UNIVERSIDADE ESTADUAL DO
SUDOESTE DA BAHIA

UNIVERSIDADE ESTADUAL DO SUDOESTE DA BAHIA
DEPARTAMENTO DE CIÊNCIAS EXATAS E TECNOLÓGICAS - DCET
LICENCIATURA EM MATEMÁTICA

ANA PAULA GAMA DOS SANTOS

Números primos: propriedades, estudiosos, problemas em aberto e avanços recentes

Vitória da Conquista - Ba
2022

ANA PAULA GAMA DOS SANTOS

Números primos: propriedades, estudiosos, problemas em aberto e avanços recentes

Monografia apresentada ao Departamento de Ciências Exatas e Tecnológicas da Universidade Estadual do Sudoeste da Bahia, Campus Vitória da Conquista - Ba, para obtenção do título de licenciado em Matemática, sob orientação Prof. Mestre Altemar Brito Lima.

Vitória da Conquista - Ba
2022

Folha de aprovação

Ana Paula Gama dos Santos

Números primos: propriedades, estudiosos, problemas em aberto e avanços recentes

Monografia apresentada ao Colegiado do Curso de Matemática como requisito parcial para aprovação na disciplina Seminário de Pesquisa II do Curso de Licenciatura em Matemática.

Aprovado em:

BANCA EXAMINADORA:

Prof. Altemar Brito Lima - UESB
Orientador

Prof. Antônio Augusto Oliveira Lima
UESB

Prof. Júlio César dos Reis
UESB

Vitória da Conquista - Ba
2022

Resumo

O presente trabalho irá abordar como temática os Números Primos cuja definição usual trata-se de um número divisível por 1 e por si mesmo.A fim de estudar esses números, neste trabalho serão abordardas as suas propriedades, tipos, história de alguns matemáticos que buscavam estudar o tema, problemas em abertos e principais avanços ao longo dos anos. Por se tratar de um trabalho de conclusão do curso, serão considerados resultados básicos que são vistos na disciplina de Teoria dos Números na graduação, deixando legível a um público mais amplo.

Palavras-chave: Números primos, matemáticos, Teoria dos Números.

Sumário

1 Introdução

A Teoria dos Números tem sido uma das áreas da Matemática que vem despertando a curiosidade e fascínio de muitos pesquisadores e nos cursos de graduação vem abordar de maneira abstrata e também algébrica o conjunto dos números inteiros e suas propriedades. Na Grécia Antiga, por volta de 776 a 323 a.C. começaram a desenvolver na Matemática, a visão de ciência dedutiva com definições, postulados, axiomas e teoremas, tornando essa área muito importante para as demais.

Por isso, este trabalho abordará os Números Primos cuja definição usual é "Um número natural diferente de 0 e de 1 e que é apenas múltiplo de 1 e de si próprio é chamado de número primo. Um número diferente de 0 e de 1 que não é primo é chamado de número composto"(HEFEZ, 2009, p. 31).

No livro VII de *Os Elementos* de Euclides está escrito que "Os números primos são uma classe de números muito importantes, e grande parte da Teoria dos Números ocupa-se de sua análise.". As suas propriedades são fundamentais para o estudo dos números inteiros e sua contribuição atualmente na Criptogrfia tem servido de grande avanço para o desenvolvimento de códigos de maneira a garantir mais segurança nesta era tecnológica.

Segundo (SAUTOY,2007, p. 07), "A importância matemática dos primos se deve a capacidade de gerar todos os números", por isso que os números primos causam tanta curiosidade nos estudiosos que se dedicam a tal tema.

No entanto, um problema relacionado aos números primos é poder encontrar um procedimento para determiná-los, pois conforme mostrado por Euclides no livro *Os Elementos*, esses números são infinitos. E com base no estudo de vários matemáticos que serão vistos no decorrer deste trabalho, nota-se que a determinação de todos esses números não é uma tarefa fácil.

Dessa forma, levando em conta a importância dos números primos, o objetivo deste trabalho é trazer um compilado de materiais sobre o tema proposto a fim de apresentar e estudar suas propriedades, seus tipos, criadores, os problemas em aberto e avanços recentes em seu estudo.

Embora o estudo dos números primos seja um tema relevante para a Teoria dos Números disciplina presente em alguns cursos de matemática que utiliza de métodos sofisticados e avaçados, poucos foram os avanços recentes em seus estudos e muitas dúvidas sobre o tema ainda permanecem como, por exemplo, se existe um padrão para determiná-los e se os tipos de primos aqui estudados são ou não infinitos.

2 Alguns conceitos e resultados preliminares

Neste capítulo serão apresentados alguns conceitos e resultados matemáticos para o estudo dos números primos. Iniciando na construção dos números naturais, passando pelas operações, máximo divisor comum, congruências e finalizando com os testes de primalidade.

2.1 Axiomas de Peano

A criação dos números naturais se deve a necessidade de se formalizar o processo de contagem. Para isso, será definido o que é um número natural, com base nos estudos Giuseppe Peano (1858-1932) que criou os axiomas para elaborar a teoria dos números naturais.

Nos axiomas de Peano observa-se que o zero "0"não seria considerado um número natural, mas tendo em vista os objetivos deste trabalho, o zero será incluído como um número natural. Sendo assim, pode-se pensar na construção do conjunto dos números naturais da seguinte forma: $\mathbb{N} = 0, 1, 2, 3, 4, 5, ...$ A notação $\mathbb{N}^*$ será usada para indicar o conjunto dos números naturais sem o zero.

Considere como não-definidos o conjunto $\mathbb{N}$ e a função $s : \mathbb{N} \to \mathbb{N}$, onde para cada $n \in \mathbb{N}$, o número s(n) será chamado de sucessor de n.

A função s satisfaz os seguintes axiomas:

Axioma 1. $s : \mathbb{N} \to \mathbb{N}$ injetiva, isto é, dados $m, n \in \mathbb{N}$, temos que $s(m) = s(n) \Rightarrow m = n$.

Esse axioma garante que números naturais diferentes possuem sucessores diferentes.

Axioma 2. $\mathbb{N} - s(\mathbb{N})$ consta de um só elemento.

Esse axioma garante que existe um número denominado "zero" e que é representado pelo símbolo "0", que não é sucessor de nenhum número. Logo, qualquer que seja $n \in \mathbb{N}$, tem-se que $0 \neq s(n)$.

Axioma 3. (Princípio de Indução) Se $X \subset \mathbb{N}$ é um subconjunto, tal que:

i. $0 \in X$

ii. $\forall n \in X$, tem-se também que $s(n) \in X$.

Então $X = \mathbb{N}$.

Esse axioma garante que se um subconjunto do conjunto dos números naturais contém o número 0 e esse conjunto contém o sucessor de cada um dos seus elementos, então esse subconjunto é o próprio $\mathbb{N}$.

O Princípio de Indução, além de ser útil para a demonstração de propriedades dos naturais, é importante para definir objetos. Essas definições por indução se baseiam na possibilidade de iterar uma função $f : \mathbb{N} \to \mathbb{N}$, um número arbitrário, n, de vezes, isto é,

para cada $n \in \mathbb{N}$ é possível associar a função $f^n : \mathbb{N} \to \mathbb{N}$ chamada de a n-ésima iterada de f de tal maneira que: $f^0 =$ identidade, $f^1 = f$ e $f^{s(n)} = f \circ f^n$.

A partir da definição de função iterada, serão definidas duas operações nos números naturais, cuja função utilizada será $s : \mathbb{N} \to \mathbb{N}$.

I) Adição

Dados $m, n \in \mathbb{N}$, diz-se que a soma de m com n, denotada por "$m + n$", é definida por:

$$m + n = s^n(m).$$

Assim, tem-se que:

i) $m + 0 = s^0(m) = id(m) = m$;

ii) $m + 1 = s^1(m)$ que é o sucessor de m;

iii) $m + s(n) = s(m + n)$, pois $m + s(n) = s^{s(n)}(m) = s \circ s^n(m) = s(s^n(m)) = s(m + n)$

Desta forma, pode-se substituir $s(n)$ por $n + 1$ que irá representar o sucessor de n. Assim pode-se representar a igualdade $m + s(n) = s(m + n)$ da seguinte maneira $m + (n + 1) = (m + n) + 1$.

A adição tem as seguintes propriedades:

1. **Associatividade** - Dados $m, n, p \in \mathbb{N}$, tem-se que $m + (n + p) = (m + n) + p$;
2. **Comutatividade** - Dados $m, n \in \mathbb{N}$, tem-se que $m + n = n + m$.
3. **Elemento neutro** - Para todo $n \in \mathbb{N}$, tem-se que $n + 0 = n$.
4. **Tricotomia** - Dados $m, n \in \mathbb{N}$ ocorrerá uma e apenas uma das três possibilidades:

i. $m = n$;

ii. $\exists p \in \mathbb{N}^*$, de modo que $m = n + p$;

iii. $\exists p \in \mathbb{N}^*$, de modo que $n = m + p$.

Com base na definição de adição em $\mathbb{N}$, pode-se definir uma relação de ordem nesse conjunto.

Definição 2.1. Dados $m, n \in \mathbb{N}$, diz se que m *é menor que* n (Notação: $m < n$) quando existir $p \in \mathbb{N}$ tal que $n = m + p$.

Essa relação satisfaz as seguintes propriedades:

Transitividade - Dados $m, n, p \in \mathbb{N}$, se $m < n$ e $n < p$, então $m < p$;

Tricotomia - Dados $m, n \in \mathbb{N}$ podem ocorrer um dos seguintes casos: $m = n$, ou $m < n$ ou $n < m$;

Monotonicidade da adição - Dados $m, n, p \in \mathbb{N}$, se $m < n$, então $m + p < n + p$.

II) Multiplicação

Dados $m, n \in \mathbb{N}$, o produto de m por n será entendido como a soma de n parcelas iguais a m, ou melhor, o resultado que se obtém quando se adiciona a m, $n-1$ vezes o mesmo número. Desta forma, a multiplicação será definida usando a função $f_m : \mathbb{N} \to \mathbb{N}$ dada por $f_m(p) = p + m$, isto é, f_m é a função "somar m".

Dados $m, n \in \mathbb{N}$, a multiplicação de m por n, denotado por "$m \cdot n$"é definido por:

$$m \cdot n = \begin{cases} 0, & se \quad n = 0 \\ f_m^{t(n)}(m), & se \quad n \neq 0 \end{cases}$$

onde t(n) é o antecessor.

Assim, tem-se que:

i) $m.0 = 0$;

ii) $m \cdot 1 = f_m^{t(1)}(m) = f_m^0(m) = id(m) = m$

iii) $m \cdot 2 = f_m^{t(2)}(m) = f_m^1(m) = m + m$

iv) $m \cdot 3 = f_m^{t(3)}(m) = f_m^2(m) = m + m + m$

v) $m \cdot (n+1) = f_m^{t(n+1)}(m) = f_m^n(m) = f_m^{s(t(n))}(m) = (f_m \circ f_m^{t(n)})(m) = f_m(f_m^{t(n)}(m)) = f_m(m \cdot n) = m \cdot n + m.$

A multiplicação no conjunto dos números naturais tem as seguintes propriedades:
Associatividade - Dados $m, n, p \in \mathbb{N}$, tem-se que $m.(n.p) = (m.n).p$;
Comutatividade - Dados $m, n \in \mathbb{N}$, tem-se que $m.n = n.m$;
Elemento neutro - Existe $1 \in \mathbb{N}$, tal que $m.1 = m$;
Distributividade - Dados $m, n, p \in \mathbb{N}$, tem-se $m.(n+p) = m.n + m.p$;
Monotonicidade - Dados $m, n, p \in \mathbb{N}$. Se $m < n$, então $m.p \leq n.p$.

III) Subtração

Ao definir as operações de adição e multiplicação no conjunto dos números naturais, fez-se necessário nesse trabalho definir também a operação de subtração.

Definição 2.1.1 Sejam $a, b \in \mathbb{N}$ com $a \leq b$. Então existe $c \in \mathbb{N}$, tal que $b = a + c$. Neste caso, diz-se que c é igual a b menos a (denotado por $b - a$).

Notação: $c = b - a$, c é o resultado da subtração de b por a.

Observação: Quando $a < b$ não se define $b - a$, pois o resultado da subtração não pertence aos números naturais.

Proposição 2.1 Sejam $a, b, c \in \mathbb{N}$. Se $a \leq b$, então $c \cdot (b - a) = cb - ca$

DEMONSTRAÇÃO: Note que se $a \leq b$ então $ac \leq bc$. Logo $cb - ca$ está bem definido nos naturais.

Suponha $b - a = d$ implica que $b = a + d$. Multiplicando por c esta última igualdade tem-se $cb = c \cdot (a + d) = ca + cd$ Assim, $cd = cb - ca$. Substituindo d na última igualdade por $b - a$, obtém-se o seguinte resultado: $c \cdot (b - a) = cb - ca$.

Exemplo: Seja $c = 6$ e a e b iguais a 7 e 5 respectivamente, tem-se:

$$\begin{cases} 6 \cdot (7-5) = 6 \cdot 2 = 12 \\ 6 \cdot 7 - 6 \cdot 5 = 42 - 30 = 12 \end{cases}$$

2.2 Divisibilidade

Definição 2.2 Dados dois números m, n, temos que:

i. Diz-se que m divide o número n se, e somente se, existe $q \in \mathbb{N}$ de modo que $n = m.q$.

Notação: $m|n \Leftrightarrow \exists q \in \mathbb{N}$ tal que $n = m.q$.

ii. Diz-se que m não divide o número n se, e somente se, não existe $q \in \mathbb{N}$ de modo que $n = m.q$.

Notação: $m \nmid n \Leftrightarrow \nexists q \in \mathbb{N}$ tal que $n = m.q$.

Exemplo 1: Note que se $m = 2$ e $n = 8$. Tem-se que $2|8$, pois $8 = 2 \cdot 4$.

Exemplo 2: Note que se $m = 4$ e $n = 9$. Tem-se que $4 \nmid 9$, pois não existe um número pertencente aos naturais, tal que 2 multiplicado por esse número seja 9.

Note, a semelhança da relação de divisibilidade e ordem em $\mathbb{N}$:

$$m < n \Leftrightarrow \exists q \in \mathbb{N}^*; n = m + q$$

$$m|n \Leftrightarrow \exists q \in \mathbb{N}; n = m.q$$

Proposição 2.2 Sejam $l, m \in \mathbb{N}^*$ e $n \in \mathbb{N}$ tem-se:

i. $1|n$, $l|l$ e $l|0$;

O item (i) decorre das igualdades que $n = 1.n$, $l = l.1$ e $0 = 0 \cdot l$. Tal item garante que todo número natural é divísivel por 1 e por si mesmo.

ii. se $l|m$ e $m|n$, então $l|n$.

DEMONSTRAÇÃO: Se $l|m$ e $m|n$, implica que existem f, g, tais que $m = l.f$ e $n = m.g$. Substituindo m na equação abaixo, temos:

$$n = m.g = (l.f).g = l.(f.g),$$

então $l|n$.

Proposição 2.2.1 Sejam $l, m, n, p \in \mathbb{N}$, tais que se $l|m$ e $n|p$ então $l.n|m.p$

DEMONSTRAÇÃO: Se $l|m$ e $n|p$ então $\exists f, g \in \mathbb{N}$, tais que $m = l.f$ e $p = n.g$. Temos que $m.p = (l \cdot f)(n \cdot g) = (l.n)(f.g)$. Logo, $l.n|m.p$.

Exemplo: Sejam $l = 4, m = 12, n = 3$ e $p = 6$. Tem-se que $l|m$, pois $12 = 4 \cdot 3$ e $3|6$, de fato $6 = 3 \cdot 2$. Observe que $l.n = 4 \cdot 3 = 12$ e $m.p = 12 \cdot 6 = 72$ implica que $12|72$, pois $72 = 12 \cdot 6$.

Proposição 2.2.2 Sejam $l, m, n \in \mathbb{N}$, tais que $l|(m + n)$. Então $l|m \Leftrightarrow l|n$.

DEMONSTRAÇÃO: Como $l|(m + n)$, existe $f \in \mathbb{N}$ tal que $m + n = l.f$.

Se $l|m$, tem-se que $\exists g \in \mathbb{N}$ tal que $m = l.g$. Juntando as igualdades acima, tem-se:

$$l.g + n = l.f \Rightarrow n = lf - lg \Rightarrow n = l.(f - g) \Rightarrow l|n$$

,

pois $f - g \in \mathbb{N}$ pela monotonicidade da multiplicação. A volta é análoga.

Exemplo: Sejam $l = 4, m = 3$ e $n = 5$. Note que $m + n = 8$ e $4|8$, pois $8 = 4 \cdot 2$.

Proposição 2.2.3 Sejam $l, m, n \in \mathbb{N}$ com $l \neq 0$ e $m \geq n$, tais que $l|(m - n)$. Então $l|m \Leftrightarrow l|n$.

Exemplo: Sejam $l = 2, m = 28$ e $n = 10$. Note que $2|(28 - 10)$, pois $18 = 2 \cdot 9$. Então, a proposição acima é satisfeita, pois $2|28$ e $2|10$.

Proposição 2.2.4 Se $l, m, n \in \mathbb{N}$ com $l \neq 0$ e $x, y \in \mathbb{N}$ são tais que $l|(xm + yn)$; se $xm \geq yn$ então $l|(xm - yn)$.

Exemplo: Tomando $l = 6, m = 9$, $n = 2$, $x = 8$ e $y = 6$. Note que $6|(8 \cdot 9 + 6 \cdot 2)$, pois $84 = 6 \cdot 14$. Como $xm \geq yn$, então $6|(8 \cdot 9 - 6 \cdot 2)$, a proposição acima é satisfeita, pois $6|60$.

Proposição 2.2.5 Dados $l, m, n \in \mathbb{N}^*$, tem-se que $l|m \Rightarrow m \geq l$.

Note que a relação de divisibilidade em $\mathbb{N}^*$ é uma relação de ordem, pois

i é reflexiva: $\forall l \in \mathbb{N}^*$ tem-se que $l|l$. (**Proposição 2.2 (i)**)

ii é transitiva: se $l|m$ e $m|n$, então $l|n$. (**Proposição 2.2 (ii)**).

iii é anti-simétrica: se $l|m$ e $m|l$, então $l = m$. (Segue-se da Proposição 1.6).

Teorema 1 ***(Divisão euclidiana)*** *Sejam m e n dois números naturais com $0 < m < n$. Existem dois únicos números naturais q e r tais que:*

$$n = m.q + r, \text{ com } 0 \leq r < m.$$

Diz-se que q e r são, respectivamente, o quociente e o resto da divisão de n por m.

Exemplo 1: Ache o resto da divisão de 17 por 3.

Considere as diferenças sucessivas:

$17 - 3 = 15$, $17 - 2.3 = 11$, $17 - 3.3 = 8$, $17 - 4.3 = 5$, $17 - 5.3 = 2$. Assim $17 = 5 \cdot 3 + 2$

Com isto, tem-se $q = 5$ e $r = 2$.

2.3 Máximo Divisor Comum

Mesmo quando um número m não divide n, Euclides mostrou em seu trabalho *Os Elementos* que é possível efetuar a divisão de m por n, com resto r.

Definição 2.3 Diz-se que d é o máximo divisor comum (mdc) de m e n (denotado por (m, n)) se possuir as seguintes propriedades:

i d é um divisor comum de m e de n;

ii d é divisível por todo divisor comum de m e n.

Ou seja, se c é um divisor comum de m e n, então $c|d$.

Lema 2.3 (Lema de Euclides) Sejam $m, n, t \in \mathbb{N}$ com $m < tm < n$. Se existe $(m, n - tm)$, então (m, n) existe e $(m, n) = (m, n - tm)$.

Definição 2.3.1 (Algoritmo de Euclides) Dados dois números $m, n \in \mathbb{N}$ e supondo $a \leq b$. Se $a = 1$ ou $a = b$ ou até mesmo $a|b$, tem-se que o $(a, b) = a$. Suponha $1 < a < b$ e que $a \nmid b$, pela divisão euclidiana tem-se:

$$b = aq_1 + r_1, \text{ com } r_1 < a, \text{ onde } q_1, r_1 \in \mathbb{N}.$$

Daí tem-se duas possiblidades:

i) $r_1|a$, nesse caso $r_1 = (a, r_1) = (a, b - q_1a) = (a, b)$

ii) $r_1 \nmid a$, nesse caso deve-se efetuar a divisão de r_1 por a, obtendo $a = r_1q_2 + r_2$ com $r_2 < r_1$.

Esse algoritmo de Euclides não continua indefinidamente, pois para algum n, $r_n|r_{n-1}$ o que implica $(a, b) = r_n$.

Exemplo: Calcule o mdc de 3887 e 637

	6	9	1	4
3887	637	65	52	13
65	52	13	0	

Tem-se então que $(3887, 637) = 13$.

2.4 Números primos

Nesta seção será abordado os números primos, seus resultados e papel que desempenham.

Definição 2.4 Um número natural maior do que l e que só é divisível por l e por si próprio é chamado de número primo.

Da definição decorrem:

i. Dados p, q números primos. Se $p|q$, então $p = q$

DEMONSTRAÇÃO: Da hipótese tem-se que $p|q$ e sendo q um número primo, da definição obtém-se que $p = 1$ ou $p = q$. Sendo p um número primo, tem-se que $p > 1$ o que acarreta em $p = q$.

ii. Seja p um número primo e a um número natural qualquer. Se $p \nmid a$, então $(p, a) = 1$.

DEMONSTRAÇÃO: Se $(p, a) = d$, tem-se que $d|p$ e $d|a$, obtém-se que $d = p$ ou $d = 1$. Mas $d \neq p$, pois $p \nmid a$, consequentemente $d = 1$.

Do livro *VII Os Elementos* de Euclides, tem-se o seguinte resultado:

Proposição 2.4 Sejam $a, b \in \mathbb{N}^*$ e p um número primo. Se $p|ab$, então $p|a$ ou $p|b$.

DEMONSTRAÇÃO: Basta provar que, se $p|ab$ e $p \nmid a$, então $p|b$. Mas, se $p \nmid a$, temos que $(p, a) = 1$.

Exemplo: Tomando $p = 5$, $a = 9$ e $b = 10$. Tem-se que $5|9 \cdot 10$, pois $90 = 5 \cdot 18$ e o $(5, 9) = 1$ e $5|10$, mas $5 \nmid 9$.

Corolário 2.4 Se $p, p_1, ..., p_n$ são números primos e, se $p|p_1 \cdots p_n$, então $p = p_i$ para algum $i = 1, ..., n$.

Teorema 2 ***(Teorema Fundamental da Aritmética)*** *Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Um exemplo simples da veracidade desse teorema seria pegar os números 11 e 12. O número 11 é um número primo, pois possui como divisor apenas o 1 e ele mesmo. Já o número 12 não é primo, sendo assim pelo teorema acima pode-se escreve-lo como o produto de números primos, e aí tem-se que $12 = 2 \cdot 2 \cdot 3$.

Conhecendo-se os números primos, pode-se questionar, tais números são infinitos? Essa questão é respondida e provada por Euclides no livro *IX Os Elementos*. Daí tem-se o seguinte teorema:

Teorema 3 *Existem infinitos números primos.*

DEMONSTRAÇÃO: Suponha que exista apenas um número finito de números primos $p_i, ..., p_r$. Considere o número natural

$$n = p_1 \cdot p_2 \cdots p_r + 1$$

Pelo **Teorema 2**, o número n possui um fator primo p que deve ser um dos seguintes fatores $p_1, ..., p_r$ e, consequentemente, divide o produto $p_1 \cdot p_2 \cdots p_r$. Mas isto implica que p divide $n - p_1 \cdot p_2 \cdots p_r = 1$, o que é absurdo, pois p é primo. Logo, como provado por Euclides, os números primos são infinitos.

2.5 Congruências

Definição 2.5 Seja m um número natural diferente de zero. Diz-se que dois números a e b são congruentes módulo m, se os restos da divisão euclidiana po m são iguais.
Notação: $a \equiv b \pmod{m}$

Exemplo 1: $42 \equiv 26 \bmod 4$, pois o resto da divisão de 42 e 26 por 4 é 2.

Exemplo 2: $42 \not\equiv 27 \bmod 4$, pois o resto da divisão de 42 e 27 por 4, respectivamente, é 2 e 3.

Quando $a \equiv b \bmod m$ não for verdadeira, diz-se que a e b são incongruentes.
Notação: $a \not\equiv b \pmod{m}$

Proposição 2.5 Sejam $m \in \mathbb{N}$, com $m > 1$. Para todos $a, b, c \in \mathbb{N}$, tem-se

i. $a \equiv a \bmod m$;

ii. Se $a \equiv b \bmod m$, então $b \equiv a \bmod m$;

iii. Se $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então $a \equiv c \bmod m$.

Proposição 2.5.1 Seja $a, b \in \mathbb{N}$ e suponha $a \leq b$. Tem-se que $a \equiv b \pmod{m}$ se, e somente se, $m|b - a$.

Exemplo 3: Quando $a = 42$ e $b = 26$, tem-se que $4|(42 - 26)$. Então $42 \equiv 26 \bmod 4$.

Exemplo 4: Quando $a = 42$ e $b = 27$, tem-se que $4 \nmid (42 - 27)$. Então $42 \not\equiv 27 \bmod 4$.

Proposição 2.5.2 Dados $a, b, c, d, m \in \mathbb{N}$ com $m > 1$, tem-se:

i) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$.

ii) $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $ac \equiv bd \pmod{m}$.

DEMONSTRAÇÃO: Suponha que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$. Pode-se supor, sem perda de generalidade, que $b \geq a$ e $d \geq c$. Tem-se que $—m|(b - a)$ e $m|(d - c)$. Daí observa-se que $m|(b - a) + (d - c)$, isto é, $m|(b + d) - (a + c)$.

i) Pela **Prop.2.5.1**, $a + c \equiv b + d \pmod{m}$.

ii) Note que $bd - ac = d(b - a) + a(d - c)$, conclui-se então que $m|bd - ac$. Pela **Prop.2.5.1**, $ac \equiv bd \pmod{m}$.

Exemplo 5: Seja $a = 42$, $b = 26$, $c = 18$, $d = 10$ e $m = 4$. Tem-se que $42 \equiv 26 \pmod 4$ deixando resto 2 e $18 \equiv 10 \pmod 4$ deixando resto 2. Se $42+18 \equiv 0 \pmod 4$ e $26+10 \equiv 0 \pmod 4$, então $42 + 18 \equiv 26 + 10 \pmod 4$.
Exemplo 6: Usando os mesmos dados do exemplo 5. Se

Proposição 2.5.3 Sejam $a, b, c, m \in \mathbb{N}$, com $m > 1$. Tem-se que $a + c \equiv b + c (\text{mod } m)$ $\Leftrightarrow a \equiv b \pmod{m}$.

DEMONSTRAÇÃO: Se $a \equiv b \bmod m$, segue da **Proposição 2.5.2** que $a + c \equiv b + c \bmod m$, pois $c \equiv c$ pela **Proposição 2.5 (i)**.

A recíproca também é válida, supondo que $a + c \equiv b + c \bmod m$. Pode-se supor que $b + c \geq a + c$, e assim $m|b + c - (a + c)$ o que implica que $m|b - a$. Logo $a \equiv b \bmod m$.

Exemplo: Observe que $7 + 4 \equiv 5 + 4 \pmod 2$, então $7 \equiv 5 \pmod 2$.

Mas, ao tomar $8 \cdot 4 - 5 \cdot 4 = 12$ e $2|12$. Note que $4 \cdot 8 \equiv 4 \cdot 5 \pmod 2$, no entanto $8 \not\equiv 5 \pmod 2$.

Proposição 2.5.4 Sejam $a, b, c, m \in \mathbb{N}$, com $c \neq 0$ e $m > 1$. Tem-se que $ac \equiv bc \bmod m$ $\Leftrightarrow a \equiv b \bmod \frac{m}{(c,m)}$.

DEMONSTRAÇÃO: Suponha $bc \geq ac$, como $\frac{m}{(c,m)}$ e $\frac{c}{(c,m)}$ são coprimos, tem-se $ac \equiv bc \bmod m \Leftrightarrow m|(b-a)c \Leftrightarrow \frac{m}{(c,m)}|(b-a)\frac{c}{(c,m)} \Leftrightarrow \frac{m}{(c,m)}|(b-a) \Leftrightarrow a \equiv b \bmod \frac{m}{(c,m)}$.

2.6 Testes de primalidade

Tendo-se que os números primos são infinitos, nesta seção serão vistos alguns métodos que permite testar se um número é primo.

2.6.1 Crivo de Eratóstenes

Método desenvolvido pelo matemático grego Eratóstenes de Cirene, que viveu por volta de 230 a.C. Permite determinar números primos até a ordem desejada, porém para ordem muito elevadas esse método se torna mais trabalhoso.

Um resultado para a construção do crivo de Eratóstenes é o seguinte lema:

Lema 2.6.1 Se um número natural $n > 1$ não é divisível por qualquer número primo p, tal que $p^2 \leq n$, então ele é primo.

Exemplo: Determine todos os números primos inferiores a 100, começando pelo 2.
Instruções:

i. Será escrito em uma tabela os números na ordem de 2 a 100.

ii. Risque todos os números múltiplos de 2, exceto o 2.

iii. Como 3 é primo, risque todos os múltiplos de 3, exceto o 3.

iv. Tem-se que 4 é múltiplo de 2, logo já foi riscado. Então agora será riscado todos os múltiplos de 5, exceto o próprio 5 que é primo.

v. O próximo número riscado será os múltiplos de 7, exceto o próprio 7 que é primo.

vi. Os números seguintes seriam o 8, 9 e 10 que são múltiplos de 2 e 3, por isso já foram riscados. O **Lema 2.6.1** permite parar com o procedimento acima, pois o próximo número primo é o 11 e esse número ao quadrado supera o número 100. Portanto, pode-se parar o procedimento acima.

Como resultado, obtém se a seguinte tabela:

Tabela 1: Crivo de Eratóstenes para números primos entre 2 e 100

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

Fonte: Elaborada pelo autor

2.6.2 Teste de primalidade de Fermat

O matemático francês Pierre de Fermat formulou um teste para determinar se um número é primo, de acordo com o seguinte teorema:

Teorema 4 ***(Pequeno teorema de Fermat)*** *Se p é um número primo, então para qualquer inteiro a tem-se*

$$a^p \equiv a \ (mod\ p)$$

Uma outra versão desse teorema permite considerar $a^{p-1} \equiv 1 \pmod{p}$, para p primo e a coprimo em relação a p. Diz-se que dois números são coprimos quando o mdc entre eles é 1, por exemplo, 11 e 49 são coprimos pois o mdc entre eles é 1.

Exemplo: Seja $a = 2$ e $p = 3$, substituindo em $a^{p-1} \equiv 1 \pmod{p}$ tem-se:
$2^2 \equiv 1 \pmod{3}$, o que comprova que 3 é um número primo, pois $3|3$.

Mas para afirmar que um número é primo usando o teste de Fermat, não basta apenas testar para um único valor de a, a relação acima pede que para qualquer valor de a menor que p a relação se mantenha. Por exemplo, ao pegar $a = 5$ e $p = 4$, tem-se que $5^3 \equiv 1 \pmod{4}$, mantendo a relação acima e o número 4 é um possível número primo. Mas, testando para $a = 3$, tem-se que $3^3 \not\equiv 1 \pmod{4}$, ou seja, 4 não é um número primo.

Esse teste é válido apenas no sentido de dizer que se p é primo então a equação do teorema de Fermat ou a outra versão são satisfeitas para qualquer a. Mas o contrário não é válido, pois existem inteiros positivos n compostos, tais que

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

gerando os não primos que serão chamados de pseudoprimos (não são primos, mas podem possuir alguma propriedade dos números primos) ou falsos primos ou números de Carmichael.

Exemplo: Seja $a = 2$ e $p = 341$, substituindo em $a^{p-1} \equiv 1 \pmod{p}$ tem-se:

$2^{340} \equiv 1 \pmod{341}$, obedece a equação do teorema de Fermat, mas $341 = 11 \cdot 31$ que é um número composto, esse tipo de resultado são os falsos primos.

O teste de primalidade de Fermat permite concluir que para cada valor de a existe uma infinidade de não primos para os quais a^{p-1} é divísivel por p. Esse procedimento permite testar o pequeno teorema de Fermat uma quantidade n de vezes para valores de a aleatórios.

Por isso, que se um determinado p testado obedecer a equação de Fermat para qualquer valor de a esse número é primo, quanto mais p for testado para os valores de a mais confiável será o resultado. Em caso de algum valor de a testado não obedecer a equação do teorema de Fermat, esse número não será primo.

O teste de primalidade de Fermat foi o primeiro teste criado para analisar a primalidade de um número específico. Foi considerado rápido e prático para determinar a primalidade de um número dado qualquer. Porém, atualmente não é mais considerado tão eficiente.

2.6.3 Teste de primalidade de Lucas-Lehmer

O matemático francês François Édouard Anatole Lucas desenvolveu um algoritmo para determinação de números primos em 1876 e seu algoritmo foi aperfeiçoado pelo também matemático Normando Lehmer do Derrick em 1930. Tal algoritmo pode ser definidido da seguinte maneira:

Teorema 5 *Sejam L_n um número de Lucas-Lehmer e M_n um número de Mersenne. Um número de Mersenne M_n será primo se, e somente se,*

$$L_{n-2} \equiv 0 \ mod(M_n),$$

onde $M_n = 2^n - 1$, $L_0 = 4$ e $L_n = {L^2}_{n-1} - 2$.

A vantagem desse teste é que ao ser gerado um número L_n, para testá-lo basta verificar se o número M_n o divide.Porém, esse teste de Lucas-Lehmer é eficiente para a linguagem computacional, que não será testado aqui pois não é o foco do trabalho.

2.6.4 Teste de primalidade Miller-Rabin

Os cientistas Gary Miller e Michael Rabin desenvolveram um algoritmo para determinar a primalidade de um número.

O teste de primalidade de Miller-Rabin diz que, dado um natural n ímpar que será testado, pode-se escrever $n-1$ na forma $2^t d$, onde t é um natural qualquer e d é um natural ímpar. Deve-se escolher um natural qualquer que será aqui chamado de r, tal que $r < n$. A partir daí deve-se realizar os seguintes testes:

i) $r^d \equiv 1 \pmod{n}$;

ii) $r^{2^i d} \equiv -1 \pmod{n}$, i variando entre 0 e $t-1$.

Se apenas um dos testes acima for verdadeiro, esse n será chamado de pseudoprimo. Mas, se os dois testes forem verdadeiros, então n será um número primo.

Devido a precisão do algoritmo de Miller-Rabin, esse é o teste mais utilizado para testar a primalidade de um número.

2.6.5 Teste de primalidade AKS

Esse algoritmo para testar a primalidade de um número, foi desenvolvido pelos cientistas indianos Manindra Agrawal, Neeraj Kayal e Nitin Saxena. O algoritmo foi desenvolvido em 2002 e o teste recebe esse nome com base na inicial dos sobrenomes de seus criadores.

O algoritmo AKS é considerado simples e não faz uso de nenhum conceito de matemática aplicada. Esse teste é baseado no pequeno teorema de Fermat já citado anteriormente. O algoritmo de AKS pode ser definido da seguinte maneira:

Teorema 6 *Seja $n \in \mathbb{N}$ e $n > 2$. Se $a \in \mathbb{N}$ e o $(a, n) = 1$, então n é um número primo se e somente se*

$$(x + a)^n \equiv x^n + a \ (mod\ n)$$

O algoritmo AKS é considerado simultaneamente polinomial, probabilistico e incondicional, ou seja, o tempo de processamento do algoritmo pode ser expresso como um polinômio por isso, o algoritmo permite determinar com certeza se um número é primo ou composto.

3 Números primos e seus estudiosos

Neste capítulo serão abordados alguns autores, suas histórias, tipos de primos e as contribuições para o estudo dos números primos.

3.1 Fibonacci

Leonardo Febonacci nasceu na Itália em 1170, cuja família era próspera e reconhecida na região. E foi através das atividades do pai como mercador que teve contato com a matemática arábe e hindu.

A sua contribuição matemática pela qual é mais conhecido é a sequência de Fibonacci. Ele também com o apoio do imperador Frederico II introduziu os algarismos arábicos na matemática, pois segundo ele, esses algarismos eram mais eficazes do que os algarismos romanos para fazer cálculos.

A sequência de Fibonacci foi desenvolvida em 1202 e os números 0 e 1 são especiais pois da início a sequência de Fibonacci. Essa seqência diz que "cada número seguinte da série é formado pela soma dos dois anteriores"(PERUZZO, 2012, p. 37). Essa sequência pode ser representada pela seguinte fórmula em $F_{n+1} = F_n + F_{n-1}$ ou $F_n = F_{n-1} + F_{n-2}$.

Daí tem-se a seguinte sequência de Fibonacci: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, ..., como pode-se notar trata-se de uma sequência infinita. Os números primos de Fibonacci são os números primos que pertencem a sequência de Fibonacci. Os 10 primeiros números primos de Fibonacci são os seguintes: 2, 3, 5, 13, 89, 233, 1597, 28.657, 514.229, 433.494.437.

3.2 Mersenne

Marin Mersenne nasceu no ano de 1588 na França, filho de camponeses. De 1609 a 1611 estudou Teologia em Sorbonne, depois entrou para a Ordem Religiosa de Minims devotando-se à oração e aos estudos. Em 1612 foi para Paris e tornou-se padre no Place Royale.

Mersenne começou a se interessar pela ciência através dos trabalhos de Galileu Galilei, a partir daí começou a se comunicar através de correspondências e encontros com alguns dos maiores cientistas da época como René Descartes, Pierre de Fermat, Evangelista Torricelli e Blaise Pascall.

Mersenne tentou escrever uma fórmula que descrevesse todos os números primos, porém não obteve sucesso. Em uma de suas correspondências, Fermat descreve uma de suas teorias sobre os primos e uma fórmula capaz de gerar alguns primos, que hoje é conhecida como os primos de Fermat. É a partir daí que Mersenne começou a estudar os números da forma $2^n \pm 1$ com $n \in \mathbb{N}$, para procurar primos desta forma.

Definição 3.2 O número da forma $M_n = 2^n - 1$, com n número natural, é dito primo de Mersenne quando for um número primo.

Note que:

$M_0 = 2^0 - 1 = 0$ não é primo
$M_1 = 2^1 - 1 = 1$ não é primo
$M_2 = 2^2 - 1 = 3$ é primo
$M_3 = 2^3 - 1 = 7$ é primo
$M_4 = 2^4 - 1 = 15$ não é primo
$M_5 = 2^5 - 1 = 31$ é primo
$M_6 = 2^6 - 1 = 63$ não é primo
$M_7 = 2^7 - 1 = 127$ é primo

Assim M_n é primo para $0 \leq n \leq 7$ se e só se n é primo. Será possível afirmar que M_n é primo se e só se n é primo?

A volta não é verdadeira, pois

$M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$ não é primo.

Com relação a ida , tem-se o seguinte resultado:

Teorema 7 *Se $M_n = 2^n - 1$ com $n \in \mathbb{N}$ é primo, então n é primo.*

Em 1644, Mersenne publicou no Cogitata Physico Mathematica uma lista, onde afirmava que M_n é primo para $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ e 257.

Três seculos mais tarde, foram verificados quais são os primos de Mersenne para n primo e $2 \leq n \leq 257$. Descobriu-se, que na verdade:

i. M_{67}, M_{267} não são primos (demonstrando um erro na lista publicada por Mersenne);

ii. M_{61}, M_{89} e M_{107} são primos (demonstrando um "esquecimento"na lista publicada por Mersenne).

Portanto, para n primo e $2 \leq n \leq 19$, temos que os números primos de Mersenne são: $3, 7, 31, 127, 8.191, 131.071, 524.287$, os demais números primos de Mersenne para $n \leq 257$ não serão aqui mostrados, pois são números que podem ultrapassar 30 digítos.

Existem algumas dificuldades sobre determinar se M_p é primo ou composto e se composto quais primos o compõe. No intuito de resolver tais dificuldades, tem-se os seguintes resultados .

Teorema 8 *Se p é um número primo e $p \equiv 3$ Mod(4), então $2p + 1$ divide M_p se, e somente se, $2p + 1$ é primo, neste caso, se $p > 3$, então M_p é composto.*

Exemplo: Seja $p = 67$, tem-se que $67 \equiv 3 \pmod 4$. Segundo o teorema acima $2 \cdot 67 + 1 = 135$ divide M_{67}, se 135 for primo. Mas, $135 = 3^3 \cdot 5$ seguindo a definição, não é um número primo. Logo $135 \nmid M_{67}$

Teorema 9 *Se k divide M_n (onde $n > 2$), então $k \equiv \pm 1$ mod(8) e $k \equiv 1$ mod(n).*

Teorema 10 *O número M_n é primo se, e somente se, M_n divide S_{n-2}, onde $S_{n+1} = S_{n-2}^2$ e $S_0 = 4$.*

Esses três resultados permitem determinar os fatores de um número de Mersenne composto.

Os 10 primeiros números primos de Mersenne são: 2, 3, 5, 7, 13, 17, 19, 31, 61 e 89.

Foram descobertos até então 51 números primos de Mersenne, o último foi descoberto em 2017 devido ao projeto de pesquisa Great Internet Mersenne Prime Search (GRIMPS) que busca primos de Mersenne e ao todo já descobriram 17 primos de Mersenne, o maior número até então encontrado é $2^{82.589.933} - 1$, com 24.862.048 digítos.

Apesar de já terem sido encontrados 51 números primos de Mersenne, alguns questionamentos ainda permanecem como, por exemplo, se esses números primos de Mersenne são infinitos ou não.

3.3 Fermat

Pierre de Fermat foi um grande matemático francês, nascido no ano de 1601, mas não vivia da Matemática era um magistrado da corte de Toulouse.

Em 1621 com a pubicação do livro em grego *Aritmética de Diofanto* por Claude-Gaspard Bachet de Méziriac, tem se o pontapé inicial da história de Fermat na Matemática. Este livro é importante, pois foi ao adquiri-lo que Fermat começou a se interessar pela teoria dos números e a partir daí ele desenvolveu várias ideais que são importantes para diversas áreas de conhecimento da matemática.

Nessa epóca, a comunicação era muito difícil, por isto muitos matemáticos da epóca se comunicavam através de cartas. Ao ser provada a infinidade dos números primos, alguns matemáticos desenvolveram métodos capazes de determinar alguns desses números. Fermat, em uma de suas cartas com Bernard Frénicle de Bessy, escreveu que os números da forma $F_n = 2^{2^n} + 1$ $n \in \mathbb{N}$, são números primos, embora não tenha completado sua prova.

Definição 3.3 O número da forma $F_n = 2^{2^n} + 1$ para $n \in \mathbb{N}$, será chamado primo de Fermat, quando for um número primo.

Note que:

$F_0 = 2^{2^0} + 1 \Rightarrow F_0 = 2 + 1 = 3$ é primo

$F_1 = 2^{2^1} + 1 = 5$ é primo

$F_2 = 2^{2^2} + 1 = 17$ é primo

$F_3 = 2^{2^3} + 1 = 257$ é primo

$F_4 = 2^{2^4} + 1 = 65537$ é primo

$F_5 = 2^{2^5} + 1 = 641 \cdot 6700417$ não é primo

Ao provar tal afirmação que $F_n = 2^{2^n} + 1$ é primo, inicialmente Fermat considerava que F_5 era um número primo. Essa hipótese só foi "derrubada"em 1732, quando o matemático Leonard Euller, demonstrou que F_5 não é um número primo e sim composto pelo produto de primos. Mas tal equivoco não foi percebido por Fermat e em uma de suas correspondências com Bernard F. de Bessy em outubro de 1640, confessou que não havia provado tal resultado e sua verificação era feita através da fatoração.

De acordo com [COUTINHO, 1997], os números citados acima de F_0 a F_4 são os únicos primos de Fermat conhecidos datados do século XVII e pouco sabe-se se esses números primos são infinitos ou não. Uma conjectura de Godfrey Harold Hardy e Edward Maitland Wright diz que esses números são finitos, mas esta também não descarta a possibilidade de existirem outros primos além dos mencionados acima. Ou seja, não há provas de que os primos de Fermat são infinitos ou não e se tem outros números primos além dos já encontrados.

Portanto o maior primo de Fermat conhecido é o número 65.537 e além disso, sabe-se que seu maior número composto é o $F_{2478782}$ com 746190 algarismos.

Fermat morreu no ano de 1665 e seu filho mais velho Clement Samuel Fermat reuniu e publicou as 48 demonstrações feitas por Fermat, que estavam dispostas em anotações no livro *Aritmética de Diofanto*, observações e cartas.

Atualmente Fermat é considerado como fundador da Teoria dos Números moderna, tendo também contribuições essenciais para a geometria analítica, para a teoria da probabilidade e também para o cálculo diferencial e integral.

3.4 Wilson

John Wilson Applethwaite nasceu na Inglaterra em 1741. Estudou na Peterhouse College a partir de 1757 e teve aulas com Edward Waring (matemático inglês). Em 1761, Wilson recebeu o título de Senior Wrangler, que era concedida aos alunos ao final do 3° ano que apresentavam excelentes resultados em matemática.

Ele é considerado como um dos maiores matemáticos ingleses e sua principal contribuição foi em teoria dos números, no estudo dos números primos.

Definição 3.4. Seja p um número primo. Dizemos que p é um primo de Wilson se $p^2|[(p-1)!+1]$, ou seja, $(p-1)! \equiv -1(mod\, p^2)$.

Note que:

Tabela 2: Testando possíveis números primos de Wilson

p	p^2	$(p-1)!+1$	**Análise**
2	4	$(2-1)!+1=2$	$4 \nmid 2$, então 2 não é primo de Wilson
3	9	$(3-1)!+1=3$	$9 \nmid 3$, então 3 não é primo de Wilson
5	25	$(5-1)!+1=25$	$25\|25$, então 5 é primo de Wilson
7	49	$(7-1)!+1=721$	$49 \nmid 721$, então 7 não é primo de Wilson
13	169	$(13-1)!+1=479.001.601$	$169\|479.001.601$, então 13 é primo de Wilson

Fonte: Elaborada pelo autor

Nota-se com base na definição, que até então foi possível determinar os números 5 e 13 como números primos de Wilson. Existe grande dificulade em determinar outros números primos, pois conforme se aumenta o fatorial de p cresce muito e não é possível determinar através da calculadora comum. O próximo número primo de Wilson é o 563, sendo assim são conhecidos, até então, três primos de Wilson.

A principal contribuição de Wilson, que o tornou um dos maiores matemáticos ingleses, é o seguinte teorema:

Teorema 11 ***(Teorema de Wilson)*** *p é um número primo se, e somente se, $(p-1)! \equiv -1$ mod(p).*

Depois Wilson dedicou-se a trabalhar como juiz e não é citada alguma outra contribuição dele para a área até sua morte em 1793.

3.5 Sophie Germain

Marie Sophie Germain foi uma estudiosa da matemática, nasceu em 1776 em Paris em meio a Revolução Francesa. Sophie é a segunda filha de Marie Madelaine Gruguelin e Ambroise François. Seu pai era um comerciante de seda, tornou-se diretor do Banco da França e depois foi nomeado na Assembleia Constituinte de 1789 como representante do Terceiro Estado.

Sophie cresceu rodeada por discussões políticas e filosóficas, mas aos 13 anos, no auge da revolução, surge seu interesse pela matemática. Ela aproveita a vasta biblioteca de seu pai para se aprofundar nesse assunto, principalmente em textos de Newton e Euller. Apesar do seu interesse pela matemática, sua família e a sociedade da epóca acreditavam que assunto tão abstrato não era para uma mulher.

Sophie ganhou um prêmio da Academia de ciência da França em 1816 por causa de seu trabalho sobre elasticidade e usava o pseudônimo masculino de Le Blanc que era um aluno que havia desistido da escola politécnica de Paris, ela usava para participar das aulas e apresentar seus estudos. Ela tinha interesse pela Teoria dos Números e voltou sua atenção para alguns números primos que apresentavam uma determinada condição os quais receberam o nome de **primo de Sophie Germain**.

Definição 3.5 Seja p um número primo. Dizemos que p é um primo de Sophie Germain, se $2p + 1$ é também um número primo.

Note que:

Tabela 3: Testando possíveis primos de Sophie Germain

p	$2 * p + 1$	**Análise**
2	$2 * 2 + 1 = 5$	5 é primo, então 2 é primo de Sophie Germain
3	$2 * 3 + 1 = 7$	7 é primo, então 3 é primo de Sophie Germain
5	$2 * 5 + 1 = 11$	11 é primo, então 5 é primo de Sophie Germain
7	$2 * 7 + 1 = 15$	15 não é primo, então 7 não é primo de Sophie Germain
11	$2 * 11 + 1 = 23$	23 é primo, então 11 é primo de Sophie Germain
13	$2 * 13 + 1 = 27$	27 não é primo, então 13 não é primo de Sophie Germain
17	$2 * 17 + 1 = 35$	35 não é primo, então 17 não é primo de Sophie Germain
19	$2 * 19 + 1 = 39$	39 não é primo, então 19 não é primo de Sophie Germain
23	$2 * 23 + 1 = 47$	47 é primo, então 23 é primo de Sophie Germain
29	$2 * 29 + 1 = 59$	59 é primo, então 29 é primo de Sophie Germain
31	$2 * 31 + 1 = 63$	63 não é primo, então 31 não é primo de Sophie Germain
37	$2 * 37 + 1 = 75$	75 não é primo, então 37 não é primo de Sophie Germain

Fonte: Elaborada pelo autor

Sua teoria contribuiu para a demonstração do seguinte teorema que leva o seu nome.

Teorema 12 ***(Teorema de Sophie Germain)*** *Se p é um primo de Sophie Germain, então não existem inteiros x, y e z, diferentes de zero e não múltiplos de p, tais que* $x^p + y^p = z^p$.

Este teorema é a sua contribuição para a matemática pela qual é mais conhecida, porém nunca foi publicado e pode ser encontrado nas notas de rodapé de um livro de 1823 de Legendre com quem trocava correspondências. Além disso, Germain provou que o Último Teorema de Fermat não vale para os primos menores que 100.

Os 10 primeiros primos de Sophie são: 2, 3, 5, 11, 23, 29, 41, 53, 83 e 89.

Em 2013 foi publicada uma suposta demonstração da infinitude dos primos de Sophie Germain realizada por Germán Andrés Paz na Argentina, usando os conceitos de primos, compostos, divisibilidade, intervalo de Breush (garante a existência de pelo menos um número primo nesse intervalo) e também o postulado de Bertrand (entre n e $2n$ existe um número primo). Porém, mais adiant em sua demonstração Paz utiliza de um resultado não conhecido, de que pares de primos gêmeos são infinitos, o que não foi ainda demonstrado. Dessa forma, sua demonstração não foi aceita e o questionamento sobre a infinitude dos primos de Sophie Germain ainda continua.

3.6 Eisenstein

Ferdinand Gotthold Max Eisenstein nasceu na Alemanha na cidade de Berlim no ano de 1823. Eisenstein graduou-se na Universidade de Berlim em matemática, especializou-se no estudo de teoria dos números e análise matemática e atuou como professor.

Eisenstein considerou que a seguinte sequência de números: $1+2, 1+2^2, 1+2^{2^2}, 1+2^{2^{2^2}}$,..., eram números primos.

Note que:

$1+2=3$, é primo
$1+2^2=5$, é primo
$1+2^{2^2}=17$, é primo
$1+2^{2^{2^2}}=65.537$, é primo

Esses números primos de Eisenstein podem ser representados pela fórmula:

$$E_{n+1} = 2^{E_{n-1}-1} + 1,$$

onde $E_0 = 3$ e E_n o enésimo número de Eisenstein.

Eisenstein morreu em 1852 aos 29 anos e sobre sua teoria dos números primos, pouco se desenvolveu. Mas ele conjecturou que existem infinitos números primos da forma $1+2^{2^n}$, porém não foi provada ainda.

3.7 Sierpinski

Waclaw Sierpinski nasceu em 1882 na Polônia, frequentava a escola em Varsóvia e foi seu professor de matemática que notou seu talento com os números. Porém nessa época a Polônia vinha sofrendo grandes mudanças devido a invasão russa, que começou a adotar suas culturas e costumes na Polônia, fazendo com que as escolas implementadas entre 1869 e 1874, se adequassem as mudanças propostas.

Apesar de todas as dificuldades da época, em 1899 Sierpinski entrou para a Universidade de Varsóvia e cursou matemática. Em 1904 graduou-se e depois tornou-se professor. Após ter doutorado em matemática, Sierpinski desempenhou pesquisas em Teoria dos Números pela Universidade de Lvov em 1908. E sua teoria para identificar alguns números primos diz o seguinte:

Definição 3.7 Seja $S_m = F_{m+2^m}$, onde F_{m+2^m} é um número de Fermat. Diz-se que S_m um número primo de Sierpinski, se S_m for primo.

Note que:
Se $m=0$, tem-se $S_0 = F_{0+2^0} \Rightarrow S_0 = F_1 \Rightarrow 5 = F_1$.
Se $m=1$, tem-se $S_1 = F_{1+2^1} \Rightarrow S_1 = F_3 \Rightarrow 257 = F_3$.
De acordo com [PERUZZO, 2017] para $m = 2, 3$ e 4 obtem-se números compostos, portanto os números 5 e 257 são os menores números de Sierpinski conhecidos, visto que por apresentar cálculos extensos, acaba por tarnar-se raro sua determinação.

Sierpinski é considerado como um dos maiores matemáticos da Polônia e ao longo de sua carreira ele publicou mais de 700 artigos e 50 livros, falecendo em 1969.

3.8 Wieferich

Arthur Josef Alwin Wieferich nasceu na Alemanha em 1884, cujo pai era um empresário.

Wieferich interessou-se principalmente pela Teoria dos Números, devido a uma palestra em 1907 de Max Dhen sobre esta área da matemática. A partir daí ele especializou-se nesta teoria e publiou 5 estudos na área enquanto ainda era estudante na Universidade de Münster.

Definição 3.8 Diz-se que um número primo p é um primo de Weiferich se $p^2|(2^{p-1}-1)$, ou seja, $2^{p-1} \equiv 1(mod\, p^2)$.

Note que:

Tabela 4: Testando possíveis números primos de Wieferich

p	p^2	$2^{p-1}-1$	**Análise**
2	4	$2^{2-1}-1=1$	$4 \nmid 1$, então 2 não é primo de Wieferich
3	9	$2^{3-1}-1=3$	$9 \nmid 3$, então 3 não é primo de Wieferich
5	25	$2^{5-1}-1=15$	$25 \nmid 15$, então 5 não é primo de Wieferich
7	49	$2^{7-1}-1=30$	$49 \nmid 30$, então 7 não é primo de Wieferich
13	169	$2^{13-1}-1=4095$	$169 \nmid 4095$, então 13 não é primo de Wieferich
17	289	$2^{17-1}-1=65535$	$289 \nmid 65535$, então 17 não é primo de Wieferich
19	361	$2^{19-1}-1=262.143$	$361 \nmid 262.143$, 19 não é primo de Wieferich
23	529	$2^{23-1}-1=4.194.303$	$529 \nmid 4.194.303$, 23 não é primo de Wieferich
29	8411	$2^{29-1}-1=268.435.455$	$841 \nmid 268.435.455$, 29 não é primo de Wieferich
31	961	$2^{31-1}-1=1.073.741.823$	$961 \nmid 1.073.741.823$, 31 não é primo de Wieferich

Fonte: Elaborada pelo autor

Com base na definição dos primos de Weiferich são conhecidos, até então, os números 1093 e 3511, descobertos respectivamente, por Waldemar Meissner em 1913 e Nicolaas G.W.H. Beeger em 1922.

4 Outras classificações dos números primos

Neste tópico serão abordadas outras classificações dadas a certos números primos que seguem um determinado "padrão".

Uma das dificuldades encontradas quando se fala sobre números primos, é saber se esses números seguem um padrão. Segundo (Sautoy, 2013, p.18) "O problema com os primos é que pode ser realmente difícil descobrir onde estará o próximo, porque não parece haver qualquer padrão na sequência que nos ajude a localizá-los.".

4.1 Primos Gêmeos

Sabe-se que o único número primo par é o 2. Dessa forma, os únicos primos consecutivos são 2 e 3 e, consequentemente, quando dois números são consecutivos, um deles é par. Portanto, qualquer número par diferente do 2 não será um número primo.

Pensando nisso, pode-se destacar os números primos cuja distância entre eles seja mínima, a saber da distância de dois. De fato, existe essa distância mínima, a exemplo temos os números primos 3 e 5 que possuem essa distância mínima. Esses números podem ser definidos da seguinte maneira:

Definição 4.1 Seja p um número primo. Se $p + 2$ for um número primo, diz-se que p e $p + 2$ são primos gêmeos.

Portanto, diz-se que dois números primos são gêmeos se a distância entre eles for de duas unidades. Além disso, diz-se que um número primo p tem um primo gêmeo se $p - 2$ ou $p + 2$ for primo.

Note que:

Tabela 5: Testando possíveis primos gêmeos

p	$p+2$	**Análise**
2	$2+2=4$	4 não é primo
3	$3+2=5$	5 é primo, então 3 e 5 são primos gêmeos
5	$5+2=7$	7 é primo, então 5 e 7 são primos gêmeos
7	$7+2=9$	9 não é primo
11	$11+2=13$	13 é primo, então 11 e 13 são primos gêmeos
13	$13+2=15$	15 não é primo, então 13 e 15 não são primos gêmeos
17	$17+2=19$	19 é primo, então 17 e 19 são primos gêmeos
19	$19+2=21$	21 não é primo
23	$23+2=25$	25 não é primo
29	$29+2=31$	31 é primo, então 29 e 31 são primos gêmeos

Fonte: Elaborada pelo autor

É possível notar que nem todo primo tem um primo gêmeo, pois o número 2 não tem um primo gêmeo e o número 5 é o único primo, até então, em dois pares distintos de primos gêmeos (3, 5) e (5, 7). A relação primos gêmeos é reflexiva, mas não é transitiva como se pode observar nos pares (3,5) e (5,7), pois 3 e 7 não são primos gêmeos.

Em 1949, P.A. Clement demonstrou o seguinte teorema:

Teorema 13 *Seja $p \geq 2$, $(p, p+2)$ são pares de primos gêmeos, se e somente se,* $4[(p-1)!+1]+p \equiv 0$ *mod* $(p(p+2))$.

Testando o teorema, teremos:

Tabela 6: Teste do teorema

p	$p*(p+2)$	$4[(p-1)!+1]+p$	**Resultado**
2	$2*4=8$	$4[(2-1)!+1]+2=10$	$8 \nmid 10$
3	$3*5=15$	$4[(3-1)!+1]+3=15$	$15 \mid 15$, pois $15=15*1$
4	$4*6=24$	$4[(4-1)!+1]+4=32$	$24 \nmid 32$
5	$5*7=35$	$5[(5-1)!+1]+5=105$	$35 \mid 105$, pois $105=35*3$
6	$6*8=48$	$6[(6-1)!+1]+6=490$	$48 \nmid 490$
7	$7*9=63$	$7[(7-1)!+1]+7=5054$	$63 \nmid 5054$
8	$8*10=80$	$8[(8-1)!+1]+8=40.336$	$80 \nmid 40.336$
9	$9*11=99$	$9[(9-1)!+1]+9=362.898$	$99 \nmid 362.898$
10	$10*12=120$	$10[(10-1)!+1]+10=3.628.820$	$80 \nmid 3.628.820$

Fonte: Elaborada pelo autor

Com base nos valores de p analisados acima, foi posssível determinar os primos gêmeos: (3,5) e (3,7). Verifica-se assim, que tal teorema não possui muita praticidade na determinação de primos gêmeos, por seus cálculos envolver fatorial a determinação desses números primos acaba ficando mais trabalhosa.

Durante as pesquisas foi encontrada uma forma de caracterizar os primos gêmeos, porém sobre quem teria encontrado tal forma não é mencionado nos materiais pesquisados. A afirmação encontrada diz que os primos gêmeos são da forma $(6k-1, 6k+1)$ com $k \in \mathbb{N}$ e $k \geq 1$, mas ao testar tal afirmação foi notada que para $k = 1$ tem-se o par de primos gêmeos (5,7) que será o menor par de primos determinado, ou seja, o par de primos (3, 5) não é possível determinar usando essa forma com as informações apresentadas.

Assim os 10 primeiros pares de primos gêmeos são: (3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), (101, 103) e (107, 109).

Assim como, os primos apresentados até aqui, não se sabe se os primos gêmeos são ou não infinitos. Conjectura-se que esses primos sejam infinitos, porém nenhuma demonstração que prove tal afirmação foi provada.

4.2 Primos trigêmeos

Agora será abordado os números primos cuja distância máxima é de 4 unidades.

Definição 4.2 Seja p um número primo. Diz-se que uma terna da forma (p, p+2, p+4) será chamada de primos trigêmeos se, p + 2 e p + 4 forem números primos.

Agora note que:

Tabela 7: Testando possíveis primos trigêmeos

p	$p+2$	$p+4$	**Análise**
2	$2+2=4$	$2+4=6$	4 e 6 não são números primos.
3	$3+2=5$	$3+4=7$	5 e 7 são números primos, então (3, 5, 7) são primos trigêmeos.
5	$5+2=7$	$5+4=9$	9 não é um número primo.
7	$7+2=9$	$7+4=11$	9 não é um número primo.
11	$11+2=13$	$11+4=15$	15 não é um número primo.
13	$13+2=15$	$13+4=17$	15 não é um número primo.
17	$17+2=19$	$17+4=21$	21 não é um número primo.
19	$19+2=21$	$19+4=23$	21 não é um número primo.
23	$23+2=25$	$23+4=27$	25 e 27 não são números primos.
29	$29+2=31$	$29+4=33$	33 não é um número primo.
31	$31+2=33$	$31+4=35$	33 e 35 não são números primos.
37	$37+2=39$	$37+4=41$	39 não é um número primo.

Fonte: Elaborada pelo autor

Sobre os números primos trigêmeos são conhecidos até então, apenas a terna de primos (3, 5, 7). Mas, apesar de ser conhecida essa única terna, não se sabe até então se a quantidade de primos trigêmeos é infinita ou não.

4.3 Primos triplos

Os primos triplos são uma outra forma de classificar alguns tipos de primos. Podendo ser definido da seguinte maneira:

Definição 4.3 Seja p um número primo. Diz-se que os números do terno $(p, p+2, p+6)$ ou $(p, p+4, p+6)$ são primos triplos se todos os números do terno forem primos.

Note que:

Tabela 8: Testando possíveis primos triplos

p	$p+2$	$p+6$	**Análise**
2	$2+2=4$	$2+6=8$	4 e 8 não são primos, então 2, 4 e 8 não são primos triplos.
3	$3+2=5$	$3+6=9$	9 não é primo, então 3, 5 e 9 não são primos triplos.
5	$5+2=7$	$5+6=11$	5, 7 e 11 são primos, então 5, 7 e 11 são primos triplos.
7	$7+2=9$	$7+6=13$	9 não é primo, então 7, 9 e 13 não são primos triplos.
11	$11+2=13$	$11+6=17$	11, 13 e 17 são primos, então 11, 13 e 17 são primos triplos.
13	$13+2=15$	$13+6=19$	15 não é primo, então 13, 15 e 19 não são primos triplos.
17	$17+2=19$	$17+6=23$	17, 19 e 23 são primos, então 17, 19 e 23 são primos triplos.
19	$19+2=21$	$19+6=25$	21 e 25 não são primos, então 19, 21 e 25 não são primos triplos.
23	$23+2=25$	$23+6=29$	25 não é primo, então 23, 25 e 29 não são primos triplos.
29	$29+2=31$	$29+6=35$	35 não é primo, então 29, 31 e 35 não são primos triplos.

Fonte: Elaborada pelo autor

Por outro lado,

Tabela 9: Testando possíveis primos triplos

p	$p+4$	$p+6$	**Análise**
2	$2+4=6$	$2+6=8$	6 e 8 não são primos, então 2, 6 e 8 não são primos triplos.
3	$3+4=7$	$3+6=9$	9 não é primo, então 3, 7 e 9 não são primos triplos.
5	$5+4=9$	$5+6=11$	9 não é primo, então 5, 9 e 11 não são primos triplos.
7	$7+4=11$	$7+6=13$	7, 11 e 13 são primos, então 7, 11 e 13 são primos triplos.
11	$11+4=15$	$11+6=17$	15 não é primo, então 11, 15 e 17 não são primos triplos.
13	$13+4=17$	$13+6=19$	13, 17 e 19 são primos, então 13, 17 e 19 são primos triplos.
17	$17+4=21$	$17+6=23$	21 não é primo, então 17, 21 e 23 não são primos triplos.
19	$19+4=23$	$19+6=25$	25 não é primo, então 19, 23 e 25 não são primos triplos.
23	$23+4=27$	$23+6=29$	27 não é primo, então 23, 27 e 29 não são primos triplos.
29	$29+4=33$	$29+6=35$	33 e 35 não são primos, então 29, 33 e 35 não são primos triplos.

Fonte: Elaborada pelo autor

Analisando as duas formas apresentadas na definição é possível perceber que os primos triplos não são encontrados com facilidade. Pois, foram encontrados usando as duas formas os seguintes primos triplos: $(5, 7$ e $11)$, $(7, 11$ e $13)$, $(11, 13$ e $17)$, $(13, 17$ e $19)$ e $(17, 19$ e $23)$. E comparando as duas formas apresentadas, a primeira forma se mostrou mais eficiente quando testado até $p = 29$, mas nada garante que tal forma será mais eficaz. O próximo primo triplo só será determinado agora quando $p = 37$ usando a segunda forma.

Vale destacar que existem mais números primos triplos além dos apresentados e uma questão que permanece é se esses primos são infinitos ou não.

4.4 Primos Primordiais

Um outro tipo de número primo são os primos primordiais e podem ser definidos da seguinte maneira:

Definição 4.4 Seja n um número natural, $n \geq 2$ e $p_n\#$ o produto de todos os primos menores ou igual a n. Diz-se que $p_n\# + 1$ ou $p_n\# - 1$ são primos primordiais se forem números primos.

Note que:

Tabela 10: Testando possíveis números primos primordiais

n	$p_n\# + 1$	**Análise**
2	$2+1=3$	então 3 é um primo primordial.
3 e 4	$6+1=7$	então 7 é um primo primordial.
5 e 6	$30+1=31$	então 31 é um primo primordial.
7, 8, 9 e 10	$210+1=211$	então 211 é um primo primordial.
11 e 12	$2310+1=2311$	então 2311 é um primo primordial.
13, 14, 15 e 16	$30030+1=30031$	30031 não é número primo.
17 e 18	$510.510+1=510.511$	510.511 não é número primo.
19, 20,21 e 22	$9.699.690+1=9.699.691$	9.699.691 não é número primo.

Fonte: Elaborada pelo autor

Por outro lado,

Tabela 11: Testando possíveis números primos primordiais

n	$p_n\# - 1$	**Análise**
2	$2 - 1 = 1$	1 não é número primo.
3 e 4	$6 - 1 = 5$	então 5 é um primo primordial.
5 e 6	$30 - 1 = 29$	então 29 é um primo primordial.
7, 8, 9 e 10	$210 - 1 = 209$	209 não é número primo.
11 e 12	$2310 - 1 = 2309$	então 2309 é um primo primordial.
13, 14, 15 e 16	$30030 - 1 = 30029$	então 30029 é um primo primordial.
17 e 18	$510.510 - 1 = 510.509$	então 510.509 não é um primo primordial.
19, 20, 21 e 22	$9.699.690 - 1 = 9.699.689$	então 9.699.689 não é um primo primordial.

Fonte: Elaborada pelo autor

Ao analisar as duas tabelas para testar as formas apresentadas para se encontrar um número primo primordial, a primeira forma se mostrou mais eficaz no quesito encontrar primos primordiais, com base nos valores analisados até $n = 19$.

Pode-se perceber que tal teoria é bem eficaz na determinação de números primos grandes. Apesar de tudo, não é possível afirmar se existe ou não uma quantidade infinita de primos primordiais.

4.5 Primos fatoriais

Uma outra forma de classificar os números primos é usando o fatorial para determiná-los. Esses números serão definidos da seguinte maneira:

Definição 4.5 Seja n um número natural. Se $n! + 1$ ou $n! - 1$ for primo, diz-se que este é um número primo fatorial.

Note que:

Tabela 12: Testando possíveis números primos fatoriais

n	$n! + 1$	**Análise**
1	$1 + 1 = 2$	2 é um n° primo, então 2 é primo fatorial.
2	$2 + 1 = 3$	3 é um n° primo, então 3 é primo fatorial.
3	$6 + 1 = 7$	7 é um n° primo, então 7 é primo fatorial.
4	$24 + 1 = 25$	25 não é um n° primo.
5	$120 + 1 = 121$	121 não é um n° primo.
6	$720 + 1 = 721$	721 não é um n° primo.
7	$5040 + 1 = 5041$	121 não é um n° primo.
8	$40320 + 1 = 40321$	40321 não é um n° primo.
9	$362880 + 1 = 362881$	362881 não é um n° primo.
10	$3.328.800 + 1 = 3.328.801$	3.328.801 não é um n° primo.
11	$39.916.800 + 1 = 39.916.801$	39.916.801 é um n° primo fatorial.
12	$479.001.600 + 1 = 479.001.601$	479.001.601 não é um n° primo.

Fonte: Elaborada pelo autor

Por outro lado, temos:

Tabela 13: Testando possíveis números primos fatoriais

n	$n! - 1$	**Análise**
1	$1 - 1 = 0$	0 não é um número primo.
2	$2 - 1 = 1$	1 não é um número primo.
3	$6 - 1 = 5$	5 é um n° primo, então 5 é primo fatorial.
4	$24 - 1 = 23$	23 é um n° primo, então 23 é primo fatorial.
5	$120 - 1 = 119$	119 não é um número primo.
6	$720 - 1 = 719$	719 é n° primo, então 719 é primo fatorial.
7	$5040 - 1 = 5039$	5039 é n° primo, então 5039 é primo fatorial.
8	$40320 - 1 = 40319$	40319 não é um número primo.
9	$362880 - 1 = 362879$	362879 não é um número primo.
10	$3.628.800 - 1 = 3.628.799$	3.628.799 não é um número primo.
11	$39.916.800 - 1 = 39.916.799$	39.916.799 não é um n° primo.
12	$479.001.600 - 1 = 479.001.599$	479.001.599 é um n° primo fatorial.

Fonte: Elaborada pelo autor

Analisando as duas formas apresentadas na definição e observando as tabelas para os 12 primeiros valores de n, a segunda forma de determinar os primos fatoriais se mostrou mais eficaz. Mas, como está sendo feito cálculo com fatorial, o qual cresce rapidamente, por isso não se pode afirmar que tal observação será sempre verdadeira.

Pode-se perceber que tais cálculos com fatorial vai ficando cada vez mais extensos e assim como os demais primos apresentados até aqui, não não pode-se que esses números são infintos ou não.

5 Problemas em aberto e avanços recentes no estudo dos números primos

Neste capítulo serão apresentados algumas dúvidas e os avanços recentes envolvendo o estudo dos números primos.

5.1 Conjectura de Goldbach

Christin Goldbach é um matemático alemão, nascido em março de 1690. Em 1742, em uma carta destinada a Leonhard Euller, Goldbach contou a Euller que acreditava que todo número maior do que 2 era a soma de três números primos. Na epóca Euller lhe respondeu que todo inteiro par é a soma de dois números primos e que esta afirmação poderia ser considerada um teorema, porém não conseguiu prová-la.

(Conjectura de Goldbach): Todo número par maior do que 2 é igual a soma de dois números primos.

Exemplo: $4 = 2 + 2$; $6 = 3 + 3$; $8 = 3 + 5$; $10 = 3 + 7$ ou $10 = 5 + 5$; $12 = 5 + 7$; $14 = 7 + 7$; $16 = 11 + 5$; $18 = 13 + 5$; $20 = 13 + 7$, ...

Note que a conjectura não é verdadeira para ímpares maiores que 2 , pois 11 é um número primo e não pode ser escrito como soma de dois números primos.

A conjectura de Goldbach foi formulada a mais de 250 anos e apesar de ter sido testada em computadores para os valores, segundo (MORIMOTO, 2014, p.57) a conjectura se mostrou verdadeira quando testada para $n \leq 4 \cdot 10^{18}$, porém ainda não foi provada. Por isso, essa conjectura, ao lado do Último Teorema de Fermat e da Hipótese de Riemann, se tornou um dos maiores mistérios da Teoria dos Números.

Goldbach considerava o número 1 um número primo e a exclusão dessa ideia permitiu a conjectura ser conhecida em duas versões, uma fraca e a outra forte. A versão fraca da conjectura de Goldbach diz que todo número ímpar maior que 5 pode ser escrito como a soma de três números primos. Já a versão forte diz que todo número par maior que 2 pode ser escrito como a soma de dois números primos. A prova da versão forte implicaria em um corolário envolvendo a versão fraca.

Sendo um dos maiores mistérios da teoria dos números, ao longo dos anos houveram estudos tentando provar essa conjectura. A partir de 2006 o matemático peruano Harald Andrés Helgoff estudou a versão fraca da conjectura de Goldbach e publicou o trabalho intitulado *Major Arcs for Goldbach's theorem* no servidor Arxiv e depois foi revisado e passou a conter 79 páginas. Esse trabalho de Helgoff serviu de inspiração para seu outro trabalho *The ternary Goldbach conjecture is true* publicado em 2013.

5.2 Música dos números primos

Georg Friedrich Bernhard Riemann criou a função intitulada Zeta de Riemann. Tal função consegue contar a quantidade de números primos em um determinado intervalo.

A função Zeta de Riemann pode ser representada por: $\zeta(s) = \prod_p \frac{1}{1-p^{-s}}$. Essa função foi reescrita por Euller da seguinte forma:

$$\zeta(s) = (1 + \frac{1}{2^s} + \frac{1}{4^s} + ...)(1 + \frac{1}{3^s} + \frac{1}{9^s} + ...) \cdots (1 + \frac{1}{p^s} + \frac{1}{(p^2)^s} + ...) \cdot ..$$

onde $s \in \mathbb{C}$ e p todos os números primos, a ideia de Riemann era testar sua função utilizando os números complexos.

Riemann acreditava que havia uma harmonia sutil, escondida sob o ruído externo dos números primos. A conjectura de Riemann diz que todos o zeros não triviais da sua função têm parte real $\frac{1}{2}$, essa conjectura é mais conhecida como Hipótese de Riemann. Os matemáticos se referem a Hipótese de Riemann ao invés de conjectura, pois acreditam que hipótese possui uma conotação mais forte, pois muitos resultados dependem de sua solução.

Inicialmente a afirmação de Riemann parece não ter relação na determinação de mais primos, mas a descoberta de Riemann de uma função $R(x)$ que estima a quantidade de números primos menores que x poderia ser aperfeiçoada se conhecida todos os zeros da função zeta.

A descoberta de Riemann é que a função zeta gera ondas senoidais semelhantes a ondas musicais. Riemann desenvolveu sua ideia após descobrir um espelho matemático na qual era possível observar os números primos, esse espelho é a forma como se observa os números primos quando dispostos. O que parecia para muitos um caos e um conjunto sem ordem, para Riemann os números primos possuem um padrão consistente apesar de por fora parecer caótico.

Solucionar a Hipótese de Riemann permitiria determinar números primos mais facilmente com 100 ou mais algarismos, essa determinação de números primos com essa quantidade de algarismos seria útil principalmente para a criptografia, tema que será visto a seguir.

5.3 Criptografia RSA

No ano de 1977 os cientistas Ronald Rivest, Adi Shamir e Leonard Adleman desenvolveram um sistema de criptografia pública, esse sistema recebe o nome de RSA com base na inicial do sobrenome de seus três criadores.

A criação desse sistema foi baseada na publicação de um artigo escrito por Whitfield Diffie e Martin Hellman em 1976, cuja ideia destes era usar uma função fácil de se calcular, mas difícil de inverter computacionalmente.

Para entender o método RSA, deve-se tomar dois números primos e a partir desses números serão encontrados dois outros números (C e D) de codificação e decodificação.

Para ilustrar o método RSA, será criptografada a palavra **RSA**, usando a tabela abaixo:

A	B	C	D	E	F	G	H	I	J	K
10	11	12	13	14	15	16	17	18	19	20
L	M	N	O	P	Q	R	S	T	U	V
21	22	23	24	25	26	27	28	29	30	31
W	Y	X	Z							
32	33	34	35							

Tabela 14: Tabela de conversão

Convertendo a palavra **RSA** letra a letra, obtém se **R**=27, **S**=28 e **A**=10, obtendo o número de encriptação da mensagem: 272810. Agora deve-se escolher dois números primos. Escolhendo $p = 5$ e $q = 7$ e tomando o produto dos dois números primos forma-se a chave pública $n = p \cdot q = 35$.

Agora deve se dividir o número da mensagem em blocos de forma que o número de cada bloco não se inicie em zero e seja menor que a chave pública ($n = 35$). Dividindo em blocos obtém-se:

B_1	B_2	B_3
27	28	10

O bloco a ser codificado será representado por $C(B)$ e o bloco decodificado por $D(B)$, onde neste trabalho $C(B) =$ o resto da divisão de B^5 por n.

O primeiro bloco B_1 será:

$27^5 \equiv 27^2 \cdot 27^3 \equiv 29 \cdot 13 \equiv 783 \equiv 27 \mod 35$ A codificação do primeiro bloco será então 27. Codificados os demais blocos, obtém-se a seguinte sequência:

$$27 - 28 - 5$$

Desta forma a mensagem encriptografada (**RSA**) será 27.28.5. Para desfazer a criptografia e observar se os cálculos realizados estão corretos, deve-se encontrar uma chave privada d, que será obtida realizando o seguinte cálculo:

$$5 \cdot d \equiv 1 \mod (p-1)(q-1)$$

Ao realizar esse cálculo obtém-se:

$$5 \cdot 5 \equiv 1 \mod 24$$

A chave de codificação será $(pq, d) = (35, 5)$. Para decodificar a mensagem, deve-se elevar cada bloco codificado a chave privada encontrada e assim será obtida a mensagem.Ou seja,

$$B_1 \equiv 27^5 \mod 35 \Rightarrow B_1 \equiv 27 \mod 35$$
$$B_2 \equiv 28^5 \mod 35 \Rightarrow B_2 \equiv 28 \mod 35$$
$$B_3 \equiv 5^5 \mod 35 \Rightarrow B_3 \equiv 10 \mod 35$$

Mas esses cálculos são bem mais difíceis, pois os números primos escolhidos costumam ter 100 ou mais algarismos, daí a importância do avanço no estudo dos números primos para a criptografia. O exemplo dado serve apenas para ilustrar um pouco do método RSA.

Ao dizer que o avanço no estudo da Hipótese de Riemann pode beneficiar a criptografia de modo a permitir encontrar números primos grandes com mais facilidade, mas esse avanço também pode tornar o código mais vulnerável. Pois, uma das principais vantagens desse método destacado pelos criptográfos é a segurança oferecida, devido a dificuldade para a determinação dos números primos envolvidos nos cálculos.

6 Considerações finais

Este trabalho revela um pouco da teoria envolta nos números primos e o magnetismo que seus estudiosos sentem por esse tema, mostrando que cada estudioso citado neste trabalho procurou uma forma de caracterizar esses números. Mas a ideia de estabelecer um "padrão"que permitisse determinar todos os números primos não foi ainda encontrada, fazendo com que esses números continuem um mistério para os matemáticos.

Um questionamento que surgiu bastante ao longo desse trabalho e que continua sem uma resposta até o final desse texto é se os tipos de números primos apresentados, são ou não infinitos. Apesar dos métodos diversos para a determinação de cada tipo de número primo e observados o tempo de criação desses métodos, muitas perguntas permanecem sem resposta.

Por isso, com base em tudo que foi apresentado e nos estudos dos matemáticos sobre o tema, sabendo que os avanços em direção ao conhecimento desses números permitirão o desenvolvimento das teorias aqui apresentadas, que se espera que tais dúvidas sejam esclarecidas. Esse não é um desejo apenas dos matemáticos, pois tem-se o exemplo da criptografia RSA, um avanço tecnológico que conta com o progresso dessa teoria, que necessita encontrar números primos cada vez maiores para garantir mais segurança para a sociedade.

Alguns desses números primos contém muitos algarismos, por exemplo, são conhecidos 51 números primos de Mersenne e o maior tem mais de 24 milhões de digítos, de Sophie Germain o número primo é o número $183027 * 2^{265440} - 1$ com 79.911 digítos, daí tem-se uma ideia da dificuldade de encontrar números primos.

Diante disso, que na tentativa de observar algum "padrão"nos números primos estudados, criou-se uma tabela a fim de compará-los. Porém, como será observado na tabela, há uma lacuna de números primos que as teorias estudadas não conseguiu determiná-los e a caracterização deles como números primos se deve apenas a definição destes números.

Tabela 15: Tipos de números primos e alguns de seus criadores

N° primo	Eisenstein	Fermat	Fibonacci	Mersenne	Sierpinski	Sophie	Wieferich	Wilson	P. Fatorial	P. primordial
2										
3										
5										
7										
11										
13										
17										
19										
23										
29										
31										
37										
41										
43										
47										
53										
59										
61										
⋮										
1093										
1097										
⋮										

Fonte: Elaborada pelo autor

7 Referências

[1] Carvalho, G. C. A. d., et al. Números primos: pequenos tópicos.

[2] Coutinho, S. C. *Números inteiros e criptografia RSA*. IMPA, 1997.

[3] Du Sautoy, M. *A música dos números primos: a história de um problema não resolvido na matemática*. Editora Schwarcz-Companhia das Letras, 2007.

[4] Du Sautoy, M. *Os mistérios dos números: Uma viagem pelos grandes enigmas da matemática (que até hoje ninguém foi capaz de resolver)*. Editora Schwarcz-Companhia das Letras, 2013.

[5] Elon, L. L. Curso de análise. *Sao Paulo: Projeto Euclides* (1929).

[6] Hefez, A. *Elementos de aritmética*. Sociedade Brasileira de Matemática, 2006.

[7] Martinez, A. G., Tazzioli, R., Munari, A., and Unica, S. Donne nella matematica. sophie germain e la lotta contro i pregiudizi e l'invisibilità.

[8] Morimoto, R. M. Números primos: propriedades, aplicações e avanços.

[9] Okumura, M. K., et al. Números primos e criptografia rsa. *Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo* (2014).

[10] Oliveira, R. A. d. Explorando o universo dos números primos.

[11] Paz, G. A. *Números primos de Sophie Germain*. 2017.

[12] Peruzzo, J. *O Fascínio Dos Números Primos*. Clube de Autores, 2017.

[13] Ribenboim, P. *Números primos: mistérios e recordes*. Instituto Nacional de Matemática Pura e Aplicada, 2001.

[14] Rizel, A. C. Números primos.