

O desenvolvimento dessa ideia não pode ser dissociado da programação. Sem ela, essas ideias viveriam no mero rascunho, e, embora a ambição original fosse encontrar algum padrão entre os números primos, o que se encontrou foi um belo caminho a se trilhar para tentar compreender a natureza desses números.

Mesmo sem uma aplicação prática, o estudo dos Caminhos intriga e é um bom incentivo para o ensino dos números primos, pois mostra que ideias simples podem tomar proporções desmedidas. Mais interessante do que isso, o trajeto tomado nesse estudo se revelou uma boa forma de apresentar os números primos no ensino básico: uma forma instigante.

Os alunos matriculados no início dos anos finais do Ensino Fundamental trazem em si uma curiosidade inerrante. Assuntos diferentes do livro didático chamam a atenção deles, principalmente se for algo que eles possam reproduzir. Então, falar sobre números primos e introduzir que esse assunto tem mais de 2 milênios de estudos e mesmo assim conta com vários problemas em aberto, é algo muito instigante. A melhor parte é poder convidar as pessoas a fazerem perguntas que não necessariamente seremos capazes de responder nesse momento, mas que precisam ser feitas.

Uma sugestão para ampliar esse trabalho seria estudar diferentes Caminhos possíveis, com diferentes movimentações, inclusive tridimensionais. Essa era uma das ideias iniciais,

mas a necessidade de saber programar algoritmos mais avançados impossibilitou tal prática. Além disso, outra sugestão seria catalogar as diferentes ideias parecidas com essa que se encontram na internet, onde essa discussão de fato atinge muito mais pessoas e alcança um nível democrático em que todos podem contribuir.

APÊNDICE

UMA BREVE FALA SOBRE NÚMEROS PRIMOS

1. Números primos

    - Euclides (Alexandria. 300 a.C.) já sabia dos números primos e deixou isso anotado em seu livro "Os elementos"

Figura A1: Ilustração do retrato de Euclides.

Fonte: Figura em domínio publico. Disponível em `https://commons.wikimedia.org/wiki/File:Euklid-von-Alexandria_1.jpg`. Acesso em 18/05/2021.

> Eis o que Euclides percebeu: Alguns números só podem ser medidos com uma única unidade.

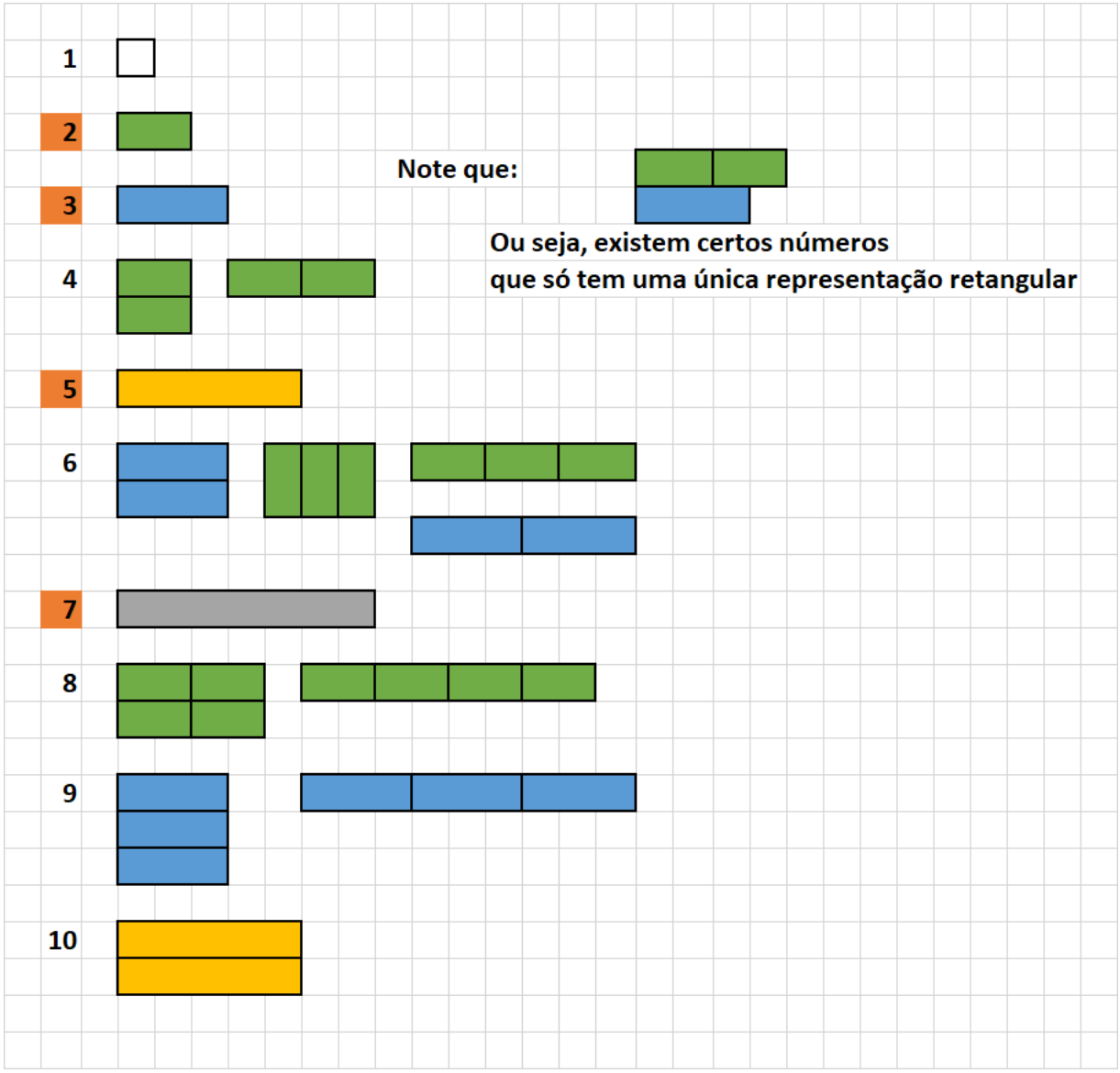

Figura A2: Representação retangular dos números de 1 a 10.

Fonte: Figura de autoria própria

- Euclides é o primeiro matemático que se tem registro que demonstrou que existem infinitos números primos.
  - Depois de Euclides, outros matemáticos mostraram isso também, alguns deles:
    - Kummer (Ernst Eduard Kummer. Żary, 1810-1893)

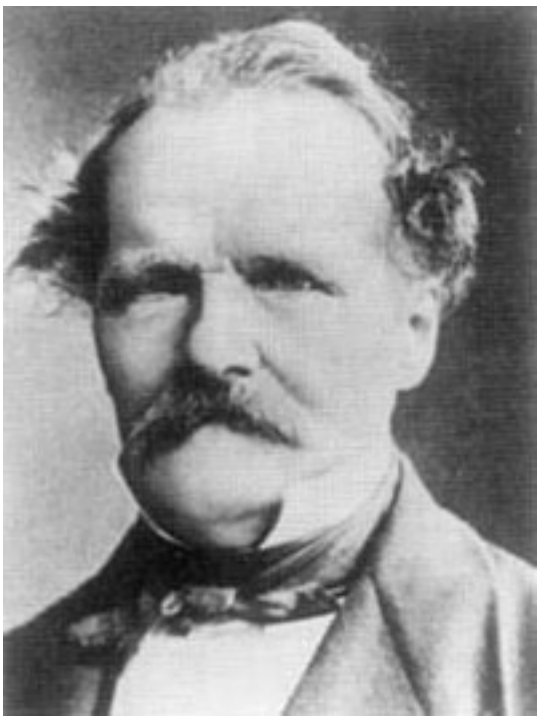

Figura A3: Retrato de Kummer.

Fonte: Figura em domínio publico. Disponível em `https://commons.wikimedia.org/wiki/File:Ernst_Eduard_Kummer.jpg`. Acesso em 18/05/2021.

* Goldbach (Christian Goldbach. Königsberg, 1690-1764)
  Curiosidade: Por algum motivo não identificado, ao pesquisar por imagens de Goldbach, o resultado que encontramos é o retrato de Hermann Grassman (1809-1877), matemático que viveu em uma era diferente da de Goldbach, uma época em que, diferente do século XVII, já existia a fotografia. Avise os alunos sobre esse fato, o senhor no retrato abaixo NÃO É GOLDBACH. (Por vezes, em vez de Grassman, a pesquisa retorna um retrato de Georg Friedrich Bernhard Riemann.)

Figura A4: Este não é um retrato de Goldbach, mas de Hermann Grassman.

Fonte: Figura em domínio publico. Disponível em `https://commons.wikimedia.org/wiki/File:Hermann_Gra%C3%9Fmann.jpg`. Acesso em 18/05/2021.

Goldbach também ficou conhecido pela sua famosa conjectura: Qualquer número par maior ou igual a 4 pode ser expresso como a soma de dois primos.

∗ Euler (Leonhard Paul Euler. Basiléia, 1707-1783)

Figura A5: Ilustração do retrato de Euler.

Fonte: Figura em domínio publico. Disponível em `https://commons.wikimedia.org/wiki/File:Leonhard_Euler.jpg`. Acesso em 18/05/2021.

O modo como Euler demonstrou isso, oferece uma imensa contribuição para a hipótese de Rienman[1], um problema que já tem 160 anos e ninguém até agora conseguiu provar se é verdadeira ou falsa, no ano 2000 o Clay Mathematics Institute anunciou que pagaria o prêmio de US$ 1 milhão ao primeiro matemático que fosse capaz de resolver esse problema.

2. Como saber se um número é primo?

   - Crivo de Eratóstenes

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	~~83~~	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Figura A6: Crivo de Eratóstenes até 100.

Fonte: Figura de autoria própria

   - Teorema de Wilson: Se p é primo, então $(p-1)! \equiv -1 \bmod p$.
     - Se pegarmos um número qualquer, 6 por exemplo, subtrairmos uma unidade, então 5, desse 5, multiplicamos ele por todos os números que vem antes dele, então $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$ e esse resultado, se, ao somar uma unidade novamente, ele for divisível pelo número original, então o número original é primo, como nesse caso temos 121 e 121 não é divisível por 6, 6 não é primo.

[1] Despretensiosamente falando, essa hipótese teria contribuições sobre a possibilidade de a distribuição de números primos não ser aleatória.

n	É primo?
1	FALSO
2	VERDADEIRO
3	VERDADEIRO
4	FALSO
5	VERDADEIRO
6	FALSO
7	VERDADEIRO
8	FALSO
9	FALSO
10	FALSO
11	VERDADEIRO
12	FALSO
13	VERDADEIRO
14	FALSO
15	FALSO
16	FALSO
17	#NÚM!
18	#NÚM!
19	#NÚM!
20	#NÚM!
21	#NÚM!

Figura A7: Tabela com teste de primalidade em uma planilha eletrônica utilizando o teorema de Wilson.

Fonte: Figura de autoria própria

- Teste de Lucas: Dados inteiros tais que $mdc(a, m) = 1$ se $a^{m-1} \equiv 1 \bmod m$ e $a^k \not\equiv 1 \bmod m, \forall 1 < k \leq m-1$ então m é primo.
- Teste de Lucas refinado: Seja $n > 1$. Assuma que para cada fator primo p de $n-1$ exista um inteiro $a = a_p > 1$ tal que: $a^{n-1} \equiv 1 \bmod n$ e $a^{\frac{n-1}{p}} \not\equiv 1 \bmod n$ então n é primo.
- (Teste probabilístico de Miller-Rabin para verificar se o número é composto) Dado n ímpar, tome $n-1 = 2^k q, q$ ímpar. Se $a^q \not\equiv 1 \bmod n$ e $a^{2^i q} \not\equiv -1 \bmod n$ *para* $i = 0, 1, \ldots, k-1$ para algum a tal que $mdc(a, n) = 1$, então n é composto.

3. O que fazer com números primos?

- Criptografia

Figura A8: Tirinha sobre números primos.

Fonte: Figura disponível em `https://dragoesdegaragem.com/cientirinhas/cientirinhas-143/`. Acesso em 18/05/2021.

Hoje em dia existem alguns sites que ajudam a entender o processo da criptografia, um deles é o `https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html`, uma calculadora RSA que usada junto com um conversor ASCII (`http://www.unit-conversion.info/texttools/ascii/`) pode ajudar a encriptar algumas mensagens.

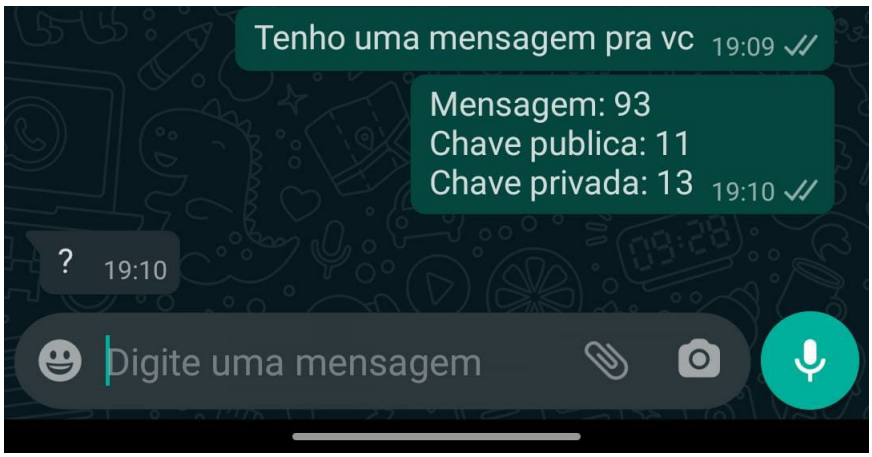

Figura A9: Exemplo de mensagem codificada.

Fonte: Figura de autoria própria

- Teste computacionais

  Existem vários métodos para averiguar a potência de super computadores, um deles é verificar quanto tempo o computador leva para averiguar a primalidade de um determinado conjunto de números.

4. Representações pictóricas

   - Espiral de Ulam

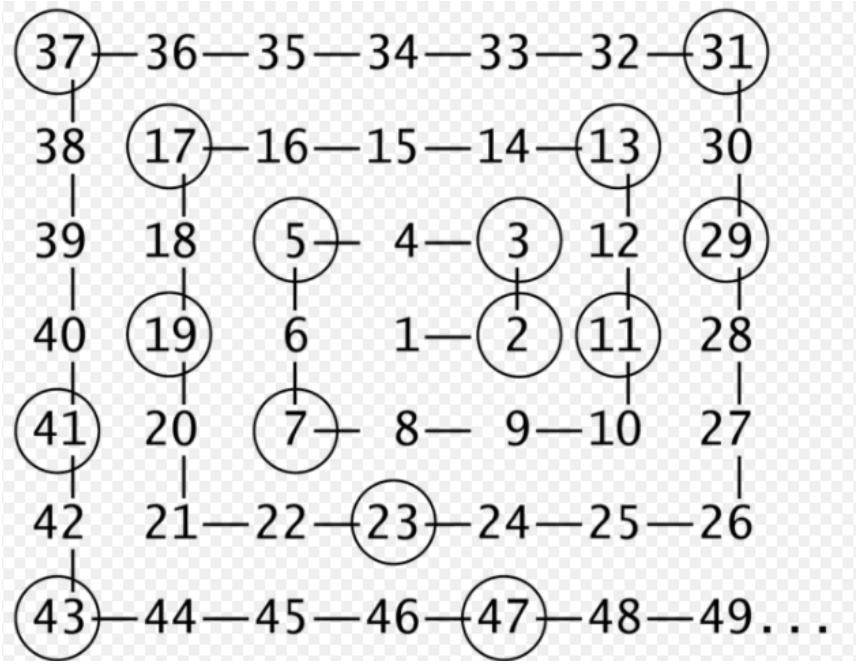

Figura A10: Construção da Espiral de Ulam.

Fonte: Figura produzida por Pubart. Disponível em <https://commons.wikimedia.org/wiki/File:Ulam-Spirale2.png>. Acesso em 18/05/2021.

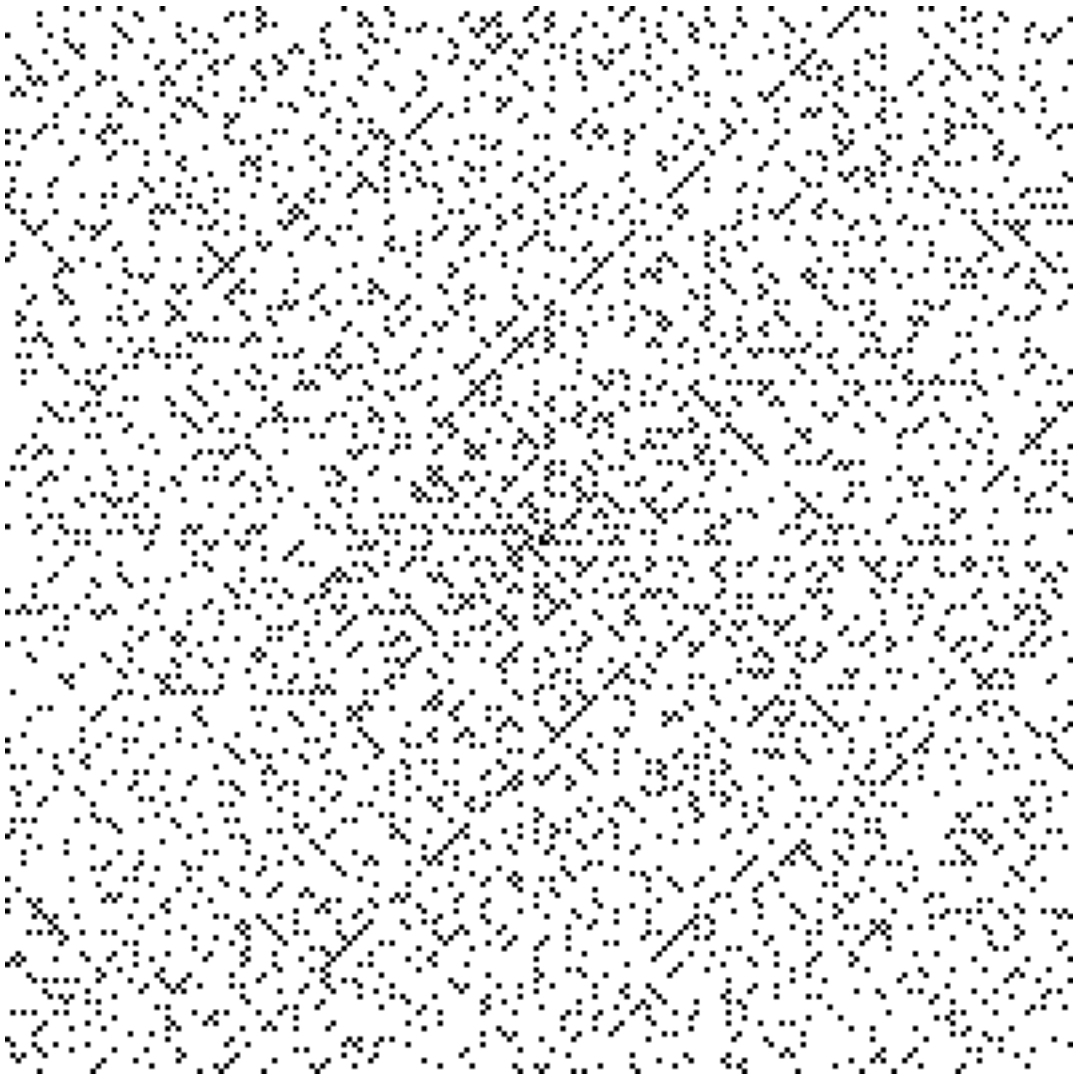

Figura A11: Espiral de Ulam com 40 mil números, primos em evidência.

Fonte: Figura de autoria própria

- Caminhos diferentes

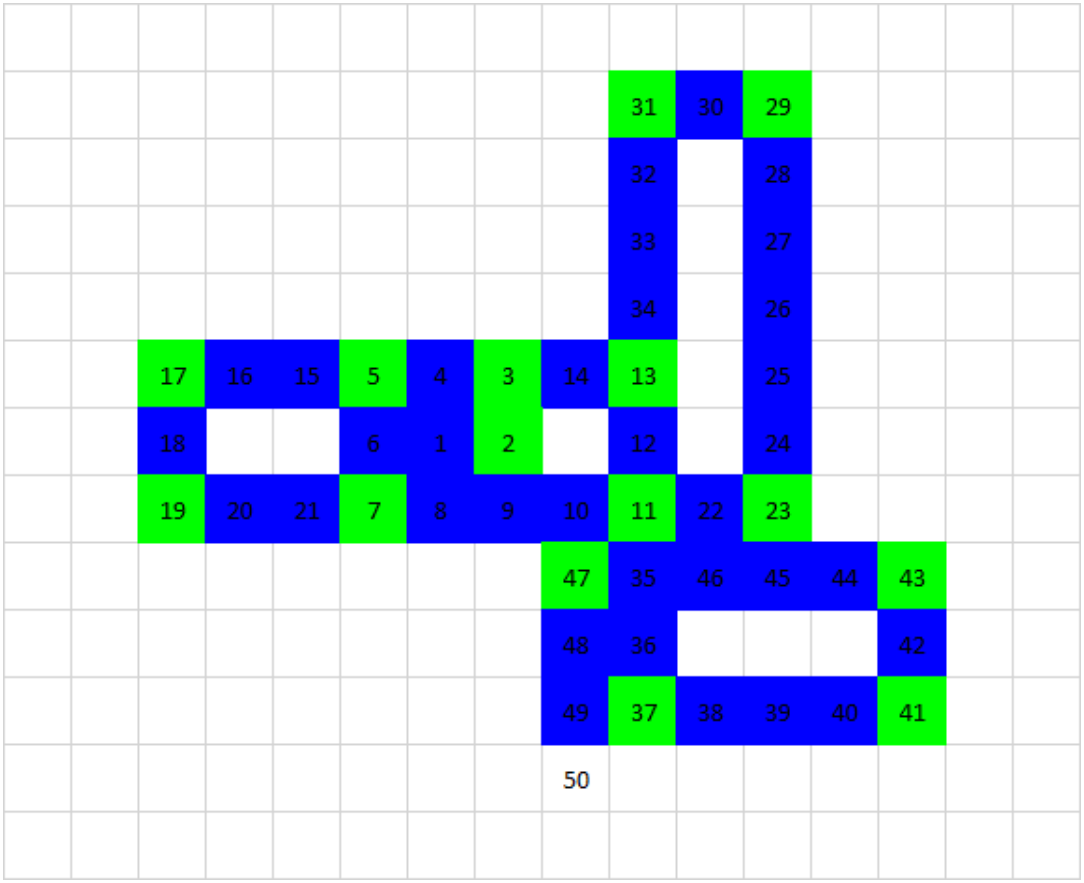

Figura A12: Construção de um caminho padrão até 50.

Fonte: Figura de autoria própria

Figura A13: Caminho padrão com 999 999 passos.

Fonte: Figura de autoria própria

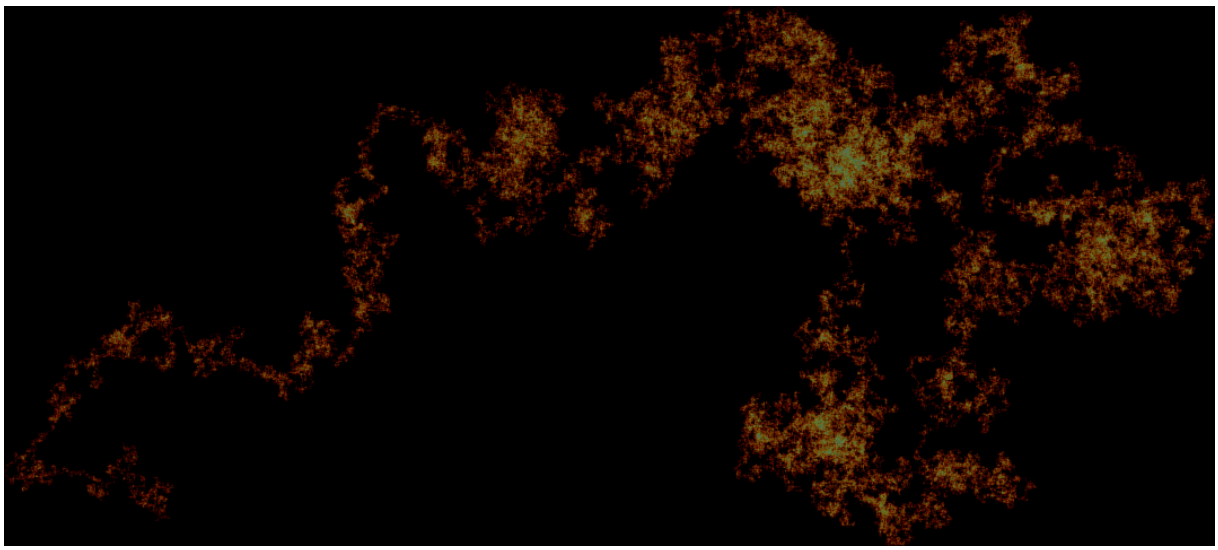

Figura A14: Caminho com sobrescrição com 10 000 000 passos.

Fonte: Figura disponível em [9]. Acesso em 18/05/2021.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] BARTHEL, Jim; SGOBBA, Pietro e ZHU, Fa. **Visualising the distribution of primes**, BASI Mathematics, Experimental Mathematics Lab, University Of Luxembourg, Luxemburgo, 2015.

https://math.uni.lu/eml/projects/reports/prime-distribution.pdf

[2] CASTRO, Francisco Daniel Carneiro de. **Oito testes de primalidade**. 2018.

http://www.repositorio.ufc.br/handle/riufc/34414

[3] CLEMENT, P. A. **Congruences for sets of primes**. The American Mathematical Monthly, v. 56, n. 1, p. 23-25, 1949.

[4] EUCLIDES, **Os elementos**, Editora Unesp, Tradução: Irineu Bicudo, 2009.

[5] FARIAS, Djalma Gomes de et al. **Um estudo do ensino de números primos na Educação Básica**. Universidade Federal de Alagoas, 2016.

http://www.repositorio.ufal.br/handle/riufal/2433

[6] HEFEZ, Abramo. **Aritmética**. Rio de Janeiro: SBM, p. 42, 2014.

[7] KINTALI, Shiva. **A Generalization of Erdös's Proof of Bertrand-Chebyshev Theorem**. Georgia Institute of Technology, 2008.

[8] MIRKOSKI, Luiz. **Números e polinômios de Bernoulli**. 2018, 64f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFOMAT) - Universidade Estadual de Ponta Grossa, Ponta Grossa, 2018.

[9] PM 2RING (https://math.stackexchange.com/users/207316/pm-2ring). **Help with a prime number spiral which turns 90 degrees at each prime**. Mathematics Stack Exchange, 2017.

https://math.stackexchange.com/q/2079346/

[10] POÇAS, Diogo. **Testes de primalidade**. Números, cirurgias e nós de gravata: 10 anos de Seminário Diagonal no IST, IST Press, 2012.

[11] RAINFORD, David. **Suggested conventions**, Prime Patterns, 2013.

https://primepatterns.tumblr.com/post/61963093263/

[12] RIBENBOIM, Paulo. **The little book of bigger primes**. Springer Science & Business Media, 2004.

[13] ROQUE, Tatiana. **História da matemática**. Editora Schwarcz-Companhia das Letras, 2012.

[14] STEIN, Myron L.; ULAM, Stanislaw M.; WELLS, Mark B. **A visual display of some properties of the distribution of primes**. The American Mathematical Monthly, v. 71, n. 5, p. 516-520, 1964.

[15] STEWART, James; CLEGG, Daniel K.; WATSON, Saleem. **Calculus: early transcendentals**. Cengage Learning, 2020.