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

Paulo José Alves Pedroza

Distribuição de Números Primos, Padrões Gráficos e a Espiral de Ulam

RECIFE
2020

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

Paulo José Alves Pedroza

Distribuição de Números Primos, Padrões Gráficos e a Espiral de Ulam

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

Orientador: Prof. Dr. Gabriel Araújo Guedes

RECIFE
2020

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

P372d Pedroza, Paulo José Alves
Distribuição de Números Primos, Padrões Gráficos e a Espiral de Ulam / Paulo José Alves Pedroza. - 2020.
102 f. : il.

Orientador: Gabriel Araujo Guedes.
Inclui referências e apêndice(s).

Dissertação (Mestrado) - Universidade Federal Rural de Pernambuco, Programa de Mestrado Profissional em Matemática (PROFMAT), Recife, 2020.

1. Números primos. 2. Distribuição dos números primos. 3. Hipótese de Riemann. 4. Espiral de Ulam. 5. Formas geométricas e primos. I. Guedes, Gabriel Araujo, orient. II. Título

CDD 510

PAULO JOSÉ ALVES PEDROZA

Distribuição de Números Primos, Padrões Gráficos e a Espiral de Ulam

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

Aprovado em 03 / 09 / 2020

BANCA EXAMINADORA

Prof. Dr. Gabriel Araújo Guedes (Orientador(a))– UFRPE

Prof. Dr. Luis Guillermo Martinez Maza – UFAL

Prof. Dr. Eudes Mendes Barboza– PROFMAT/UFRPE

À minha mãe (in memoriam).

Agradecimentos

Agradeço, primeiramente, a Deus, pelo dom da vida e por todas as bençãos e graças com as quais o Senhor tem me presenteado.
Aos meus pais, Abel Alves Pedroza e Esmeralda Alves Pedroza (in memoriam), que me educaram, oportunizaram e incentivaram meus estudos.
À minha esposa, Lucineide Gomes da Silva Pedroza, pelo apoio e dedicação.
Às minhas filhas, Sabrina Gomes Alves Pedroza e Maísa Gomes Alves Pedroza, pelo carinho e por deixarem minha vida mais feliz.
Aos colegas Andréia Simone da Silva, Débora Simone Ferreira de Queiroz e Luiz Manoel de Santana Neto, pelas caronas e pelos momentos de estudo em grupo de grande importância no meu aprendizado.
Aos demais colegas da turma PROFMAT 2018, também pelos momentos de estudo em grupo e apoio.
Ao meu professor orientador Dr. Gabriel Araújo Guedes, por todas as dicas e orientações, que me levaram a um novo patamar de conhecimento.
A todos os professores das disciplinas do PROFMAT, pelos ensinamentos e orientações.
Ao meu amigo Emanoel Rodrigues de Souza, pelo incentivo e colaboração.
Enfim, a todos que de uma forma ou de outra contribuíram para que eu chegasse a este ponto da minha vida.

"A Matemática Aplicada
necessita da Matemática Pura
tanto como os formigueiros
necessitam das formigas.
(Paul Halmos)

Declaração

Eu, PAULO JOSÉ ALVES PEDROZA, declaro para devidos fins e efeitos, que a dissertação sob título DISTRIBUIÇÃO DE NÚMEROS PRIMOS, PADRÕES GRÁFICOS E A ESPIRAL DE ULAM, entregue como Trabalho de Conclusão de curso para obtenção do título de mestre, com exceção das citações diretas e indiretas claramente indicadas e referenciadas, é um trabalho original. Eu estou consciente que a utilização de material de terceiros incluindo uso de paráfrase sem a devida indicação das fontes será considerado plágio, e estará sujeito a processos administrativos da Universidade Federal Rural de Pernambuco e sanções legais. Declaro ainda que respeitei todos os requisitos dos direitos de autor e isento a Pós-graduação PROFMAT/UFRPE, bem como o professor orientador DR. GABRIEL ARAÚJO GUEDES, de qualquer ônus ou responsabilidade sobre a sua autoria.

Recife, 03 de SETEMBRO de 2020.

Assinatura: _____

Resumo

Este trabalho tem como tema a distribuição dos números primos, com foco em figuras geométricas, inspiradas na espiral de Ulam, que apresentem determinadas propriedades vinculadas com os primos. Inicia-se com a apresentação de algumas ideias fundamentais sobre primos e conceitos básicos para a compreensão do que virá adiante e a exposição de alguns números especiais que têm relação com os primos, como os números de Fermat e os de Mersenne, entre outros. A partir do capítulo 3 entra-se no tema central, que é a distribuição dos números primos, ou seja, a busca dos matemáticos para encontrar um padrão na distribuição desses números. No capítulo 4 é feita uma breve apresentação da maior promessa de resposta para o padrão dos números primos, discutido no capítulo anterior, a hipótese de Riemann. O capítulo 5 apresenta a espiral de Ulam e sua variação, a espiral de Sacks. Nossa proposta de figuras geométricas nas quais são destacados os números primos, com a possível verificação de propriedades relativas a esses números, é apresentada no capítulo 6. Finaliza-se com as atividades desenvolvidas com estudantes de Ensino Médio e os resultados dessas atividades.

Palavras-chave: Números primos; distribuição dos números primos; hipótese de Riemann; espiral de Ulam; formas geométricas e primos.

Abstract

This work has as its theme the distribution of prime numbers, with a focus on geometric figures, inspired by Ulam's spiral, which present certain properties linked to the primes. It starts with the presentation of some fundamental ideas about primes and basic concepts for the understanding of what is to come and the exposition of some special numbers that have a relation with the primes, such as Fermat and Mersenne numbers, among others. Starting from chapter 3, the central theme is entered, which is the distribution of prime numbers, that is, the search for mathematicians to find a pattern in the distribution of these numbers. In chapter 4, a brief presentation is given of the greatest promise of response to the prime number pattern, discussed in the previous chapter, the Riemann hypothesis. Chapter 5 presents Ulam's spiral and its variation, Sacks' spiral. Our proposal of geometric figures in which prime numbers are highlighted, with the possible verification of properties related to these numbers, is presented in chapter 6. It ends with the activities developed with high school students and the results of these activities.

Keywords: Prime numbers; prime number distribution; Riemann hypothesis; Ulam's spiral; geometric shapes and primes.

Lista de ilustrações

Sumário

Introdução

> – O que você precisa saber é que existem esses números comuns pra cachorro que podem ser divididos, mas existem outros também, e com esses outros a coisa não dá certo. Sabe por quê? Porque esses outros são primos. Com eles, os matemáticos vêm quebrando a cabeça há mais de mil anos. São números maravilhosos. O 11, por exemplo, ou o 13 e o 17. Robert se admirou, pois de repente o diabo dos números parecia encantado, como se estivesse saboreando algum petisco delicioso. (ENZENSBERGER, 2009).

A Matemática abrange uma infinidade de problemas ou situações práticas, do nosso Universo. Ela está presente no dia a dia de qualquer pessoa em situações de simples contagem, compra e venda, etc., mas está presente também em contextos de outras ciências como nas fórmulas da Física ou Economia. Além disso, temos também a Matemática Pura, que, a princípio, envolve temas abordados apenas pela Matemática, contudo, isto não significa que tais temas não possam ter aplicações futuras em algum outro ramo científico. Se a Matemática tem uma alma, essa alma é o conjunto formado pelos números primos. A matéria-prima da Matemática são os números e os números primos são os tijolos formadores de todos os números. Por isto, esses números (os primos) são o tema deste trabalho. Apesar dessa importância dos números primos para a Matemática, a Base Nacional Comum Curricular (BNCC) cita os primos somente em dois momentos: quando coloca os números primos e compostos como objeto de estudo no 6º ano do Ensino Fundamental; e na descrição da habilidade EF06MA05 que diz

> 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 (BRASIL, 2017).

Neste trabalho, em um primeiro momento, apresenta-se os números primos, os primeiros trabalhos realizados sobre eles e as primeiras ideias. É apresentado o crivo de Eratóstenes e algumas demonstrações da infinitude desses números. Em seguida teremos a apresentação de alguns números primos específicos, como os primos de Fermat e os de Mersenne. Depois, chega-se ao ponto central deste trabalho, que é a distribuição dos números primos, ou melhor, a busca dos matemáticos por uma regularidade na distribuição dos números primos (ponto crucial para o futuro da Matemática e, consequentemente, para o futuro da humanidade).

Platão, em seu mito da caverna, coloca que a realidade é bem mais do que nossos sentidos podem perceber, e só o mundo das ideias podem nos mostrar a realidade. A hipótese de Riemann é, como veremos neste trabalho, uma versão do mito da caverna voltada para os números, com sua promissora possibilidade de determinação de todos os números primos (inteiros) usando números imaginários. Há uma infinidade de trabalhos baseados nesta hipótese e, portanto, a comprovação de sua veracidade desencadeará uma verdadeira

revolução na Matemática. Além disso, a hipótese de Riemann está relacionada com o que chamamos de "alma" da Matemática: os números primos. Logo, esta hipótese é de fundamental importância para todos e, portanto, devemos preparar muito bem nossos estudantes, para que possa surgir entre eles aquele que provará a hipótese de Riemann.
É destacado, então, o trabalho de Ulam, com sua espiral. Ela é constituída por uma malha quadrangular na qual são colocados os números inteiros positivos de tal forma que, começando do 1, os números são colocados "enrolando-se" em uma espiral. Nesta espiral um fato, um tanto quanto curioso, é notado: os números primos surgem, em boa parte, em diagonais, com destaque para algumas destas diagonais. Assim, pela complexidade da hipótese de Riemann, a espiral de Ulam e outras formas, combinadas com números, podem ser inspiradores para nossos alunos da educação básica aprofundarem seus estudos referentes aos números primos e sua distribuição. A espiral de Ulam é, portanto, a fonte inspiradora das atividades propostas aqui para se trabalhar com estudantes do Ensino Médio. Atividades que buscam motivar o aluno a ser protagonista no estudo da Matemática, criando e pesquisando novas formas de distribuição dos números em figuras geométricas, e levando-os a conjecturas e demonstrações próprias.

1 Os Números Primos

Os números, em particular os números primos, povoam os pensamentos de filósofos e matemáticos e encantam os leigos desde a Antiguidade até os dias atuais. Foram criados sistemas de numeração, processos para realização de operações com números e muito mais. Os números que possuem apenas dois divisores inteiros positivos são estudados há muito tempo, e as primeiras questões relativas a estes números foram:
1. Quais são os números primos e como determiná-los?
2. O conjunto dos números primos é finito ou infinito?
3. Como os números primos estão distribuídos, ou seja, há alguma regularidade ou padrão na distribuição dos números primos?
Consideremos o conjunto dos números naturais $\mathbb{N} = \{1, 2, 3, 4, 5, 6, ...\}$, podemos separar esses números em três categorias: números primos; números compostos; e a sua unidade o 1. Os números primos são aqueles que, como dito anteriormente, possuem nem mais nem menos que dois divisores inteiros positivos, que são o 1 (um) e o próprio número. Por exemplo, o 37 (trinta e sete). Já os números compostos são aqueles que possuem mais de dois divisores inteiros positivos, por exemplo o 36 que tem como divisores inteiros positivos os números 1, 2, 3, 4, 6, 9, 12, 18 e 36.
A partir daí, para responder aos questionamentos expostos acima, os estudos desses números possibilitaram várias e impressionantes descobertas por parte de grandes matemáticos no decorrer da história. Processos foram desenvolvidos para a determinação dos números primos, foram criadas dezenas de demonstrações da infinitude desses números, mas o maior desafio continua sendo relacionado à regularidade dos mesmos.

Definição 1.1. Sendo p um número inteiro positivo maior que 1, p será **primo** se seus únicos divisores positivos forem 1 e p. Se p não for primo ele é chamado de **composto**.

Assim, os números primos menores que 100 são:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 e 97. Vejamos, no entanto, que se um número inteiro é composto, então ele tem outro(s) divisor(es) além do 1 e dele mesmo, daí:

Teorema 1.2 (Teorema Fundamental da Aritmética)**.** *Todo inteiro n maior que* 1 *pode ser expresso como o produto finito de primos, sendo os fatores iguais ou não.*

Demonstração. Façamos por indução na segunda forma sobre n:
i) Se $n = 2$ tudo certo, pois 2 é primo.
ii) Supondo válida para $2, 3, ..., n$, devemos mostrar que é válida para $n + 1$.
Se $n + 1$ for primo não há nada a se mostrar.

Se $n+1$ for composto, então $n+1 = ab$, com $a, b \in \mathbb{N}$ e $1 < a, b < n$. Portanto a, b podem ser decompostos em fatores primos (hipótese), logo $n+1$ também poderá ser decomposto em fatores primos. □

A princípio, para se determinar se um número inteiro p é primo, devemos dividir p pelos naturais $n = 2, 3, 4, ..., n-1$, se p for divisível por um desses números, então p é composto, caso contrário ele é primo. No entanto, se p é divisível por n e este é divisível por q, então p é divisível por q, logo só precisamos dividir p pelos primos menores que ele. Mas, será que temos que dividir p por todos os primos menores que ele? Em outras palavras: até onde devemos ir para ter certeza que um determinado número inteiro p é primo? Esta pergunta é respondida com a proposição a seguir.

Proposição 1.3 (Eratóstenes)**.** *Sendo n um número composto maior que* 1*, então n possui um divisor primo p, tal que $p \leq \sqrt{n}$.*

Observemos a demonstração a seguir, adaptada de (N., 2013).

Demonstração. Seja $n = ab$, com $1 < a \leq b$. Se p é um divisor primo de a, então $p|n$ e

$$p^2 \leq a^2 \leq ab = n,$$

assim $p \leq \sqrt{n}$. □

Ou seja, se, ao dividirmos sucessivamente n pelos primos $p \leq \sqrt{n}$, não encontrarmos uma divisão exata, então n é primo. Caso contrário ele será composto.

Exemplo 1.4. Consideremos o número 211. $196 = 14^2 < 211 < 225 = 15^2$, portanto, a raiz quadrada de 211 está entre 14 e 15, assim, devemos verificar se 211 é divisível por algum primo menor que 14, isto é, 2, 3, 5, 7, 11 ou 13. Obviamente ele não é divisível por 2, pois é ímpar. Dividindo 211 por 3 obtemos quociente 70 e resto 1, dividindo por 5 obtemos quociente 42 e resto 1, por 7, quociente 30 e resto 1, por 11, quociente 19 e resto 2, e, ao dividirmos por 13, chegamos ao quociente 16 e resto 3. Logo, 211 é primo, já que nenhuma divisão, até esse ponto, foi exata.

1.1 Conceitos Básicos

Antes de continuarmos, devemos ver alguns conceitos que serão muito importantes para a compreensão e também para as demonstrações de teoremas, proposições e corolários.

1.1.1 Congruência

Congruência é a relação entre números inteiros, tais que, dados a, b e n inteiros, dizemos que $a \equiv b\ (mod\ n)$ (lê-se: a é congruente a b módulo n) se $n|a-b$ (lê-se: n divide a menos b), isto é, se a e b deixam o mesmo resto quando divididos por n.

Exemplo 1.5. $59 \equiv 25 \pmod{17}$, pois $17|59-25=34$.

Proposição 1.6. *Se a, b, m e d são inteiros e $m > 0$, as seguintes sentenças são verdadeiras:*
1. $a \equiv a\ (mod\ m)$
2. Se $a \equiv b\ (mod\ m)$, então $b \equiv a\ (mod\ m)$
3. Se $a \equiv b\ (mod\ m)$ e $b \equiv d\ (mod\ m)$, então $a \equiv d\ (mod\ m)$.

Demonstração. (1) $m|0$, portanto $m|a-a$, logo $a \equiv a \pmod{m}$.
(2) Se $a \equiv b \pmod{m}$, então $m|a-b$ e isto implica que $m|-(a-b) = b-a$, logo $b \equiv a \pmod{m}$.
(3) Se $a \equiv b \pmod{m}$ e $b \equiv d \pmod{m}$, então $a-b = k_1 m$ e $b-d = k_2 m$, com $k_1, k_2 \in \mathbb{Z}$. Somando-se, membro a membro, estas últimas equações, obtemos $a-d = (k_1+k_2)m$, o que implica $a \equiv d \pmod{m}$. □

"Esta proposição nos diz que a relação de congruência, definida no conjunto dos inteiros, é uma relação de equivalência, pois acabamos de provar que ela é reflexiva, simétrica e transitiva." (SANTOS, 2018).

Teorema 1.7. *Sejam a, b, c e m inteiros tais que $a \equiv b\ (mod\ m)$, então*
1. $a+c \equiv b+c\ (mod\ m)$
2. $a-c \equiv b-c\ (mod\ m)$
3. $ac \equiv bc\ (mod\ m)$

Demonstração. (1) Como $a \equiv b \pmod{m}$, temos que existe um k inteiro tal que $km = a-b = a-b+c-c = (a+c)-(b+c)$, logo $a+c \equiv b+c \pmod{m}$.
(2) Similar a (1).
(3) $a-b = km \Rightarrow c(a-b) = ac-bc = ckm \Rightarrow ac-bc = k'm$, com $k' = ck$, portanto $m|ac-bc$, logo $ac \equiv bc \pmod{m}$. □

Teorema 1.8. *Sejam a, b, c, d e m inteiros tais que $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$, então*
1. $a+c \equiv b+d\ (mod\ m)$
2. $a-c \equiv b-d\ (mod\ m)$
3. $ac \equiv bd\ (mod\ m)$.

Demonstração. (1) De $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$ temos que $a - b = k_1 m$ e $c - d = k_2 m$, daí, somando-se membro a membro obtemos $(a + c) - (b + d) = (k_1 + k_2)m$, e isto implica $a + c \equiv b + d \pmod{m}$.
(2) Similar a (1), subtraindo membro a membro.
(3) Fazendo $c(a - b) = ac - bc = ck_1 m = k'_1 m$ e $b(c - d) = bc - bd = bk_2 m = k'_2 m$, temos $ac - bc = k'_1 m$ e $bc - bd = k'_2 m$, daí, somando membro a membro, obtemos $ac - bd = (k'_1 + k'_2)m$, logo $ac \equiv bd \pmod{m}$. □

Corolário 1.9. *Se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m}$.*

Demonstração. Sendo $a \equiv b \pmod{m}$, usando o item (3) do teorema 1.8, temos $\underbrace{aa \cdots a}_{n \text{ vezes}} \equiv \underbrace{bb \cdots b}_{n \text{ vezes}} \pmod{m}$, daí, $a^n \equiv b^n \pmod{m}$. □

O cálculo de restos de divisões por um determinado número inteiro n, por meio de congruências, fica bastante facilitado quando se conhece expoentes que torna certa potência congruente a 1 módulo n.

Exemplo 1.10. Se quisermos saber qual o resto da divisão de 13^{256} por 36, sabendo que 13^3 é congruente a 1 módulo 36, teremos:

$$13^{257} \equiv (13^3)^{85} \cdot 13^2 \equiv 1^{85} \cdot 13^2 \equiv 1 \cdot 169 \equiv 25 \pmod{36}$$

Logo, o resto da divisão de 13^{257} por 36 é 25.

1.1.2 O Anel de Inteiros Módulo n

Uma relação $\sim$ sobre um dado conjunto X é de equivalência se ela é reflexiva ($a \sim a$ para todo $a \in X$), simétrica ($a \sim b \iff b \sim a$) e transitiva ($a \sim b$ e $b \sim c \Rightarrow a \sim c$).
Uma relação de equivalência em X é uma coleção de subconjuntos não vazios de X, dois a dois disjuntos, de tal forma que a união de todos estes subconjuntos seja igual a X. Assim, se $\sim$ é uma relação de equivalência, então, dado um elemento a pertencente a X, define-se a classe de equivalência $\overline{a}$ de a como o conjunto de todos os elementos que são equivalentes a a, ou seja, $\overline{a} = \{b \in X \mid b \sim a\}$.
Com isso podemos observar que $\overline{a} \bigcap \overline{b} = \emptyset$, se $a \not\sim b$, ou $\overline{a} = \overline{b}$, se $a \sim b$. O conjunto $\{\overline{a} \mid a \in X\}$ das classes de equivalência de $\sim$ é denominado de **quociente** de X por $\sim$ e é denotado por $X/\sim$. "O quociente de $\mathbb{Z}$ pela relação $\equiv \pmod{n}$ é chamado de *anel de inteiros módulo n* e é denotado por uma das notações $\mathbb{Z}/(n)$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/n$ ou às vezes $\mathbb{Z}_n$." (MOREIRA, 2012).
Sendo $n > 0$, todo inteiro a é congruente a um único inteiro a', com $0 \leq a' < n$. Assim, podemos escrever

$$\mathbb{Z}/(n) = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}.$$

Podemos, então, dizer que as operações de adição, subtração e multiplicação passam ao quociente, isto é, podemos definir a soma, a diferença e o produto de classes de congruência, respectivamente, por

$$\overline{a} + \overline{b} = \overline{a+b}$$

$$\overline{a} - \overline{b} = \overline{a-b}$$

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

A proposição seguinte revela-nos quando podemos "dividir" por a módulo n, ou seja, quando existe o "inverso multiplicativo" de a módulo n.

Proposição 1.11. *Sendo $a, n \in \mathbb{Z}$, com $n > 0$. Existe $b \in \mathbb{Z}$ com $ab \equiv 1 \pmod{n}$ se, e somente se, $(a, n) = 1$.*

Uma demonstração desta proposição pode ser obtida em (MOREIRA, 2012).
Portanto, dizemos que a é invertível módulo n quando $(a, n) = 1$ e b é chamado de inverso multiplicativo de a módulo n, quando $ab \equiv 1 \pmod{n}$.
Assim, b está bem definido e se temos $\overline{a} \cdot \overline{b} = \overline{1}$ podemos denotar b por $(\overline{a})^{-1}$, quando trabalhamos com classes de congruência.
O subconjunto formado pelos elementos invertíveis de $\mathbb{Z}/(n)$ é definido como o grupo das unidades $(\mathbb{Z}/(n))^{\times}$ do anel dos inteiros módulo n, daí:

$$(\mathbb{Z}/(n))^{\times} = \{\overline{a} \in \mathbb{Z}/(n) \mid (a, n) = 1\}.$$

Uma observação que pode ser feita é que o conjunto $(\mathbb{Z}/(n))^{\times}$ possui a propriedade do fechamento para a multiplicação.

1.1.3 Sistema de Resíduos Módulo n

Definição 1.12. Tomando $n \in \mathbb{N}$ e $r_1, r_2, ..., r_n$ os possíveis restos das divisões por n, chamamos de sistema completo de resíduos módulo n a um conjunto formado por n elementos $\{a_1, a_2, ..., a_n\}$, tais que $a_i \equiv r_i \pmod{n}$, para todo r_i.

Ou seja, se tivermos n números, tais que cada um deles tem um resto diferente quando os dividimos por n, então dizemos que o conjunto formado por esses números é um sistema completo de resíduos módulo n.

Exemplo 1.13. Tomemos o conjunto $\{10, 18, 35, 42, 49, 56, 61, 66, 77\}$ e $n = 9$, assim, os restos das divisões dos elementos do conjunto por 9 são, respectivamente, 1, 0, 8, 6, 4, 2, 7, 3, 5, isto é, todos os restos possíveis em uma divisão por 9, logo, o conjunto $\{10, 18, 35, 42, 49, 56, 61, 66, 77\}$ é um sistema completo de resíduos módulo 9.

Definição 1.14. Sendo $\{a_1, a_2, ..., a_n\}$ um sistema completo de resíduos módulo n, os a_i tais que $(a_i, n) = 1$ formarão o conjunto denominado de sistema reduzido de resíduos módulo n.

Portanto, o sistema reduzido de resíduos módulo n é formado pelos elementos de um sistema completo de resíduos módulo n que são coprimos com n. Observemos que o número de elementos do sistema reduzido de resíduos módulo n é igual a $\varphi(n)$ (que será visto mais adiante).

Proposição 1.15. *Seja* $\{r_1, r_2, r_3, ..., r_{\varphi(n)}\}$ *um sistema reduzido de resíduos módulo* n*, então* $\{ar_1, ar_2, ar_3, ..., ar_{\varphi(n)}\}$ *é um sistema reduzido de resíduos módulo* n*, para* $a \in \mathbb{Z}$ *e* $(a, n) = 1$.

Demonstração. (Adaptada de (HEFEZ, 2016)) Consideremos $\{b_1, b_2, b_3, ..., b_n\}$ um sistema completo de resíduos módulo n do qual foi extraído o sistema reduzido de resíduos módulo n $\{r_1, r_2, r_3, ..., r_{\varphi(n)}\}$ e, consideremos também, $a \in \mathbb{Z}$ tal que $(a, n) = 1$. Sendo assim, $(ab_i, n) = 1$ se, e somente se, $(b_i, n) = 1$, daí $\{ar_1, ar_2, ar_3, ..., ar_{\varphi(n)}\}$ também é um sistema reduzido de resíduos módulo n. □

Exemplo 1.16. Tomando o sistema reduzido de resíduos módulo 14, $\{1, 3, 5, 9, 11, 13\}$, se multiplicarmos cada elemento desse conjunto por 27 que é coprimo com 14, obteremos o conjunto $\{27, 81, 135, 243, 297, 351\}$, sendo que $27 \equiv 13 \pmod{14}$, $81 \equiv 11 \pmod{14}$, $135 \equiv 9 \pmod{14}$, $243 \equiv 5 \pmod{14}$, $297 \equiv 3 \pmod{14}$ e $351 \equiv 1 \pmod{14}$, assim, esse segundo conjunto também é um sistema reduzido de resíduos módulo 14.

1.2 Reconhecendo Números Primos

A partir do momento que se constata a participação dos números primos na formação dos compostos e, portanto, na de todos números inteiros, surge a necessidade de se determinar quais são os números que estão incluídos entre estes "tijolos" fundamentais do conjunto numérico dos inteiros. Com esse intuito foram criados alguns processos para se verificar se um número é primo ou não.

Sabemos que, se um número é divisível por outro que não seja 1 nem ele mesmo, então esse número é composto, dessa forma, o processo básico de verificação da primalidade de um número n e consequentemente sua fatoração em primos (caso ele não seja primo) consiste em dividi-lo sucessivamente pelos números primos menores que ele (supostamente conhecidos) até o primo mais próximo da raiz quadrada de n, sem extrapolá-la. Se, até chegarmos a esse valor máximo, não obtivermos uma divisão exata, então n é primo, como exposto acima. Caso contrário, n será composto e, assim, podemos prosseguir o processo quantas vezes for necessário com o quociente obtido na divisão exata até chegar ao quociente 1, obtendo, desta forma, uma fatoração em fatores primos de n, ou seja, se

$n = n_0 \cdot n_1$, com $n_0, n_1 \neq 1$, repete-se o processo para n_0 e n_1, e assim sucessivamente, até que se chegue apenas a produtos de primos, obtendo-se a decomposição de n em fatores primos, também como já foi colocado anteriormente.
Contudo, o processo descrito acima se mostra muito repetitivo quando se está trabalhando com números muito grandes, exigindo, portanto, a obtenção de uma forma mais prática e que exija menos passos para se descobrir se um determinado número é primo. A seguir, serão apresentadas algumas ideias, desenvolvidas no decorrer da história da Matemática, direcionadas para esse objetivo.

1.2.1 O Crivo de Eratóstenes

Eratóstenes (276-194 a.C.), matemático grego, criou um método pelo qual lista-se números naturais consecutivos até o valor máximo que se deseja encontrar os números primos e, em seguida, elimina-se o número 1 (se ele estiver presente na lista) e os múltiplos de todos os primos menores ou igual à raiz quadrada do valor limite da lista. Desta forma, os números que não forem eliminados serão os primos. Note que a lista não precisa começar do 1, pois se já forem conhecidos os números primos até n podemos começar a listar os números a partir de $n + 1$.

Exemplo 1.17. Sabendo que os números primos até 100 são 2, 3, 5, 7, 11, 13, 17, 19 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 e 97, então, para encontrar os números primos entre 101 e 200, escreve-se a sequência de 101 a 200 e inicia-se o processo de cortes descrito acima.

101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

Eliminando os múltiplos de 2:

101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

Eliminando os múltiplos de 3:

101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

Eliminando os múltiplos de 5:

101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
142	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

E repetindo o processo para os demais primos menores que $\sqrt{200}$, teremos:

101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

Desta forma, os números que não foram eliminados (de preto) são primos. E mais, se conhecemos os primos até 100, então, pelo crivo de Eratóstenes, podemos obter os primos até 10000, pois $\sqrt{10000} = 100$.

1.3 A Infinitude dos Números Primos

Quando começamos a falar com as crianças sobre os números primos, algumas perguntas são feitas pelos mesmos, tais como: então os números primos são os ímpares? Há outro primo par, além do 2? Por que o 9 não é primo? Qual o maior número primo? Quantos números primos existem?

Para as três primeiras perguntas, podemos argumentar da seguinte maneira: Há apenas um número par que é primo, e este é o 2, pois todos os outros números pares são divisíveis por 2, logo têm mais de dois divisores. Todos os demais primos são ímpares, mas nem todo ímpar é primo como, por exemplo, o 9 que é ímpar porém não é primo, pois, além do 1 e do próprio 9, ele tem um outro divisor, que é o 3.

Contudo, o que nos interessa nesse momento são as duas últimas perguntas. Respondê-las significa responder à pergunta mais geral: os números primos são finitos ou infinitos? Muitas foram as demonstrações desenvolvidas na história da Matemática para mostrar que os números primos são infinitos. Adiante veremos algumas dessas demonstrações.

(RIBENBOIM, 2014) apresenta várias demonstrações da infinitude dos números primos, porém, aqui, serão expostas apenas a demonstração de Euclides, uma variante dessa demonstração, atribuída a Kummer, por sua "perfeita simplicidade", e uma outra variante da demonstração de Euclides, atribuída a Hermite, encontradas na obra supracitada. As demais demonstrações da infinitude dos números primos, foram deixadas de lado aqui, por se tratarem de demonstrações um tanto complexas ou porque envolvem conceitos fora do alcance de compreensão da quase totalidade dos estudantes do Ensino Médio.

1.3.1 A Demonstração de Euclides

Sabemos que, se um número inteiro divide a soma (ou a diferença) de duas parcelas e também divide uma das parcelas, então esse número inteiro divide a outra parcela. De outra maneira, se $a|b \pm c$ e $a|b$, então $a|c$. Este é o princípio envolvido na demonstração de Euclides.

Euclides. Consideremos que a sucessão $p_1 = 2$, $p_2 = 3$, ..., p_n dos n números primos seja finita. Se considerarmos o número $P = p_1 \cdot p_2 \cdots p_n + 1$. Como todos números primos são fatores da primeira parcela da soma, então, pelo que vimos anteriormente, um desses números primos divide o 1 (absurdo), portanto, ou o número P é primo maior que todos os outros primos da lista inicial, ou existe um outro número primo, ausente na lista inicial, que divide P. Logo, os números primos não são finitos. □

A variante de Kummer para a demonstração de Euclides, baseia-se no mesmo princípio colocado anteriormente, substituindo-se o sinal de + pelo de −. Portanto, seguimos um processo análogo para se chegar à mesma conclusão.
"Você gostou da demonstração de Kummer? Compare com a que segue, quiçá ainda mais linda." (RIBENBOIM, 2014). Ribenboim está se referindo nesta citação à demonstração atribuída a Hermite, por H. Brocard em sua publicação **Intermédiaire des Mathématiciens**, 22, página 253, de 1915. A mesma consiste em mostrar que para todo número natural n existe um número primo p, tal que $p > n$. Para tanto, basta escolher um número primo p que divida $n! + 1! = n! + 1$. Como temos uma quantidade i de números primos menores que n, então teremos que $n! + 1 = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_i^{\alpha_i} + 1$, daí, pelo mesmo raciocínio da demonstração de Euclides, concluímos que existe um p primo que é obviamente maior que n, com $n \in \mathbb{N}$. Logo, como $\mathbb{N}$ é infinito então os números primos são infinitos.
Observemos que, por meio dessas demonstrações, podemos encontrar alguns números primos da seguinte forma: consideremos o número primo 2, fazendo $2 + 1 = 3$, chegamos ao primo 3; acrescentando o 3, teremos $2 \cdot 3 + 1 = 7$ primo; acrescentando o 7, teremos $2 \cdot 3 \cdot 7 + 1 = 43$ primo; acrescentando o 43, $2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807 = 13 \cdot 139$, sendo 13 e 139 primos. E variações como: $2^2 + 1 = 5$ primo; $2 \cdot 5 + 1 = 11$ primo; $2 \cdot 11 + 1 = 23$ primo; $2 \cdot 23 + 1 = 47$ primo; $2 \cdot 47 + 1 = 95 = 5 \cdot 19$, onde 5 e 19 são primos. Notemos que se quisermos obter números primos com este método, o número 2 sempre deve ser um dos primos utilizados, haja vista que, com exceção do próprio 2, todos os números primos são ímpares, assim, ao utilizarmos o 2 como um dos fatores do produto de primos, encontraremos um número par que quando somado com o 1 resultará em um número ímpar.

1.3.2 Testes Clássicos de Primalidade Baseados em Congruência

"Os testes clássicos de primaridade são, na nossa opinião, os que são baseados nas congruências, indicadas por Lehmer como extensões de testes anteriores de Lucas, Pocklington e Proth." (RIBENBOIM, 2014). Deixemos claro que (RIBENBOIM, 2014) usa o termo primaridade enquanto neste trabalho será usado o termo primalidade.

Teorema 1.18 (Pequeno Teorema de Fermat)**.** *Se p é primo e $a \in \mathbb{N}$, então $a^p \equiv a \ (mod\ p)$. Em particular, se $(a,p) = 1$, então $a^{p-1} \equiv 1 \ (mod\ p)$.*

A demonstração a seguir é uma adaptação da demonstração contida em (HEFEZ, 2016).

Demonstração. Primeiro mostremos que $a^p \equiv a \pmod{p}$.

$$a^p \equiv a \pmod{p} \Rightarrow p \mid a^p - a.$$

Se $p = 2$ o resultado está claro, pois $a^p - a = a(a^{p-1} - 1)$ que é par, visto que se a for par, então o produto também será par e, se a for ímpar, então a^{p-1} será ímpar que subtraído de 1 se tornará par, deixando o produto par novamente. Portanto basta verificarmos para p ímpar.
Façamos isso por indução em a.
i) Se $a = 0$ ou $a = 1$ está claro, pois $p|0$, assim $0^n \equiv 0 \pmod{p}$ para todo n, como também $1^n \equiv 1 \pmod{p}$ para todo n.
ii) Supondo válida para a, devemos mostrar que é válida para $a+1$. Faremos isso por meio do Binômio de Newton.

$$(a+1)^p - (a+1) = a^p + pa^{p-1} + ... + pa + 1 - a - 1$$

$$(a+1)^p - (a+1) = a^p - a + p(a^{p-1} + ... + a).$$

Como $p|a^p - a$ (hipótese) e $p|p(a^{p-1} + ... + a)$, logo $p|(a+1)^p - (a+1)$.
Agora, mostremos que se $(a,p) = 1$, então $a^{p-1} \equiv 1 \pmod{p}$.
Pelo resultado anterior, vimos que

$$a^p \equiv a \pmod{p} \ \Rightarrow \ p|a^p - a = a(a^{p-1} - 1).$$

Como $p \nmid a$, então $p|a^{p-1} - 1$. □

A descoberta de Fermat, expressa por seu pequeno teorema, foi a de que se tomarmos um número primo p e um outro número inteiro qualquer a, ao multiplicarmos a por ele mesmo p vezes, o resultado obtido deixará o mesmo resto que a quando divididos por p. "A descoberta de Fermat é o tipo de coisa que deixa um matemático inquieto. O que há de especial nos números primos para gerar uma magia dessas?" (SAUTOY, 2007). Fermat,

em uma carta escrita a Bernard Frenicle de Bessy, afirmava ter uma prova de que esta propriedade era válida para todos os primos, mas nunca apresentou sua prova. Foi só em 1736 que Leonard Euler provou o que hoje é conhecido como o Pequeno Teorema de Fermat. Vale salientar que, como veremos adiante, nem sempre que temos $a^n \equiv a \pmod{n}$ n é primo, mas se n é primo essa congruência ocorre.

Exemplo 1.19. Tomemos o número primo 11.
$1^{10} \equiv 1 \pmod{11}$;
$2^{10} \equiv (2^5)^2 \equiv 32^2 \equiv 10^2 \equiv 100 \equiv 1 \pmod{11}$;
$3^{10} \equiv (3^5)^2 \equiv 243^2 \equiv 1^2 \equiv 1 \pmod{11}$;
$4^{10} \equiv (2^2)^{10} \equiv (2^{10})^2 \equiv 1^2 \equiv 1 \pmod{11}$;
$5^{10} \equiv (5^2)^5 \equiv 25^5 \equiv 3^5 \equiv 243 \equiv 1 \pmod{11}$;
$6^{10} \equiv (2 \cdot 3)^{10} \equiv 2^{10} \cdot 3^{10} \equiv 1 \cdot 1 \equiv 1 \pmod{11}$;
$7^{10} \equiv (7^2)^5 \equiv 49^5 \equiv 4^5 \equiv 1 \pmod{11}$;
$8^{10} \equiv (2^3)^{10} \equiv (2^{10})^3 \equiv 1^3 \equiv 1 \pmod{11}$;
$9^{10} \equiv (3^2)^{10} \equiv (3^{10})^2 \equiv 1^2 \equiv 1 \pmod{11}$;
$10^{10} \equiv (2 \cdot 5)^{10} \equiv 2^{10} \cdot 5^{10} \equiv 1 \cdot 1 \equiv 1 \pmod{11}$.

Definição 1.20. Sendo $n \in \mathbb{N}$, a função φ de Euler, denotada por $\varphi(n)$, é definida como sendo a função que determina o número de inteiros positivos, menores que ou igual a n, que são coprimos com n.

Exemplo 1.21. Vamos determinar $\varphi(14)$. Os inteiros positivos menores ou igual a 14 são 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 e 14. Destes os que são coprimos com 14 são 1, 3, 5, 9, 11 e 13 (seis números), assim $\varphi(14) = 6$.

Podemos perceber que $\varphi(n) \leq n - 1$ para todo $n \geq 2$ e, em particular, se n for primo, então $\varphi(n) = n - 1$. Contudo, como calcular $\varphi(n)$ quando n é composto?
O sistema completo de resíduos módulo n é de suma importância na demonstração da proposição a seguir.

Proposição 1.22. *Sejam $a, b \in \mathbb{N}$ tais que $(a, b) = 1$, então*

$$\varphi(ab) = \varphi(a)\varphi(b).$$

A demonstração seguinte também é uma demonstração adaptada de (HEFEZ, 2016).

Demonstração. Vamos supor que $a, b > 1$, pois para $a, b = 1$ o resultado é trivial.
Consideremos a tabela a seguir, com a colunas e b linhas.

$$\begin{array}{ccccccc} 1 & 2 & 3 & \cdots & k & \cdots & a \\ a+1 & a+2 & a+3 & \cdots & a+k & \cdots & 2a \\ 2a+1 & 2a+2 & 2a+3 & \cdots & 2a+k & \cdots & 3a \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ (b-1)a+1 & (b-1)a+2 & (b-1)a+3 & \cdots & (b-1)a+k & \cdots & ba \end{array}$$

Sabemos que $(t, ab) = 1$ (lê-se: o mdc entre t e ab é igual a 1) se, e somente se, $(t, a) = (t, b) = 1$. Assim, $\varphi(ab)$ será dado por todos os elementos da tabela que são simultaneamente coprimos com a e b.

Observemos que se o primeiro elemento de uma coluna é coprimo com a, então todos os elementos dessa coluna são também coprimos com a, e, da mesma forma, se o primeiro elemento de uma coluna não for coprimo com a, então todos os elementos da coluna também não são coprimos com a.

Portanto, devemos determinar dentre os elementos das colunas de elementos coprimos com a quantos são coprimos com b. Como $(a, b) = 1$, assim os elementos dessas colunas formam um sistema completo de resíduos módulo b, desta forma, o número de colunas de coprimos com a é igual a $\varphi(a)$ e em cada uma dessas colunas o número de elementos coprimos com b é igual a $\varphi(b)$. Logo,

$$\varphi(ab) = \varphi(a)\varphi(b).$$

□

Exemplo 1.23. Sabendo que $\varphi(5) = 4$ e $\varphi(7) = 6$, qual é $\varphi(35)$?
$\varphi(35) = \varphi(5 \cdot 7) = \varphi(5) \cdot \varphi(7) = 4 \cdot 6 = 24$.

Proposição 1.24. *Se p é primo e $n \in \mathbb{N}$, então tem-se que*

$$\varphi(p^n) = p^n \left(1 - \frac{1}{p}\right).$$

Demonstração. Temos p^n números naturais de 1 até p^n. Destes, os que têm o máximo divisor comum com p^n diferente de 1 são os múltiplos de p, ou seja, $p, 2p, 3p, ..., p^{n-1}p$, totalizando p^{n-1} números.

Logo,

$$\varphi(p^n) = p^n - p^{n-1} = p^n - \frac{p^n}{p} = p^n \left(1 - \frac{1}{p}\right).$$

□

Como em demonstrações anteriores, esta é uma adaptação da observada em (HEFEZ, 2016).

Teorema 1.25. *Considere $n > 1$ e $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ a decomposição de n em fatores primos. Temos,*

$$\varphi(n) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

Demonstração.

$$\varphi(n) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_r^{\alpha_r})$$

$$\varphi(n) = p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots p_r^{\alpha_r}\left(1 - \frac{1}{p_r}\right)$$

$$\varphi(n) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

□

Exemplo 1.26. $\varphi(360) = \varphi(2^3 \cdot 3^2 \cdot 5) = 2^3 \cdot 3^2 \cdot 5\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) =$
$= 8 \cdot 9 \cdot 5 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 360 \cdot \frac{8}{30} = 96.$

Teorema 1.27 (Euler)**.** *Seja $n \in \mathbb{N}$ e $a \in \mathbb{Z}$, com $(n, a) = 1$, então*

$$a^{\varphi(n)} \equiv 1 \ (mod\ n).$$

Demonstração. (Adaptada de (HEFEZ, 2016)) Sendo $\{r_1, r_2, r_3, ..., r_{\varphi(n)}\}$ um sistema reduzido de resíduos módulo n. Portanto, $\{ar_1, ar_2, ar_3, ..., ar_{\varphi(n)}\}$ também é um sistema reduzido de resíduos módulo n e, desta forma,

$$ar_1 ar_2 ar_3 \ldots ar_{\varphi(n)} \equiv r_1 r_2 r_3 \ldots r_{\varphi(n)} \pmod{n}$$

consequentemente

$$a^{\varphi(n)} r_1 r_2 r_3 \ldots r_{\varphi(n)} \equiv r_1 r_2 r_3 \ldots r_{\varphi(n)} \pmod{n}$$

logo, como $(r_i, n) = 1$, temos

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

□

Este teorema de Euler é uma generalização do pequeno teorema de Fermat, visto que, se $n = p$ com p primo e p não divide a, e sabendo que $\varphi(p) = p - 1$, então substituindo n por p em $a^{\varphi(n)} \equiv 1 \pmod{n}$ teremos $a^{\varphi(p)} \equiv a^{p-1} \equiv 1 \pmod{p}$, que é o que diz o pequeno teorema de Fermat. No entanto, o teorema de Euler é mais amplo, pois expõe que o que Fermat havia percebido para os números primos pode ser ampliado para números compostos, contanto que o número composto n seja coprimo com o também número composto a, e considerando a função φ de Euler.

Proposição 1.28. *A congruência $aX \equiv 1\ (mod\, m)$ tem solução se, e somente se, $(a, m) = 1$, com $a, m \in \mathbb{Z}$ e $m > 1$. Além disso, se $x_0 \in \mathbb{Z}$ é uma solução, então x também é solução da congruência se, e somente se, $x \equiv x_0\ (mod\ m)$.*

Demonstração. A congruência $aX \equiv 1 \pmod{m}$ tem uma solução x_0 se, e somente se, $m|ax_0 - 1$, ou seja, a equação diofantina $aX - mY = 1$ possui solução pertencente ao conjunto dos números inteiros, portanto $(a, m) = 1$.
Ainda, se x_0 e x são soluções da congruência $aX \equiv 1 \pmod{m}$, então $ax \equiv ax_0 \pmod{m}$ e $(a, m) = 1$, o que implica que $x \equiv x_0 \pmod{m}$.
Daí, se x_0 é solução da congruência $aX \equiv 1 \pmod{m}$ e $x \equiv x_0 \pmod{m}$, então x também é solução da mesma congruência, pois

$$ax \equiv ax_0 \equiv 1 \pmod{m}.$$

□

Teorema 1.29 (Wilson)**.** *Seja $n > 1$ inteiro, se $n = p$, p primo, então $(n-1)! = (p-1)! \equiv -1 \pmod{p}$, e $(n-1)! \equiv 0 \pmod{n}$ se n é composto e $n \neq 4$.*

Demonstração. Consideremos, inicialmente, que n é composto mas sem ser o quadrado de um número primo. Dessa forma podemos escrever $n = ab$ com $1 < a < b < n$. Assim, tanto a quanto b são fatores de $(n-1)!$ e, portanto, $ab|(n-1)!$, ou seja, $n|(n-1)!$ logo $(n-1)! \equiv 0 \pmod{n}$.
Consideremos, agora, que $n = p^2$ com $p > 2$, então p e $2p$ são fatores de $(n-1)!$ pois, nesse caso, $2p < p^2$ para $p > 2$, e novamente $(n-1)! \equiv 0 \pmod{n}$; isto mostra que para todo $n \neq 4$ composto e quadrado perfeito temos $(n-1)! \equiv 0 \pmod{n}$.
Se n for ímpar, temos que o teorema é obviamente válido para $n = 3$. Suponhamos, então, $n \geq 5$ primo. Para todo $i \in 1, ..., n-1$, pela proposição, temos que $iX \equiv 1 \pmod{n}$ possui apenas uma solução, ou seja, dado $i \in 1, ..., n-1$ existe só um $j \in 1, ..., n-1$ tal que $ij \equiv 1 \pmod{n}$. Por outro lado, se i é tal que $i^2 \equiv 1 \pmod{n}$, então $n|i^2 - 1$, o que equivale a $n|i-1$ ou $n|i+1$, o que só pode ocorrer se $i = 1$ ou $i = n-1$. Logo, $2 \cdots (n-2) \equiv 1 \pmod{n}$, e, desta forma, $1 \cdot 2 \cdots (n-2)(n-1) \equiv n-1 \equiv -1 \pmod{n}$. □

Pelo exposto, podemos ver que o teorema de Wilson caracteriza os números primos, haja vista que apenas os números inteiros primos p fornecem uma congruência a -1, módulo p, do fatorial do antecessor de p. Contudo, essa caracterização dos números primos não é prática para testar a primalidade de um número inteiro qualquer n, porque não se conhece um algoritmo para calcular, de forma rápida, o fatorial de um número. O que temos é o processo oriundo da própria definição de fatorial, que se torna cada vez mais trabalhoso ao passo que n aumenta.

Exemplo 1.30. Tomando $n = 13$, teremos:
$(13-1)! \equiv 12! \equiv 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \equiv 132 \cdot 90 \cdot 56 \cdot 30 \cdot 24 \equiv 2 \cdot 12 \cdot 4 \cdot 4 \cdot 11 \equiv 24 \cdot 16 \cdot 11 \equiv 11 \cdot 3 \cdot 11 \equiv 33 \cdot 11 \equiv 7 \cdot 11 \equiv 77 \equiv 12 \equiv -1 \pmod{13}$;
Tomando $n = 12$, teremos:
$(12-1)! \equiv 11! \equiv 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \equiv 11 \cdot 90 \cdot 56 \cdot 30 \cdot 24 \equiv 11 \cdot 6 \cdot 8 \cdot 6 \cdot 0 \equiv 0 \pmod{12}$.

Uma aplicação do teorema de Wilson está presente no teorema de Wolstenholme, anotado a seguir.

Teorema 1.31 (Wolstenholme)**.** *Seja $p \geq 5$ um número primo, então o numerador da fração irredutível equivalente à soma*

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{p-1}$$

é divisível por p^2.

Vejamos uma adaptação da demonstração encontrada em (MARTINEZ et al., 2018).

Demonstração. Notemos que, como $p \geq 5$ e primo, então $p-1$ é par, assim a soma em questão tem uma quantidade par de parcelas e, portanto, podemos formar pares de parcelas simétricas em relação aos extremos da soma. Daí

$$\sum_{i=1}^{p-1} \frac{1}{i} = \sum_{i=1}^{\frac{p-1}{2}} \left(\frac{1}{i} + \frac{1}{p-i} \right) = p \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i(p-i)} = \frac{p}{(p-1)!} \sum_{i=1}^{\frac{p-1}{2}} \frac{(p-1)!}{i(p-i)}$$

como $p \nmid (p-1)!$ (teorema de Wilson), temos que mostrar que o inteiro

$$S = \sum_{i=1}^{\frac{p-1}{2}} \frac{(p-1)!}{i(p-i)}$$

é um múltiplo de p. Para $1 \leq i \leq p-1$, denotemos por r_i o inverso de i mod p, ou seja, $ir_i \equiv 1 \pmod{p}$. Notemos que $r_{p-i} \equiv -r_i \pmod{p}$, desta forma

$$S \equiv \sum_{i=1}^{\frac{p-1}{2}} \frac{(p-1)!}{i(p-i)} ir_i(p-i)r_{p-i} \equiv \sum_{i=1}^{\frac{p-1}{2}} (p-1)! r_i r_{p-i} \equiv \sum_{i=1}^{\frac{p-1}{2}} r_i^2 \pmod{p}$$

pelo teorema de Wilson. Notemos, agora, que como cada r_i é congruente a um dos números ± 1, ± 2, ..., $\pm\frac{p-1}{2}$, então os r_i^2 são congruentes a um dos números 1^2, 2^2, ..., $\left(\frac{p-1}{2}\right)^2$ módulo p. Portanto, temos que mostrar, primeiramente, que todos eles aparecem.

$$r_i^2 \equiv r_j^2 \pmod{p} \implies p | r_i^2 - r_j^2 = (r_i - r_j)(r_i + r_j),$$

ou seja,

$$r_i \equiv \pm r_j \pmod{p}.$$

Multiplicando por ij, temos

$$r_i ij \equiv \pm r_j ij \pmod{p} \implies j \equiv \pm i \pmod{p} \implies i = j, \text{pois } 1 \leq i, j \leq \frac{p-1}{2}.$$

Logo, $S \equiv \sum_{i=1}^{\frac{p-1}{2}} i^2 \pmod{p}$ e como $\sum_{i=1}^{\frac{p-1}{2}} i^2 = \frac{p(p^2-1)}{24}$ (haja vista que $\sum_{i=1}^{n} i^2 = \frac{n(n-1)(2n+1)}{6}$) é, portanto, um múltiplo de p, pois $(p, 24) = 1$ (já que p é primo maior ou igual a 5 e os fatores primos de 24 são 2 e 3), então S é múltiplo de p. □

1.3.3 Ordem Módulo n

Sabemos, pelo teorema de Euler, que existe um $k \in \mathbb{N}$, tal que $a^k \equiv 1 \pmod{n}$, se $k = \varphi(n)$, $a, n \in \mathbb{Z}$, $n > 1$ e a é coprimo com n. Mas, isso não quer dizer, necessariamente, que k é o menor número que torna a congruência acima verdadeira. Daí surge a motivação para a definição a seguir.

Definição 1.32. Dados $a, n \in \mathbb{Z}$ coprimos, com $n > 1$, a ordem de a, módulo n, denotada $\text{ord}_n\ (a)$, é o menor $h \in \mathbb{N}$ para o qual

$$a^h \equiv 1 \pmod{n}.$$

Disso, conclui-se que $h = \text{ord}_n\ (a) \leq \varphi(n)$, nem sempre ocorrendo a igualdade. A proposição seguinte estabelece algumas propriedades elementares do número h.

Proposição 1.33. *Sejam $a, n \in \mathbb{Z}$, com $n > 1$ e $(a, n) = 1$.*
(a) Se $ord_n\ (a) = h$, então os inteiros $1, a, a^2, ..., a^{h-1}$ são, dois a dois, incongruentes, módulo n. Assim, se $ord_n\ (a) = \varphi(n)$, então o conjunto $\{1, a, a^2, ..., a^{\varphi(n)-1}\}$ é um sistema completo de invertíveis módulo n.
(b) $a^k \equiv 1\ (mod\ n) \iff ord_n\ (a) \mid k$. Portanto, $ord_n\ (a) \mid \varphi(n)$.

Dizemos que os números inteiros $b_1, b_2, ..., b_{\varphi(n)}$ formam um sistema completo de invertíveis módulo n se, e somente se, $(b_i, n) = 1$ para todo i e $b_i \equiv b_j \pmod{n}$ implica $i = j$.

Demonstração. (a) Considerando que existissem dois inteiros k e l, com $0 \leq k < l < h$ tais que $a^l \equiv a^k \pmod{n}$, então teríamos que $a^{l-k} \equiv 1 \pmod{n}$, com $0 < l - k < h$. Mas isso contrariaria a definição 1.32. Consequentemente, se $h = \varphi(n)$, então o conjunto $\{1, a, a^2, ..., a^{\varphi(n)-1}\}$ tem $\varphi(n)$ inteiros primos com n e dois a dois incongruentes módulo n, portanto é um sistema completo de invertíveis (sci) módulo n.
(b) Sendo $\text{ord}_n\ (a) = h$, então $a^h \equiv 1 \pmod{n}$. Se $k = hq$, então

$$a^k = a^{hq} = (a^h)^q \equiv 1^q \equiv 1 \pmod{n}.$$

Reciprocamente, sendo $k \in \mathbb{N}$ tal que $a^k \equiv 1 \pmod{n}$, pelo algoritmo da divisão, temos que existem inteiros q e r, com $0 \leq r < h$, tais que $k = hq + r$. Desta forma, temos

$$1 \equiv a^k = a^{hq+r} = (a^h)^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r \pmod{n}.$$

Se $r > 0$, teremos $a^r \equiv 1 \pmod{n}$, mas r é um inteiro positivo menor que h e isto contraria a definição 1.32. Logo, $r = 0$ e então $h|k$, ou seja, $\text{ord}_n\ (a) \mid k$.
Finalmente, considerando $k = \varphi(n)$, o teorema de Euler e a primeira parte deste item (b), concluímos que $\text{ord}_n\ (a) \mid \varphi(n)$. □

E não fica por aí, a proposição a seguir nos aponta outras propriedades úteis da ordem módulo n de inteiros.

Proposição 1.34. *Sejam a e n inteiros coprimos, com $n > 1$.*
(a) $ord_n\ (a) = ord_n\ (a+n)$.
(b) Se $t > 1$ é um natural tal que $t|n$, então $ord_t\ (a) \mid ord_n\ (a)$.
(c) Se $ord_n\ (a) = h$ e k é natural, então $ord_n\ (a^k) = \frac{h}{(h,\ k)}$.
(d) Se k é natural, então $ord_n\ (a^k) = ord_n\ (a) \iff (ord_n\ (a),\ k) = 1$.
(e) Se $ord_n\ (a) = h$, então o conjunto $\{a, a^2, ..., a^h\}$ tem exatamente $\varphi(h)$ elementos com ordem h módulo n.

Demonstração. (a) Sabemos que $a \equiv a+n \pmod{n}$ e, assim, $a^k \equiv (a+n)^k \pmod{n}$ para todo $k \in \mathbb{N}$. Daí, $a^k \equiv 1 \pmod{n}$ se, e somente se, $(a+n)^k \equiv 1 \pmod{n}$ e, desta forma, a e $a+n$ têm ordens iguais, módulo n.
(b) Como t divide n, se $a^h \equiv 1 \pmod{n}$, então $a^h \equiv 1 \pmod{t}$. Em particular, como $a^h \equiv 1 \pmod{n}$ quando $h = \text{ord}_n\ (a)$, temos que $a^{\text{ord}_n\ (a)} \equiv 1 \pmod{t}$. O item (b) da proposição 1.33 garante que $\text{ord}_t\ (a) \mid \text{ord}_n\ (a)$.
(c) Sendo $d = (h, k)$. Pelo item (b) da proposição 1.33, temos

$$(a^k)^j \equiv 1 \pmod{n} \iff a^{kj} \equiv 1 \pmod{n} \iff h|kj \iff \frac{h}{d}|\frac{k}{d} \cdot j \iff \frac{h}{d}|\ j.$$

Portanto, é imediato que

$$\text{ord}_n\ (a^k) = \frac{h}{d} = \frac{h}{(h,k)}.$$

(d) Segue de (c).
(e) Pelo item (d), o número de expoentes $1 \leq k \leq h$ tais que a^k tem ordem h módulo n é igual ao número de tais expoentes coprimos com h, ou seja, é igual a $\varphi(h)$. □

Exemplo 1.35. Façamos $a = 5$ e $n = 16$, assim teremos:
(a) $5^1 \equiv 5 \pmod{16}$ e $21^1 \equiv 5 \pmod{16}$;
$5^2 \equiv 9 \pmod{16}$ e $21^2 \equiv 9 \pmod{16}$;
$5^3 \equiv 13 \pmod{16}$ e $21^3 \equiv 13 \pmod{16}$;
$5^4 \equiv 1 \pmod{16}$ e $21^4 \equiv 1 \pmod{16}$.
Assim, $\text{ord}_{16}\ (5) = \text{ord}_{16}\ (21) = 4$.
(b) Consideremos, agora, $t = 8$, assim:
$5^1 \equiv 5 \pmod{8}$;
$5^2 \equiv 1 \pmod{8}$, portanto, $\text{ord}_8\ (5) = 2$. Logo, $\text{ord}_8\ (5) \mid \text{ord}_{16}\ (5)$.
(c) Fazendo $k = 6$, teremos $a^k = 5^6 = 15625$, daí:
$15625^1 \equiv 9 \pmod{16}$;
$15625^2 \equiv 1 \pmod{16}$.
Como $(16, 6) = 2$ e $\text{ord}_{16}\ (15625) = 2$, temos que $\text{ord}_{16}\ (15625) = 2 = \frac{4}{2} = \frac{\text{ord}_{16}\ (5)}{(\text{ord}_{16}\ (5),\ 6)}$.
(d) Fazendo $k = 3$, teremos $a^k = 5^3 = 125$, daí:

$125^1 \equiv 13 \pmod{16}$;
$125^2 \equiv 9 \pmod{16}$;
$125^3 \equiv 5 \pmod{16}$;
$125^4 \equiv 1 \pmod{16}$.
Ou seja, $\text{ord}_{16}\ (5^3) = \text{ord}_{16}\ (5) = 4 = \frac{4}{1} = \frac{\text{ord}_{16}\ (5)}{(\text{ord}_{16}\ (5),\ 3)}$.

1.3.4 Outros Testes de Primalidade

Veremos a seguir outros testes de primalidade, além do teste clássico usando congruência, tais como o teste probabilístico de Miller-Rabin, testes baseados em fatorações de $n-1$ e o teste de Agrawal, Kayal e Saxena, com ênfase neste último.

> Com o advento dos computadores, a partir da década de 60, surgiram inúmeras tentativas de se obter um algoritmo eficiente para o teste de primalidade de um número. A relevância desse problema tem crescido imensamente em anos recentes devido à utilização intensa de números primos em algoritmos de criptografia, como os algoritmos RSA e El Gamal para criptografia pública. Dessa forma o problema do teste de primalidade se tornou um importante problema para a ciência da computação teórica. (MARTINEZ et al., 2018).

Mas, é preciso ter certeza que o algoritmo funciona e, além disso, considerar a eficiência do algoritmo, que está relacionada com o uso dos recursos computacionais usados pelo algoritmo, tais como o tempo ou número de passos executados e a memória utilizada.

1.3.4.1 Teste Probabilístico de Miller-Rabin

Para começarmos, precisamos saber o que são pseudoprimos.

Definição 1.36. Dados b e n inteiros, com n composto, se $(b,n) = 1$ e $b^{n-1} \equiv 1 \pmod{n}$, dizemos que n é um pseudoprimo na base b.

Em outras palavras, pseudoprimos são números compostos que satisfazem o pequeno teorema de Fermat em alguma base b.

Proposição 1.37. *Sendo $a > 1$ e natural, $p > 2$ primo e p não divide $a^2 - 1$, então*

$$n = \frac{a^{2p}-1}{a^2-1} = \frac{a^p-1}{a-1} \cdot \frac{a^p+1}{a+1}$$

é um pseudoprimo na base a.

Demonstração. Sendo $a+1$ e $a-1$ inversíveis módulo p e $a^p \equiv a \pmod{p}$ temos, pelo pequeno teorema de Fermat, que

$$\frac{a^p-1}{a-1} \equiv \frac{a^p+1}{a+1} \equiv 1 \pmod{p}$$

e podemos verificar facilmente que estes números são ímpares, daí $n \equiv 1 \pmod{2p}$, ou seja, $n = 2kp + 1$ para k inteiro. Portanto, como $a^{2p} \equiv 1 \pmod{n}$ temos $a^n = a^{2kp+1} = (a^{2p})^k \cdot a \equiv a \pmod{n}$. □

É interessante destacar o fato de que existem alguns raros números compostos n com a propriedade de que se $0 < a < n$ e $(a, n) = 1$ então $a^{n-1} \equiv 1 \pmod{n}$, conhecidos como números de Carmichael. Os primeiros números de Carmichael são 561, 1105, 1729, 2465 e 2821. Isto é, os números de Carmichael são números compostos n tais que se tomarmos qualquer número natural a menor que n com o mdc entre a e n igual a 1, então $a^{n-1} \equiv 1 \pmod{n}$. Tomemos um exemplo: $561 = 3 \cdot 11 \cdot 17$, assim qualquer número natural menor que 561, que não seja múltiplo de 3, 11 ou 17, será congruente a 1 módulo 561 quando elevado a 560, logo $2^{560} \equiv 1 \pmod{561}$; $5^{560} \equiv 1 \pmod{561}$; $7^{560} \equiv 1 \pmod{561}$; $13^{560} \equiv 1 \pmod{561}$; etc.

> Podemos refinar o conceito de pseudoprimo para definir pseudoprimos fortes na base a. Para definir quando n é um pseudoprimo forte na base a inicialmente escrevemos $n - 1 = 2^k \cdot b$, com b ímpar. Se $n > 2$ é primo deve existir um menor valor de j para o qual $(a^b)^{2^j} \equiv 1 \pmod{n}$ (observe que por Fermat $(a^b)^{2^k} \equiv 1 \pmod{n}$). Se $j = 0$ isto significa que $a^b \equiv 1 \pmod{n}$; caso contrário temos $(a^b)^{2^{j-1}} \equiv -1 \pmod{n}$ já que -1 é o único valor de x diferente de 1 (módulo n) para o qual $x^2 \equiv 1 \pmod{n}$. Assim, dizemos que n composto ímpar é um pseudoprimo forte na base a se ou $a^b \equiv 1 \pmod{n}$ ou existe $j' < k$ com $(a^b)^{2^{j'}} \equiv -1 \pmod{n}$. Claramente todo pseudoprimo forte na base a é um pseudoprimo na base a mas pseudoprimos fortes são mais raros do que pseudoprimos. (MARTINEZ et al., 2018).

Teorema 1.38. *Se*

$$\alpha(n) = \tfrac{1}{\varphi(n)} \, |\{a \mid 0 < a < n, \ n \text{ é um pseudoprimo forte na base } a\}|.$$

Então para todo número composto ímpar $n > 9$ temos $\alpha(n) \leq 1/4$. A igualdade vale exatamente para os compostos n das seguintes formas:
$n = p_1 p_2$, p_1, p_2 primos, $p_1 \equiv 3 \pmod 4$, $p_2 = 2p_1 - 1$;
$n = p_1 p_2 p_3$, p_1, p_2, p_3 primos, $p_i \equiv 3 \pmod 4$, n número de Carmichael.

Uma demonstração desse teorema pode ser encontrada em (MARTINEZ et al., 2018).
O teste probabilístico de Miller-Rabin é baseado no teorema acima e consiste em

> Dado n, tomamos t valores de a ao acaso no intervalo $1 < a < n$ e verificamos para cada a se n passa no teste de primalidade na base a. Se n for ímpar composto, a probabilidade de que um dado a acuse a não-primalidade de n é maior do que 3/4 (pelo teorema); assim, a probabilidade de que n escape a t testes é menor do que 4^{-t}. (MARTINEZ et al., 2018).

1.3.4.2 Testes de Primalidade Baseados em Fatorações de $n - 1$

O teste comentado acima, como o próprio nome diz e como colocado no último parágrafo da subseção anterior, é um teste probabilístico, ou seja, ele nos dá a probabilidade

de um dado número n ser primo. Contudo, um teste com resultado mais afirmativo, ou melhor, determinístico, é bem mais interessante. Nessa categoria encaixam-se os próximos testes apresentados aqui. Comecemos pelos testes de primalidade baseados em fatorações de $n-1$.

Proposição 1.39. *Sendo $n > 1$. Se para cada fator primo p de $n-1$ existe um inteiro a_p tal que $a_p^{n-1} \equiv 1 \ (mod\ n)$ e $a_p^{(n-1)/p} \not\equiv 1 \ (mod\ n)$ então n é primo.*

Demonstração. Sendo p^{k_p} a maior potência de p que divide $n-1$. Desta forma, a ordem de a_p em $(\mathbb{Z}/(n))^\times$ será um múltiplo de p^{k_p}, daí $\varphi(n)$ será um múltiplo de p^{k_p}. Como isto vale para qualquer fator primo p de $n-1$, então $\varphi(n)$ será um múltiplo de $n-1$ e, portanto, n será primo. □

Isto quer dizer que, se n é primo e $n-1$ tem, por exemplo, três fatores primos p_1, p_2 e p_3, então existem pelo menos três números inteiros a_{p_i} tais que $a_{p_i}^{(n-1)/p_i} \not\equiv 1 \pmod{n}$, isto é, se testarmos três números naturais e eles satisfizerem as condições postas, então n é primo. Porém, se forem testados três números inteiros e eles passarem na primeira condição (pequeno teorema de Fermat) mas não passarem na segunda, isto não quer dizer que n não é primo, pois podem existir outros números que satisfaçam as condições.
Tomemos dois exemplos:

Exemplo 1.40. $n = 15 \ \Rightarrow \ n - 1 = 14 = 2 \cdot 7$ (dois fatores primos).

a_p	a_p^{14} módulo 15	a_p^{7} módulo 15	a_p^{2} módulo 15
1	1	1	1
2	4	8	4
3	9	12	9
4	1	4	1
5	10	5	10
6	6	6	6
7	4	13	4
8	4	2	4
9	6	9	6
10	10	10	10
11	1	11	1
12	9	3	9
13	4	7	4
14	1	14	1

Podemos ver que não há como selecionar dois números de tal forma que as condições postas na proposição sejam satisfeitas, portanto, 15 não é primo. É interessante observar que só

precisamos fazer essa verificação de 1 até $n-1$, pois $n+a \equiv a \pmod{n}$ e, consequentemente, $(n+a)^t \equiv a^t \pmod{n}$.

Exemplo 1.41. $n = 13 \Rightarrow n - 1 = 12 = 2^2 \cdot 3$ (dois fatores primos).

a_p	a_p^{12} módulo 13	a_p^6 módulo 13	a_p^4 módulo 13
1	1	1	1
2	1	12	3
3	1	1	3
4	1	1	9
5	1	12	1
6	1	12	9
7	1	12	9
8	1	12	1
9	1	1	9
10	1	1	3
11	1	12	3
12	1	1	1

Neste caso, usando o 2 e qualquer outro número da tabela, com exceção do 1 e do 12, além de outras combinações, teremos as condições da proposição satisfeitas, logo o número 13 é primo.

Proposição 1.42 (Pocklington)**.** *Se $n-1 = p^k R$ onde p é primo e existe um inteiro a tal que $a^{n-1} \equiv 1 \pmod{n}$ e $(a^{(n-1)/p} - 1,\ n) = 1$ então qualquer fator primo de n é congruente a 1 módulo p^k.*

Demonstração. Seja q um fator primo de n, então $a^{n-1} \equiv 1 \pmod{q}$ e q não divide $a^{(n-1)/p} - 1$, daí $ord_q\ a$ divide $n-1$ mas não divide $(n-1)/p$. Portanto, $p^k | ord_q\ a | q-1$, logo $q \equiv 1 \pmod{p^k}$. □

Nesta proposição não é necessário conhecermos a fatoração completa de $n-1$, se obtivermos um fator primo p de $n-1$ com seu respectivo expoente k e se existir um inteiro a tal que $a^{n-1} \equiv 1 \pmod{n}$ e o mdc entre $a^{(n-1)/p} - 1$ e n é 1, então qualquer fator primo p' de n satisfaz a congruência $p' \equiv 1 \pmod{p^k}$.

Exemplo 1.43. Fazendo $n = 85$ temos que:
$n = 85 = 5 \cdot 17$ e $n-1 = 84 = 2^2 \cdot 3 \cdot 7$, assim, considerando $p = 2$, teremos $13^{84} \equiv 1 \pmod{85}$ e $(13^{42} - 1,\ 85) = 1$, portanto, pela proposição devemos ter todos os fatores primos de $n = 85$ congruentes a 1 módulo 2^2, que pode ser confirmado no nosso exemplo, pois $5 \equiv 1 \pmod{2^2}$ e $17 \equiv 1 \pmod{2^2}$.

Corolário 1.44. *Se $n-1 = FR$, com $F > R$ e para todo fator primo p de F existe $a > 1$ tal que $a^{n-1} \equiv 1 \pmod{n}$ e $(a^{(n-1)/p} - 1, n) = 1$ então n é primo.*

Demonstração. Sendo p um fator primo de F e p^k a maior potência de p que divide F, então, todo fator primo de n deve ser congruente a 1 módulo p^k. Como isto vale para todo fator primo de F, segue que todo fator primo de n deve ser congruente a 1 módulo F. Como $F > R$, então $F > \sqrt{n}$, isto implica que n é primo. □

Ou, de outra forma, sendo $n - 1 = p_1 \cdot p_2 \cdots p_r$, p_i primo, se escolhermos alguns fatores primos de $n-1$, tais que o produto desses fatores seja maior que a raiz quadrada de $n-1$ e a proposição anterior ocorrer com cada um desses fatores, então n é primo.

Exemplo 1.45. Fazendo $n = 31$, então $n - 1 = 30 = 6 \cdot 5$. Os fatores primos de 6 (6 é maior que a raiz quadrada de 30) são 2 e 3 e temos $11^{30} \equiv 1 \pmod{31}$ e $(11^{15} - 1, 31) = 1$ e, ainda, $5^{30} \equiv 1 \pmod{31}$ e $(5^{10} - 1, 31) = 1$, assim, 31 é primo.

Fermat acreditava que todo número da forma $F_n = 2^{2^n} + 1$ fosse primo e verificou isso até F_4, porém Euler mostrou que F_5 não é primo e já se sabe que F_n é composto para vários outros valores de n. Além de F_0, F_1, F_2, F_3 e F_4 nenhum outro primo da forma $F_n = 2^{2^n} + 1$ é conhecido. O teste a seguir mostra como verificar se F_n é primo.

Corolário 1.46 (Teste de Pépin)**.** *Sendo $F_n = 2^{2^n} + 1$, F_n é primo se, e somente se, $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.*

Este corolário é uma aplicação da proposição 1.39 aos números de Fermat, pois $F_n - 1 = 2^{2^n} + 1 - 1 = 2^{2^n}$ que possui apenas um fator primo e, portanto, de acordo com a proposição mencionada, basta um número inteiro que elevado a $F_n - 1$ seja congruente a 1 e elevado a $(F_n - 1)/2$ não seja congruente a 1, mas de forma mais restrita, pois considera $p = 2$, e com a recíproca sendo verdadeira também, nesse caso. Como pode ser visto na demonstração desse corolário encontrada em (MARTINEZ et al., 2018), se F_n é primo então $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$, e, consequentemente, $3^{F_n-1} = (3^{(F_n-1)/2})^2 \equiv (-1)^2 \equiv 1 \pmod{F_n}$, o que não acontece com alguns outros primos, que sendo p primo pode ocorrer $3^{(p-1)/2} \equiv 1 \pmod{p}$.

Corolário 1.47 (Teorema de Proth)**.** *Sendo $n = h \cdot 2^k + 1$, com $2^k > h$, então n é igual a um p primo se, e somente se, existe um inteiro a com $a^{(n-1)/2} \equiv -1 \pmod{n}$.*

Como no caso anterior, este corolário é um caso mais restrito do corolário 1.44 e, também, com a afirmação de que a recíproca é verdadeira. A demonstração deste e do próximo corolário também podem ser vistas em (MARTINEZ et al., 2018).

Corolário 1.48. *Sendo $n = h \cdot p^k + 1$ com p primo e $p^k > h$, então $n = q$, q primo, se, e somente se, existe um inteiro a com $a^{n-1} \equiv 1 \ (mod\ n)$ e $(a^{(n-1)/p} - 1,\ n) = 1$.*

Aqui, temos mais uma vez um caso restrito do corolário 1.44, já que estamos considerando $F = p^k$, ou seja, F possui apenas um fator primo, mas com o complemento de que a recíproca também é verdadeira.

1.3.4.3 Teste de Agrawal, Kayal e Saxena

Você, leitor, deve ter notado que todos os testes de primalidade vistos aqui baseiam-se no pequeno teorema de Fermat, isto é, no fato de que p é primo se, e somente se, $a^{p-1} \equiv 1 \pmod{p}$ para todo a inteiro e $1 \leq a < p$. Percebamos que há casos em que temos um número n composto e obtemos $a^{n-1} \equiv 1 \pmod{n}$, mas isso não ocorre para todo $1 \leq a < n$ como no caso dos primos.
O algoritmo AKS também não foge do pequeno teorema de Fermat. Para começo de conversa, consideremos uma variável x, um inteiro a e um número primo p. Com base no binômio de Newton temos que

$$(x + a)^p = \sum_{i=0}^{p} \left(\begin{array}{c} p \\ i \end{array} \right) x^{p-i} a^i,$$

entretanto, nos casos em que i é diferente de 0 e p, o coeficiente binomial $\binom{p}{i}$ é divisível por p, como pode ser verificado facilmente, já que p não tem nenhum divisor menor que ele, exceto o 1, portanto todos os termos que não sejam extremos do desenvolvimento binomial são divisíveis por p, assim

$$(x + a)^p \equiv x^p + a^p \equiv x^p + a \pmod{p}$$

observe que na última congruência foi usado o pequeno teorema de Fermat. Podemos então considerar que se $(x + a)^N \equiv x^N + a \pmod{N}$ para todo $a < N$, então fazendo $a = 1$ temos que N divide todos os coeficientes binomiais $\binom{N}{i}$ com $0 < i < N$. Por outro lado, se N fosse composto e q um fator primo de N, então

$$\left(\begin{array}{c} N \\ q \end{array} \right) = \frac{N(N-1)...(N-q+1)}{q(q-1)...1}.$$

Portanto, os únicos termos que são divisíveis por q nesta expressão são o N no numerador e o q no denominador, logo, se q^k é a maior potência de q que divide N, então $q^k \nmid \binom{N}{q}$, logo $p \nmid \binom{N}{q}$, absurdo. Assim, N é primo. Com isto obtemos outro critério de primalidade:

$$N \text{ é primo} \iff (x + a)^N \equiv x^N + a \pmod{N}, \text{ para todo}$$
$$a < N \iff (x + a)^N \equiv x^N + a \pmod{N}, \text{ para algum } a < N, \text{ com } (a, N) = 1.$$

É importante observar que se $(x+a)^N$ e x^N+a são iguais módulo N, então eles deixam o mesmo resto módulo N quando divididos por qualquer outro polinômio. Consideremos, então, o polinômio x^r-1 e, assim teremos que

$$N \text{ é primo} \Longrightarrow (x+a)^N \equiv x^N + a \pmod{x^r-1, N} \text{ para todo } a < N,\ r \in \mathbb{N}.$$

> O fato importante, mostrado por Agrawal, Kayal e Saxena, é que para garantir a primalidade de N só precisamos testar que esta congruência é válida para um valor especial de r (na versão original um r primo para o qual $r-1$ tem um fator primo $q \geq 4\sqrt{r}\log N$, o qual divide a ordem de n módulo r) que depende polinomialmente de $\log N$ e alguns poucos valores de a. (MARTINEZ et al., 2018).

A versão original do AKS foi feita utilizando um teorema devido a Fouvry e considerava a existência de um r da ordem $O((\log_2 N)^6)$. Aqui será exposta uma versão modificada da simplificação do AKS original feita por H. Lenstra, na qual não é necessário usar o teorema de Fouvry.

Teorema 1.49 (Agrawal, Kayal, Saxena, Lenstra)**.** *Sejam $N, r, v \in \mathbb{Z}$ e maiores que 1, com r uma potência de primo. Seja $S \subset \mathbb{N}$ um conjunto finito com s elementos menores que N. Vamos supor que*
i. N e r são coprimos e a ordem de N módulo r é v, ou seja, v é o menor valor tal que $N^v \equiv 1 \pmod{r}$.
ii. $(N, a-b) = 1$ para quaisquer $a, b \in S$, $a \neq b$.
iii. $\binom{s+t-1}{s} \geq N^{\sqrt{t/2}}$ para todo t divisor de $\varphi(r)$ que seja múltiplo de v.
iv. $(x+a)^N \equiv x^N + a \pmod{x^r-1, N}$ para todo $a \in S$.
Então N é potência de um primo.

Para maiores detalhes, pode-se consultar a demonstração desse teorema contida em (MARTINEZ et al., 2018).

Lema 1.50. *Seja $N \geq 9$ um inteiro, existe uma potência de primo r menor do que $(\log_2 N)^5$ tal que $v = ord_r\ N > \frac{1}{2}(\log_2 N)^2$.*

Demonstração desse lema também pode ser encontrada em (MARTINEZ et al., 2018). Após o trabalho de M. Agrawal, N. Kayal e N. Saxena, Pomerance e Lenstra obtiveram um algoritmo de complexidade $\tilde{O}((\log\ N)^6)$ que trabalha com polinômios mais gerais.

> O algoritmo AKS é interessante do ponto de vista teórico, já que mostrou que o problema de determinar a primalidade de um número está na classe P, mas na prática o tempo de processamento é muito inferior com relação aos algoritmos probabilísticos clássicos, tais como Miller-Rabin e Solovay-Strassen, que são altamente eficientes e amplamente usados

> nos métodos de criptografia." [...] "Por outro lado, caso a Hipótese de Riemann Generalizada seja verdadeira, o teste de Miller-Rabin torna-se um teste determinístico, mas esta conjectura ainda está em aberto. (MARTINEZ et al., 2018).

As demonstrações e descobertas matemáticas das últimas décadas, em geral, envolvem "uma seção transversal expressiva da matemática contemporânea, de modo que não são acessíveis, senão ao especialista"(COUTINHO, 2004). Mas isto não acontece com o algoritmo AKS.

> Isto explica o enorme impacto produzido na comunidade matemática pela descoberta de um algoritmo polinomial de primalidade por Agrawal, Kayal e Saxena. Eles não apenas resolveram, de maneira brilhante, um problema que está conosco há milênios, como a solução é tão simples que pode ser compreendida por um estudante de graduação em matemática ou ciência da computação. (COUTINHO, 2004).

Em outras palavras, computacionalmente o teste de Miller-Rabin é mais vantajoso que o teste AKS, contudo o primeiro é probabilístico enquanto que o segundo é determinístico. Porém se a Hipótese de Riemann Generalizada for provada, o teste de Miller-Rabin, que é baseado nessa hipótese, se tornará determinístico e, portanto, mais apropriado, pelo menos para os números que são trabalhados hoje em criptografia.
Quem desejar se aprofundar nesse tema pode consultar (COUTINHO, 2004), entre outras obras.

2 Números Primos Particulares

Quando estamos em sala de aula, ensinando algum processo para resolver um determinado problema matemático que, a princípio, parece ser difícil de se entender, os alunos, em muitos casos, logo perguntam se não tem uma maneira mais fácil, ou se existe uma fórmula para ser aplicada que possa dar a resposta de forma mais rápida. Apesar de um matemático profissional estar interessado nas correlações existentes entre os entes matemáticos e em propriedades desses entes, eles também têm interesse na descoberta de fórmulas.
Um dos sonhos dos matemáticos que trabalham com a Teoria dos Números é encontrar uma fórmula simples que gere todos os números primos, mas até o momento essa fórmula não foi descoberta, apesar dos esforços de muitos e grandes matemáticos. Assim, se encontrar uma fórmula simples que gere todos os números primos é muito difícil, os matemáticos buscam fórmulas que deem pelo menos uma lista de primos. Com esse intuito, alguns matemáticos conseguiram obter algum êxito. Neste capítulo veremos algumas dessas fórmulas, sem, contudo, nos atermos a maiores detalhes, pois, se assim o fizéssemos, fugiríamos do foco desse trabalho.

2.1 Os Números de Fermat

Os números da forma $2^m + 1$ sempre foram muito pesquisados e Pierre de Fermat acreditava que todos os números da forma $2^{2^n} + 1$, isto é, $m = 2^n$, com n inteiro e $n \geq 0$, eram primos. Contudo, ele estava errado. Seu erro é justificado pelo fato de que os números dessa forma crescem rapidamente e, assim, o sexto número dessa sequência, ou seja, quando $n = 5$ já é 4.294.967.297 (que inclusive é o primeiro número de Fermat não primo, pois é igual a $641 \cdot 6.700.417$), o que tornava os cálculos, de verificação se os números obtidos eram primos, demorados, ou até mesmo impossíveis, na época de Fermat.
Os quatro primeiros números de Fermat são: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$ e $F_3 = 257$. Algumas propriedades dos números de Fermat, são as seguintes:

- Um número de Fermat é igual ao produto de todo os anteriores, mais 2 unidades;
- Todo número de Fermat composto pode ser fatorado em fatores na forma $k \cdot 2^{n+1} + 1$, com k inteiro positivo;
- Dois números de Fermat distintos são coprimos;
- Se F_n é um número primo, então o polígono regular de F_n lados pode ser construído usando-se régua e compasso.

> O resultado que talvez mais tenha contribuído para que os números de Fermat adquirissem uma certa notoriedade foi a descoberta por Gauss em 1796, de que uma circunferência pode ser dividida (com régua e compasso) em n partes iguais, se e somente se $n = 2^m \cdot p_1 p_2 \cdots p_k$ onde m é um natural e $p_1 p_2, ..., p_k$ são primos de Fermat distintos. (LEITE, 1986).

Não se conhece outros números de Fermat primos, além de F_0, F_1, F_2, F_3 e F_4, então há algumas perguntas esperando por resposta, como:

- F_n é composto para todos $n > 4$?
- Existem infinitos números de Fermat primos?
- Existem infinitos números de Fermat compostos?

2.2 Os Números de Mersenne

Os números de Mersenne, representados por M_q, são os números da forma $M_q = 2^q - 1$ com q primo e seus estudos foram motivados pelo estudo dos números perfeitos. "Euclides demonstrou, nos Elementos, Livro IX, proposição 36, que se q é primo e $M_q = 2^q - 1$ é primo, então $n = 2^{q-1}(2^q - 1)$ é um número perfeito" (RIBENBOIM, 2014). "Dizemos que um número n é perfeito se ele for igual à soma de seus divisores próprios, i.e., dos divisores positivos menores do que n." (SANTOS, 2018). Esses números são chamados de números de Mersenne em homenagem a Marin Mersenne, matemático francês que compilou uma lista de primos dessa forma até $n = 257$. Entretanto, posteriormente verificou-se que a lista de Mersenne estava incorreta, pois ele havia omitido M_{61}, M_{89} e M_{107}, que são primos, e havia incluído M_{67} e M_{257}, que são compostos.

Em artigo publicado postumamente, Euler demonstrou a recíproca da proposição de Euclides, ou seja, se $n = 2^{q-1}(2^q - 1)$ é um número perfeito par, então q é primo e $M_q = 2^q - 1$ é primo. Assim, os números perfeitos pares estão diretamente ligados aos números primos de Mersenne.

Já na época de Mersenne, sabia-se que alguns números de Mersenne são primos e que outros são compostos. Os quatro primeiros números de Mersenne são: $M_2 = 3$, $M_3 = 7$, $M_5 = 31$ e $M_7 = 127$.

Na criptografia são usados números primos gigantes, com milhares de dígitos, e os números de Mersenne são bastante utilizados para se encontrar primos desse tipo (gigantes), verificando-se a primalidade dos números de Mersenne por meio do teste de Lucas-Lehmer. O maior número de Mersenne primo descoberto até o momento é $2^{82589933} - 1$, um número com 24862048 dígitos, descoberto pelo projeto Great Internet Mersenne Prime Search (GIMPS), em dezembro de 2018, sendo este o 51º número primo de Mersenne. Um resultado sobre os números de Mersenne diz que se $2^n - 1$ é primo, então n também

é um número primo, pois se não o fosse, então $n = ab$, com $1 < a, b < n$ e, assim, $x^n - 1 = x^{ab} - 1 = (x^b - 1)(x^{b(a-1)} + x^{b(a-2)} + ... + x^{2b} + x^b + 1)$, ou seja, $x^n - 1$ teria outros dois fatores além de 1 e ele mesmo. Também devemos observar que se $x^n - 1$ é primo, então x só pode ser igual a 2, tendo em vista que $x^n - 1$ é divisível por $x - 1$ que, portanto, por definição, deve ser igual a 1. A pergunta se existem finitos ou infinitos primos de Mersenne ainda é uma questão em aberto na Matemática.

2.3 Os Números Primos de Sophie Germain

Um número p primo, é um primo de Sophie Germain se $2p + 1$ também é um número primo. Acredita-se que exista uma quantidade infinita de números primos de Sophie Germain, todavia, ainda não há uma demonstração dessa conjectura.
Os doze primeiros números primos de Sophie Germain são: 2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113 e 131.
Os números primos de Sophie Germain ficaram famosos porque Sophie Germain provou que o Último Teorema de Fermat é verdadeiro para esses números.

> Germain desenvolveu um argumento elegante para demonstrar que provavelmente não existem soluções para $x^n + y^n = z^n$ para valores de n iguais a esses primos de Germain. Com o 'provavelmente' ela queria dizer que era improvável existirem soluções porque se existisse uma solução então x, y e z seriam múltiplos de n e isso colocaria uma séria restrição em qualquer solução. Seus colegas examinaram sua lista de primos um por um, tentando provar que x, y ou z poderiam não ser múltiplos de n e acabaram demonstrando que para aqueles valores particulares de n não havia soluções. (SINGH, 1999).

O maior número primo de Sophie Germain conhecido até o momento é $183027 \cdot 2^{265440} - 1$ que tem 79911 dígitos, descoberto em março de 2010. Uma sequência $\{p, 2p+1, 2(2p+1)+1, ...\}$ de primos de Sophie Germain é chamada de cadeia de Cunningham de primeira classe.

2.4 Os Números Primos de Wieferich

Um número primo p que satisfaça a congruência

$$2^{p-1} \equiv 1 \pmod{p^2}$$

é chamado primo de Wieferich. Observemos que $2^{p-1} \equiv 1 \pmod{p}$ é satisfeita para todo p primo ímpar, no entanto, a congruência $2^{p-1} \equiv 1 \pmod{p^2}$ é raramente verificada. Meissner, em 1913, e Beeger, em 1922, descobriram que os primos 1093 e 3511 satisfazem a congruência de Wieferich. Estes são os dois únicos primos de Wieferich conhcecidos até hoje. Em 1909, Wieferich demonstrou o seguinte teorema:

Teorema 2.1. *Seja p um número primo e sejam x, y e z números inteiros, de tal forma que $x^p + y^p + z^p = 0$ e, além disso, o produto $x \cdot y \cdot z$ é divisível por p, então p é um número primo de Wieferich.*

2.5 Os Números Primos de Wilson

Se p é um número primo, então $(p-1)! \equiv -1 \pmod{p}$. Este é o teorema de Wilson. Daí, $W(p)$ é o quociente de Wilson determinado por

$$W(p) = \frac{(p-1)!+1}{p}.$$

Sendo p um número primo, ele é chamado primo de Wilson quando $W(p) \equiv 0 \pmod{p}$, ou, equivalentemente,

$$(p-1)! \equiv -1 \pmod{p^2}.$$

Considerando os números naturais até $5 \cdot 10^8$, são conhecidos apenas três primos de Wilson: 5, 13 e 563.

2.6 Os Números de Sierpiński

Teorema 2.2 (Sierpiński)**.** *Existe uma infinidade de inteiros ímpares k, tais que $k \cdot 2^n + 1$ é composto para todo $n \geq 1$.*

Os números inteiros ímpares k, tais que $k \cdot 2^n + 1$ é composto para todo $n \geq 1$ natural, é dito um número de Sierpiński. O menor número de Sierpiński conhecido é 78557 e "O menor número de Sierpiński primo conhecido é $k = 271129$." (RIBENBOIM, 2014). Em março de 2002 teve início o projeto Seventeen or Bust, com o objetivo de provar que 78557 é o menor número de Sierpiński. No início do projeto haviam dezessete números menores que 78557 candidatos a serem números de Sierpiński. Até abril de 2016 o Seventeen or Bust já havia descartado onze dos candidatos, quando teve de ser interrompido por causa de uma perda de servidor. A tarefa foi então transferida para o projeto PrimeGrid (www.primegrid.com), que resolveu um décimo segundo caso, restando, hoje, apenas cinco candidatos (21181, 22699, 24737, 55459 e 67607), como também busca-se descobrir se 271129 é o menor número primo de Sierpiński.

2.7 Os Números de Riesel

Semelhante aos números de Sierpiński, temos os números de Riesel, que são os números inteiros ímpares k, tais que $k \cdot 2^n - 1$ é composto para todo inteiro $n \geq 1$. Riesel demonstrou que existe uma infinidade desses números k e, também, que existe uma infinidade de k primos.
O menor número de Riesel conhecido é $k = 509203$ (que é primo), descoberto pelo próprio Riesel, em 1956. Todavia, depois de cálculos muito trabalhosos feitos por colaboradores de L. Stephens, há 64 números menores que 509203 passíveis de serem números de Riesel.

Alguns deles são: 2293, 9221, 23669, 31859, 38473 e 40597. O projeto PrimeGrid também está responsável pela verificação desses números, como também o projeto Riesel Sieve (www.rieselsieve.com).

2.8 Os Números de Fermat Generalizados

Vimos que os números de Fermat são da forma $2^{2^n}+1$. Os números de Fermat generalizados são os números da forma $b^{2^n}+1$, com $n \geq 1$ e $b \geq 2$.

> Em artigo de 2002, Dubner e Gallot descreveram um método de computação para determinar a primaridade desses números, o qual é tão rápido quanto o método para testar a primaridade dos números de Mersenne. (RIBENBOIM, 2014).

Por meio deste processo, antes que o ano de 2002 terminasse já eram conhecidos mais de 100 números de Fermat generalizados primos com mais de 100000 algarismos. Hoje, o maior número de Fermat generalizado primo conhecido tem mais de um milhão de algarismos.

2.9 Os Números de Cullen

São chamados de números de Cullen os números da forma $Cn = n \cdot 2^n + 1$. Para todo $1 < n \leq 1000$ Cn é composto, com exceção de $C141$ que é primo, como mostrou Robinson, em 1958. Assim, dentre os 1000 primeiros números de Cullen, apenas o $C1 = 3$ e o $C141$ são primos. Os sete primeiros números de Cullen são: $C1 = 1 \cdot 2^1 + 1 = 3$, $C2 = 2 \cdot 2^2 + 1 = 9$, $C3 = 3 \cdot 2^3 + 1 = 25$, $C4 = 4 \cdot 2^4 + 1 = 65$, $C5 = 5 \cdot 2^5 + 1 = 161$, $C6 = 6 \cdot 2^6 + 1 = 385$ e $C7 = 7 \cdot 2^7 + 1 = 897$.
Os quatro primeiros números de Cullen primos são: $C1 = 1 \cdot 2^1 + 1 = 3$, $C141 = 141 \cdot 2^{141} + 1$, $C4713 = 4713 \cdot 2^{4713} + 1$ e $C5795 = 5795 \cdot 2^{5795} + 1$.

> Em 1987 (publicado em 1995), Keller determinou todos os números de Cullen primos Cn, com $n \leq 30000$. Estes cálculos foram prosseguidos por J. Young (1997) até $n \leq 100000$ e novos Cn primos foram encontrados em 1998 graças à impulsão de Y. Gallot. Dentro do projeto PrimeGrid todos os números de Cullen com $n < 7870000$ foram identificados... (RIBENBOIM, 2014).

Há indicações de que quase todos os números de Cullen são compostos.

2.10 Os Números de Woodall

São chamados números de Woodall (ou números de Cullen de segunda espécie) os números $Wn = n \cdot 2^n - 1$. Os sete primeiros números de Woodall são: $W1 = 1 \cdot 2^1 - 1 = 1$, $W2 = 2 \cdot 2^2 - 1 = 7$, $W3 = 3 \cdot 2^3 - 1 = 23$, $W4 = 4 \cdot 2^4 - 1 = 63$, $W5 = 5 \cdot 2^5 - 1 = 159$, $W6 = 6 \cdot 2^6 - 1 = 383$ e $W7 = 7 \cdot 2^7 - 1 = 895$.
Notemos que os três primeiros números de Woodall primos são: $W2 = 7$, $W3 = 23$ e $W6 = 383$.

Os únicos Wn primos, para $n \leq 20000$, são os que correspondem a $n = 2, 3, 6, 30, 75, 81$ (Riesel, 1969), 115, 123, 249, 362, 384, 462, 512, 751, 822, 5312, 7755, 9531, 12379, 15822 e 18885 (Keller, 1987). Os cálculos foram prosseguidos por J. Young até $n \leq 100000$, por Y. Gallot e seus colaboradores até $n \leq 1000000$, e o projeto PrimeGrid prosseguiu até $n < 8090000$. (RIBENBOIM, 2014).

3 A Distribuição dos Números Primos

A Matemática é de uma beleza ímpar, pelo menos essa é a opinião dos matemáticos, e seus campos de estudo são extensos e variados, como a Geometria, a Álgebra e a Teoria dos Números, com contribuições importantíssimas para chegarmos às condições de vida que temos hoje. A variedade de problemas relacionados com os números primos, estudados pela Teoria dos Números, é imensa, ou, melhor dizendo, riquíssima. Muitos já foram resolvidos e outros esperam por uma prova.
O problema mais básico sobre os números primos é em relação à infinitude dos mesmos (que já foi discutida no capítulo 2). Mas, veremos neste capítulo, outros problemas que estão relacionados com a caracterização dos primos e sua distribuição. Dentre eles, veremos conjecturas e problemas em aberto que ainda hoje provocam os matemáticos. Como, por exemplo, a distribuição e infinitude dos primos gêmeos, a também infinitude dos primos de Sophie Germain, entre outros.

3.1 O Teorema dos Números Primos

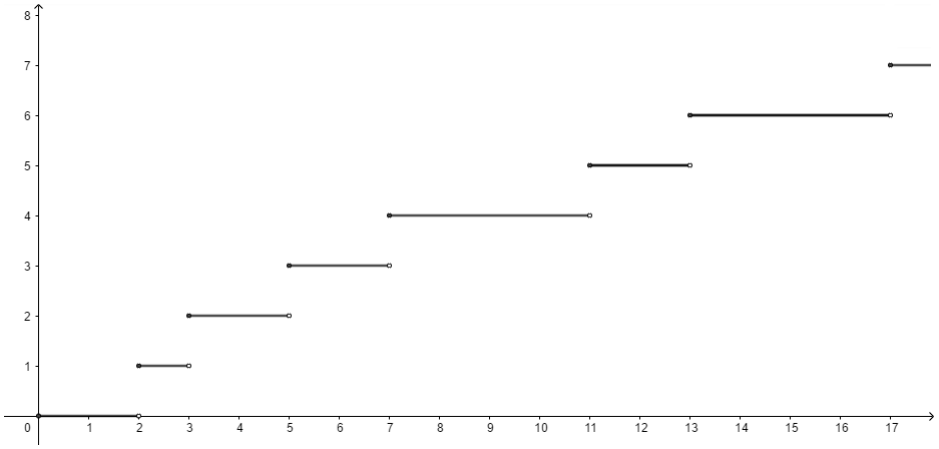
Antes de enunciarmos o teorema dos números primos é necessário que definamos a função $\pi(x)$. $\pi(x)$ é a chamada função de contagem dos números primos e, portanto, designa o número de primos p tais que $0 \leq p \leq x$.
O teorema dos números primos dá uma aproximação da quantidade de primos existentes entre 1 e um inteiro x, isto é, descreve a distribuição dos números primos. Todavia, observemos que se trata de uma aproximação que fica cada vez mais precisa quando x tende ao infinito.

Teorema 3.1 (Teorema dos Números Primos)**.**

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

"Este resultado foi conjecturado por vários matemáticos, inclusive por Legendre e Gauß, mas a demonstração completa só foi encontrada em 1896, por de la Vallée Poussin e Hadamard (independentemente)." (MARTINEZ et al., 2018).
Podemos concluir desse teorema que $\pi(x)$ tende a ficar, proporcionalmente, cada vez mais próximo a $\frac{x}{\log x}$, ao se aumentar o valor de x indefinidamente. Contudo, vale salientar que $\pi(x)$ não é uma função contínua, pois a cada x primo o valor de $\pi(x)$ aumenta em uma unidade, ou seja, o gráfico de $\pi(x)$ se apresenta com linhas horizontais que vão ficando cada vez mais elevadas a cada vez que se chega a um número primo, como podemos observar na figura seguinte.

Figura 1 – Gráfico de $\pi(x)$



Fonte: produzida pelo autor

3.2 Primos Gêmeos

Diz-se que p e q são primos gêmeos se $|p - q| = 2$, com p e q primos. Conjectura-se que hajam infinitos pares de primos gêmeos, mas ainda não se conhece uma demonstração para essa conjectura. São conhecidos pares de primos gêmeos com centenas de milhares de dígitos, como, por exemplo, $2996863034895 \cdot 2^{1290000} \pm 1$, que têm 388342 dígitos cada um. Acredita-se que $\pi_2(x)$ (número de primos gêmeos menores ou igual a x) seja assintótico a $cx/(log\ x)^2$, isto é,

$$\lim_{x\to\infty} \frac{\pi_2(x)}{cx/(\log\ x)^2} = 1$$

onde c é um número real, mas não se conhece uma demonstração.

3.3 Primos de Sophie Germain

Como já visto anteriormente, os primos de Sophie Germain são os primos p tais que $2p + 1$ também é primo.

Teorema 3.2 (Sophie Germain - Legendre)**.** *Considere p e q primos ímpares, tais que*
(a) Toda solução da congruência $x^p + y^p + z^p \equiv 0\ (mod\ q)$ satisfaz $q|xyz$;
(b) A congruência $w^p \equiv p\ (mod\ q)$ não possui solução.
Então não existem inteiros x, y, z, com $(x, y, z) = 1$ e $p \nmid xyz$, tais que $x^p + y^p + z^p = 0$.

Demonstração. Consideremos, por absurdo, que exista a solução da equação $x^p+y^p+z^p = 0$. Desta forma, temos que

$$-x^p = y^p + z^p$$

$$(-x)^p = (y + z)(y^{p-1} - y^{p-2}z + \cdots - yz^{p-2} + z^{p-1})$$

pois p é ímpar.
Devemos mostrar, agora, que os dois fatores da direita são primos entre si. Consideremos k um primo que divide ambos os termos, então

$$z + y \equiv 0 \pmod{k} \implies z \equiv -y \pmod{k} \text{ e}$$
$$0 \equiv y^{p-1} - y^{p-2}z + \cdots + z^{p-1} \equiv py^{p-1} \pmod{k};$$

assim $k|py^{p-1}$ e $k \neq p$, pois $k|x$ enquanto $p \nmid x$, que implica $k|y$, dessa forma $z \equiv -y \equiv 0 \pmod{k}$ e, portanto, k dividiria simultaneamente x, y e z, contradizendo a hipótese de que $(x, y, z) = 1$. Daí, pela fatoração única em primos há inteiros a e d tais que

$$ad = -x,\ a^p = y + z \text{ e } d^p = y^{p-1} - y^{p-2}z + \cdots - yz^{p-2} + z^{p-1}$$

e, analogamente, para os inteiros b, c, e e f.

$$be = -y,\ b^p = x + z \text{ e } e^p = x^{p-1} - x^{p-2}z + \cdots - xz^{p-2} + z^{p-1}$$
$$cf = -z,\ c^p = x + y \text{ e } f^p = x^{p-1} - x^{p-2}y + \cdots - xy^{p-2} + y^{p-1}.$$

Como $q|xyz$, suporemos, sem perda de generalidade, que $q|x$ e, consequentemente, $q|2x$, assim, de

$$2x = x + y + x + z - y - z = (x + y) + (x + z) - (y + z) = b^p + c^p - a^p$$

temos que

$$b^p + c^p - a^p \equiv b^p + c^p + (-a)^p \equiv 0 \pmod{q} \Rightarrow q|abc \text{ pela primeira hipótese do teorema.}$$

Mas se $q|b$ teríamos que $q|b^p = x + z$; como $q|x$ e $x^p + y^p + z^p = 0$, então $q|z$ e, consequentemente, $q|y$, ou seja, $q|(x, y, z) = 1$, um absurdo. Temos um resultado análogo se $q|c$.
Por outro lado, se $q|a$ então $q \nmid d$ (pois a e d são primos entre si) e, como $q|x$, temos que

$$f^p \equiv y^{p-1} \pmod{q},$$

e

$$y \equiv -z \pmod{q} \implies d^p \equiv py^{p-1} \pmod{q}.$$

Portanto, $q|f$, pois, se não fosse assim, f teria inverso módulo q e $(df^{-1})^p \equiv p \pmod{q}$, o que contraria a segunda hipótese do teorema. Logo,

$$q|f \implies q|z$$

$$q|a \implies q|x$$

e daí

$$x^p + y^p + z^p = 0 \implies q|y,$$

o que é impossível, pois $(x, y, z) = 1$, ou seja, não existem inteiros x, y e z com $(x, y, z) = 1$ e $p \nmid xyz$, tais que $x^p + y^p + z^p = 0$, como queríamos demonstrar. □

Proposição 3.3 (Sophie Germain)**.** *Se p e $2p+1$ são primos com $p > 2$, então não existem inteiros x, y e z, com $(x, y, z) = 1$ e $p \nmid xyz$, tais que $x^p + y^p + z^p = 0$.*

Demonstração. Basta verificarmos que as condições (a) e (b) do teorema antecedente são satisfeitas, tomando como primo $q = 2p + 1$. Observemos que, se $(2p + 1) \nmid xyz$, então, pelo pequeno teorema de Fermat, temos

$$x^{(2p+1)-1} \equiv 1 \pmod{2p+1}$$

$$x^{2p} \equiv 1 \pmod{2p+1}$$

$$x^{2p} - 1 \equiv 0 \pmod{2p+1}$$

$$(x^p - 1)(x^p + 1) \equiv 0 \pmod{2p+1}$$

daí,

$$x^p \equiv \pm 1 \pmod{2p+1}$$

e, analogamente, $y^p \equiv \pm 1 \pmod{2p+1}$ e $z^p \equiv \pm 1 \pmod{2p+1}$. Portanto, $x^p + y^p + z^p \equiv \pm 1 \pm 1 \pm 1 \not\equiv 0 \pmod{2p+1}$, logo, a condição (a) do teorema antecedente é satisfeita. Temos, também, que $w^p \equiv -1, 0, 1 \not\equiv p \pmod{2p+1}$, logo a condição (b) também é satisfeita. □

Como no caso dos primos gêmeos, são conhecidos alguns primos de Sophie Germain muito grandes, como $2618163402417 \cdot 2^{1290000} - 1$, que tem 388342 dígitos. Além disso, sabe-se que, denotando o número de primos de Sophie Germain menores do que x por $\pi_{SG}(x)$, então existe C tal que

$$\pi_{SG} < C\frac{x}{(log\ x)^2}$$

para todo x, e acredita-se que π_{SG} seja assintótico a $cx/(log\ x)^2$, no entanto, não se conhece uma demonstração sequer de que existam infinitos primos de Sophie Germain.

3.4 Números Primos e Funções

Como foi visto nas páginas anteriores, o sonho de se encontrar uma função simples que gere todos os números primos parece distante, mas podemos obter uma função simples que, se não gere todos os números primos, possa gerar, ao menos, uma infinidade de primos.

Deve-se observar que existem fórmulas que geram todos os números primos, porém "que são tão complicadas que não ajudam muito nem a gerar números primos explicitamente nem a responder perguntas teóricas sobre a distribuição dos primos." (MARTINEZ et al., 2018). Ou seja, existem fórmulas que geram todos os primos, mas que são muito complexas de se trabalhar e que não contribuem para se tirar conclusões sobre a distribuição dos

números primos. Em outros casos, existem fórmulas que só geram números primos, contudo sem gerar todos, mas que por um motivo ou outro servem apenas como curiosidade, caso da fórmula de Mills. Pode-se encontrar alguns exemplos destas fórmulas na obra citada acima, além de (RIBENBOIM, 2014) e a dissertação do PROFMAT de Ambrósio da Silva Marques intitulada **Disposição dos Números Naturais em Arranjo Plano e Polinômios que Geram Números Primos**.

Assim, o foco volta-se, como dito acima, para funções simples que gerem uma infinidade de números primos. Este é um tema, portanto, que pode ser utilizado como tema de pesquisa a ser realizada por estudantes da Educação Básica. Até pouco tempo, o recorde de polinômios geradores de primos para inteiros consecutivos era o polinômio $p(n) = n^2 + n + 41$, proposto por Euler, que gera números primos para todos os $0 \leq n \leq 39$, com n inteiro. Perceba que esse recorde não se refere à quantidade total de números primos gerados pelo polinômio, mas à quantidade de primos gerados em sequência, pois se tomarmos $n = 42$, por exemplo, voltamos a obter um número primo: $p(42) = 1847$.

Desta forma, os estudantes podem determinar outros polinômios ou funções que gerem uma sequência de primos, que se aproxime da quantidade de primos gerada pelo polinômio de Euler, ou, até mesmo, a ultrapasse. Neste sentido, a Espiral de Ulam, que será tratada mais adiante, e variações dela podem ser muito úteis. Além disso, não podemos, nem devemos, ficar presos a polinômios. Há uma variedade de tipos de funções que podem ser de grande valia nas pesquisas com números primos, dentre elas as funções exponenciais, logarítmicas, trigonométricas, etc. Vimos alguns exemplos de aplicações dessas funções quando estudamos os números de Fermat, de Mersenne, de Sierpiński, de Cullen, entre outros.

3.5 Criptografia RSA

A criptografia estuda as formas de se codificar uma mensagem de forma que só aquele a quem a mesma foi destinada possa compreendê-la.

> A criptografia tem uma irmã gêmea na arte de decifrar códigos secretos, ou *criptoanálise*. Naturalmente todo código vem acompanhado de duas receitas: uma para codificar uma mensagem; outra para decodificar uma mensagem codificada. Decodificar é o que um usuário legítimo do código faz quando recebe uma mensagem codificada e deseja lê-la. Já decifrar significa ler uma mensagem codificada *sem ser um usuário legítimo*. Portanto para decifrar é preciso "quebrar" o código. (COUTINHO, 2014).

Quem nunca brincou, quando criança, de decifrar mensagens escritas em código por amigos? A maioria desses códigos infantis, é feito trocando-se uma letra por outra, ou por um número, ou uma figura. Muitos códigos desse tipo foram criados no decorrer da história, no entanto, qualquer código que tenha como característica substituir uma letra por outro símbolo qualquer é muito fácil de ser decifrado. Principalmente quando se tem um computador. Com a existência dos computadores, que podem verificar uma quantidade

muito grande de dados em poucos minutos, os códigos precisam ser difíceis de decifrar. Uma mensagem enviada por um cliente ao seu banco, por meio da internet, envolvendo milhões de reais, precisa ser protegida para que não possa ser lida por um terceiro que tenha interceptado a mesma. Além disso, o banco precisa ter certeza de que a mensagem recebida foi enviada, realmente, pelo cliente, ou seja, a mensagem precisa ter uma assinatura digital. Esses códigos difíceis de serem decifrados foram criados para aplicações comerciais, e não para comunicação de espiões, por isso esses códigos são todos de chave pública. O mais conhecido método de criptografia de chave pública é o RSA, criado por R. L. Rivest, A. Shamir e L. Adleman, em 1978. "Há vários outros códigos de chave pública, mas o RSA é, atualmente, o mais usado em aplicações comerciais." (COUTINHO, 2014).

O método RSA de criptografia consiste em escolher dois primos muito grandes, com mais de 100 dígitos. O produto desses dois primos é usado para codificar a mensagem. Já para decodificar a mensagem, é necessário conhecer os dois primos. Cada usuário do método possui uma chave de codificação, que é tornada pública, por isso o produto entre os dois primos gigantes é conhecido como a "chave pública". Já a chave de decodificação, constituída pelos primos, tem que ser mantida em segredo ou a segurança do método estará em risco.

Tão simples que fica difícil acreditar que o método RSA é seguro. Mas o obstáculo para se decifrar o RSA é de natureza tecnológica. Não há, até o momento, um método ou algoritmo que consiga fatorar números tão grandes de forma simples e com poucos passos. Assim, fatorar números dessa magnitude levaria, a princípio, alguns anos, mesmo usando-se supercomputadores.

> Rivest usou a generalização do pequeno teorema de Fermat, descoberta por Euler, que funciona em calculadoras-relógio construídas a partir de dois primos, em vez de um. Euler demonstrou que, nessas calculadoras, o padrão se repete após embaralharmos as cartas $(p-1)\cdot(q-1)+1$ vezes. Assim, só é possível descobrir quanto tempo é necessário para que o padrão se repita no relógio com $N = p \cdot q$ horas conhecendo-se os primos p e q. Saber quais são esses dois primos se torna, portanto, a chave para descobrir os segredos do RSA. (SAUTOY, 2007).

A calculadora-relógio, citada pelo autor do texto acima, trata-se do cálculo de congruência e as horas N a que ele se refere é o módulo da congruência. Vejamos um exemplo, com números pequenos, para entendermos melhor como funciona o sistema RSA. Consideremos os números primos $p = 11$ e $q = 17$, assim a chave pública N será $N = 11 \cdot 17 = 187$ e $(11-1)\cdot(17-1)+1 = 161 = 7 \cdot 23$, ou seja, o 7 será o número de codificação e o 23 será o número de decodificação. Consideremos, agora, que o número a ser codificado é 12, desta forma, para codificarmos esse número usando a chave pública e o número de codificação, faremos:

$$12^7 \equiv 177 \pmod{187}.$$

Depois, para decodificar, devemos fazer:

$$177^{23} \equiv 12 \pmod{187}.$$

Mas, esta apresentação do método RSA é um tanto simplista, pois falta alguns outros detalhes como, por exemplo, quando a mensagem a ser codificada/decodificada contém

outros símbolos além de números. Vejamos agora, então, esses detalhes omitidos na apresentação do RSA acima.

Em primeiro lugar é preciso fazer uma pré-codificação, ou seja, converter a mensagem em uma sequência de números. Para tanto devemos fazer corresponder cada símbolo que pode ser usado nas mensagens a um número. Dessa forma, se formos trabalhar com um sistema que utilize, digamos, 50 símbolos, o ideal seria utilizar números de dois dígitos para cada símbolo. Se o sistema adotado utilizar 600 símbolos, por exemplo, seria mais adequado usar números de três dígitos para cada símbolo. Por que isso? Para evitar ambiguidades. Por exemplo, vamos supor que usássemos um sistema no qual tivéssemos símbolos pré-codificados com os números 45, 52, 67, 455 e 267, entre outros é claro, assim, se a mensagem enviada fosse composta da seguinte forma 455267, não teríamos certeza se os símbolos corresponderiam a 45, 52 e 67, ou a 455 e 267.

Depois de feito o passo anterior, transformamos a mensagem em uma sequência numérica. Vejamos um exemplo.

Exemplo 3.4. Consideremos a tabela de conversão a seguir:

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E
11	12	13	14	15	16	17	18	19	21	22	23	24	25	26
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
27	28	29	31	32	33	34	35	36	37	38	39	41	42	43
U	V	W	X	Y	Z	,	.	;	:	?	!	(	)	
44	45	46	47	48	49	51	52	53	54	55	56	57	58	59

Assim, a mensagem "Boa noite! Qual o seu nome?", ficaria assim:
233722593637314326565939442234593759422644593637352655.

Para continuarmos é necessário determinarmos os parâmetros do sistema RSA que vamos adotar. Como visto no início desta seção, os parâmetros são dois números primos distintos, que podemos, para efeito de exemplo, adotar os números $p = 11$ e $q = 17$, que foram adotados anteriormente, e, consequentemente, $n = 11 \cdot 17 = 187$. O próximo passo da pré-codificação é separar em blocos o longo número obtido acima. Cada um desses blocos devem ser números menores que n, no nosso caso 187. Pode-se determinar os blocos de várias maneiras, contudo é preciso tomar alguns cuidados como, por exemplo, não deixar nenhum bloco começando por zero. No nosso caso isto não será um problema, pois na pré-codificação não foram usados números com o dígito zero. Desta forma, os blocos do nosso exemplo, poderiam ser: 23-3-72-25-93-63-73-143-26-56-5-93-9-44-22-3-45-93-75-94-2-26-4-45-9-36-3-73-52-65-5.

Encerra-se, assim, a etapa de pré-codificação e podemos passar à etapa de codificação. Para a codificação precisamos de n, aqui $n = 187$, e de um inteiro positivo e que seja

inversível módulo $\varphi(n)$, ou seja, $(e, \varphi(n)) = 1$. No nosso exemplo anterior $e = 7$, mas pode ser qualquer outro inteiro positivo coprimo com $\varphi(n)$, que no nosso exemplo temos $\varphi(n) = (11-1)(17-1) = 10 \cdot 16 = 160$. O par (n, e) é, portanto, a *chave de codificação*. Finalmente, para codificar, devemos fazer como no exemplo anterior, ou seja, determinar b^e módulo n, onde b representa cada um dos blocos da mensagem, isto é, fazendo 23^7 módulo 187, 3^7 módulo 187, 72^7 módulo 187, etc., obtemos: 133-130-30-185-168-24-61-165-104-78-146-168-70-22-44-130-122-168-114-19-128-104-115-122-70-9-130-61-35-142-146.

A partir daí chegamos ao momento da decodificação, que consiste em repetir o processo, só que desta vez utilizando d que é o inverso de e módulo $\varphi(n)$ e é muito fácil calcular d se conhecemos $\varphi(n)$ e e, basta aplicar o algoritmo euclidiano estendido, assim o par (n, d) é a *chave de decodificação*. Em nosso exemplo, $d = 23$ e, portanto, devemos fazer 133^{23} módulo 187, 130^{23} módulo 187, 30^{23} módulo 187, e assim por diante, obtendo os blocos originais e, por conseguinte, a mensagem original.

Surge, então, uma pergunta: será que esse método funciona sempre, ou seja, sempre que decodificarmos um bloco codificado obteremos o bloco original? A resposta é "sim" e é isto que vamos verificar agora.

Se representarmos cada bloco da mensagem pré-codificada por b, o que devemos ter é que $(b^e)^d \equiv b \pmod{n}$, isto é, $b^{ed} \equiv b \pmod{n}$ para todo b. Como $n = pq$, onde p e q são primos distintos, calcularemos a forma reduzida de b^{ed} módulo p (o cálculo para b^{ed} módulo q é análogo e, portanto, basta executar um deles). Sendo d o inverso de e módulo $\varphi(n)$, então $ed = k \cdot \varphi(n) + 1 = k(p-1)(q-1) + 1$, com k inteiro, logo

$$b^{ed} \equiv b^{k(p-1)(q-1)+1} \equiv (b^{p-1})^{k(q-1)} \cdot b \pmod{p}.$$

A princípio vamos supor que $p \nmid b$, assim, usando o pequeno teorema de Fermat, teremos $b^{p-1} \equiv 1 \pmod{p}$ e obtemos

$$b^{ed} \equiv 1^{k(q-1)} \cdot b \equiv b \pmod{p}.$$

Caso $p|b$, então $b \equiv 0 \pmod{p}$, portanto, $b^{ed} \equiv b \equiv 0 \pmod{p}$, logo $b^{ed} \equiv b \pmod{p}$ para todo b. Notemos que não podemos usar o mesmo argumento para n, porque $(n, b) \neq 1$ não significa que $b \equiv 0 \pmod{n}$, pois n é composto. Analogamente $b^{ed} \equiv b \pmod{q}$, portanto, $p|b^{ed} - b$ e $q|b^{ed} - b$. Como p e q são primos distintos, temos que $(p, q) = 1$, logo $pq|b^{ed} - b$, ou seja, $n|b^{ed} - b$, assim $b^{ed} \equiv b \pmod{n}$ para qualquer b inteiro. Desta forma, vemos que o método funciona sempre.

Uma outra questão importante é: o RSA é seguro? Lembremos que o RSA é um método de chave pública, portanto, o par (n, e) é acessível a qualquer usuário, logo, para que o RSA seja um método seguro é necessário que seja difícil calcular d quando são conhecidos apenas n e e.

> Na prática, só sabemos calcular d aplicando o algoritmo euclidiano estendido a $\varphi(n)$ e e. Por outro lado, só sabemos calcular $\varphi(n)$ se soubermos fatorar n para obter p e q. Portanto, na prática, só podemos quebrar o código se conseguirmos fatorar n. Mas sabemos que, se n for grande, este é um problema muito difícil, já que não são conhecidos algoritmos rápidos de fatoração. (COUTINHO, 2014).

Entretanto, alguém pode descobrir uma maneira de chegar a d sem ter que fatorar n, ou descobrir um algoritmo rápido para fatorar n, isto poria em risco a segurança do método RSA, mas não se tem notícia de que alguém tenha conseguido encontrar esses processos. Portanto, quebrar o código RSA é muito difícil. Mas, para isso, é preciso considerar uma outra coisa: a escolha dos primos p e q.
Como já foi dito linhas atrás, o RSA utiliza-se de números primos muito grandes, com pelo menos 90 dígitos. Mas não basta escolher grandes números primos, é importante que a diferença entre eles também seja grande, pois, se não for assim, torna-se relativamente fácil descobri-los. Isto acontece porque, neste caso, p e q estariam muito próximos da raiz quadrada de n, então bastaria calcular a raiz quadrada de n e ir verificando se n é divisível por números próximos a essa raiz (o que não demoraria muito para encontrar, já que p e q são próximos). Portanto, a diferença entre p e q também deve ser grande para garantir a segurança do RSA.

> Isto não é puro papo furado. Em 1995 dois estudantes de uma universidade americana quebraram uma versão do RSA em uso público. O feito só foi possível porque a escolha dos primos usada neste sistema era inteiramente inadequada. Por outro lado, o RSA está em uso há anos e, se os primos forem bem escolhidos, o sistema tem-se mostrado muito seguro. Portanto, uma receita para escolher primos bons é essencial para a "caixa de ferramentas" de qualquer um que deseje programar o RSA. (COUTINHO, 2014).

Além disso, um outro cuidado deve ser tomado. Precisamos ter certeza que $p-1$, $p+1$, $q-1$ e $q+1$ não têm fatores primos pequenos (além do 2, é claro), pois, se isso acontecer, tornaria-se relativamente fácil fatorar n usando alguns algoritmos de fatoração conhecidos.
Um outro tema relativo ao RSA é a assinatura eletrônica. Uma empresa que realize transações bancárias por computador, via rede telefônica, precisa, por medida de segurança, ter uma assinatura eletrônica. Segundo (COUTINHO, 2014) "Não é difícil mandar uma mensagem assinada usando o RSA, ou qualquer outro sistema de chave pública". Em linhas gerais o sistema funciona assim: A empresa tem suas funções de codificação e decodificação e o banco tem as suas funções, também de codificação e decodificação, lembremos, no entanto, que as funções de codificação, tanto da empresa quanto do banco, são públicas. Quando a empresa vai enviar uma mensagem ao banco, ela aplica sua função de decodificação à mensagem e depois a função de codificação do banco, conhecida pela empresa, por ser pública. Ao receber a mensagem, o banco aplica sua função de decodificação e depois a função de codificação da empresa, conhecida pelo banco, por ser pública, obtendo, assim, a mensagem original. A probabilidade de que uma mensagem, que tenha sido enviada sem passar por todo o processo de assinatura eletrônica, tenha sentido ao ser decodificada pelo banco é quase zero. Assim o banco terá certeza que a mensagem foi enviada pela empresa.

> Recentemente descobriu-se que o uso pouco cuidadoso da técnica de autenticação de assinaturas torna vulneráveis certos métodos de chave pública como o RSA. No final de 1995, um consultor em assuntos de segurança de computadores (mas formado em biologia!) descobriu que é possível usar o sistema de assinaturas para quebrar o RSA. O método consiste em enviar uma mensagem assinada e marcar o tempo que o sistema leva para confirmar a assinatura. Fazendo isto para mensagens de tamanhos ligeiramente diferentes, é possível obter informações suficientes

> para encontrar a chave de decodificação do sistema RSA que esteja sendo usado. Portanto, a segurança do RSA não depende exclusivamente da nossa capacidade de inventar novos algoritmos de fatoração. Há muitos outros fatores importantes, que não têm um caráter puramente matemático. (COUTINHO, 2014).

Sendo assim, não se sabe por quanto tempo o sistema RSA de criptografia continuará sendo seguro, contudo, na atualidade, ele ainda é um dos mais seguros e mais utilizados sistemas para realização de atividades que exigem confidencialidade dos dados transmitidos em redes de computadores e afins.

4 A Hipótese de Riemann

A história das pesquisas envolvendo números primos passou pelo crivo de Eratóstenes, as demonstrações da infinitude dos primos por Euclides e outros grandes matemáticos, o pequeno teorema de Fermat, demonstrado por Euler, que o aprimorou utilizando sua função φ, o teorema dos números primos de Gauss, provado por Poussin e Hadamard, e muitos outros trabalhos que não foram expostos aqui, até chegarmos aos trabalhos de Bernhard Riemann, com sua função zeta, e de outros importantes matemáticos do final do século XIX até os dias atuais, como Edmund Landau, Srinivasa Ramanujan, Godfrey Harold Hardy, John Edensor Littlewood, Atle Selberg e Alan Turing, entre outros.
Neste capítulo será apresentada a hipótese de Riemann, sem, contudo, entrarmos no campo dos cálculos, pois esses cálculos fogem ao escopo desse trabalho.

4.1 A Função Zeta ζ de Riemann

Uma função zeta é uma função formada por um somatório de infinitas potências. A função zeta de Riemann $\zeta(s) = \sum_{k=1}^{\infty} k^{-s}$ é definida para todo valor complexo s, exceto para $s = 1$. Ou seja, a variável s é do tipo $\sigma + it$, em que i é a unidade imaginária igual a $\sqrt{-1}$.

> A raiz quadrada de menos um, a estrutura básica dos números imaginários, esta parece ser uma contradição em termos. Para alguns, o que separa os matemáticos do resto das pessoas é o fato de admitirem a possibilidade de que existam números como esses. Para que tenhamos acesso a essa parte do mundo matemático, é necessário dar um salto criativo. À primeira vista, não aparentam ter qualquer relação com o mundo físico, que parece haver sido construído a partir de números cuja raiz quadrada é sempre um número positivo. Porém, os números imaginários não são apenas uma brincadeira abstrata – eles contêm a chave para o mundo das partículas subatômicas do século XX. Em última análise, os aviões não teriam chegado aos céus se os engenheiros não houvessem se aventurado pelo mundo dos números imaginários. Esse mundo novo nos fornece uma flexibilidade que é negada àqueles que se limitam aos números comuns. (SAUTOY, 2007).

A utilização de números complexos foi o "salto criativo" de Riemann ao considerar sua função zeta. A geração de Euler foi a qual os matemáticos começaram a inserir números imaginários em funções. É de se admirar que a função zeta de Riemann seja de tão simples escrita, mas de tão grande capacidade de nos revelar segredos dos números primos. Contudo, sua escrita simples não quer dizer que os cálculos para determinar seus zeros sejam simples. Todavia, aqui nos ateremos apenas ao que esses zeros podem nos revelar.
Ao se considerar os zeros da função zeta de Riemann, obtemos os zeros triviais, que são os inteiros pares negativos, e os zeros não triviais, que estão na faixa chamada de faixa

crítica ou domínio crítico, que é a faixa na qual a parte real de s está entre 0 e 1, isto é, $0 < \sigma < 1$. Além disso, os zeros no domínio crítico são simétricos em relação ao eixo real e também em relação à reta de equação $\sigma = \frac{1}{2}$.

4.2 A Hipótese de Riemann

Gauss havia determinado sua função $\pi(x) = \frac{x}{\log x}$, em que $\pi(x)$ indica o número de primos menores ou igual a x, e, em 1792, conjecturou que $\pi(x)$ era assintoticamente igual à função integral logarítmica definida por

$$Li(x) = \int_2^x \frac{dt}{\log t}.$$

Contudo, o valor encontrado por $\pi(x)$ ou mesmo por $Li(x)$ não é exato, sendo apenas uma aproximação. Riemann demonstrou que considerando os zeros não triviais de sua função zeta pertencentes ao domínio crítico obtinha-se o número exato de primos até x. Posteriormente, Riemann, ao calcular alguns zeros não triviais de sua função zeta, percebeu que esses zeros estavam todos alinhados no que passou a ser chamada de linha ou reta crítica, na qual $\sigma = \frac{1}{2}$. A hipótese de Riemann é a de que todos os zeros não triviais da função zeta estão sobre a linha crítica.

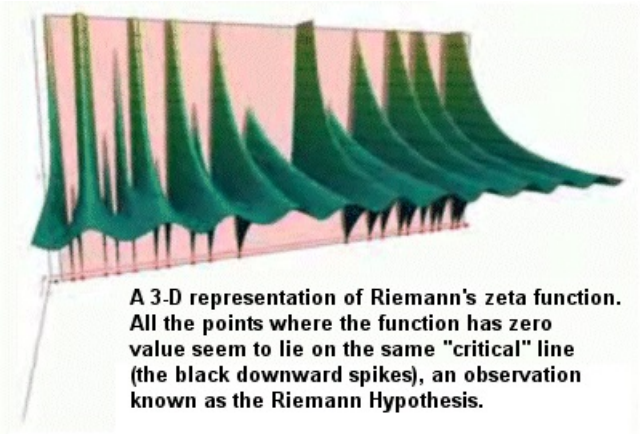
> Riemann havia encontrado uma passagem que comunicava o universo familiar dos números com uma matemática que teria sido completamente estranha aos gregos que estudaram os primos há dois mil anos. Misturando inocentemente os números imaginários com sua função zeta, Riemann descobriu, como um alquimista matemático, que dessa mescla de elementos surgiria o tesouro que era buscado há gerações. Ele compilou suas ideias em um artigo de dez páginas, mas estava plenamente consciente de que elas serviriam para abrir perspectivas radicalmente novas sobre os primos. (SAUTOY, 2007).

Desta forma, a demonstração da hipótese de Riemann torna-se de suma importância, pois soluciona um problema estudado por matemáticos a milhares de anos, e que envolve temas de utilidade prática da atualidade, como o sistema RSA de criptografia, que é um padrão para os números primos, além de confirmar centenas de outros trabalhos que foram demonstrados ao considerar a hipótese de Riemann verdadeira.
A visualização gráfica da função zeta de Riemann nos é impossível, por se tratar de um gráfico que envolve quatro dimensões, porém, como uma sombra é uma imagem bidimensional de um objeto tridimensional, assim

> Ao girarmos esse objeto, obtemos diferentes sombras, que revelam diversos aspectos do objeto. Da mesma forma, existem muitas maneiras de se registrar a altura da paisagem acima de cada número imaginário do mapa sobre a mesa. Entretanto, uma das sombras que podemos escolher retém informações suficientes para que consigamos entender a revelação de Riemann. Essa é uma perspectiva que o auxiliou em sua jornada pelo mundo através do espelho. Desse modo, qual seria a aparência dessa sombra tridimensional específica da função zeta? (SAUTOY, 2007).

Temos um exemplo da aparência dessa "sombra" tridimensional da função zeta de Riemann a seguir.

Figura 2 – "Sombra" tridimensional da função zeta de Riemann



Fonte: storyofmathematics.com

Nesse gráfico "sombra" vemos todos os zeros não triviais da função, representados pelos pontos na parte inferior do gráfico, alinhados na linha crítica de $\sigma = \frac{1}{2}$.

4.3 A Corrida para Provar a Hipótese de Riemann

Em 1885, um matemático holandês pouco conhecido, Thomas Stieltjes, alegava ter uma prova para a hipótese de Riemann, mas não apresentou essa prova até sua morte em 1894, porém, ele não foi o único. Outros matemáticos respeitáveis diziam ter provas da hipótese de Riemann, todavia não mostraram as mesmas.
Na mesma época um outro matemático, Jacques Hadamard, provou, por meio da função zeta de Riemann, o teorema dos números primos de Gauss, que até aquele momento era apenas uma conjectura. No entanto, ele teve de dividir a glória por seu feito com outro matemático, Charles de la Vallée-Poussin, que, de forma independente de Hadamard, também encontrou uma prova. "Hadamard não foi capaz de demonstrar que todos os zeros se situavam na linha crítica de Riemann sobre $\frac{1}{2}$, mas provou que não havia zeros a leste da fronteira que passa pelo número 1." (SAUTOY, 2007).
Em 1900, David Hilbert apresentou em uma palestra 23 problemas matemáticos que ainda não tinham solução. O oitavo problema dessa lista era bem específico: provar a hipótese de Riemann. Em uma entrevista, posterior ao anúncio da lista de 23 problemas, Hilbert disse que considerava a hipótese de Riemann o problema mais fundamental, não só para a Matemática.
Em 1914, os matemáticos Edmund Landau e Harald Bohr mostraram que a maior parte dos zeros não triviais da função zeta de Riemann estavam amontoados próximos à linha crítica de Riemann. Depois foi a vez de Godfrey Harold Hardy mostrar que havia uma infinidade de zeros pertencentes à reta formada pelos pontos que representam os números complexos com parte real igual a $\frac{1}{2}$. Entretanto, afirmar que existem infinitos zeros na linha crítica não significa que todos os zeros estão nessa linha. Podem haver, também, infinitos zeros fora dessa linha, da mesma forma que existem infinitos números pares mas

também existem infinitos números ímpares.
Gauss havia criado a função integral logarítmica $Li(N)$, que determinaria a quantidade de primos até N, com precisão crescente para N cada vez maior. Mas ele também conjecturava que a estimativa dada por $Li(N)$ sempre superestimaria o número de primos, ou seja, $Li(N)$ nunca indicaria uma quantidade de primos menor que o número verdadeiro de primos. Porém, a hipótese de Riemann aponta para a possibilidade da estimativa ficar abaixo do número real de primos. John Edensor Littlewood, matemático inglês, amigo de G. H. Hardy, demonstrou que essa segunda conjectura de Gauss era falsa, embora isso só ocorra quando N chegasse a um valor extremamente grande. Assim, a descoberta de Litlewood reforça, mas não prova, a veracidade da hipótese de Riemann.

> A prova de Littlewood também forneceu as armas perfeitas para os que argumentavam que a matemática era uma ciência essencialmente diferente das demais. Os matemáticos não poderiam mais se contentar com o experimentalismo dos séculos XVII e XVIII, nos quais as teorias eram propostas após cálculos mínimos. O empirismo não era mais um veículo adequado para se navegar no mundo matemático. Milhões de observações experimentais podiam ser suficientes para a formulação de teorias nas demais ciências, mas Littlewood havia provado que, na matemática, este seria um jogo arriscado. Daquele momento em diante, a prova era tudo o que importava. Não se podia confiar em nada que não fosse demonstrado conclusivamente. (SAUTOY, 2007).

Outros avanços foram feitos, como a descoberta de fórmulas de Riemann, por Carl Ludwig Siegel, que facilitavam os cálculos dos zeros da função zeta e o surgimento dos computadores que, utilizando essas fórmulas, calcularam milhões de zeros (todos pertencentes à linha crítica), a descoberta de Atle Selberg de que pelo menos 5% dos zeros estavam sobre a linha crítica, mas até o momento não há uma prova definitiva da hipótese de Riemann.

5 As Espirais de Ulam e Sacks

Como visto nos capítulos anteriores, muitos matemáticos estudaram e fizeram descobertas impressionantes sobre os números primos: o pequeno teorema de Fermat; o teorema dos números primos de Gauss; a função zeta de Riemann e suas raízes não triviais; e muito mais. Entretanto, esses matemáticos, em sua maioria, abordavam esse tema apenas no campo da Aritmética. Este capítulo tem o objetivo de apresentar trabalhos que saem um pouco desse formato, passando a utilizar formas geométricas na busca por propriedades ainda não conhecidas dos números primos: a espiral de Ulam e a espiral de Sacks.

5.1 A Espiral de Ulam

Em 1963, durante a apresentação de um artigo longo, em um encontro científico, o matemático polonês Stanislaw Marcin Ulam pegou uma folha de papel e, para passar o tempo, começou a escrever os números inteiros positivos em uma espiral, de forma semelhante à mostrada na figura a seguir.

Figura 3 – Espiral de Ulam 10x10

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

Fonte: zeletron.com.br/2013/07/primos-na-espiral-de-ulam.html

Em seguida, Ulam marcou, de forma despretensiosa, os números primos naquela espiral, obtendo algo semelhante à próxima figura.

Assim, Ulam percebeu algo: “vários números primos se concentravam em certas diagonais da espiral” (F.; ROCHA, 2019). Essa espiral ficou conhecida, então, como espiral de Ulam.

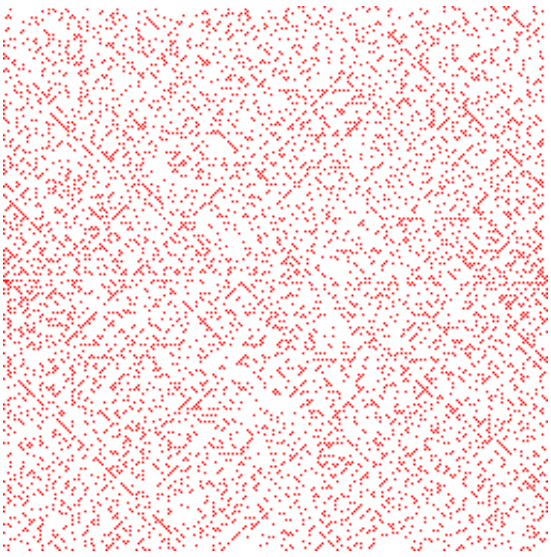
Figura 4 – Espiral de Ulam 10x10 com primos destacados

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

Fonte: zeletron.com.br/2013/07/primos-na-espiral-de-ulam.html

Se ampliarmos essa espiral até $255^2 = 65025$ chegaremos ao mostrado na figura seguinte, onde podemos perceber mais claramente a concentração de alguns primos em determinadas diagonais.

Figura 5 – Espiral de Ulam 255x255



Fonte: zeletron.com.br/2013/07/primos-na-espiral-de-ulam.html

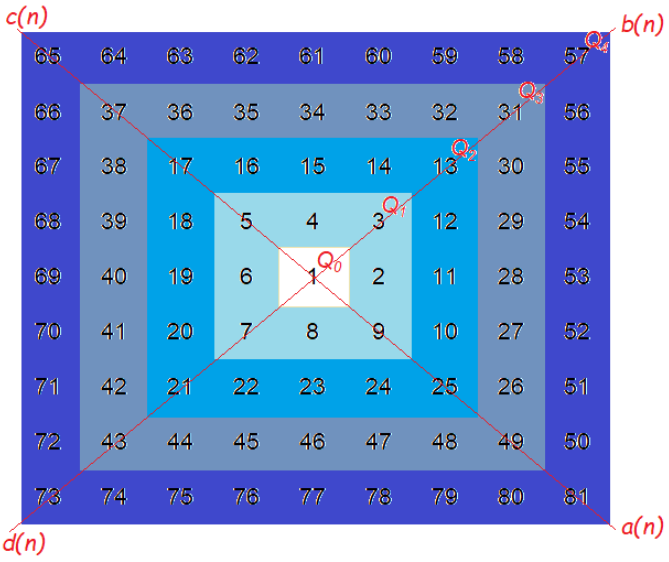
A existência de muitos números primos em diagonais da espiral de Ulam não deve ter ligação com nenhuma aleatoriedade, indicando a existência de algum padrão na distribuição dos números primos, devendo, por isso, ser investigado e, por outro lado, apresentando uma complexidade bem menor que a função zeta ζ de Riemann, portanto, podendo ser trabalhada sem dificuldades por estudantes do Ensino Médio.
A espiral de Ulam pode auxiliar no estudo de expressões matemáticas simples, que forneçam uma boa quantidade de primos. Com o surgimento de métodos de criptografia baseados

em primos, como o RSA, essas expressões matemáticas simples tornam-se de grande importância.

> Identificar se um número é primo ou não, ou ter à disposição muitos números primos dados por uma expressão matemática elementar não é tarefa simples. Um polinômio gerador de primos (polinômio com coeficientes inteiros que forneça vários primos) seria o achado ideal! (F.; ROCHA, 2019).

Temos o exemplo do polinômio $E(x) = x^2 + x + 41$, dado por Euler, que foi por muito tempo o polinômio que deteve o recorde de geradores de primos para inteiros consecutivos, determinando 40 números primos para $x = 0, 1, 2, ..., 39$. Hoje, temos o polinômio $\frac{1}{4}(x^5 - 133x^4 + 6729x^3 - 158379x^2 + 1720294x - 6823316)$, com 57 primos distintos para $0 \leq x \leq 56$. Contudo, observemos que o recorde se refere à obtenção de números primos em sequência, isto não quer dizer que o polinômio em questão não determine outros primos. Por exemplo, para $x = 42$ teremos $E(42) = 42^2 + 42 + 41 = 1847$ que é primo. Mas, é preciso saber que há demonstrações de que não existe polinômio em uma variável que gere apenas números primos (veja (F.; ROCHA, 2019)), ou seja, qualquer polinômio em uma variável, por mais que gere números primos, terá também números compostos entre os elementos do conjunto de números gerados por ele. O objetivo, então, passa a ser o de se obter um polinômio que gere infinitos números primos, embora gere também alguns números compostos, e a espiral de Ulam, ou outra forma geométrica de distribuição dos primos, pode ajudar nisso. (F.; ROCHA, 2019) em seu artigo diz que "é preciso 'algebrizar' a espiral de Ulam". Para tanto consideremos, a princípio, a seguinte figura:

Figura 6 – "Algebrizando" a espiral de Ulam



Fonte: produzida pelo autor

De início, determinaremos uma expressão algébrica para as semidiagonais $a(n)$, $b(n)$, $c(n)$ e $d(n)$. Na figura, temos os quadrados Q_n, tais que, o que contém o número 1 é

denotado por Q_0, o que contém os números de 1 a 9 é denotado por Q_1, o que contém os números de 1 a 25 é denotado por Q_2, e assim sucessivamente. Sendo a quantidade de números nos lados desses quadrados igual a $2n+1$, não é difícil perceber que os elementos da semidiagonal que começa no 1 e desce para a direita são dados pela expressão $a(n) = (2n+1)^2 = 4n^2 + 4n + 1$, e os elementos da semidiagonal oposta a esta são dados por $c(n) = (2n)^2 + 1 = 4n^2 + 1$. Assim, as outras duas semidiagonais têm seus elementos determinados pelas expressões $b(n) = c(n) - 2n = 4n^2 + 1 - 2n = 4n^2 - 2n + 1$ e $d(n) = a(n) - 2n = 4n^2 + 4n + 1 - 2n = 4n^2 + 2n + 1$.

> Note que todas possíveis diagonais presentes na Espiral de Ulam são translações dessas semidiagonais. Entretanto, ao transladar qualquer dessas diagonais, as expressões algébricas podem só fazer sentido para valores grandes de n. Por exemplo, ao transladar $a(n)$, k posições para esquerda, encontramos a semidiagonal $a_{-k}(n) = a(n) - k$, cuja expressão algébrica só faz sentido para $k \leq 2n$. Ou seja, os inteiros $a_{-k}(n)$, para $2n < k$, não estão sobre a diagonal a_{-k}. Caso semelhante ocorre com as outras semidiagonais. (F.; ROCHA, 2019).

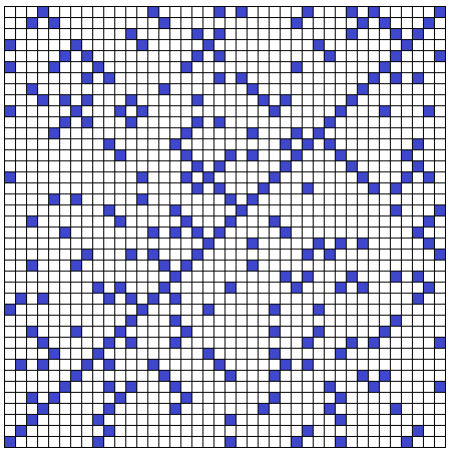
De outra forma, se tomarmos qualquer uma das sequências das semidiagonais na espiral e fizermos as diferenças entre dois termos consecutivos e, depois, repetirmos o processo com as diferenças encontradas, chegaremos a novas diferenças que serão sempre iguais a 8. Isto significa que os termos de uma semidiagonal dessas formam uma progressão aritmética de segunda ordem e, potanto, o termo geral de cada uma dessas semidiagonais são polinômios de segundo grau, daí:
$p(n) = an^2 + bn + c; p(n+1) = a(n+1)^2 + b(n+1) + c; p(n+2) = a(n+2)^2 + b(n+2) + c$
e
$\Delta(n) = p(n+1) - p(n) = 2an + a + b;\ \Delta(n+1) = p(n+2) - p(n+1) = 2an + 3a + b$
Logo, $\Delta^2(n) = \Delta(n+1) - \Delta(n) = 2a$. Então temos que $2a = 8 \Rightarrow a = 4$, assim, a forma dos polinômios que determinam os valores de semidiagonais na espiral de Ulam será $4n^2 + bn + c$, com $b, c \in \mathbb{Z}$ e a variável n assumindo valores inteiros crescentes a partir de um determinado valor, negativo ou positivo, de tal forma que o polinômio assuma somente valores inteiros positivos. Vale salientar que os polinômios em questão podem determinar não só valores das semidiagonais da espiral, mas de qualquer semirreta com valores crescentes da espiral.

Exemplo 5.1. O polinômio $p(n) = 4n^2 + 3n + 2$ assume os valores $2, 9, 24, 47, 78, ...$ para $n = 0, 1, 2, 3, 4, ...$ que, como pode ser observado na espiral de Ulam, são valores presentes em uma semirreta vertical para baixo.

É interessante notar que polinômios da forma $P(x) = x^2 + x + k$ determinam os valores encontrados na diagonal principal (união das semidiagonais b_n e d_n) da espiral de Ulam, quando começamos a espiral com o valor k e fazemos $x = 0, 1, 2, ...$ Assim, ao inciarmos a espiral com o número 41, encontramos na diagonal principal os números

determinados pelo polinômio de Euler e, por conseguinte, neste caso, os primeiros 40 números obtidos nessa diagonal são primos.

Figura 7 – Espiral de Ulam iniciando em 41



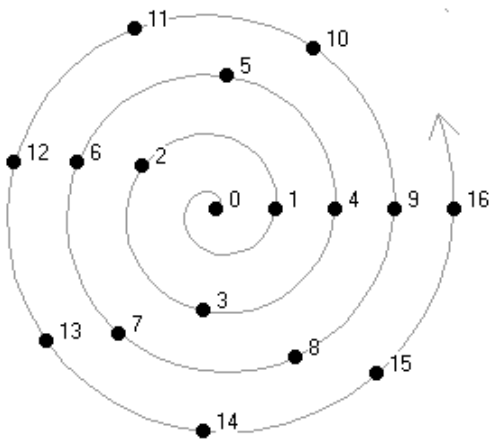
Fonte: produzida pelo autor

O mesmo acontece fazendo $k = 17$, obtendo os primeiros 16 números na diagonal principal, primos.

5.2 A Espiral de Sacks

A espiral de Sacks é uma variação da espiral de Ulam, criada pelo matemático Robert Sacks, em 1994. Na espiral de Sacks os números inteiros não negativos são marcados numa espiral de Arquimedes, espaçados de tal forma que os números quadrados perfeitos coincidam ao final de cada rotação. Conforme figura a seguir.

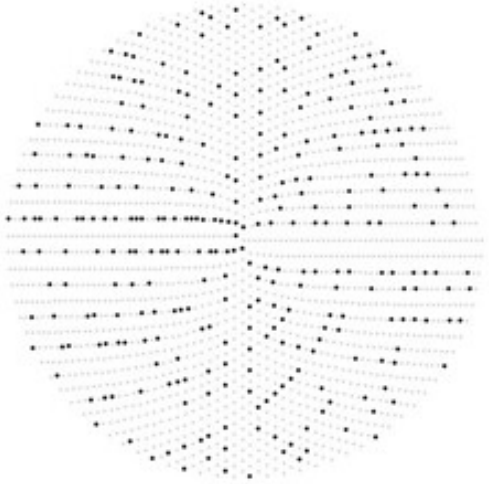
Figura 8 – Espiral de Sacks 1



Fonte: gaussianos.com/la-espiral-de-sacks

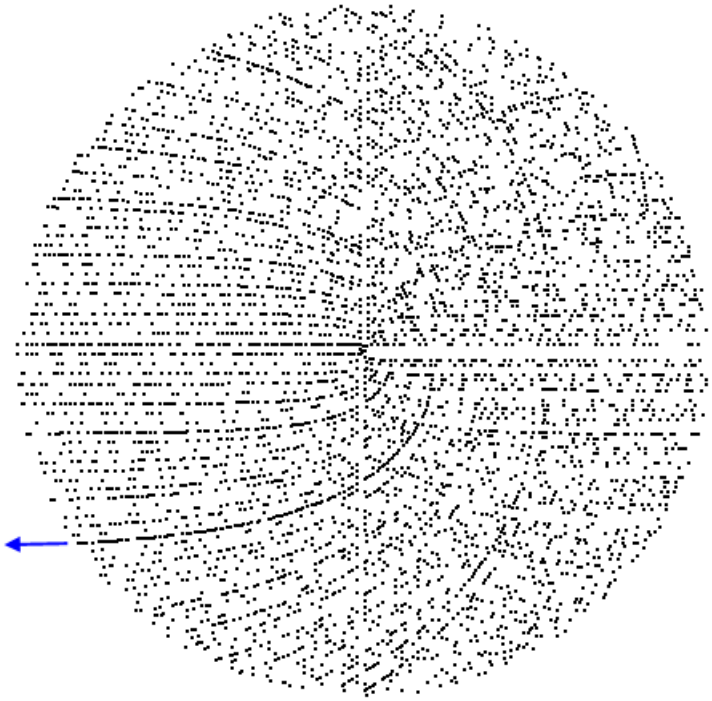
Aumentando o número de pontos marcados sobre essa espiral chegamos ao mostrado nas próximas figuras, que, destacando os números primos, começamos a perceber uma maior presença desses números em determinadas linhas, como pode ser observado.

Figura 9 – Espiral de Sacks 2



Fonte: gaussianos.com/la-espiral-de-sacks

Figura 10 – Espiral de Sacks 3



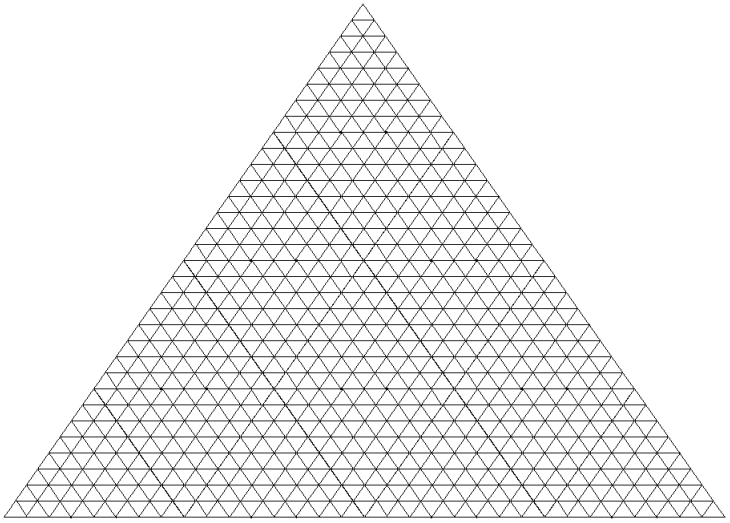
Fonte: gaussianos.com/la-espiral-de-sacks

6 Indo Além da Espiral de Ulam

As formas estão presentes em toda parte do nosso Universo e, como disse Pitágoras, os números governam o mundo. Sendo assim, é de se esperar que encontremos relações entre as formas e os números. Portanto, buscamos, com o presente trabalho, incentivar professores a trabalhar com seus alunos uma metodologia voltada para essa relação entre formas e números, no caso específico de números primos, levando os estudantes a uma prática mais participativa e criativa na compreensão dos conteúdos da disciplina de Matemática.
A espiral de Ulam é um exemplo e inspiração para as atividades propostas aqui. A hipótese de Riemann pode estar correta e, assim, determinar cada número primo, contudo ela é muito complexa para se trabalhar com alunos do Ensino Básico. Logo, formas simples podem, se não determinar cada número primo, apresentar-nos propriedades dos primos ainda não exploradas, e essa pode ser uma motivação para nossos alunos empenharem-se mais no estudo da Matemática.
Assim, propõe-se neste trabalho, além da apresentação de conteúdos tais como o pequeno teorema de Fermat, os teoremas de Euler e Wilson, entre outros, algumas formas que podem ser apresentadas inicialmente aos estudantes, começando pela espiral de Ulam, seguida da espiral de Sacks e, posteriormente, outras formas apresentadas adiante, neste trabalho. Em um primeiro momento, neste capítulo, serão apresentadas figuras pensadas pelo autor, nas quais são destacados alguns números. Vejamos.

6.1 Triângulo de Triângulos

Figura 11 – Triângulo de triângulos



Fonte: produzida pelo autor

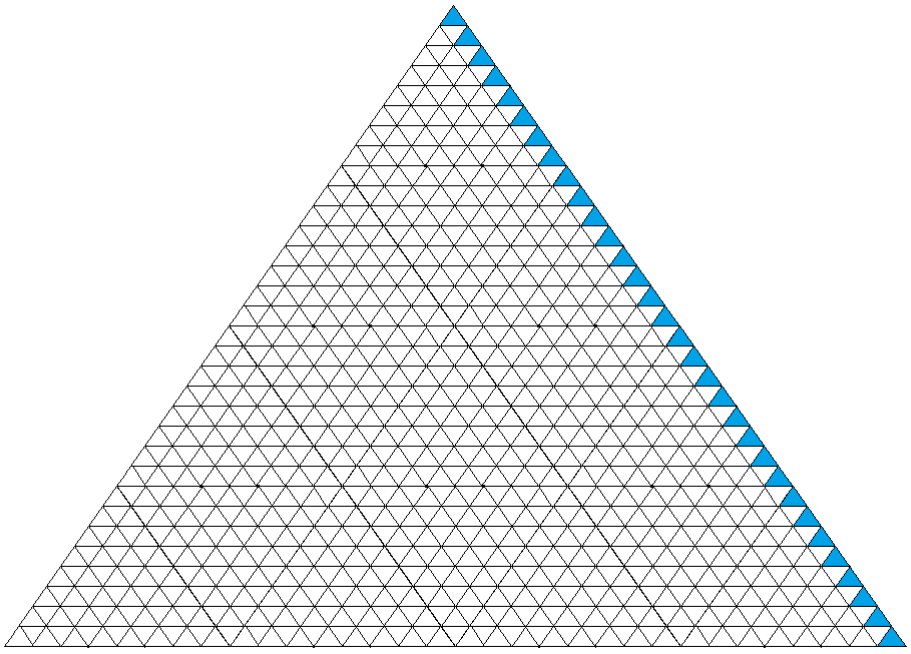
Devemos considerar esta figura, como na espiral de Ulam, infinita, ou seja, sua base vai aumentando indefinidamente, e podemos numerar cada triângulo da seguinte forma:

Figura 12 – Numeração dos triângulos

Fonte: produzida pelo autor

Assim, notemos que cada fileira dessa figura é composta por uma quantidade ímpar de pequenos triângulos e, como sabemos, a soma dos números ímpares consecutivos resulta em um quadrado perfeito, então os números quadrados perfeitos localizam-se nos triângulos destacados na figura a seguir.

Figura 13 – Distribuição dos quadrados perfeitos



Fonte: produzida pelo autor

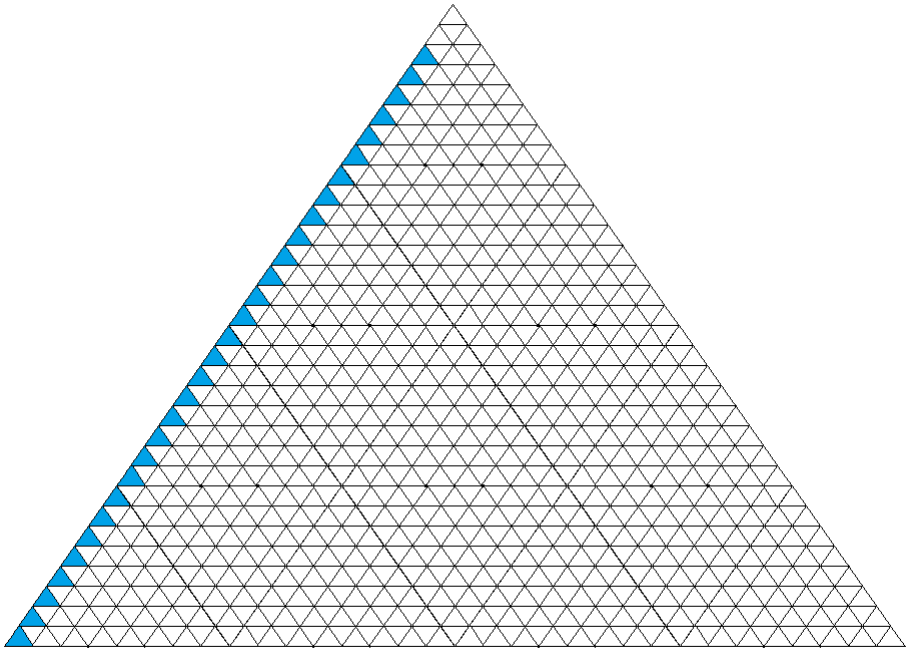
Portanto, os números de Fermat generalizados, $b^{2^m}+1$, com $b \geq 2$ e $m \geq 1$ naturais, localizam-se nos triângulos em destaque na figura seguinte.

Pois, sendo $m \geq 1$, então 2^m é par, logo:

$$b^{2^m}+1 = b^{2k}+1 = (b^k)^2+1,$$

com $k \in \mathbb{N}$, ou seja, os números de Fermat generalizados são sucessores de quadrados perfeitos, com o menor número de Fermat generalizado, correspondendo a $b = 2$ e $k = 1$,

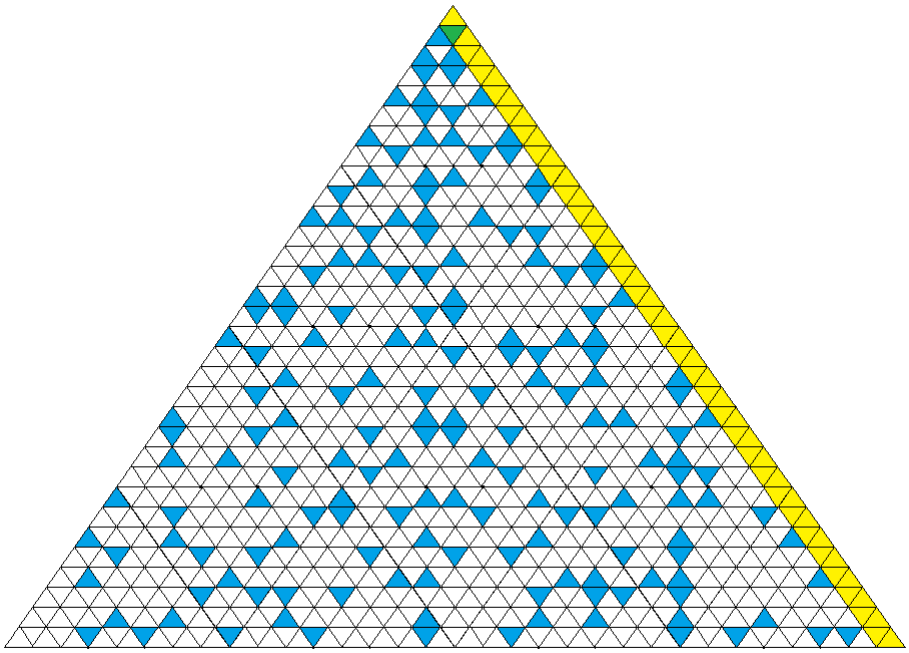
Figura 14 – Distribuição dos números de Fermat generalizados



Fonte: produzida pelo autor

ou melhor, $m = 1$, igual a $2^{2^1} + 1 = 4 + 1 = 5$.
Agora, consideremos os números primos. Na figura abaixo estão destacados, de azul e verde, os números primos até 1024.

Figura 15 – Números primos até 1024

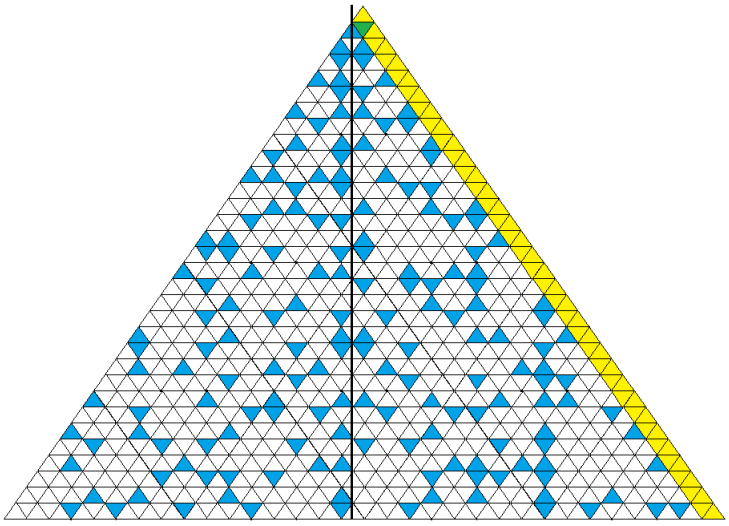


Fonte: produzida pelo autor

Observemos que na fileira em destaque, de amarelo, não há nenhum número primo,

com a exceção do número 3, tendo em vista que esta fileira é formada pelos quadrados perfeitos, que têm uma quantidade ímpar de divisores, e por seus antecessores, que podem ser representados por $x^2 - 1$ que, como trabalhado em muitas obras de Teoria dos Números como exercícios ou exemplos, tem o 3 como único caso de primo desta forma.
Entretanto, o mais interessante que podemos notar nessa figura é que, se excluirmos a fileira em destaque obtemos uma quase simetria em relação ao eixo vertical da figura restante, como ilustrado na próxima figura.

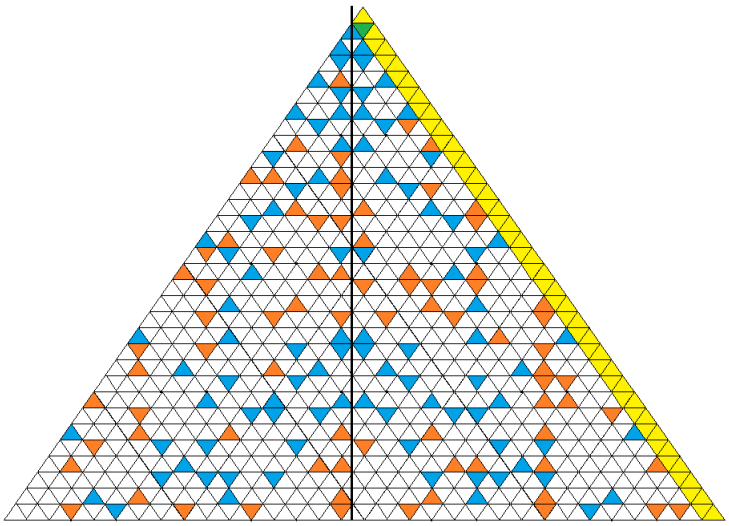
Figura 16 – Uma quase simetria de primos



Fonte: produzida pelo autor

Notemos que alguns primos não têm um correspondente do lado oposto ao seu em relação ao eixo. Estes números estão destacados de laranja na figura a seguir.

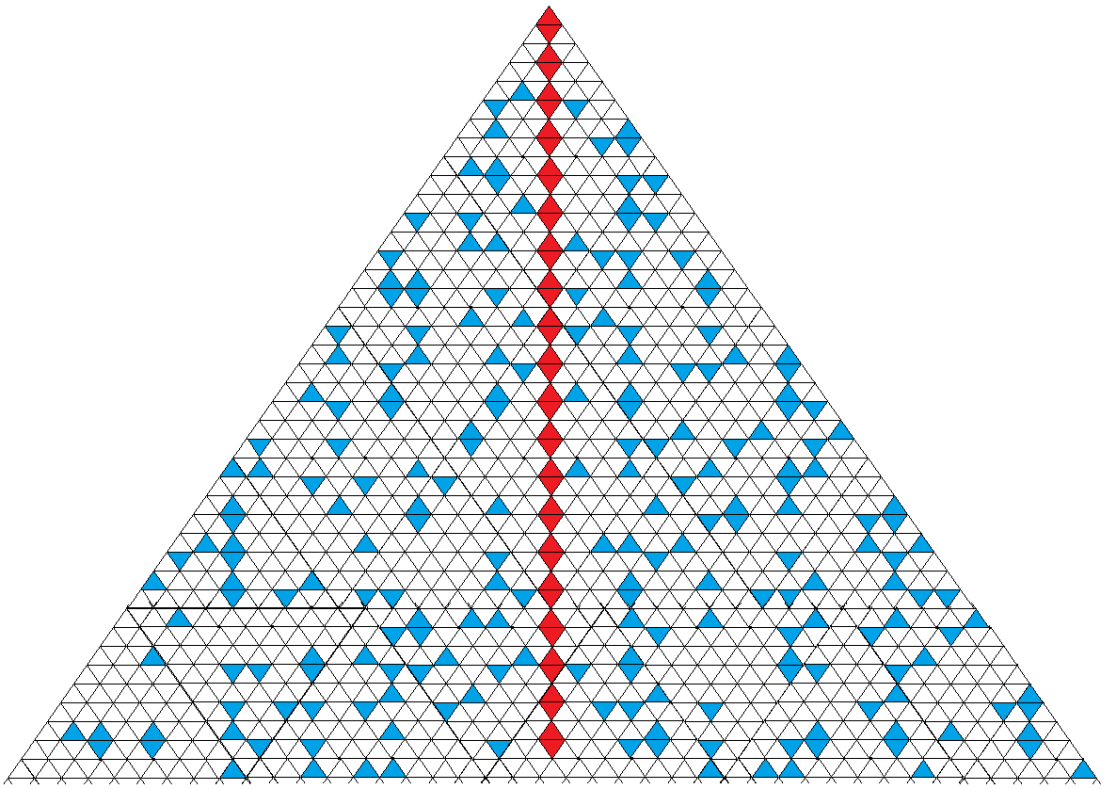
Figura 17 – Primos sem simétrico



Fonte: produzida pelo autor

E se fizermos como feito na espiral de Ulam com o polinômio de Euler, $E(x) = x^2 + x + 41$ com $x \geq 0$ e inteiro, ou seja, começarmos a numerar a partir do 41. A figura a seguir nos mostra o resultado dessa operação.

Figura 18 – Iniciando do 41



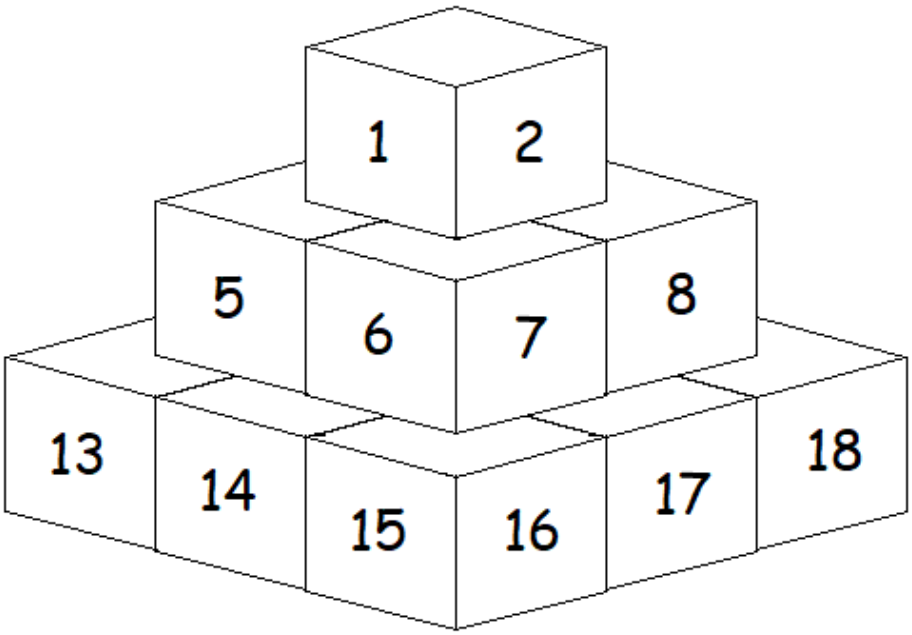
Fonte: produzida pelo autor

Assim, os triângulos pintados de vermelho denotam os primeiros 40 primos obtidos com o polinômio de Euler.

6.2 A Pirâmide Numerada

Consideremos agora uma forma espacial, a pirâmide. A pirâmide representada na figura a seguir deve ser considerada de tal forma que sua base vá aumentando indefinidamente, como no caso anterior. Então numeramos as faces laterais totalmente visíveis dos blocos dessa pirâmide, começando pelo bloco do topo da pirâmide e continuando nas demais camadas da pirâmide, como exibido na mesma figura. Pode-se pensar em outros tipos de pirâmide, contudo trabalharemos aqui com uma pirâmide de base quadrada e formada por blocos cúbicos.

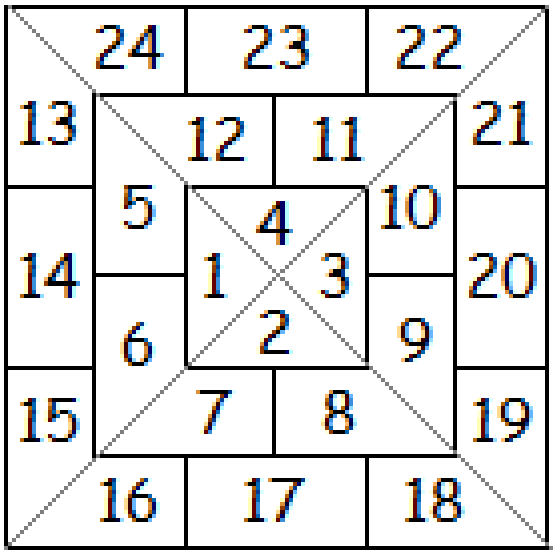
Figura 19 – Pirâmide numerada



Fonte: produzida pelo autor

No entanto, para simplificar, consideremos a figura a seguir como sendo uma vista superior da pirâmide, com a exibição da numeração das faces laterais dos blocos.

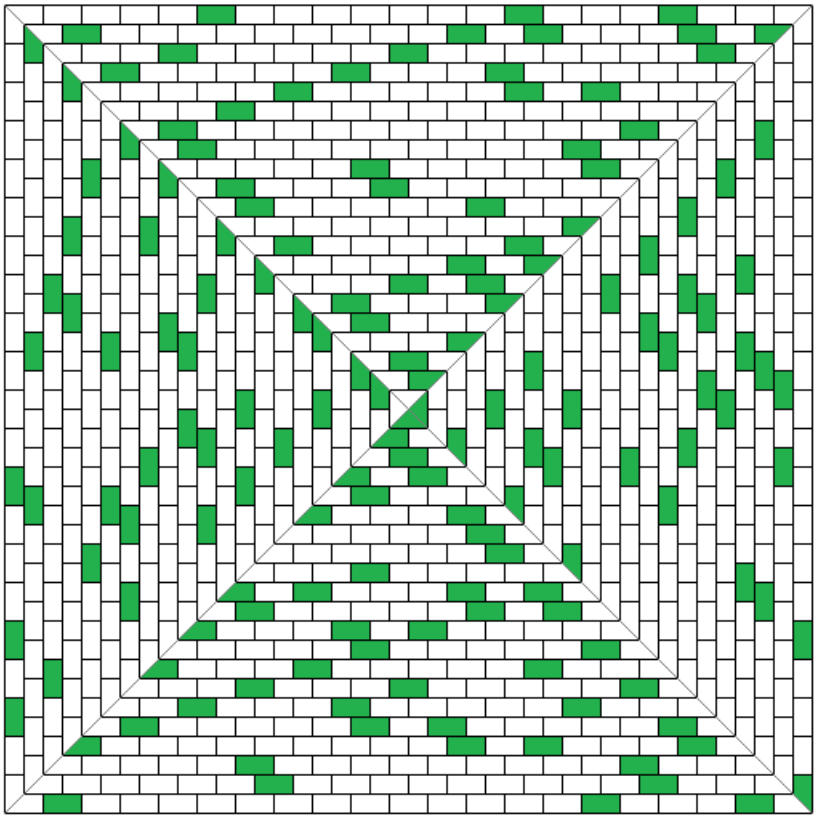
Figura 20 – Pirâmide numerada vista superior



Fonte: produzida pelo autor

Assim, ampliando o número de camadas da pirâmide até chegarmos ao número 924 e destacando os números primos, obtemos a próxima figura.

Figura 21 – Primos na pirâmide



Fonte: produzida pelo autor

Consideremos, agora, a potência 2^n com n ímpar.

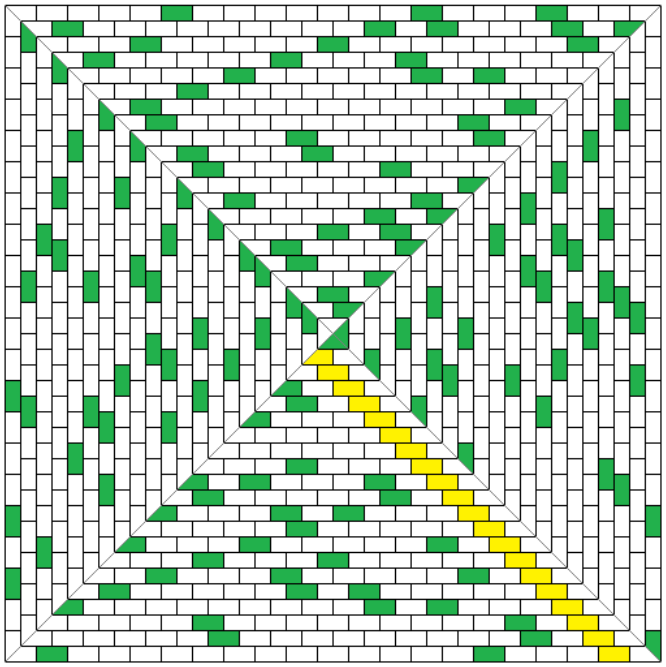
$2^n = 2^{n-1+1} = 2^{n-1} \cdot 2 = (2^{\frac{n-1}{2}})^2 \cdot 2 = 2^{\frac{n-1}{2}} \cdot 2^{\frac{n-1}{2}} \cdot 2 = (2^{\frac{n-1}{2}} - 1 + 1) \cdot 2^{\frac{n-1}{2}} \cdot 2 = (2^{\frac{n-1}{2}} - 1) \cdot 2^{\frac{n-1}{2}} \cdot 2 + 2^{\frac{n-1}{2}} \cdot 2 = (2^{\frac{n-1}{2}} - 1) \cdot (2^{\frac{n-1}{2}}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

Fazendo $m = 2^{\frac{n-1}{2}} - 1$, teremos:

$4 \cdot \frac{(m+1) \cdot m}{2} + 2 \cdot (m+1) = 4 \cdot S_m + 2 \cdot (m+1)$, onde S_m é a soma dos naturais menores ou igual a m. Ou seja, considerando que cada lado de uma determinada camada da pirâmide tem 1 bloco a mais que em cada lado da camada imediatamente acima, então $4 \cdot S_m$ representa todas as faces laterais visíveis dos blocos até a camada m e $2 \cdot (m+1)$ representa todas as faces laterais visíveis de dois lados da pirâmide na camada $m+1$. Portanto, todas as potências de 2 com expoente ímpar localiza-se na última face lateral do segundo lado de determinadas camadas da pirâmide.

Sendo os números de Mersenne $M_q = 2^q - 1$, com q primo, e como os números primos são ímpares (exceto o 2), então os números de Mersenne são (exceto o 3) 1 unidade menor que certas potências de 2 com expoente ímpar (expoente primo), dessa forma podemos afirmar que os números de Mersenne estão localizados em algumas das faces destacadas na figura a seguir (exceto o 3).

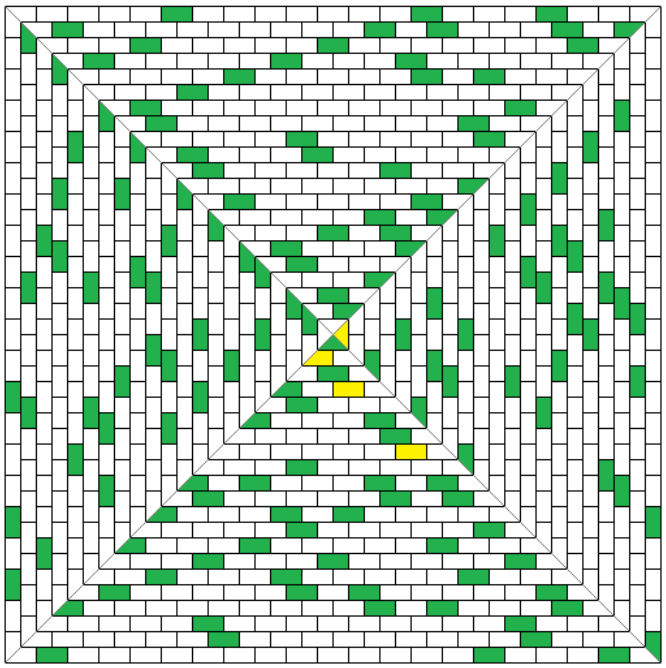
Figura 22 – Números de Mersenne na pirâmide



Fonte: produzida pelo autor

Mais precisamente

Figura 23 – Números de Mersenne na pirâmide 2



Fonte: produzida pelo autor

Estes são apenas alguns exemplos de formas geométricas e distribuição dos números naturais nas mesmas, com algumas propriedades observadas relativas aos números primos

ou outros números particulares, como os números de Fermat, Mersenne, etc. A variedade de formas geométricas e distribuição de números naturais nelas é enorme, para não dizer infinita, com a vantagem de ter uma relativa facilidade na criação e observação de propriedades, por se tratar de uma atividade mais visual, podendo, portanto, ser aplicada tranquilamente com estudantes do Ensino Básico, em particular, do Ensino Médio.

7 A Proposta de Ensino

Na Base Nacional Comum Curricular (BNCC) encontramos dez competências gerais para a Educação Básica, em que o Ensino Médio está incluído. Dentre essas competências destacam-se, por estarem mais ligadas ao tema aqui apresentado, as de número 2 e 4, citadas abaixo:

> Exercitar a curiosidade intelectual e recorrer à abordagens próprias das ciências, incluindo a investigação, a reflexão, a análise crítica, a imaginação e a criatividade, para investigar causas, elaborar e testar hipóteses, formular e resolver problemas e criar soluções (inclusive tecnológicas) com base nos conhecimentos das diferentes áreas. (BRASIL, 2017).

> Utilizar diferentes linguagens – verbal (oral ou visual-motora, como libras, e escrita), corporal, visual, sonora e digital –, bem como conhecimentos das linguagens artística, matemática e científica, para se expressar e partilhar informações, experiências, ideias e sentimentos em diferentes contextos e produzir sentidos que levem ao entendimento mútuo. (BRASIL, 2017).

Logo, vemos que a BNCC incentiva uma formação científica, embora se discuta sempre que o ensino de Matemática deve ser direcionado para aplicações práticas, com o intuito de atrair o interesse do estudante. Para unir, então, essas duas visões é que entra em jogo a criptografia, pois a mesma envolve temas e ferramentas do dia a dia de todos, inclusive dos estudantes, como atividades de compra e venda pela internet e meios de comunicação como o WhatsApp, o Skype e muitos outros, que utilizam métodos de criptografia na transmissão e recepção de dados. E a criptografia, como vimos, está intimamente ligada a números primos, assim, esta é uma ótima ferramenta para incentivar a pesquisa matemática e aplicações práticas da Matemática.
Apesar da BNCC não citar números primos para o Ensino Médio, a mesma coloca como competência específica da área de Matemática e suas tecnologias, entre outras,

> Investigar e estabelecer conjecturas a respeito de diferentes conceitos e propriedades matemáticas, empregando recursos e estratégias como observação de padrões, experimentações e tecnologias digitais, identificando a necessidade, ou não, de uma demonstração cada vez mais formal na validação das referidas conjecturas. (BRASIL, 2017).

Mas, a área da Teoria dos Números é riquíssima em conjecturas, principalmente ligadas aos números primos, que os próprios alunos podem elaborar a cada novo conhecimento adquirido sobre tais números. Além disso, a competência mencionada cita o emprego de recursos e estratégias como observação de padrões, experimentações e tecnologias digitais, daí a busca por um padrão na distribuição dos primos é algo que pode ser usada para exemplificar o estudo de padrões na Matemática, e ainda, as experimentações e tecnologias digitais, que têm sua importância no momento de se fazer os cálculos, que podem ser bem trabalhosos, quando se trabalha com números grandes, assim, a calculadora científica do

Windows nos computadores são muito úteis por, além de outras funcionalidades, apresentar a função *módulo*, aplicada em congruências de números inteiros. A competência em questão ainda coloca a ideia de demonstração formal, tão comum em pesquisa matemática.
Cogitou-se, em um primeiro momento, a possibilidade de pesquisa com inteligência artificial na construção das formas geométricas e na descoberta de padrões na distribuição dos números primos nessas formas. Todavia, essa ideia foi abandonada pelo fato dos envolvidos não terem experiência na utilização dessa tecnologia. Mas, isso não impossibilita, obviamente, a aplicação de inteligência artificial em trabalhos futuros sobre esse tema.
Este trabalho vem, portanto, propor a utilização dos conteúdos listados abaixo, ligados à distribuição dos números primos, com destaque para a espiral de Ulam e suas variações, por meio da disciplina de Matemática, aos estudantes de 3º ano do Ensino Médio. Desta forma, tornar conteúdos de Teoria dos Números conhecidos por alunos da Educação Básica.

7.1 Objetivos Gerais

As atividades aqui propostas têm como objetivos gerais levar o aluno a:

- Compreender que os números primos são muito mais do que simplesmente números com apenas dois divisores;
- Reconhecer a importância do conhecimento de propriedades ligadas aos números primos e sua distribuição;
- Conhecer os efeitos teóricos e práticos da possível prova da hipótese de Riemann;
- Praticar a experimentação matemática, a criatividade, a elaboração de conjecturas e a linguagem matemática aplicada na demonstração de teoremas, proposições, lemas, corolários, etc.

7.2 Objetivos Específicos

Os objetivos específicos são:

- Formular conjecturas a partir de observações de situações envolvendo números primos;
- Conhecer o teorema fundamental da Airtmética;
- Operar com a relação de congruência;
- Conhecer os teoremas de Euler, Fermat e Wilson e suas demonstrações;

- Empregar o teorema chinês dos restos na resolução de problemas;
- Demonstrar propriedades de números indicadas em exercícios;
- Determinar $\varphi(n)$ conhecendo n;
- Conhecer o teorema dos números primos;
- Identificar os primos de Sophie Germain;
- Reconhecer os pontos fortes e fracos de alguns testes de primalidade;
- Aplicar formas geométricas na distribuição de números, em particular números primos, destacando propriedades nessa distribuição;
- Conhecer a função zeta (ζ) de Riemann;
- Diferenciar prova matemática de indício;
- Conhecer a hipótese de Riemann;
- Compreender o método RSA de criptografia;
- Empregar o método RSA de criptografia em exercícios simples de codificação/decodificação de mensagens.

7.3 Conteúdo Programático

- O princípio da indução;
- Divisibilidade;
- O algoritmo da divisão;
- O máximo divisor comum;
- O algoritmo de Euclides;
- Números primos;
- O teorema fundamental da Aritmética;
- Mínimo múltiplo comum;
- Critérios de divisibilidade;
- Congruência;
- A função fi (φ) de Euler;

- Os teoremas de Fermat, Euler e Wilson;
- O teorema chinês dos restos;
- O conjunto quociente $\mathbb{Z}_n$;
- Ordem módulo n;
- O teorema dos números primos;
- Primos gêmeos;
- Primos de Sophie Germain;
- Fórmulas para primos;
- Testes de primalidade;
- A espiral de Ulam;
- A espiral de Sacks;
- Outras maneiras de distribuir números em formas geométricas;
- A função zeta (ζ) de Riemann;
- A hipótese de Riemann;
- Tentativas de provar a hipótese de Riemann;
- O uso de computadores no processo de comprovação de uma conjectura;
- O método RSA de criptografia;
- Porque o método RSA funciona;
- Porque o RSA é seguro;
- A assinatura eletrônica.

7.4 Etapas

As etapas previstas foram: uma revisão sobre divisibilidade, o algoritmo da divisão, mdc, o algoritmo de Euclides, números primos, o teorema fundamental da Aritmética, mmc e critérios de divisibilidade, complementada pelo princípio da indução e seguida de exercícios para praticar, que poderia ser feita em duas aulas de 50 minutos. Depois seriam apresentados os conceitos de congruência e suas propriedades básicas, também seguidos de exercícios, em duas aulas de 50 minutos. Dando prosseguimento, deveria ser apresentada a

função fi (φ) de Euler e os teoremas de Fermat, Euler e Wilson, acompanhados, também, por exercícios de fixação, em mais duas aulas. As atividades prosseguiriam com o teorema chinês dos restos, ordem módulo n, o conjunto quociente $\mathbb{Z}_n$, o teorema dos números primos, primos gêmeos e primos de Sophie Germain e mais exercícios, em outras duas aulas. Continuar-se-ia com fórmulas para primos e testes de primalidade em mais duas aulas e com mais exercícios de fixação.
As próximas quatro aulas seriam trabalhadas com a espiral de Ulam, a espiral de Sacks e outras formas geométricas na distribuição de números, com exercícios nos quais os alunos deveriam exercitar a imaginação e a criatividade para produzir novas figuras e encontrar propriedades interessantes sobre os números, principalmente os números primos. Depois seria apresentada a função zeta (ζ) de Riemann, seguida da hipótese de Riemann, as tentativas de provar a hipótese e o uso de computadores no processo de comprovação/negação de uma conjectura, isso deveria ser feito em duas aulas, também com exercícios no final. As últimas três aulas seriam utilizadas para apresentar o método RSA de criptografia, mostrar porque o RSA funciona e porque é seguro, e explicar o que é e como é feita uma assinatura eletrônica, finalizando com uma atividade onde os estudantes trocariam mensagens através de um sistema criado por eles, com base no método RSA de criptografia. Deve-se destacar que todos os exercícios deveriam ser de nível fundamental por estar se trabalhando com estudantes de Ensino Médio.

7.5 Metodologia

Antes de tudo deveria ser aplicado um questionário (pré-teste) simples para se ter uma noção dos conhecimentos que os estudantes tinham sobre números primos e suas capacidades de observação e análise de padrões. O foco do trabalho é a distribuição de números em formas geométricas, como na espiral de Ulam, buscando sempre a descoberta de propriedades interessantes nessas distribuições. No entanto, o mote para atrair o interesse do estudante seria a criptografia. Assim, a criptografia deveria ser apresentada logo de início de forma mais geral, por meio de indagações do tipo: Vocês sabem o que é criptografia? Onde a criptografia é empregada? Vocês sabem como são criptografadas as mensagens que vocês mandam por WhatsApp ou as informações dadas na hora de uma compra pela internet? Em seguida, seria colocado que a partir daquele momento eles teriam acesso aos conhecimentos por trás da criptografia.
Após os passos descritos acima, as atividades deveriam ser desenvolvidas por meio de aula expositiva-dialogada, com bastante exemplos para facilitar o entendimento por parte dos estudantes; soluções de problemas, pois é impossível aprender matemática de verdade apenas lendo e ouvindo, é preciso arregaçar as mangas e resolver muitos problemas e exercícios; estudo de caso, especialmente quando estiver-se trabalhando com as espirais de Ulam e Sacks e as outras formas geométricas; estudos dirigidos, entre outros. No término

das atividades, devria ser aplicado um novo questionário (pós-teste) que serviria para diagnosticar os possíveis avanços na aprendizagem dos estudantes.

7.6 Avaliação

A avaliação contaria com uma avaliação diagnóstica, o pré-teste, feita normalmente no início de uma nova fase de ensino, abrangendo parte dos conteúdos trabalhados durante as atividades relativas à proposta de trabalho aqui apresentada, com o intuito de captar o que os alunos sabem e o que eles não sabem, dando uma visão do que deveria ser trabalhado com mais ênfase. No entanto, há de se considerar que boa parte dos conteúdos que seriam trabalhados não são de conhecimento de estudantes do Ensino Médio e, portanto, esta avaliação diagnóstica teria maior importância na determinação do ponto de partida, mas pouca relevância na indicação do trajeto a ser percorrido.

A avaliação formativa, utilizada para medir a aprendizagem do estudante durante o transcorrer de cada aula, também estaria presente ao levarmos em consideração o envolvimento dos estudantes durante todo o processo, através de suas posturas e comportamentos e, principalmente, por meio dos questionamentos levantados pelos mesmos no transcorrer das aulas.

O desempenho dos estudantes na resolução dos exercícios e atividades propostas, em cada aula, faria parte da avaliação comparativa, que serviria para indicar quais conteúdos os alunos estariam dominando e quais não estariam, servindo, portanto, como "bússola" e "termômetro" das atividades a serem desenvolvidas, indicando o caminho a ser seguido e o momento de parar e "remediar" as dificuldades.

Por fim, teria-se a avaliação somativa, feita no final do curso para avaliar quantos conteúdos os discentes aprenderam no geral, com base nas respostas dadas pelos alunos no questionário final (pós-teste). Neste questionário final, cada estudante demonstraria sua capacidade de desempenho dentro de um padrão determinado, indicando assim sua proficiência geral para todos os conteúdos trabalhados.

7.7 Atividades Desenvolvidas

Por causa do isolamento social, ocasionado pela pandemia do novo coronavírus, as atividades presenciais não puderam ser desenvolvidas. Assim, foram realizadas aulas à distância, usando-se o Google Meet, com alunos participantes do programa OBMEP na Escola, do qual o autor faz parte como professor da educação básica (PEB), no período entre os dias 15 de junho e 1º de julho de 2020, nas segundas, quartas e sextas-feiras de cada semana, com duração de 3 horas cada aula, tendo início às 13h30min e terminando às 16h30min. No entanto, por motivos variados, a participação dos alunos foi baixa, tendo participado das aulas 8 alunos de um total de 20 que participam do programa (apenas 13

receberam o convite via WhatsApp).

Primeiramente, foi aplicado um questionário com perguntas simples como: O que é um número primo? O que é um número composto? Como se faz para descobrir se um número é primo? Quantos números primos existem? Quais os 10 primeiros números primos em ordem crescente?

Curiosamente, todos responderam corretamente a primeira pergunta, mas a maioria não soube responder à segunda. Outro fato interessante, foi que, mesmo respondendo corretamente a primeira pergunta, quando eles foram responder a quinta questão (dos 10 primeiros números primos), a maioria colocou algum número que possuía mais de dois divisores inteiros positivos, contrariando sua resposta à primeira questão. Em boa parte porque não utilizaram nenhum método prático para encontrar esses primos, como, por exemplo, o crivo de Eratóstenes, dando a resposta "de cabeça".

Como planejado, as aulas tiveram início sendo discutido o tema da criptografia nos dias atuais. Depois os conteúdos foram sendo apresentados seguindo a ordem apresentada no planejamento. Nas primeiras 3 aulas houve problemas de conexão quando era feita a apresentação dos slides com o conteúdo da aula, então, a partir da quarta aula, foram enviados para os alunos, via WhatsApp, os resumos dos conteúdos em PDF.

Na primeira aula, em 15 de junho, foi discutido sobre o princípio da indução finita, divisibilidade, o algoritmo da divisão, mdc, o algoritmo de Euclides, números primos, o teorema fundamental da Aritmética e mmc, e ficou faltando falar sobre critérios de divisibilidade, que fazia parte do planejamento, por causa da queda de conexão ocorrida.

Em 17 de junho foi realizada a segunda aula, iniciando por critérios de divisibilidade, que havia deixado de ser dado na aula anterior, e prosseguindo com congruência e suas propriedades básicas, a função φ de Euler e os teoremas de Fermat e Euler, e, mais uma vez por motivo de queda na conexão, não houve a explanação do teorema de Wilson, que também fazia parte do planejamento para aquela aula, apesar da acelerada na explanação dos conteúdos que foi posta em prática após a conexão retornar.

O teorema de Wilson foi o ponto de partida da terceira aula, prosseguindo com o teorema chinês dos restos, ordem módulo n, e, pela perda de conexão mais uma vez, foi pulado o conteúdo do conjunto quociente $\mathbb{Z}_n$, continuando então com o teorema dos números primos, primos gêmeos e primos de Sophie Germain.

A quarta aula foi dada em 22 de junho, com os conteúdos sobre fórmulas para primos, testes de primalidade e as espirais de Ulam e Sacks.

Não houve aula dia 24 de junho e, desta forma, a quinta aula foi realizada no dia 26 de junho com a apresentação de outras formas geométricas, nas quais são distribuídos números naturais e destacados os primos, para possíveis descobertas de propriedades envolvendo a distribuição dos primos. A parte final da aula foi deixada para que os alunos criassem suas próprias figuras e procurassem descobrir alguma propriedade interessante sobre a distribuição dos primos naquelas figuras, para depois apresentarem aos demais colegas.

A sexta aula foi utilizada para expor sobre a função zeta de Riemann, a hipótese de Riemann, as tentativas de provar a hipótese de Riemann e o uso de computadores na tentativa de comprovação ou negação de uma conjectura, além de ser discutido também sobre o método RSA de criptografia, mostrar porque o RSA funciona e porque é seguro e como é posta em prática uma assinatura eletrônica.

A última aula foi realizada no dia 1º de julho e nela os estudantes praticaram o que aprenderam sobre criptografia, criando um sistema baseado no método RSA de criptografia e trocando mensagens por ele. Entretanto, por questão de tempo, a troca de mensagens não foi realizada, porque eles demoraram para criar o sistema e depois para codificarem as mensagens. Na parte final da aula os estudantes responderam ao questionário final, abrangendo todos os conteúdos abordados.

Os alunos participantes, em sua maioria, ao serem questionados sobre os conteúdos abordados durante aquelas aulas, responderam terem ficado mais entusiasmados quando discutiu-se sobre congruência, os teoremas de Fermat e Euler, o teorema chinês dos restos, os testes de primalidade, a espiral de Ulam e a criptografia, é claro.

Durante a quinta aula, quando os alunos tinham de criar figuras com números naturais e procurar propriedades dos primos nessas distribuições, apenas três estudantes enviaram as fotos e, por coincidência, as figuras enviadas eram, basicamente, a mesma, uma espécie de "escadaria" onde cada degrau era composto por retângulos, de tal forma que a cada nível havia um retângulo a mais que no nível anterior.

Os problemas encontrados podem ser justificados pelo distanciamento, que faz com que os estudantes se acomodem e não deem o melhor de si e o professor não está presente para chamá-los à atenção e orientá-los com maior pertinência. Entretanto, apesar das dificuldades encontradas por causa do isolamento social, os trabalhos obtiveram êxito no que se pretendia, tendo em vista que a maioria dos estudantes que participaram das aulas tomaram conhecimento de que há muito mais sobre números primos que simplesmente o fato de serem números com apenas dois divisores positivos, reconheceram a importância do conhecimento de propriedades ligadas aos números primos e sua distribuição, ficaram cientes dos efeitos teóricos e práticos da possível prova da hipótese de Riemann e exercitaram a criatividade, a elaboração de conjecturas e a linguagem matemática aplicada nas demonstrações de teoremas, proposições, lemas e corolários por meio de experimentação matemática, além de exercitarem a curiosidade intelectual e utilizarem a linguagem matemática e científica para se expressar e partilhar informações e ideias.

Conclusão

Como já foi posto anteriormente, a BNCC não coloca os números primos como conteúdo a ser abordado no Ensino Médio, mas por outro lado ela orienta que o foco dos trabalhos dos professores e professoras deve estar nos objetivos a serem alcançados, sendo os conteúdos apenas as ferramentas para se alcançar esses objetivos e, assim, os professores e professoras têm uma certa liberdade na escolha dos conteúdos que trabalharão durante o ano letivo. Além disso, a Lei de Diretrizes e Bases da Educação (LDB), em seu artigo 35, alínea I, estabelece que uma das finalidades do Ensino Médio é "a consolidação e o aprofundamento dos conhecimentos adquiridos no ensino fundamental, possibilitando o prosseguimento de estudos" (FEDERAL, 2005) e o Novo Ensino Médio traz o desenvolvimento de atividades por meio dos itinerários formativos que possibilitam àqueles que se interessam por Matemática se aprofundarem nos temas abordados por essa ciência maravilhosa.

Sendo assim, é importante que os estudantes tenham contato com demonstrações matemáticas e, para tanto, é de suma importância, inicialmente, que eles conheçam e saibam aplicar o princípio da indução finita, em suas duas formas. O trabalho com congruência e suas propriedades é também bastante interessante para os estudantes do Ensino Médio, como também os teoremas de Fermat, Euler e Wilson, o teorema chinês dos restos, os testes de primalidade e, principalmente, a espiral de Ulam.

A espiral de Ulam e suas variações são formas simples e criativas de se trabalhar com todos os conteúdos relacionados com os números primos. Por meio dessas figuras é possível se investigar polinômios geradores de primos, números particulares, congruências, testes de primalidade e muito mais, de forma que possibilita, ainda, que os estudantes criem suas próprias conjecturas e tentem demonstrá-las, motivando, desta forma, o trabalho de pesquisa em Matemática, em particular, no campo da Teoria dos Números.

Assim, ao imaginar novas formas geométricas nas quais os números inteiros positivos serão escritos e observando possíveis características no posicionamento dos números primos, o estudante passa a se sentir protagonista no estudo da Matemática e não somente um receptor de conhecimentos adquiridos por gerações passadas. Portanto, ele começa a adotar uma postura mais positiva frente à Matemática e, consequentemente, melhora seu desempenho na mesma e até mesmo em outras disciplinas escolares.

Referências

BRASIL. *Base nacional comum curricular*. Brasília: MEC/SEB, 2017.

COUTINHO, S. C. *Primalidade em tempo polinomial*. Rio de Janeiro: Sociedade Brasileira de Matematica, 2004.

COUTINHO, S. C. *Números Inteiros e Criptografia RSA*. Rio de Janeiro: IMPA, 2014.

ENZENSBERGER, H. M. *O diabo dos números*. São Paulo: Companhia das Letras, 2009.

F., D. C. d. M.; ROCHA, L. S. Enrolando os primos dos primos de nossos primos. *Revista do Professor de Matemática*, SBM, Rio de Janeiro, n. 98, p. 28–32, 2019.

FEDERAL, S. *Lei de diretrizes e bases da educação nacional*. [S.l.]: Brasília, 2005.

HEFEZ, A. *Aritmética*. Rio de Janeiro: SBM, 2016.

LEITE, P. F. Números de fermat. *Revista do Professor de Matemática*, SBM, Rio de Janeiro, n. 7, p. 30–33, 1986.

MARTINEZ, F. B. et al. *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro*. Rio de Janeiro: IMPA, 2018.

MOREIRA, C. T. d. A. e. a. *Tópicos de Teoria dos Números*. Rio de Janeiro: SBM, 2012.

N., A. M. *Tópicos de Matemática Elementar: Teoria dos Números*. Rio de Janeiro: SBM, 2013.

RIBENBOIM, P. *Números primos: velhos mistérios e novos recordes*. Rio de Janeiro: IMPA, 2014.

SANTOS, J. P. O. *Introdução à Teoria dos Números*. Rio de Janeiro: IMPA, 2018.

SAUTOY, M. D. *A música dos números primos: a história de um problema não resolvido na matemática*. Rio de Janeiro: Zahar, 2007.

SINGH, S. *O último teorema de Fermat*. Rio de Janeiro: Record, 1999.

Apêndices

APÊNDICE A – Pré-teste

PRÉ-TESTE COM ALUNOS PARTICIPANTES DO PROGRAMA OBMEP NA ESCOLA SOBRE NÚMEROS PRIMOS

NOME:_____

IDADE:_____ SÉRIE:_____

A ESCOLA QUE VOCÊ CONCLUIU O ENSINO FUNDAMENTAL ERA:

( ) MUNICIPAL ( ) ESTADUAL ( ) PRIVADA

1) O que é um número primo?

_____

_____

_____

2) O que é um número composto?

_____

_____

_____

3) Como se faz para descobrir se um número é primo?

_____

_____

_____

_____

4) Quantos números primos existem?

_____

5) Quais os 10 primeiros números primos em ordem crescente?

_____

APÊNDICE B – Pós-teste

AVALIAÇÃO FINAL DOS TRABALHOS SOBRE A DISTRIBUIÇÃO DOS NÚMEROS PRIMOS

NOME:_____

1) Demonstre por indução que para $n \geq 1$ natural

a) $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$

b) $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$

c) $(1^5 + 2^5 + \cdots + n^5) + (1^7 + 2^7 + \cdots + n^7) = 2(1 + 2 + \cdots + n)^4$

2) Encontre todos os inteiros positivos tais que

a) $n + 1 | n^3 - 1$

b) $2n - 1 | n^3 + 1$

3) Sejam a e b dois inteiros positivos e d seu máximo divisor comum. Demonstre que existem dois inteiros positivos x e y tais que $ax - by = d$.

4) Calcule o resto da divisão de 2^{2011} por 97.

5) Encontrar uma sequência de pelo menos 30 inteiros consecutivos e compostos.

6) Mostrar que se a e b são inteiros positivos com $(a,\ b) = [a,\ b]$, então $a = b$.

7) Resolver os seguintes sistemas:

a) $\begin{cases} x \equiv 1\ (mod\ 2) \\ x \equiv 2\ (mod\ 3) \\ x \equiv 5\ (mod\ 7) \end{cases}$

b) $\begin{cases} 2x \equiv 1\ (mod\ 5) \\ 3x \equiv 2\ (mod\ 7) \\ 5x \equiv 7\ (mod\ 11) \end{cases}$

8) Mostrar que $a^7 \equiv a\ (mod\ 21)$ para todo inteiro a.

9) Mostrar que se p e q são primos, $p \geq q \geq 5$, então $p^2 - q^2 \equiv 0 (mod\ 24)$.

10) Encontrar o máximo divisor comum de $(p-1)! - 1$ e $p!$ (p primo).