UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ - UTFPR
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

JOÃO EUGÊNIO CAMILO COELHO

UMA INTRODUÇÃO AOS PRIMOS GÊMEOS: CARACTERIZAÇÕES E ILUSTRAÇÕES

CURITIBA

2021

JOÃO EUGÊNIO CAMILO COELHO

UMA INTRODUÇÃO AOS PRIMOS GÊMEOS: CARACTERIZAÇÕES E ILUSTRAÇÕES

An introduction to twin primes: characterizations and illustrations

Dissertação apresentada como requisito para obtenção do título de Mestre Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Tecnológica Federal do Paraná (UTFPR).
Orientador: Prof. Dr. Andres David Baez Sanchez

CURITIBA

2021

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Campus Curitiba

JOAO EUGENIO CAMILO COELHO

UMA INTRODUÇÃO AOS PRIMOS GÊMEOS: CARACTERIZAÇÕES E ILUSTRAÇÕES

Trabalho de pesquisa de mestrado apresentado como requisito para obtenção do título de Mestre Profissional Em Matemática Para A Escola Básica da Universidade Tecnológica Federal do Paraná (UTFPR). Área de concentração: Matemática.

Data de aprovação: 15 de Outubro de 2021

Prof Andres David Baez Sanchez, Doutorado - Universidade Tecnológica Federal do Paraná

Prof Marcio Rostirolla Adames, Doutorado - Universidade Tecnológica Federal do Paraná

Prof Rafael Aleixo De Carvalh, Doutorado - Universidade Federal de Santa Catarina (Ufsc)

Documento gerado pelo Sistema Acadêmico da UTFPR a partir dos dados da Ata de Defesa em 15/10/2021.

Dedico este trabalho a minha esposa Érica, minha filha Nathália, meus pais Querino e Rosa, meus irmãos Everton e Evandro, minhas irmãs Perla, Carla e Carolina e a todos meus professores pelos ensinamentos desde a educação básica até o ensino superior que me mostraram o quanto a educação pode transformar a nossa vida.

AGRADECIMENTOS

- A Deus por me dar força para superar os obstáculos desse período.
- A minha esposa Érica e minha filha Nathália Luanda por estarem ao meu lado nos momentos bons e ruins me apoiando nesta longa caminhada.
- Aos meus pais Querino e Rosa que mesmo na simplicidade me mostraram a importância dos estudos.
- Aos meus irmãos Evandro e Everton e minhas irmãs Perla, Carla e Carolina que sempre me apoiaram no estudo.
- Ao meu orientador Prof. Dr. Andres David Baez Sanchez, pela compreensão, dedicação e orientação durante essa jornada.
- Aos professores do PROFMAT da UTFPR - câmpus Curitiba pelos ensinamentos.
- Aos meu colegas de curso (Ricardo, Paulo, Felippe, Fábio, Enoque, Hugo, Isaías, Cleomar, Mariana, Jéssica e Victória) pela troca de experiência, pelo estudo coletivo e companheirismo.
- Aos meus amigos João Carlos, Nelson, André e Jonas que me incentivaram ainda na graduação a ingressar no mestrado.
- Aos colegas Roberto e Marilete que tiveram seu sonho interrompido, mas sei que um dia irão concluir o Mestrado.
- Aos professores Keiji Nakanura e Fabinho que são as minhas maiores inspirações na busca pelo conhecimento matemático.
- Ao meu primo Válber que mesmo distante sempre lembrou de mim através das suas orações.
- À Sociedade Brasileira de Matemática que, na busca da melhoria do ensino de matemática na Educação Básica, viabilizou a implementação do PROFMAT.
- À CAPES, pela recomendação do PROFMAT por meio do parecer do Conselho Técnico Científico da Educação Superior.
- O presente trabalho foi realizado com apoio da Universidade Tecnológica Federal do Paraná - Brasil (UTFPR) - Código de Financiamento 001.

Os encantos dessa sublime ciência se revelam apenas àqueles que tem coragem de irem a fundo nela. Carl Friedrich Gauss (1777 - 1855): matemático, astrônomo e físico alemão.

RESUMO

COELHO, João Eugênio Camilo. **Uma introdução aos primos gêmeos: caracterizações e ilustrações**. 68 f. Dissertação - Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Universidade Tecnológica Federal do Paraná. Curitiba, 2021.

O presente trabalho aborda diferentes propriedades e caracterizações dos números primos gêmeos. Nesta dissertação serão apresentadas demonstrações de proposições e teoremas específicos da teoria dos números, além de ilustrações, que elucidam o estudo dos números primos gêmeos. Além disso, será exposta a relação dos primos gêmeos com os números binomiais e com o Pequeno Teorema de Fermat. Serão utilizadas também, a caracterização dos primos gêmeos e a Congruência de Clement, para gerar primos gêmeos e apresentar ilustrações numéricas das séries dos inversos dos primos e dos inversos dos primos gêmeos, usando os recursos computacionais MAXIMA e Python.

Palavras-chave: Primos Gêmeos; Congruência de Clement; Pequeno Teorema de Fermat; Ilustrações computacionais.

ABSTRACT

COELHO, João Eugênio Camilo. **An introduction to twin primes: characterizations and illustrations**. 68 pg. Dissertation - Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Universidade Tecnológica Federal do Paraná. Curitiba, 2021.

The present work considers different properties and characterizations of the twin primes numbers. This dissertation will present proofs of specific propositions and theorems from number theory, as well as examples, that elucidate the study of twin prime numbers. In addition, it will be presented the relationships between twin prime numbers and binomial numbers, as well as the reltionship with Fermat's Little Theorem. The characterization of twin prime numbers and the Clement's Congruence will be used to obtain twin primes and to present numerical illustrations of the series of reciprocals of primes and twin prime reciprocals, using computational resources as MAXIMA and Python.

Keywords: Twin Primes; Clement's Congruence; Fermat's Little Theorem; Computational illustrations.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

A história da teoria dos números é repleta de teoremas interessantes e até mesmo conjecturas sem solução, como por exemplo a conjetura de Goldbach e a conjetura dos primos cuja diferença é igual a 4. Foi justamente um destes problemas que despertou a curiosidade para o desenvolvimento deste trabalho: "A conjectura dos números primos gêmeos".

Desde a Grécia antiga por volta do ano 250 a.C. alguns matemáticos se perguntam se há infinitos primos gêmeos, isto é, infinitos primos cuja diferença entre eles seja igual a 2. Esta é precisamente a conjectura dos primos gêmeos (HOSCH, 2017). Apesar de diversos avanços teóricos relacionados, ainda não há demonstração ou resultado que permita determinar se é ou não válida esta afirmação, fato este o qual torna o trabalho mais motivador.

Ao começar o estudo acerca dos primos gêmeos é interessante analisar a série dos inversos dos primos gêmeos,

$$\sum_{(p,p+2)\in\mathcal{P}_g} \frac{1}{p}+\frac{1}{p+2} = \left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\cdots+\left(\frac{1}{p}+\frac{1}{p+2}\right)+\cdots$$

Se a soma dos inversos dos primos gêmeos fosse divergente, então, não teria pesquisa, pois haveria infinitos primos gêmeos, já que se fosse uma quantidade finita de primos gêmeos, a soma seria convergente. Contudo, a série dos inversos dos gêmeos converge. Este foi um dos primeiros resultados teóricos demonstrado por Viggo Brun em 1915. Este matemático norueguês provou que de fato a soma dos inversos dos primos gêmeos convergia para uma constante, mais tarde, denominada Constante de Brun. Com a utilização de computadores, os matemáticos Shanks e Wrench em 1974, Brent em 1976 e também Nicely em 2001 obtiveram o valor aproximado da constante dado por $B = 1.9021605823....$

> Este resultado não exclui que existam infinitos pares de primos gêmeos, mas informam que esses pares são encontrados cada vez mais longe separados, então a soma de seus inversos permanece finita. Com base em considerações heurísticas sobre a distribuição de primos gêmeos, B foi calculado, por exemplo, por Shanks & Wrench (1974), por Brent (1976), e mais recentemente por Nicely (2001), que obtiveram, B = 1,9021605823 (RIBENBOIM, 2004, p. 193).

Outro considerável avanço ocorreu em 1949 quando o matemático P.A Clement provou que $p, p+2$ são primos gêmeos se, e somente se, $4[(p-1)!+1]+p \equiv 0 \bmod (p(p+2))$ conforme Ribenboim (2004). Trata-se da congruência de Clement (Teorema 2.2) que será demonstrada neste trabalho, sendo o principal teorema e será utilizado, tanto para gerar pares de primos gêmeos, quanto para gerar somas parciais dos inversos dos gêmeos ou ainda para ilustrar numericamente a série dos inversos dos gêmeos.

Ao considerar p_n como o enésimo primo, pode-se definir lacunas entres primos (em inglês, *prime gap*), como a diferença entre primos consecutivos, ou seja, $g_n = p_{n+1} - p_n$. Note que, todo número primo pode ser escrito em função de todas as lacunas que o antecedem, já que, $p_{n+1} = 2 + \sum_{k=1}^{n} g_i$.

Tabela 1.1 – Primeiras lacunas entre primos

n	$g_n = p_{n+1} - p_n$
1	$g_1 = p_2 - p_1 = 3 - 2 = 1$
2	$g_2 = p_3 - p_2 = 5 - 3 = 2$
3	$g_3 = p_4 - p_3 = 7 - 5 = 2$
4	$g_4 = p_5 - p_4 = 11 - 7 = 4$
5	$g_5 = p_6 - p_5 = 13 - 11 = 2$
6	$g_6 = p_7 - p_6 = 17 - 13 = 4$
7	$g_7 = p_8 - p_7 = 19 - 17 = 2$
8	$g_8 = p_9 - p_8 = 29 - 23 = 6$
9	$g_9 = p_{10} - p_9 = 31 - 29 = 2$
10	$g_{10} = p_{11} - p_{10} = 37 - 31 = 6$
11	$g_{11} = p_{12} - p_{11} = 41 - 37 = 4$
12	$g_{12} = p_{13} - p_{12} = 43 - 41 = 2$
13	$g_{13} = p_{14} - p_{13} = 47 - 43 = 4$
14	$g_{14} = p_{15} - p_{14} = 53 - 47 = 6$
15	$g_{15} = p_{16} - p_{15} = 59 - 53 = 6$
16	$g_{16} = p_{17} - p_{16} = 61 - 59 = 2$
17	$g_{17} = p_{18} - p_{17} = 67 - 61 = 6$
18	$g_{18} = p_{19} - p_{18} = 71 - 67 = 4$
19	$g_{19} = p_{20} - p_{19} = 73 - 71 = 2$
20	$g_{20} = p_{21} - p_{20} = 79 - 73 = 6$

Fonte: O autor.

Observando a Tabela 1.1 constata-se que há primos consecutivos cuja diferença é igual a $1, 2, 4$ ou 6. Mas, ainda há lacunas muito maiores, por exemplo, a lacuna entre os primos $p_{31545} = 370261$ e $p_{31546} = 370373$ é de 112.

Sendo assim, o que se pode afirmar sobre estas lacunas? Existem infinitos primos cuja lacuna é igual a 4? E quanto a 6? Qual a menor lacuna em que há infinitos pares de primos com distância N entre si?

Na verdade, a conjectura dos primos cuja lacuna é igual a 2, ou seja, os primos gêmeos, assim como outras (lacunas iguais a 4 e 6), ainda permanecem sem solução. No entanto, Yitang Zhang, matemático chinês, em 17 de abril de 2013 apresentou um artigo (ZHANG, 2014) onde provou que há infinitos pares de primos cuja diferença entre eles não excede a 70 milhões. Sua prova sobre lacunas limitadas entre os primos não será demonstrada por se tratar de uma demonstração muito avançada e estar fora do escopo do trabalho.

O resultado de Zhang foi significativo nos avanços posteriores relacionados a lacunas entre primos, pois, sua demonstração permitiu alavancar o PolyMath (Projeto criado para resolver problemas matemáticos importantes e difíceis), em particular o projeto PolyMath8b em que o jovem britânico James Maynard participou.

Em 2015 James Maynard utilizou o trabalho de Zhang juntamente a equipe do PolyMath8b, para provar que há infinitos primos cuja diferença não excede a 246. Uma retrospectiva dos avanços do projeto PolyMath8b pode ser encontrada em Polymath (2014).

A evolução dos computadores permitiu não só o crescimento do projeto PolyMath8b na limitação de lacunas entre primos pequenos, como também a obtenção de primos gêmeos grandes. Até porque os números primos são cada vez mais difíceis de serem encontrados quando pesquisa-se em intervalos maiores.

Até a data 11 de junho de 2021, os maiores primos gêmeos conhecidos são

$$2996863034895 \cdot 2^{1290000} - 1 \text{ e } 2996863034895 \cdot 2^{1290000} + 1 \text{ com } 388342$$

dígitos, estes pares foram descobertos em 14 de setembro de 2016. Esta informação, assim como, a Tabela 1.2 que classifica os maiores primos gêmeos e a data da descoberta, são expressas conforme Caldwell (2020).

Tabela 1.2 – Maiores primos gêmeos conhecidos

Classificação	Primos	Data
1	$2996863034895 \cdot 2^{1290000} \pm 1$	Setembro (2016)
2	$3756801695685 \cdot 2^{666669} \pm 1$	Dezembro (2011)
3	$65516468355 \cdot 2^{333333} \pm 1$	Agosto (2009)
4	$12770275971 \cdot 2^{222225} \pm 1$	Julho (2007)
5	$70965694293 \cdot 2^{200006} \pm 1$	Abril (2016)
6	$66444866235 \cdot 2^{200003} \pm 1$	Abril (2016)
7	$4884940623 \cdot 2^{198800} \pm 1$	Julho (2015)
8	$4884940623 \cdot 2^{198800} \pm 1$	Janeiro (2007)
9	$191547657 \cdot 2^{173372} \pm 1$	Julho (2020)
10	$38529154785 \cdot 2^{173250} \pm 1$	Julho (2014)
11	$194772106074315 \cdot 2^{171960} \pm 1$	Junho (2007)
12	$100314512544015 \cdot 2^{171960} \pm 1$	Junho (2006)
13	$16869987339975 \cdot 2^{171960} \pm 1$	Setembro (2005)
14	$33218925 \cdot 2^{169690} \pm 1$	Setembro (2002)
15	$3706785456 \cdot 13^{42069} \pm 1$	Setembro (2020)
16	$22835841624 \cdot 7^{54321} \pm 1$	Novembro (2010)
17	$1679081223 \cdot 2^{151618} \pm 1$	Fevereiro (2012)
18	$9606632571 \cdot 2^{151515} \pm 1$	Julho (2014)
19	$84966861 \cdot 2^{140219} \pm 1$	Abril (2012)
20	$12378188145 \cdot 2^{140002} \pm 1$	Dezembro (2010)

Fonte: Caldwell (2020).

Ao observar a Tabela 1.2, identifica-se que as datas da descoberta não estão em ordem cronológica. Isto acontece porque os programas e projetos utilizados na pesquisa foram diferentes.

Neste trabalho, procura-se apresentar conceitos básicos e resultados preliminares sobre os primos gêmeos, recorrendo a caracterizações e ilustrações. Em detalhes, busca-se demonstrar proposições e teoremas que caracterizem os primos gêmeos, destacando suas relações com outros teoremas clássicos como o Teorema de Wilson (Teorema 2.1), o Pequeno Teorema de Fermat (Teorema 4.1) e os coeficientes binomiais (Teoremas 3.1 e 3.2). Posteriormente, utiliza-se tais teoremas para gerar lista de primos e também ilustrações acerca dos primos gêmeos, especialmente da convergência da série dos inversos dos primos gêmeos, contrapondo com a divergência da série dos inversos dos primos.

1.1 JUSTIFICATIVA PARA A ESCOLHA DO TEMA

As propriedades e problemas relacionados à aritmética despertam o interesse devido a facilidade na resolução dos seus problemas e também por abordarem questões presentes em sala de aula desde os anos iniciais.

Além disso, ao analisar as provas da Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP) durante a graduação de matemática e também nas aplicações aos alunos do Ensino Fundamental e Médio algumas questões propostas despertavam a curiosidade, em particular quando abordavam propriedades aritméticas. Tal interesse foi estimulado ainda mais, durante o PROFMAT, especialmente na disciplina de Aritmética.

Estudar conceitos em Aritmética e que estavam muito próximos da realidade em sala de aula, como propriedades de aritmética dos restos, máximo divisor comum, divisibilidade e números primos, tornando mais forte a base dos ensinamentos futuros, sempre foi objeto de motivação. Além disso, o fato dos primos gêmeos ser objeto de uma das conjecturas das mais antigas na teoria dos números, torna ainda mais interessante estudar diferentes caracterizações e teoremas importantes sobre os mesmos.

Ademais, o uso de recursos computacionais, inicialmente considerados para entender as demonstrações, tornaram-se fundamentais para obter as ilustrações numéricas. Além do que, a curiosidade em entender, ainda que de uma maneira simples, “qual procedimento os computadores usam para gerar primos gêmeos” e “como determinar os contraexemplos”, para mostrar que a recíproca de alguns resultados eram inválidos, também impulsionaram a expectativa pela pesquisa.

Desta forma, este trabalho também pretende mostrar a utilidade dos recursos computacionais para contribuir no desempenho matemático, seja como facilitador das demonstrações matemáticas ou na compreensão das ilustrações criadas a partir de um teorema.

1.2 OBJETIVOS

1.2.1 OBJETIVO GERAL

Adquirir mais conhecimento na área de Teoria dos Números e estudar sobre as caracterizações e teoremas relacionados aos números primos gêmeos.

1.2.2 OBJETIVOS ESPECÍFICOS

- Compreender e estudar algumas demonstrações clássicas de Aritmética, em particular o teorema de Wilson e o pequeno teorema de Fermat.
- Gerar computacionalmente os pares de primos gêmeos a partir dos teoremas demonstrados neste trabalho.
- Expressar a relação entre os números primos gêmeos e os números binomiais.
- Demonstrar as relações entre os números primos gêmeos e o pequeno teorema de Fermat.
- Demonstrar e ilustrar computacionalmente a divergência da série do inverso dos naturais e dos inversos dos números primos.
- Calcular com o auxílio dos recursos computacionais os valores para as somas parciais dos inversos dos primos gêmeos.
- Ilustrar a convergência da soma dos inversos dos primos gêmeos a partir dos teoremas destacados neste trabalho.
- Ilustrar a série dos inversos dos números naturais, dos números primos e dos primos gêmeos em comparação com a constante de Brun.

1.3 PROCEDIMENTOS METODOLÓGICOS

Este trabalho foi desenvolvido a partir de consultas em referências bibliográficas, publicações científicas e outros materiais digitais. O sistema de computação algébrica MAXIMA foi utilizado para gerar alguns pares de primos gêmeos menores que 100000 e também para obter contraexemplos nas recíprocas de alguns resultados.

A linguagem de programação Python foi utilizada na ilustração das somas parciais da série dos inversos dos números naturais, da série dos inversos dos números primos e da série dos inversos dos números primos gêmeos. Ademais, as tabelas foram construídas pelo autor no próprio LaTeX e as informações nela contidas resultaram de sites que abordavam os primos gêmeos com destaque.

1.4 ESTRUTURA DO TRABALHO

O presente trabalho está organizado em 6 capítulos:

- Capítulo 1: Introdução do tema, breve apresentação de avanços em relação aos primos gêmeos, tabelas de lacunas de primos e dos maiores primos gêmeos obtidos por computadores.
- Capítulo 2: Apresentação dos resultados preliminares de aritmética modular (proposições, definições e exemplos), caracterizações e demonstrações do teorema de Wilson e da congruência de Clement.
- Capítulo 3: Descrição dos coeficientes binomiais, demonstração da relação de Stifel, exposição de teoremas que relacionam primos gêmeos, números binomiais e o triângulo de Pascal.
- Capítulo 4: Exposição e demonstração do pequeno teorema de Fermat, demonstração de teoremas que relacionam primos gêmeos com o pequeno teorema de Fermat, generalização para obtenção de números primos gêmeos e utilização do MAXIMA para determinar contraexemplos.
- Capítulo 5: Ilustrações e comparações da série harmônica, série dos inversos dos primos e série dos inversos dos primos gêmeos. Ilustrações numéricas destas séries.
- Capítulo 6: Considerações e comentários finais.

2 CONCEITOS BÁSICOS E RESULTADOS PRELIMINARES

Para o estudo dos números primos gêmeos que será feito neste trabalho, é necessário considerar algumas proposições e resultados preliminares que serão apresentados nesta seção.

Inicialmente, são apresentadas algumas definições e proposições básicas da aritmética modular. As demonstrações destes resultados podem ser encontradas em Hefez (2016).

Definição 2.1. *Ao considerar m um número natural, estabelece-se que, dois números inteiros a e b são $congruentes$ módulo m se os restos de sua divisão euclidiana por m são iguais. Assim, quando os números inteiros a e b são $congruentes$ módulo m, escreve-se, a relação, $a \equiv b$ mod m. Quando a e b não são $congruentes$ módulo m, denota-se, $a \not\equiv b$ mod m .*

O exemplo a seguir, ilustra a definição anterior.

Exemplo 2.1. *Note que, $37 \equiv 62$ mod 5, pois o resto da divisão de 37 por 5 é 2 e o resto da divisão de 62 por 5 também é 2. Sob outra perspectiva, tem -se que, $7 \not\equiv 16$ mod 5, pois o resto da divisão de 7 por 5 é 2 e o resto da divisão de 16 por 5 é 1.*

A proposição seguinte mostra como se comporta a soma e o produto na aritmética modular.

Proposição 2.1. *Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$.*

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

ii) Se $a \equiv b$ mod m e $c \equiv d$ mod m, então, $ac \equiv bd$ mod m.

iii) Tem - se que, $a + c \equiv b + c$ mod m, se, e somente se, $a \equiv b$ mod m.

Demonstração. i) Se $a \equiv b$ mod m, então, pode-se escrever, $a = mq_0 + r$ e $b = mq_1 + r$ com r, q_0 e $q_1 \in \mathbb{Z}$ e $0 \leq r < m$. Analogamente, se $c \equiv d$ mod m, então, $c = mq_2 + r'$ e $d = mq_3 + r'$ com r', q_2 e $q_3 \in \mathbb{Z}$ e $0 \leq r' < m$ Logo,

$$\begin{aligned} a + c &= (mq_0 + r) + (mq_2 + r') \\ &= m(q_0 + q_2) + r + r'. \end{aligned}$$

Além disso,

$$\begin{aligned} b + d &= (mq_1 + r) + (mq_3 + r') \\ &= m(q_1 + q_3) + r + r'. \end{aligned}$$

Como, $a+c \equiv r+r'$ mod m e $b+d \equiv r+r'$ mod m, conclui-se que $a+c \equiv b+d$ mod m.

ii) Do mesmo modo do item anterior, tem-se que, se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então,

$$\begin{aligned} a \cdot c &= (mq_0 + r) \cdot (mq_2 + r') \\ &= m^2 q_0 q_2 + mq_0 r' + mq_2 r + r \cdot r' \\ &= m(mq_0 q_2 + q_0 r' + q_2 r) + r \cdot r'. \end{aligned}$$

Além disso,

$$\begin{aligned} b \cdot d &= (mq_1 + r) \cdot (mq_3 + r') \\ &= m^2 q_1 q_3 + mq_1 r' + mq_3 r + r \cdot r' \\ &= m(mq_1 q_3 + q_1 r' + q_3 r) + r \cdot r'. \end{aligned}$$

Portanto, $a \cdot c \equiv b \cdot d \bmod m$.

iii) ($\Rightarrow$) Se $a + c \equiv b + c \bmod m$, então, $m \mid (b + c) - (a + c)$, ou seja, $m \mid b - a$. Logo $b - a = m \cdot q$, com $q \in \mathbb{Z}$, consequentemente, $a \equiv b \bmod m$.

($\Leftarrow$) Se $a \equiv b \bmod m$ e $c \equiv c \bmod m$, então, pelo item i) tem-se que,

$$a + c \equiv b + c \bmod m$$

□

A Proposição 2.1 pode ser ilustrada nos seguintes exemplos.

Exemplo 2.2. *Dado que,* $25 \equiv 2$ *mod* 23 *e* $27 \equiv 4$ *mod* 23*, então,* $25 + 27 \equiv 2 + 4$ *mod* 23*, ou seja,* $52 \equiv 6$ *mod* 23 .

Exemplo 2.3. *Dado que,* $20 \equiv 3$ *mod* 17 *e* $38 \equiv 4$ *mod* 17*, então,* $20 \cdot 38 \equiv 3 \cdot 4$ *mod* 17*, isto é,* $760 \equiv 12$ *mod* 17 .

Exemplo 2.4. *Dado que,* $33 + 29 \equiv 2 + 29$ *mod* 31*, se, e somente se,* $33 \equiv 2$ *mod* 31.

Proposição 2.2. *Sejam* $a, b, c, d, m \in \mathbb{Z}$*, com* $m > 1$ *e* $mdc(c, m) = 1$

Tem-se que, $ac \equiv bc$ *mod* m*, se, e somente se,* $a \equiv b$ *mod* m*.*

A Proposição 2.2, estabelece condições para a simplificação de multiplicações. A demonstração deste resultado pode ser encontrada em Hefez (2016). Para ilustrar a validade da Proposição 2.2 pode-se considerar o seguinte exemplo.

Exemplo 2.5. *Considere* $a = 15$*,* $b = 4$*,* $c = 13$ *e* $m = 11$*.*

Percebe-se que, $15 \cdot 13 = 195$ *e* $4 \cdot 13 = 52$*. Deste modo, tem-se respectivamente,* $15 \cdot 13 = 195 \equiv 8$ *mod* 11 *e* $4 \cdot 13 = 52 \equiv 8$ *mod* 11*, isto é,* $15 \cdot 13 \equiv 4 \cdot 13$ *mod* 11*, se, e somente se,* $15 \equiv 4$ *mod* 11*.*

O exemplo a seguir mostra uma congruência em que a simplificação de fatores utilizada na Proposição 2.2 não é válida.

Exemplo 2.6. *Sejam* $a = 10$*,* $b = 7$*,* $c = 8$ *e* $m = 6$*.*

Nota-se que, $10 \cdot 8 = 80 \equiv 2$ *mod* 6 *e* $7 \cdot 8 = 56 \equiv 2$ *mod* 6*. Deste modo , tem-se que,* $10 \cdot 8 \equiv 7 \cdot 8$ *mod* 6*, mas* $10 \not\equiv 7$ *mod* 6*.*

Note que, neste caso não é possível usar a Proposição 2.2 pois, o $mdc(8, 6) = 2$*.*

A seguinte proposição estabelece condições para que dois números sejam primos entre si. A demonstração deste resultado pode ser encontrada em Hefez (2016).

Proposição 2.3. *Dois números inteiros* a *e* b *são primos entre si, se e somente se, existem* m *e* $n \in \mathbb{Z}$*, tais que* $ma + nb = 1$*.*

Exemplo 2.7. *Estabelecendo* $a = 25$ *e* $b = 13$ *primos entre si, será determinado* m *e* $n \in \mathbb{Z}$*, tais que* $25m + 13n = 1$*.*

Utilizando o Algoritmo estendido de Euclides obtém-se:

$$25 = 1 \cdot 13 + 12 \Rightarrow 12 = 25 - 1 \cdot 13 \tag{2.1}$$

$$13 = 1 \cdot 12 + 1 \Rightarrow 1 = 13 - 1 \cdot 12. \tag{2.2}$$

Assim, substituindo (2.1) *em* (2.2) *conclui-se que,*

$$1 = 13 - 1 \cdot (25 - 1 \cdot 13) = 13 - 1 \cdot 25 + 1 \cdot 13 = 2 \cdot 13 - 1 \cdot 25.$$

Portanto, $m = -1$ *e* $n = 2$*.*

A seguinte proposição estabelece critérios de divisibilidade para o produto. A demonstração deste resultado pode ser encontrada em Hefez (2016).

Proposição 2.4. *Dados* $a, b, c \in \mathbb{Z}$*, com* b *e* c *não ambos nulos, tem-se que,*

$$b \mid a \quad e \quad c \mid a \Longleftrightarrow \frac{bc}{mdc(b, c)} \mid a.$$

Exemplo 2.8. *Considere* $a = 12$*,* $b = 2$ *e* $c = 3$*, onde,* $mdc(2, 3) = 1$*.*

Assim, pode-se estabelecer que,

$$2 \mid 12 \quad e \quad 3 \mid 12 \Longleftrightarrow \frac{2 \cdot 3}{mdc(2, 3)} = \frac{6}{1} = 6 \mid 12.$$

A Proposição 2.5 indica uma relação entre congruências lineares e máximo divisor comum.

Proposição 2.5. *Sejam $a, m \in \mathbb{Z}$, com $m > 1$. A congruência $aX \equiv 1$ mod m, possui solução se e somente se $mdc(a, m) = 1$. Além disso, se $x_0 \in \mathbb{Z}$ é uma solução, então x é uma solução da congruência se, e somente se, $x \equiv x_0$ mod m.*

Demonstração. A congruência $aX \equiv 1 \bmod m$ tem uma solução x_0 se, e somente se, $m \mid ax_0 - 1$, o que ocorre exatamente quando a equação diofantina $aX - mY = 1$ possui solução em $\mathbb{Z}$. Pela Proposição 2.3, isso ocorre se, e somente se $mdc(a, m) = 1$.

Ademais, se x_0 e x são soluções da congruência $aX \equiv 1 \bmod m$, então $ax \equiv ax_0 \bmod m$ e o $mdc(a, m) = 1$. Assim, utiliza-se a Proposição 2.2 para obter que $x \equiv x_0 \bmod m$. Note, que se x_0 é solução da congruência $aX \equiv 1 \bmod m$ e $x \equiv x_0 \bmod m$, então x é também uma solução da mesma congruência, pois, $aX \equiv ax_0 \equiv 1 \bmod m$. □

Deste modo, ao considerar que duas soluções congruentes módulo m, representam, em módulo, a mesma solução, define-se a unicidade da solução da congruência $aX \equiv 1 \bmod m$.

O exemplo a seguir, ilustra a aplicação desta proposição.

Exemplo 2.9. *Resolva a congruência $3X \equiv 5$ mod 7.*

Se x_0 é uma solução da congruência $3X \equiv 5$ mod 7, tem - se:

$3x_0 \equiv 5$ *mod* $7 \iff 3x_0 - 5 \equiv 0$ *mod* $7 \iff 7 \mid 3x_0 - 5$. *Assim, existe um y_0 tal que,* $7y_0 = 3x_0 - 5 \iff 3x_0 - 7y_0 = 5$.

Observe, que $mdc(3, 7) = 1$, ou seja, a equação diofantina $3x_0 - 7y_0 = 5$ possui uma única solução módulo 7.

A resolução desta equação diofantina poderia ser feita pelo algoritmo de Euclides, contudo, por inspeção, conclui-se que, $x_0 = 4, y_0 = 1$ é uma das soluções. Além disso, $x = 11$ também é solução, pois, $33 = 3 \cdot 11 \equiv 5$ mod 7. Mas, $11 \equiv 4$ mod 7, portanto, $x_0 = 4$ é a única solução módulo 7.

A Proposição 2.5 será usada na demonstração do Teorema 2.1 atribuído a John Wilson (1741 - 1793).

Além das proposições de aritmética modular já apresentadas, será demonstrado na sequência o Lema 2.1 que será utilizado na prova da convergência da série dos inversos dos primos (Teorema 5.3).

Lema 2.1. *Todo número natural n pode ser escrito como $n = a \cdot b^2$, com $a, b \in \mathbb{N}$ com a livre de quadrados ou $a = 1$*

Demonstração. Seja b o maior divisor de n tal que b^2 também é divisor de n. Assim, existe $a \in N$ tal que $n = a \cdot b^2$. Será provado que $a = 1$ ou a é livre de quadrados.

Se n é um quadrado perfeito, então, $a = 1$.

Se n não for um quadrado perfeito, e $n = a \cdot b^2$, com a não livre de quadrados, então, pode-se escrever $a = k^2 \cdot m$ para algum $k > 1$e m naturais, ou seja, $n = k^2 \cdot m \cdot b^2 = (kb)^2 \cdot m$. Note que a igualdade anterior implica que $kb > b$ é um divisor de n, tal que, seu quadrado também é divisor de n, o que contradiz a definição de b. Logo, a é livre de quadrados. □

O exemplo ilustra o processo de demonstração do Teorema de Wilson (Teorema 2.1).

Exemplo 2.10. *Mostre que* $16! \equiv -1$ *mod* 17.

Note que, dentre os números {1, 2, 3, ... , 14, 15, 16} apenas os números 1 e 16 são seus próprios inversos multiplicativos módulo 17, ou seja, $1 \cdot 1 = 1 \equiv 1$ *mod* 17 *e* $16 \cdot 16 = 256 \equiv 1$ *mod* 17. *Além disso, os outros números {2, 3, 4, ... 14, 15} todos possuem um inverso módulo 17 diferente, já que são primos com 17, isto é,*

$$2 \cdot 9 = 18 \equiv 1 \text{ } mod \text{ } 17;$$
$$3 \cdot 6 = 18 \equiv 1 \text{ } mod \text{ } 17;$$
$$4 \cdot 13 = 52 \equiv 1 \text{ } mod \text{ } 17;$$
$$5 \cdot 7 = 35 \equiv 1 \text{ } mod \text{ } 17;$$
$$8 \cdot 15 = 120 \equiv 1 \text{ } mod \text{ } 17;$$
$$10 \cdot 12 = 120 \equiv 1 \text{ } mod \text{ } 17;$$
$$11 \cdot 14 = 154 \equiv 1 \text{ } mod \text{ } 17.$$

Além disso, tem-se que, $1 \equiv 1$ *mod* 17 *e* $16 \equiv -1$ *mod* 17. *Sendo assim, pode-se utilizar a Proposição 2.1 para concluir que,*

$$(2 \cdot 9) \cdot (3 \cdot 6) \cdot (4 \cdot 13) \cdot (5 \cdot 7) \cdot (8 \cdot 15) \cdot (10 \cdot 12) \cdot (11 \cdot 14) \cdot 1 \cdot 16 \equiv 1 \cdot 1 \cdot (-1) \text{ } mod \text{ } 17$$
$$16! \equiv -1 \text{ } mod \text{ } 17.$$

A demostração do seguinte resultado usa ideias similares às consideradas no Exemplo 2.10.

Teorema 2.1. *(Teorema de Wilson) Seja* $p \in \mathbb{Z}$, $p > 1$. p *é um número primo, se e somente se,* $(p-1)! \equiv -1$ *mod* p.

Demonstração. Para $p = 2$, $p = 3$ e $p = 4$ o resultado é válido pois tem-se respectivamente que, $(2-1)! = 1 \equiv -1 \text{ mod } 2$; $(3-1)! = 2 \equiv -1 \text{ mod } 3$; e $(4-1)! = 3! = 6 \not\equiv -1 \text{ mod } 4$. Assim, pode-se considerar $p \geq 5$.

($\Rightarrow$) Se p é um número primo, então, $(p-1)! \equiv -1 \text{ mod } p$.

Se p é primo, pela Proposição 2.5, dado $a \in \{1, 2, 3, ... , p - 1\}$ existe um único $b \in \{1, 2, 3, ... , p - 1\}$ tal que $ab \equiv 1 \text{ mod } p$, pois todos os números $\{1, 2, 3, ... , p - 1\}$ são primos com p.

Além disso, se $a \in \{1, 2, 3, ... , p - 1\}$ é tal que, $a^2 \equiv 1 \bmod p$, então $a^2 - 1 \equiv 0 \bmod p$, desse modo, $p \mid a^2 - 1 = (a-1) \cdot (a+1)$, ou seja, $p \mid (a-1)$ ou $p \mid (a+1)$. Mas isso só ocorre se $a - 1$ for igual a 0 ou $a + 1$ for igual a p, ou seja, quando $a = 1$ ou $a = p - 1$. Logo, de todos os números entre 1 e $p - 1$, os únicos que são seus próprios inversos módulo p são 1 e $p - 1$.

Deste modo, ao omitir 1 e $p - 1$ pode-se agrupar os números $\{2, 3, ... , p - 2\}$ em pares (o número e seu inverso) e o produto de cada par é congruente a 1 módulo p, o que mostra que, $[2 \cdot 3 \cdot ... \cdot (p-2)] \equiv 1 \bmod p$. Além disso, $1 \equiv 1 \bmod p$ e $(p-1) \equiv -1 \bmod p$.

Considerando estas 3 congruências tem-se:

$$[2 \cdot 3 \cdot ... \cdot (p-2)] \equiv 1 \bmod p; \tag{2.3}$$

$$1 \equiv 1 \bmod p; \tag{2.4}$$

$$(p-1) \equiv -1 \bmod p. \tag{2.5}$$

Multiplicando ambos os membros das congruências (2.3), (2.4) e (2.5), conclui-se que,

$$\begin{aligned} [2 \cdot 3 \cdot ... \cdot (p-2)] \cdot 1 \cdot (p-1) &\equiv 1 \cdot 1 \cdot (-1) \bmod p \\ (p-2)! \cdot (p-1) &\equiv -1 \bmod p \\ (p-1)! &\equiv -1 \bmod p. \end{aligned}$$

($\Leftarrow$) Será mostrado por contraposição que se p não é um número primo, então, $(p-1)! \not\equiv -1 \bmod p$.

De fato, será demonstrado que $p \mid (p-1)!$. Para tal, considera-se $p = a \cdot b$ com $a > 1$ e $b > 1$.

Se $a \neq b$, supõe-se que $1 < a < b$, logo, $(p-1)! = 1 \cdot 2 \cdot ... \cdot a \cdot ... \cdot b \cdot ... \cdot (p-1) \equiv 0 \bmod p$, pois p é igual a $a \cdot b$.

Se $a = b > 2$, tem-se que, $(p-1)! = 1 \cdot 2 \cdot ... \cdot a \cdot ... \cdot 2a \cdot ... \cdot (p-1) \equiv 0 \bmod p$, pois p é igual a $a \cdot a$. Portanto, $p \mid (p-1)!$

Se $p \mid (p-1)!$, então, $p \nmid (p-1)! + 1$ o que mostra que $(p-1)! + 1 \not\equiv 0 \bmod p$, isto é, $(p-1)! \not\equiv -1 \bmod p$, e assim, obtém - se o resultado desejado. □

O lema seguinte será utilizado na demonstração da Congruência de Clement (Teorema 2.2).

Lema 2.2. *Se n é par maior que 4, então $(n-1)! + 1 \equiv 1$ mod n.*

Demonstração. Se n é par maior que 4, então, pode-se escrever $n = 2k$, com $k > 2$. Além disso, tem-se que,

$$(n-1)! = (n-1) \cdots k \cdots 3 \cdot 2 \cdot 1.$$

Como $2k \equiv 0 \bmod n$ conclui-se que, $(n-1)! \equiv 0 \bmod n$, e portanto, $(n-1)! + 1 \equiv 1 \bmod n$. □

Para ilustrar o Lema 2.2 pode-se considerar o seguinte exemplo.

Exemplo 2.11. *Ao estabelecer* $n = 8$ *tem-se que,*

$$\begin{aligned}(8-1)! + 1 &\equiv 1 \ mod\ 8\\ (7!) + 1 &\equiv 1 \ mod\ 8\\ 5040 + 1 &\equiv 1 \ mod\ 8\\ 5041 &\equiv 1 \ mod\ 8.\end{aligned}$$

2.1 NÚMEROS PRIMOS GÊMEOS

No estudo dos primos gêmeos serão apresentados caracterizações indispensáveis ao trabalho. A definição, assim como a Congruência de Clement (Teorema 2.2) são expostos, conforme os resultados considerados em Ribenboim (2004) e Pantoja (2012).

Definição 2.2. *Se dois números ímpares* p *e* $p+2$ *são primos, então, estes são chamados de primos gêmeos.*

Para elucidar a definição apresenta-se alguns pares de primos gêmeos na Tabela 2.1:

Tabela 2.1 – Os primeiros pares de primos gêmeos

p	$p+2$
3	5
5	7
11	13
17	19
29	31
41	43
59	61
71	73
101	103
107	109
137	139
149	151
179	181
191	193
197	199

Fonte: O autor.

A Congruência de Clement é uma caracterização completa para determinar primos gêmeos e será demonstrada de maneira detalhada, por meio de proposições de aritmética modular e também do Teorema de Wilson (Teorema 2.1).

Teorema 2.2. *(Congruência de Clement) Seja $n \geq 2$. Os números inteiros $n, n+2$ formam um par de primos gêmeos se, e somente se,*

$$4[(n-1)!+1]+n \equiv 0 \textit{ mod } (n(n+2)). \tag{2.6}$$

Demonstração. ($\Rightarrow$) Se a congruência $4[(n-1)!+1]+n \equiv 0 \bmod (n(n+2))$ é satisfeita , então, n e $n+2$ são primos.

Note que, se $4[(n-1)!+1]+n \equiv 0 \bmod (n(n+2))$ então $n \neq 2$ e $n \neq 4$.

Note também que a congruência, $4[(n-1)!+1]+n \equiv 0 \bmod (n(n+2))$ implica que $4[(n-1)!+1]+n \equiv 0 \bmod n$ e $4[(n-1)!+1]+n \equiv 0 \bmod (n+2)$.

De, $4[(n-1)!+1]+n \equiv 0 \bmod n$, tem-se que,

$$4[(n-1)!+1] \equiv 0 \bmod n \tag{2.7}$$

pois $n \equiv 0 \bmod n$. Se n for par maior que 4, então, pelo Lema 2.2, chega-se a $4[(n-1)!+1] \equiv 4 \bmod n$ contradizendo a congruência (2.7).

Como $n \neq 2$ e $n \neq 4$, tem-se que, n é ímpar e assim $mdc(4,n) = 1$, logo, pela Proposição 2.2, obtém-se da congruência (2.7) que $(n-1)!+1 \equiv 0 \bmod n$, portanto, pelo Teorema de Wilson (Teorema 2.1), n é primo.

Por outro lado,

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

Multiplicando ambos os membros da congruência por $n(n+1)$, obtém-se:

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

Somando e subtraindo 4, tem-se:

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

$$4[(n+1)!+1] \equiv 0 \text{ mod } (n+2). \tag{2.8}$$

Se n for par maior que 4, então pelo Lema 2.2, chega-se a $4[(n+1)!+1] \equiv 4$ mod $(n+2)$ contradizendo a congruência (2.8).

Como n não é zero nem 2, segue que $n+2$ é ímpar e $mdc(n+2,4) = 1$. Assim, pela Proposição 2.2 tem - se da congruência (2.8) que $(n+1)!+1 \equiv 0$ mod $(n+2)$, portanto, pelo Teorema de Wilson (Teorema 2.1), $n+2$ é primo.

($\Leftarrow$) Se n e $n+2$, são primos, então, a congruência $4[(n-1)!+1]+n \equiv 0$ mod $(n(n+2))$ é satisfeita.

Como, n e $n+2$ são primos $n \geq 2$, utilizando o Teorema de Wilson 2.1, constata-se que, $(n-1)! \equiv -1$ mod n, ou seja,

$$(n-1)!+1 \equiv 0 \text{ mod } n. \tag{2.9}$$

Por outro lado pelo Teorema de Wilson 2.1, pode-se estabelecer,

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

Note que, $n^2+n \equiv (n+2)\cdot(n-1)+2 \equiv 2$ mod $(n+2)$, consequentemente, $(n^2+n)\cdot(n-1)!+1 \equiv 2(n-1)!+1$ mod $(n+2)$.

Desta forma, pode-se escrever,

$$2(n-1)!+1 = (n+2)\cdot k \tag{2.10}$$

para algum k inteiro, ou seja, $2(n-1)!+1 = kn+2k$ e isso implica que, $2(n-1)!+1 \equiv 2k$ mod n.

Na congruência (2.9), pode-se multiplicar ambos os membros por 2, para assim, obter:

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

Voltando na igualdade (2.10) e multiplicando ambos os membros da igualdade por 2, estabelece-se que, $4(n-1)!+2 = 2k\cdot(n+2)$.

Como $2k \equiv -1 \bmod n$, ou seja, $2k = nq - 1$, com q inteiro conclui-se que,

$$\begin{aligned}
4(n-1)! + 2 &= (nq-1)\cdot(n+2)\\
4(n-1)! + 2 &= (nq)\cdot(n+2) - 1\cdot(n+2)\\
4(n-1)! + 2 &\equiv (nq)\cdot(n+2) - 1\cdot(n+2) \bmod n(n+2)\\
4(n-1)! + 2 &\equiv -1\cdot(n+2) \bmod n(n+2)\\
4(n-1)! + 2 &\equiv -n-2 \bmod n(n+2)\\
4(n-1)! + 4 + n &\equiv 0 \bmod n(n+2)\\
4[(n-1)! + 1] + n &\equiv 0 \bmod n(n+2).
\end{aligned}$$

E assim, a congruência (2.6) é satisfeita. □

O exemplo a seguir mostra que para o par de primos gêmeos $(11, 13)$ a Congruência de Clement (Teorema 2.2) é satisfeita.

Exemplo 2.12. *Verifique que, os primos gêmeos 11 e 13 satisfazem a congruência*

$$4[(11-1)! + 1] + 11 \equiv 0 \textit{ mod } (11\cdot(11+2)).$$

Desenvolvendo a congruência e utilizando propriedades de aritmética modular obtém-se:

$$\begin{aligned}
4[(11-1)! + 1] + 11 &\equiv 4[(10)! + 1] + 11 \textit{ mod } (11\cdot(11+2))\\
&\equiv 4[(10\cdot 9\cdot 8\cdot 7!) + 1] + 11 \textit{ mod } (11\cdot 13)\\
&\equiv 4[720\cdot 7! + 1] + 11 \textit{ mod } (11\cdot 13)\\
&\equiv 4[5\cdot 7! + 1] + 11 \textit{ mod } 143\\
&\equiv 4[5\cdot 5040 + 1] + 11 \textit{ mod } 143\\
&\equiv 4[5\cdot 35 + 1] + 11 \textit{ mod } 143\\
&\equiv 4[175 + 1] + 11 \textit{ mod } 143\\
&\equiv 4\cdot 176 + 11 \textit{ mod } 143\\
&\equiv 4\cdot 33 + 11 \textit{ mod } 143\\
&\equiv 132 + 11 \textit{ mod } 143\\
&\equiv 143 \textit{ mod } 143\\
&\equiv 0 \textit{ mod } 143.
\end{aligned}$$

Com o objetivo de verificar se é possível usar a Congruência de Clement (Teorema 2.2) para obter pares de primos gêmeos, foi feito um experimento de programar tal congruência (Figura 2.1) em um computador com configurações básicas, no sistema de computação algébrica MAXIMA. Para isso, considerou-se $3 \leq n \leq 100000$ obtendo 1224 pares de primos gêmeos.

A Figura 2.1 mostra os últimos 21 pares de primos gêmeos obtidos no MAXIMA.

Figura 2.1 – Últimos pares de primos gêmeos menores que 100000 gerados no MAXIMA

```
for p from 3 thru 100000 do if
   mod (4·(p-1)!+4+p,p·(p+2))=0
        then print (p,p+2);
         98009  98011
         98297  98299
         98321  98323
         98387  98389
         98561  98563
         98639  98641
         98711  98713
         98729  98731
         98807  98809
         98867  98869
         98897  98899
         98909  98911
         98927  98929
         99131  99133
         99137  99139
         99257  99259
         99347  99349
         99527  99529
         99707  99709
         99719  99721
         99989  99991
         done
```

Fonte: O autor.

Na tentativa de obter primos gêmeos maiores, ampliou-se o experimento, estabelecendo $n > 1000000$. Contudo, não houve êxito, já que após algumas horas o MAXIMA seguiu calculando sem atualizar novos valores. Tal pausa na obtenção de pares de primos gêmeos aconteceu devido ao trabalho com fatorial, tendo em vista que é extremamente lento até mesmo para o computador trabalhar uma congruência com fatorial de um número maior que 100000. Logo, compreende-se que este critério não é útil para caracterizar primos gêmeos muito grandes.

Apesar da considerável importância da Congruência de Clement (Teorema 2.2) é possível obter outro tipo de propriedade necessária para ter um par de primos gêmeos como mostra o Teorema 2.3 que será ilustrado antes da demonstração.

A Tabela 2.2 ilustra em azul os pares de primos gêmeos da forma $6k-1$ e $6k+1$ e em branco pares da forma $6k-1$ e $6k+1$ que não são primos gêmeos:

Tabela 2.2 – Ilustração demonstrada no Teorema 2.3

k	$x = 6 \cdot k - 1$	$y = 6 \cdot k + 1$	(x, y)
1	$6 \cdot 1 - 1 = 5$	$6 \cdot 1 + 1 = 7$	$(5, 7)$
2	$6 \cdot 2 - 1 = 11$	$6 \cdot 2 + 1 = 13$	$(11, 13)$
3	$6 \cdot 3 - 1 = 17$	$6 \cdot 3 + 1 = 19$	$(17, 19)$
4	$6 \cdot 4 - 1 = 23$	$6 \cdot 4 + 1 = 25$	$(23, 25)$
5	$6 \cdot 5 - 1 = 29$	$6 \cdot 5 + 1 = 31$	$(29, 31)$
6	$6 \cdot 6 - 1 = 35$	$6 \cdot 6 + 1 = 37$	$(35, 37)$
7	$6 \cdot 7 - 1 = 41$	$6 \cdot 7 + 1 = 43$	$(41, 43)$
8	$6 \cdot 8 - 1 = 47$	$6 \cdot 8 + 1 = 49$	$(47, 49)$
9	$6 \cdot 9 - 1 = 53$	$6 \cdot 9 + 1 = 55$	$(53, 55)$
10	$6 \cdot 10 - 1 = 59$	$6 \cdot 10 + 1 = 61$	$(59, 61)$
11	$6 \cdot 11 - 1 = 65$	$6 \cdot 11 + 1 = 67$	$(65, 67)$
12	$6 \cdot 12 - 1 = 71$	$6 \cdot 12 + 1 = 73$	$(71, 73)$
13	$6 \cdot 13 - 1 = 77$	$6 \cdot 13 + 1 = 79$	$(77, 79)$
14	$6 \cdot 14 - 1 = 83$	$6 \cdot 14 + 1 = 85$	$(83, 85)$
15	$6 \cdot 15 - 1 = 89$	$6 \cdot 15 + 1 = 91$	$(89, 91)$
16	$6 \cdot 16 - 1 = 95$	$6 \cdot 16 + 1 = 97$	$(95, 97)$
17	$6 \cdot 17 - 1 = 101$	$6 \cdot 17 + 1 = 103$	$(101, 103)$
18	$6 \cdot 18 - 1 = 107$	$6 \cdot 18 + 1 = 109$	$(107, 109)$
19	$6 \cdot 19 - 1 = 113$	$6 \cdot 19 + 1 = 115$	$(113, 115)$
20	$6 \cdot 20 - 1 = 119$	$6 \cdot 20 + 1 = 121$	$(119, 121)$

Fonte: O autor.

Teorema 2.3. *Todo número primo p maior que 3 pode ser escrito da forma $p = 6k + 1$ ou da forma $p = 6k - 1$, para algum $k \in \mathbb{Z}$. Com exceção de $(3, 5)$, todos os pares de primos gêmeos $(p, p + 2)$ podem ser escritos como $(p, p + 2) = (6k - 1, 6k + 1)$ para algum $k \in \mathbb{Z}$.*

Demonstração. Pela divisão euclidiana, todo número p, pode ser escrito como $p = 6k + r$, para algum $k \in \mathbb{Z}$. Desta forma, para,

$r = 0,$ tem-se , $p = 6k$ e $p + 2 = 6k + 2 = 2 \cdot (3k + 1)$;

$r = 1,$ tem-se , $p = 6k + 1$ e $p + 2 = 6k + 3 = 3 \cdot (2k + 1)$;

$r = 2,$ tem-se , $p = 6k + 2 = 2 \cdot (3k + 1);$ e $p + 2 = 6k + 4 = 2 \cdot (3k + 2)$;

$r = 3,$ tem-se , $p = 6k + 3 = 3 \cdot (2k + 1)$ e $p + 2 = 6k + 5$;

$r = 4,$ tem-se , $p = 6k + 4 = 2 \cdot (3k + 2)$ e $p + 2 = 6k + 6 = 6 \cdot (k + 1)$;

$r = 5,$ tem-se , $p = 6k + 5$ e $p + 2 = 6k + 7 = 6k + 1$.

Ao considerar p nas igualdades anteriores, percebe-se que únicas formas de obter um primo são $p = 6k + 1$ ou $p = 6k + 5$. No entanto, $6k + 5 \equiv 6k - 1 \bmod 6$. Logo, todo número primo maior que 3 pode ser escrito como $6k + 1$ ou $6k - 1$.

Analogamente, ao analisar p e $p+2$, nota-se que as únicas formas para se obter primos gêmeos são $p = 6k+5$ e $p+2 = 6k+1$. Contudo, $6k+5 \equiv 6k-1 \bmod 6$ e, portanto com exceção de $(3,5)$, todos os pares de primos gêmeos podem ser escritos como $(6k-1, 6k+1)$ para algum $k \in \mathbb{Z}$. □

Teorema 2.4. *A soma de qualquer par de números primos gêmeos (exceto 3 e 5) é divisível por 12 .*

Demonstração. Pelo Teorema 2.3, foi estabelecido que todos os pares de primos gêmeos p e $p+2$ podem ser escritos como $(6k-1, 6k+1)$ para algum $k \in \mathbb{Z}$.

Assim, efetuando a soma, chega-se a,

$$p + (p+2) = (6k-1) + (6k+1) = 12k$$

para algum $k \in \mathbb{Z}$.

Portanto, a soma de qualquer par de números primos gêmeos, exceto $(3,5)$ é divisível por 12. □

Os próximos resultados, Teoremas 2.5, 2.6 e 2.7 são extensões do Teorema 2.4 para primos gêmeos.

Teorema 2.5. *Se x e y são dois primos gêmeos maiores que três, então, tem-se que $x^2 - y^2$ é divisível por 24, para todo $x > y$.*

Demonstração. Se x e y são dois primos gêmeos maiores que três, então, pelo Teorema 2.4 $x + y = 12k$ para algum $k \in \mathbb{Z}$. Desta forma, para todo $x > y$ pode-se estabelecer que,

$$\begin{aligned} x^2 - y^2 &= (x+y) \cdot (x-y) \\ &= 12k \cdot (x-y) \\ &= 12k \cdot 2 \\ &= 24k. \end{aligned}$$

Portanto, $x^2 - y^2$ é divisível por 24, para todo $x > y$, para todo $x > y$. □

Exemplo 2.13. *Nota-se que o par de primos gêmeos $(227, 229)$ satisfaz o Teorema demonstrado, ou seja, $229^2 - 227^2 = 24k$ para algum $k \in \mathbb{Z}$. De fato,*

$$\begin{aligned} 229^2 - 227^2 &= (229 + 227) \cdot (229 - 227) \\ &= 456 \cdot 2 \\ &= 912 \\ &= 24 \cdot 38. \end{aligned}$$

A Tabela 2.3 ilustra o Teorema 2.5 com outros pares de primos gêmeos.

Tabela 2.3 – Ilustração do Teorema 2.5

x	y	$x^2 - y^2$	$24k$
241	239	$241^2 - 239^2 = 58081 - 57121 = 960$	$24 \cdot 40$
271	269	$271^2 - 269^2 = 73441 - 72361 = 1080$	$24 \cdot 45$
283	281	$283^2 - 281^2 = 80089 - 78961 = 1128$	$24 \cdot 47$
313	311	$313^2 - 311^2 = 97969 - 96721 = 1248$	$24 \cdot 52$
349	347	$349^2 - 347^2 = 121801 - 120409 = 1392$	$24 \cdot 58$
421	419	$421^2 - 419^2 = 177241 - 175561 = 1680$	$24 \cdot 70$

Fonte: O autor.

Exemplo 2.14. *A recíproca do Teorema 2.5 não é válida. De fato, ao substituir x e y, respectivamente, por 25 e 23 obtém-se que,*

$$\begin{aligned} x^2 - y^2 &= 25^2 - 23^2 \\ &= 625 - 529 \\ &= 96 \\ &= 24 \cdot 4. \end{aligned}$$

Deste modo, compreende-se que a igualdade $x^2 - y^2 = 24k$ se satisfaz, entretanto, 25 é composto.

Teorema 2.6. *Se x e y são dois primos gêmeos maiores que três, então, tem-se que $x^3 + y^3$ é divisível por 36.*

Demonstração. Se x e y são dois primos gêmeos maiores que três, então, pelo Teorema 2.3 será considerado, $x = 6k + 1$ e $y = 6k - 1$, para algum $k \in \mathbb{Z}$. Assim,

$$\begin{aligned} x^3 + y^3 &= (6k+1)^3 + (6k-1)^3 \\ &= 216k^3 + 108k^2 + 18k + 1 + 216k^3 - 108k^2 + 18k - 1 \\ &= 432k^3 + 36k \\ &= 36 \cdot (13k^3 + k). \end{aligned}$$

Portanto, $x^3 + y^3$ é divisível por 36. □

Exemplo 2.15. *Constata-se que o par de primos gêmeos $(17, 19)$ satisfaz o Teorema demonstrado, ou seja, $17^3 + 19^3 = 36k$ para algum $k \in \mathbb{Z}$. Segue que,*

$$\begin{aligned} 17^3 + 19^3 &= 4913 + 6859 \\ &= 11772 \\ &= 36 \cdot 327. \end{aligned}$$

A Tabela 2.4 ilustra o Teorema 2.6 com outros pares de primos gêmeos.

Tabela 2.4 – Ilustração do Teorema 2.6

x	y	x^3+y^3	$36k$
29	31	$29^3+31^3=24389+29791=54180$	$36\cdot 1505$
41	43	$41^3+43^3=68921+79507=148428$	$36\cdot 4123$
59	61	$59^3+61^3=205379+226981=432360$	$36\cdot 12010$
71	73	$71^3+73^3=357911+389017=746928$	$36\cdot 20748$
191	193	$191^3+193^3=6967871+7189057=14156928$	$36\cdot 393248$
197	199	$197^3+199^3=7645373+7880599=15525972$	$36\cdot 431277$

Fonte: O autor.

Exemplo 2.16. *A recíproca do Teorema 2.6 é inválida. De fato, ao considerar* $x=20$ *e* $y=22$ *tem-se que,*

$$\begin{aligned} x^3+y^3 &= 20^3+22^3 \\ &= 8000+10648 \\ &= 18648 \\ &= 36\cdot 565. \end{aligned}$$

Assim, nota-se que a igualdade $x^3+y^3=36k$ *é satisfeita, porém,* 20 *e* 22 *não são primos.*

Teorema 2.7. *Se* x *e* y *são dois primos gêmeos maiores que três, então,* x^4-y^4 *é divisível por* 48*, para todo* $x>y$ *.*

Demonstração. Se x e y são dois primos gêmeos maiores que três, então, pelo Teorema 2.3 será considerado, $x=6k+1$ e $y=6k-1$, para algum $k\in\mathbb{Z}$. Assim, para todo $x>y$ tem-se que,

$$\begin{aligned} x^4-y^4 &= (6k+1)^4-(6k-1)^4 \\ &= 1296k^4+864k^3+216k^2+24k+1-(1296k^4-864k^3+216k^2-24k+1) \\ &= 1296k^4+864k^3+216k^2+24k+1-1296k^4+864k^3-216k^2+24k-1 \\ &= 1728k^3+48k \\ &= 48\cdot(36k^3+k). \end{aligned}$$

Portanto, x^4-y^4 é divisível por 48. □

Exemplo 2.17. *Percebe-se que o par de primos gêmeos* $(5, 7)$ *satisfaz o Teorema demonstrado, ou seja,* $7^4 - 5^4 = 48k$ *para algum* $k \in \mathbb{Z}$. *De fato,*

$$\begin{aligned} 7^4 - 5^4 &= 2401 - 625 \\ &= 1776 \\ &= 48 \cdot 37. \end{aligned}$$

A Tabela 2.5 ilustra o Teorema 2.7 com outros pares de primos gêmeos.

Tabela 2.5 – Ilustração do Teorema 2.7

x	y	$x^4 - y^4$	$48k$
13	11	$13^4 - 11^4 = 28561 - 14641 = 13920$	$48 \cdot 290$
19	17	$19^4 - 17^4 = 130321 - 83521 = 46800$	$48 \cdot 975$
31	29	$31^4 - 29^4 = 923521 - 707281 = 216240$	$48 \cdot 4505$
43	41	$43^4 - 41^4 = 3418801 - 2825761 = 593040$	$48 \cdot 12355$
103	101	$103^4 - 101^4 = 112550881 - 104060401 = 8490480$	$48 \cdot 176885$
109	107	$109^4 - 107^4 = 141158161 - 131079601 = 10078560$	$48 \cdot 209970$

Fonte: O autor.

Exemplo 2.18. *A recíproca do Teorema 2.7 não é verdadeira. De fato, ao estabelecer* $x = 16$ *e* $y = 14$ *verifica-se que,*

$$\begin{aligned} x^4 - y^4 &= 16^4 - 14^4 \\ &= 65536 - 38416 \\ &= 27120 \\ &= 48 \cdot 564. \end{aligned}$$

Desta forma, percebe-se que a igualdade $x^4 - y^4 = 48k$ *é satisfeita, contudo* 14 *e* 16 *não são primos.*

Ao analisar os Teoremas 2.5, 2.6 e 2.7 é natural que se conjecture uma possível generalização.

Conjectura 1: Se x e y são dois primos gêmeos maiores que três, com $x > y$ e n par, então, $x^n - y^n$ é divisível por $12n$. Contudo, quando considera-se $x = 7$, $y = 5$, $n = 10$ e $12n = 120$ tem-se que,

$$\begin{aligned} \frac{(x^{10} - y^{10})}{120} &= \frac{7^{10} - 5^{10}}{120} \\ &= \frac{282475249 - 9765625}{120} \\ &= \frac{272709624}{120} = \frac{11362901}{5}. \end{aligned}$$

Logo, $7^{10} - 5^{10}$ não é divisível por 120, o que invalida a Conjectura 1.

Conjectura 2: Se x e y são dois primos gêmeos maiores que três e n é ímpar, então, $x^n + y^n$ é divisível por $12n$. Contudo, quando considera-se $x = 11$, $y = 13$, $n = 5$ e $12n = 60$ obtém-se que,

$$\begin{aligned}\frac{(x^5 + y^5)}{60} &= \frac{11^5 + 13^5}{60} \\ &= \frac{161051 + 371293}{60} \\ &= \frac{532344}{60} = \frac{44362}{5}.\end{aligned}$$

Assim , conclui-se que, $11^5 + 13^5$ não é divisível por 60, o que invalida a Conjectura 2.

Portanto, os Teoremas 2.5, 2.6 e 2.7 não podem ser generalizados através das conjecturas 1 e 2, e em princípio, só pode-se afirmar que, tanto a diferença $x^n - y^n$, com n par, quanto a soma $x^n + y^n$, com n ímpar são divisíveis por 12.

Teorema 2.8. *Seja x e y dois primos gêmeos maiores que três. Se $x > y$, n natural par, então, $x^n - y^n$ é divisível por 12. Se n é natural ímpar, então, $x^n + y^n$ é divisível por 12.*

Demonstração. As prova serão feitas por indução em n.

Assim, ao considerar x e y dois primos gêmeos maiores que três com $x > y$ e $n = 2$ tem-se que, pelo Teorema 2.5, $x^2 - y^2$ é divisível por 12. Supondo-se por hipótese indutiva que $x^n - y^n$ seja divisível por 12 e será mostrado que $x^{n+2} - y^{n+2}$ é divisível por 12. Segue que,

$$\begin{aligned}x^{n+2} - y^{n+2} &= x^n \cdot x^2 - y^n \cdot y^2 \\ &= x^n \cdot x^2 - x^2 \cdot y^n + x^2 \cdot y^n - y^n \cdot y^2 \\ &= x^2(x^n - y^n) + y^n(x^2 - y^2).\end{aligned}$$

Logo, o Teorema 2.5 e a hipótese de indução permitem concluir que, $x^{n+2} - y^{n+2}$ é divisível por 12 para todo n par.

Analogamente, ao considerar $n = 1$ tem-se que, $x + y$ é divisível por 12, conforme o Teorema 2.4. Supondo-se por hipótese indutiva que $x^n + y^n$ seja divisível por 12 e será mostrado que $x^{n+2} + y^{n+2}$ é divisível por 12. Segue que,

$$\begin{aligned}x^{n+2} + y^{n+2} &= x^n \cdot x^2 + y^n \cdot y^2 \\ &= x^n \cdot x^2 + x^2 \cdot y^n - x^2 \cdot y^n + y^n \cdot y^2 \\ &= x^2(x^n + y^n) - y^n(x^2 - y^2) \\ &= x^2(x^n + y^n) - y^n(x + y) \cdot (x - y).\end{aligned}$$

Assim, o Teorema 2.4 e a hipótese de indução permitem concluir que, $x^{n+2} + y^{n+2}$ é divisível por 12 para todo n ímpar. □

Os resultados preliminares apresentados por meio das proposições foram fundamentais para as demonstrações dos teoremas desta seção. Principalmente, o Teorema de Wilson (Teorema 2.1), o teorema de caracterização dos primos gêmeos (Teorema 2.3) e a Congruência de Clement (Teorema 2.2). Estes resultados serão utilizados nas ilustrações numéricas da convergência da série dos inversos dos primos gêmeos (Figura 5.5) e na divergência das séries harmônica (Figura 5.1) e dos primos (Figura 5.3) na Seção 5.1.

3 NÚMEROS PRIMOS GÊMEOS E COEFICIENTES BINOMIAIS

Neste capítulo apresenta-se uma relação entre os números primos gêmeos e os coeficientes binomiais, através de exemplos, definições e demonstrações baseadas nos resultados apresentados em Talapadtur (2002).

A definição e as propriedades referentes a soma de coeficientes binomiais, em particular, a Relação de Stifel (Lema 3.1), embasam-se no livro Matemática Discreta dos autores Morgado e Carvalho (2015).

Definição 3.1. *Sejam n e p dois números naturais com $n \geq p$, denota-se por coeficiente binomial de classe p, do número n, a seguinte expressão:*

$$\binom{n}{p} = \frac{n!}{p!(n-p)!} = \frac{n \cdot (n-1) \cdot (n-2) \cdots (n-p+1)}{p!}.$$

No estudo dos primos gêmeos, algumas propriedades relacionadas a coeficientes binomiais são de fundamental importância para o trabalho. O Exemplo 3.1 é uma ilustração da identidade binomial conhecida como Relação de Stifel (Lema 3.1).

Exemplo 3.1. *Verifique que* $\binom{144}{64} = \binom{143}{63} + \binom{143}{64}$.

Desenvolvendo os coeficientes binomiais, obtém-se que:

$$\begin{aligned}
\binom{144}{64} &= \binom{143}{63} + \binom{143}{64} \\
\frac{144!}{64!80!} &= \frac{143!}{63!80!} + \frac{143!}{64!79!} \\
&= \frac{143!}{63!80!} \cdot \frac{64}{64} + \frac{143!}{64!79!} \cdot \frac{80}{80} \\
&= \frac{143!64}{64!80!} + \frac{143!80}{64!80!} \\
&= \frac{143!(64+80)}{64!80!} \\
&= \frac{143!144}{64!80!} \\
&= \frac{144!}{64!80!}.
\end{aligned}$$

As manipulações algébricas utilizadas no Exemplo 3.1 ajudam no entendimento da Relação de Stifel que será demonstrado a seguir.

Lema 3.1. *(Relação de Stifel) Para $n, r \in \mathbb{N}$ vale a identidade,* $\binom{n+1}{r+1} = \binom{n}{r} + \binom{n}{r+1}$.

Demonstração. Desenvolvendo os coeficientes binomiais, estabelece-se que:

$$\begin{aligned}
\binom{n+1}{r+1} &= \binom{n}{r} + \binom{n}{r+1} \\
\frac{(n+1)!}{(r+1)!(n-r)!} &= \frac{n!}{r!(n-r)!} + \frac{n!}{(r+1)!(n-r-1)!} \\
&= \frac{n!}{r!(n-r)!} \cdot \frac{(r+1)}{(r+1)} + \frac{n!}{(r+1)!(n-r-1)!} \cdot \frac{(n-r)}{(n-r)} \\
&= \frac{n!(r+1)}{(r+1)!(n-r)!} + \frac{n!(n-r)}{(r+1)!(n-r)!} \\
&= \frac{n!(r+1+n-r)}{(r+1)!(n-r)!} \\
&= \frac{n!(n+1)}{(r+1)!(n-r)!} \\
&= \frac{(n+1)!}{(r+1)!(n-r)!}.
\end{aligned}$$

Portanto, é válida a identidade binomial. □

O Lema 3.2, trata-se de uma relação entre números primos e os coeficientes binomiais.

Lema 3.2. *$p > 1$ é primo, se, e somente se p divide $\binom{p}{q}$ para todo $1 \leq q < p$.*

Demonstração. ($\Rightarrow$) Se $p > 1$ é primo, então, p divide $\binom{p}{q}$ para todo $1 \leq q < p$.

Desenvolvendo o coeficiente binomial, tem-se:

$$\begin{aligned}
&\binom{p}{q} = \frac{p!}{q!(p-q)!} \\
\iff &\binom{p}{q} q!(p-q)! = p! \\
\iff &\binom{p}{q} q!(p-q)! = p(p-1)!.
\end{aligned}$$

Nota-se que, da igualdade anterior, p divide $\binom{p}{q} q!(p-q)!$, como p é primo isso implica que, p tem que dividir $\binom{p}{q}$ ou $q!$ ou $(p-q)!$.

Como p é primo e $q < p$, constata-se que p não divide nenhum dos termos do produto $q \cdot (q-1) \cdots 3 \cdot 2 \cdot 1$ e portanto p também não divide $q!$. De forma análoga, p não divide $(p-q)!$, o que leva a concluir que, p divide $\binom{p}{q}$.

($\Leftarrow$) A prova será feita por contraposição. Será mostrado que, se p é composto, então, p não divide $\binom{p}{q}$ para algum $1 \leq q < p$.

Inicialmente, supõe-se que p é composto. Assim, para um divisor primo q de p, será mostrado que, $p \nmid \binom{p}{q}$. Desta forma, ao considerar $p = q^l m$ com $l \geq 1$ e $mdc(q, m) = 1$. Deste modo, da divisão de $\binom{p}{q}$ por p, chega-se a:

$$\frac{\binom{p}{q}}{p} = \frac{p!}{q!(p-q)!} \cdot \frac{1}{p} = \frac{p \cdot (p-1) \cdots (p-q+1) \cdot (p-q)!}{q!(p-q)!} \cdot \frac{1}{p} = \frac{(p-1) \cdots (p-q+1)}{q!}.$$

Se existe $N \in \mathbb{N}$, tal que,

$$\frac{(p-1) \cdots (p-q+1)}{q!} = N,$$

ou seja,

$$(p-1) \cdot (p-2) \cdot (p-3) \cdots (p-q+1) = Nq(q-1)!,$$

isso implica que o produto

$$(p-1) \cdot (p-2) \cdot (p-3) \cdots (p-q+1),$$

teria que ser congruente a 0 módulo q e, portanto, q deveria dividir algum dos termos do produto. Entretanto,

$$\begin{aligned} p-1 &= q^l m - 1 \equiv -1 \equiv q-1 \bmod q; \\ p-2 &= q^l m - 2 \equiv -2 \equiv q-2 \bmod q; \\ p-3 &= q^l m - 3 \equiv -3 \equiv q-3 \bmod q; \\ &\vdots \\ p-q+1 &= q^l m - q + 1 \equiv 1 \bmod q; \end{aligned}$$

ou seja, q não divide nenhum dos termos do produto, assim, não existe nenhum $N \in \mathbb{N}$ que satisfaça a igualdade

$$\frac{\binom{p}{q}}{p} = \frac{(p-1) \cdots (p-q+1)}{q!} = N.$$

Portanto, p não divide $\binom{p}{q}$. □

O Exemplo 3.2 auxilia no entendimento do método por contradição utilizado no Lema 3.2.

Exemplo 3.2. *Será considerado* $p = 12$ *e* $q = 2$.

Da divisão de $\binom{12}{2}$ *por* 12*, obtém-se:*

$$\frac{\binom{12}{2}}{12} = \frac{12!}{2!(12-2)!} \cdot \frac{1}{12} = \frac{12 \cdot 11 \cdot 10!}{2!10!} \cdot \frac{1}{12} = \frac{11}{2!} = \frac{11}{2}.$$

Logo, 12 *não divide* $\binom{12}{2}$.

O Exemplo 3.3 ilustra a primeira parte do Lema 3.2, ou seja, se $p > 1$ é primo, então, p divide $\binom{p}{q}$ para todo $1 \leq q < p$.

Exemplo 3.3. *Ao considerar* $p = 7$ *e* $1 \leq q < 7$*, estabelece-se que* 7 *divide* $\binom{7}{q}$*. Segue que,*

$$\binom{7}{1} = \frac{7!}{1!6!} = 7 \cdot 1; \qquad \binom{7}{2} = \frac{7!}{2!5!} = 7 \cdot 3;$$
$$\binom{7}{3} = \frac{7!}{3!4!} = 7 \cdot 5; \qquad \binom{7}{4} = \frac{7!}{4!3!} = 7 \cdot 5;$$
$$\binom{7}{5} = \frac{7!}{5!2!} = 7 \cdot 3; \qquad \binom{7}{6} = \frac{7!}{6!1!} = 7 \cdot 1.$$

O Teorema 3.1 que será demonstrado a seguir, trata-se de uma extensão do Lema 3.2 para primos gêmeos.

Teorema 3.1. *Seja* $m > 3$ *e* $m+2$ *dois números ímpares consecutivos. Então, ambos são primos, se, e somente se, o produto* $m \cdot (m+2)$ *divide cada um dos coeficientes binomiais,*

$$\binom{m+2}{3}, \binom{m+2}{4}, \binom{m+2}{5}, ..., \binom{m+2}{m-1}. \tag{3.1}$$

Demonstração. ($\Rightarrow$) Se m e $m+2$ são primos, então, $m \cdot (m+2)$ divide, cada um dos coeficientes binomiais de (3.1).

Suponha que m e $m+2$ sejam primos. Assim, pelo Lema 3.2, $m+2$ divide cada um dos coeficientes binomiais de (3.1) e m divide cada um dos coeficientes binomiais $\binom{m}{r}$, com $1 \leq r \leq m-1$.

Isso implica que, se $3 \leq r \leq m-1$ então $m \left| \binom{m}{r-1} + \binom{m}{r-2} \right.$ e $m \left| \binom{m}{r} + \binom{m}{r-1} \right.$.

Usando a Relação de Stifel 3.1 tem-se que, $\binom{m}{r-1} + \binom{m}{r-2} = \binom{m+1}{r-1}$ e $\binom{m}{r} + \binom{m}{r-1} = \binom{m+1}{r}$, e assim pode-se estabelecer que, $m \left| \binom{m+1}{r-1} \right.$ e $m \left| \binom{m+1}{r} \right.$, para $3 \leq r \leq m-1$.

Sabendo que,

$m \left| \binom{m+1}{r} \right.$ e $m \left| \binom{m+1}{r-1} \right.$, então, $m \left| \binom{m+1}{r} + \binom{m+1}{r-1} \right.$ e novamente, pela Relação de Stifel (3.1), tem-se que, $m \left| \binom{m+2}{r} \right.$, com $3 \leq r \leq m-1$, pois, $\binom{m+1}{r} + \binom{m+1}{r-1} = \binom{m+2}{r}$.

Sendo assim, m, assim como $m+2$ dividem cada um dos coeficientes binomiais de (3.1).

Uma vez que, $mdc(m, m+2) = 1$, a Proposição 2.4 permite concluir que $m \cdot (m+2)$ divide todos os coeficientes binomiais de (3.1).

($\Leftarrow$) Se $m \cdot (m+2)$ divide cada um dos coeficientes binomiais de (3.1), então, m e $m+2$ são primos.

Suponha que $m \cdot (m+2)$ divide cada um dos coeficientes binomiais de (3.1), então, tanto m quanto $m+2$ também dividem estes coeficientes binomiais.

Observe também que,

$\binom{m+2}{2} = \frac{(m+2)!}{2!m!} = \frac{(m+2)\cdot(m+1)\cdot m!}{2!m!} = \frac{(m+2)\cdot(m+1)}{2}$, como $m+2$ é ímpar, tem-se que, $m+1$ é par, e consequentemente $m+2$ também divide $\binom{m+2}{2}$. Como adicionalmente por hipótese, $m+2$ divide todos os coeficientes binomiais de (3.1), logo, o Lema 3.2 mostra que $m+2$ deve ser primo.

Agora, será mostrado que m também é primo. De fato, é possível estabelecer que,

$\binom{m+1}{2} = \frac{(m+1)!}{2!(m-1)!} = \frac{(m+1)\cdot m\cdot(m-1)!}{2!(m-1)!} = \frac{(m+1)\cdot m}{2}$ e

$\binom{m}{2} = \frac{m!}{2!(m-2)!} = \frac{m\cdot(m-1)\cdot(m-2)!}{2!(m-2)!} = \frac{m\cdot(m-1)}{2}$.

Como m é ímpar, ambos $\binom{m+1}{2}$ e $\binom{m}{2}$ são múltiplos de m.

Por hipótese, m divide $\binom{m+2}{3}, \binom{m+2}{4}, \binom{m+2}{5}, ..., \binom{m+2}{m-1}$.

Assim, aplicando a Relação de Stifel $\binom{m+1}{r+1} = \binom{m+2}{r+1} - \binom{m+1}{r}$, sucessivas

vezes tem-se:

$$m\left|\binom{m+2}{3}\right. \text{ e } m\left|\binom{m+1}{2}\right. \Longrightarrow m\left|\binom{m+1}{3}\right. = \binom{m+2}{3} - \binom{m+1}{2};$$

$$m\left|\binom{m+1}{3}\right. \text{ e } m\left|\binom{m}{2}\right. \Longrightarrow m\left|\binom{m}{3}\right. = \binom{m+1}{3} - \binom{m}{2};$$

$$m\left|\binom{m+1}{3}\right. \text{ e } m\left|\binom{m+2}{4}\right. \Longrightarrow m\left|\binom{m+1}{4}\right. = \binom{m+2}{4} - \binom{m+1}{3};$$

$$m\left|\binom{m}{3}\right. \text{ e } m\left|\binom{m+1}{4}\right. \Longrightarrow m\left|\binom{m}{4}\right. = \binom{m+1}{4} - \binom{m}{3};$$

$$m\left|\binom{m+1}{4}\right. \text{ e } m\left|\binom{m+2}{5}\right. \Longrightarrow m\left|\binom{m+1}{5}\right. = \binom{m+2}{5} - \binom{m+1}{4};$$

$$m\left|\binom{m+1}{5}\right. \text{ e } m\left|\binom{m}{4}\right. \Longrightarrow m\left|\binom{m}{5}\right. = \binom{m+1}{5} - \binom{m}{4}.$$

Continuando este processo é possível concluir que, m divide $\binom{m+1}{r}$ com $3 \leq r \leq m-1$, e m divide $\binom{m}{r}$ com $3 \leq r \leq m-1$. Mais uma vez, o Lema 3.2 mostra que m tem que ser um primo. Isso prova o teorema.

□

Para ilustrar a demonstração, destacam-se três exemplos referentes ao Teorema 3.1. O Exemplo 3.4 mostra o processo principal utilizado na demonstração, o Exemplo 3.5 evidencia a validade do resultado e o Exemplo 3.6 mostra uma situação em que não se satisfazem as condições do Teorema.

Exemplo 3.4. *A Relação de Stifel (Lema 3.1) será aplicada para mostrar que, se 11 divide* $\binom{13}{r}$*, então, 11 divide* $\binom{12}{r}$*, e também divide* $\binom{11}{r}$*, com* $3 \leq r \leq 10$*.*

Observe que, 11 divide $\binom{12}{2} = 66 = 11 \cdot 6$ *e* $\binom{11}{2} = 55 = 11 \cdot 5$*. Ademais, por hipótese 11 divide* $\binom{13}{r}$ *com* $3 \leq r \leq 10$*. Assim sendo, pode-se aplicar a Relação de Stifel (Lema 3.1) sucessivas vezes para todos os coeficientes binomiais do enunciado de modo análogo ao processo utilizado no Teorema 3.1.*

Assim sendo, ao considerar, $m = 11$ *obtém-se a Tabela 3.1:*

Tabela 3.1 – Processo principal utilizado na demonstração do Teorema 3.1

m	r	$\binom{m+1}{r+1} = \binom{m+2}{r+1} - \binom{m+1}{r}$	$\binom{m}{r+1} = \binom{m+1}{r+1} - \binom{m}{r}$
11	2	$\binom{12}{3} = \binom{13}{3} - \binom{12}{2}$	$\binom{11}{3} = \binom{12}{3} - \binom{11}{2}$
11	3	$\binom{12}{4} = \binom{13}{4} - \binom{12}{3}$	$\binom{11}{4} = \binom{12}{4} - \binom{11}{3}$
11	4	$\binom{12}{5} = \binom{13}{5} - \binom{12}{4}$	$\binom{11}{5} = \binom{12}{5} - \binom{11}{4}$
11	5	$\binom{12}{6} = \binom{13}{6} - \binom{12}{5}$	$\binom{11}{6} = \binom{12}{6} - \binom{11}{5}$
11	6	$\binom{12}{7} = \binom{13}{7} - \binom{12}{6}$	$\binom{11}{7} = \binom{12}{7} - \binom{11}{6}$
11	7	$\binom{12}{8} = \binom{13}{8} - \binom{12}{7}$	$\binom{11}{8} = \binom{12}{8} - \binom{11}{7}$
11	8	$\binom{12}{9} = \binom{13}{9} - \binom{12}{8}$	$\binom{11}{9} = \binom{12}{9} - \binom{11}{8}$
11	9	$\binom{12}{10} = \binom{13}{10} - \binom{12}{9}$	$\binom{11}{10} = \binom{12}{10} - \binom{11}{9}$

Fonte: O autor.

Para entendimento da Tabela 3.1 basta observar que, na coluna da esquerda utiliza-se o fato de 11 *dividir todos os coeficientes binomiais da hipótese (em vermelho) e emprega também o coeficiente binomial provado na linha acima (em azul).*

Na coluna da direita opera-se com o coeficiente binomial obtido na coluna da esquerda (em laranja) juntamente ao coeficiente binomial determinado na linha acima (em roxo).

E assim, conclui-se que, 11 divide $\binom{12}{r}$*, e também divide* $\binom{11}{r}$*, com* $3 \leq r \leq 10$.

Exemplo 3.5. *Observe que* $m = 11$ *satisfaz o Teorema 3.1, isto é, o produto de primos gêmeos* $11.13 = 143$ *divide,* $\binom{13}{r}$*, com* $3 \leq r \leq 10$.

De cada um dos coeficientes binomiais, pode-se determinar:

$$\binom{13}{3} = \frac{13!}{3!10!} = 286 = 2 \cdot 143; \qquad \binom{13}{4} = \frac{13!}{4!9!} = 715 = 5 \cdot 143;$$

$$\binom{13}{5} = \frac{13!}{5!8!} = 1287 = 9 \cdot 143; \qquad \binom{13}{6} = \frac{13!}{6!7!} = 1716 = 12 \cdot 143;$$

$$\binom{13}{7} = \frac{13!}{7!6!} = 1716 = 12 \cdot 143; \qquad \binom{13}{8} = \frac{13!}{8!5!} = 1287 = 9 \cdot 143;$$

$$\binom{13}{9} = \frac{13!}{9!4!} = 715 = 5 \cdot 143; \qquad \binom{13}{10} = \frac{13!}{10!3!} = 286 = 2 \cdot 143.$$

Logo, 143 divide cada um dos coeficientes binomiais.

Exemplo 3.6. *Verifique que quando considera-se* $m = 7$ *o Teorema. 3.1 não é satisfeito.*

De fato, desenvolvendo cada um dos coeficientes binomiais correspondentes, chega-se a:

$$\binom{9}{3} = \frac{9!}{3!6!} = 84 = 1 \cdot 63 + 21; \qquad \binom{9}{4} = \frac{9!}{4!5!} = 126 = 2 \cdot 63;$$
$$\binom{9}{5} = \frac{9!}{5!4!} = 126 = 2 \cdot 63; \qquad \binom{9}{6} = \frac{9!}{6!3!} = 84 = 1 \cdot 63 + 21.$$

Note que, $\binom{9}{4} = \binom{9}{5}$ *são divisíveis por* $7 \cdot 9 = 63$*, contudo,* $\binom{9}{3} = \binom{9}{6}$ *não são.*

No Exemplo 3.5 constatou-se que 143 divide $\binom{13}{r}$, com $3 \leq r \leq 10$, ou seja, divide todos os termos da primeira linha no Triângulo de Pascal (Figura 3.1). No Exemplo 3.7 poderá se comprovar que 143 também divide todos os coeficientes binomiais das demais linhas no mesmo Triângulo de Pascal (Figura 3.1). Trata-se de uma ilustração do Teorema 3.2.

Exemplo 3.7. *Perceba que* $11 \cdot 13 = 143$ *divide cada um dos coeficientes binomiais no triângulo de Pascal expresso na Figura 3.1.*

Desenvolvendo todos os coeficientes binomiais pode-se obter, na linha 1:

$$\binom{13}{3} = \binom{13}{10} = 286 = 143 \cdot 2; \qquad \binom{13}{4} = \binom{13}{9} = 715 = 143 \cdot 5;$$
$$\binom{13}{5} = \binom{13}{8} = 1287 = 143 \cdot 9; \qquad \binom{13}{6} = \binom{13}{7} = 1716 = 143 \cdot 12.$$

Na linha 2:

$$\binom{14}{4} = \binom{14}{10} = 1001 = 143 \cdot 7; \qquad \binom{14}{5} = \binom{14}{9} = 2002 = 143 \cdot 14;$$
$$\binom{14}{6} = \binom{14}{8} = 3003 = 143 \cdot 21; \qquad \binom{14}{7} = 1001 = 143 \cdot 7.$$

Na linha 3:

$$\binom{15}{5} = \binom{15}{10} = 3003 = 143 \cdot 21; \qquad \binom{15}{6} = \binom{15}{9} = 5005 = 143 \cdot 35;$$
$$\binom{15}{7} = \binom{15}{8} = 6435 = 143 \cdot 45.$$

Na linha 4:

$$\binom{16}{6} = \binom{16}{10} = 8008 = 143 \cdot 56; \qquad \binom{16}{7} = \binom{16}{9} = 11440 = 143 \cdot 80;$$
$$\binom{16}{8} = 12870 = 143 \cdot 90.$$

Na linha 5:

$$\binom{17}{7} = \binom{17}{10} = 19448 = 143 \cdot 136; \qquad \binom{17}{8} = \binom{17}{9} = 24310 = 143 \cdot 170.$$

Na linha 6:

$$\binom{18}{8} = \binom{18}{10} = 43758 = 143 \cdot 306; \qquad \binom{18}{9} = 48620 = 143 \cdot 340;$$

Na linha 7:

$$\binom{19}{9} = \binom{19}{10} = 92378 = 143 \cdot 646;$$

Na última linha :

$$\binom{20}{10} = 184756 = 143 \cdot 1292.$$

Figura 3.1 – Triângulo de Pascal com linhas divisíveis por $11 \cdot 13$

$$\begin{array}{c}
\binom{13}{3}\binom{13}{4}\binom{13}{5}\binom{13}{6}\binom{13}{7}\binom{13}{8}\binom{13}{9}\binom{13}{10} \\
\binom{14}{4}\binom{14}{5}\binom{14}{6}\binom{14}{7}\binom{14}{8}\binom{14}{9}\binom{14}{10} \\
\binom{15}{5}\binom{15}{6}\binom{15}{7}\binom{15}{8}\binom{15}{9}\binom{15}{10} \\
\binom{16}{6}\binom{16}{7}\binom{16}{8}\binom{16}{9}\binom{16}{10} \\
\binom{17}{7}\binom{17}{8}\binom{17}{9}\binom{17}{10} \\
\binom{18}{8}\binom{18}{9}\binom{18}{10} \\
\binom{19}{9}\binom{19}{10} \\
\binom{20}{10}
\end{array}$$

Fonte: O autor.

Portanto, 143 divide todos os coeficientes binomiais.

Teorema 3.2. *Seja $m > 3$ um número ímpar, então, m e $m+2$ são primos gêmeos, se, e somente se, o produto $m \cdot (m+2)$ divide cada um dos coeficientes binomiais na Figura 3.2.*

Figura 3.2 – Triângulo de Pascal com linhas divisíveis por $m \cdot (m+2)$

$$\binom{m+2}{3}\binom{m+2}{4}\binom{m+2}{5}\binom{m+2}{6}\cdots\binom{m+2}{m-4}\binom{m+2}{m-3}\binom{m+2}{m-2}\binom{m+2}{m-1}$$

$$\binom{m+3}{4}\binom{m+3}{5}\binom{m+3}{6}\cdots\binom{m+3}{m-3}\binom{m+3}{m-2}\binom{m+3}{m-1}$$

$$\binom{m+4}{5}\binom{m+4}{6}\cdots\binom{m+4}{m-2}\binom{m+4}{m-1}$$

$$\begin{array}{ccc} . & \cdots & . \\ . & & . \\ . & \cdots & . \end{array}$$

$$\binom{2m-4}{m-3}\binom{2m-4}{m-2}\binom{2m-4}{m-3}$$

$$\binom{2m-3}{m-2}\binom{2m-3}{m-1}$$

$$\binom{2m-2}{m-1}.$$

Fonte: O autor.

Demonstração. ($\Rightarrow$) Se $m > 3$ e $m+2$ são primos, então, $m \cdot (m+2)$ divide cada um dos coeficientes binomiais do Triângulo de Pascal (Figura 3.2).

Se, m e $m+2$ são primos, então, pelo Teorema 3.1, $m \cdot (m+2)$ divide cada um dos coeficientes binomiais da primeira linha .

Pela Relação de Stifel 3.1, $\binom{m+3}{r} = \binom{m+2}{r-1} + \binom{m+2}{r}$, tem-se que na segunda linha, cada termo é igual a soma de dois termos adjacentes na primeira linha. Na terceira linha, cada termo é igual a soma de dois termos adjacentes na segunda linha. E este processo se mantém até esgotar todas as linhas do triângulo.

Como $m \cdot (m+2)$ divide os termos da primeira linha, então $m \cdot (m+2)$ divide os termos da segunda linha. Procedendo de forma análoga, conclui-se que $m \cdot (m+2)$ divide todos os termos do triângulo expresso na Figura 3.2.

($\Leftarrow$) Se $m \cdot (m+2)$ divide cada um dos coeficientes binomiais do triângulo de Pascal (Figura 3.2), então, m e $m+2$ são primos.

Se $m \cdot (m+2)$ divide cada um dos coeficientes binomiais do Triângulo de Pascal (Figura 3.2), é evidente que, $m \cdot (m+2)$ divide cada um dos coeficientes binomiais da primeira linha do triângulo, ou seja, $m \cdot (m+2)$ divide $\binom{m+2}{3}, \binom{m+2}{4}, ..., \binom{m+2}{m-1}$, mas, se isso ocorre, então, pelo Teorema 3.1, m e $m+2$ são primos. □

Os Lemas 3.1 e 3.2 foram essenciais nas demonstrações dos Teoremas 3.1 e 3.2. Tais teoremas apresentados nesta seção são mais belos pela demonstração que propriamente pelo uso nas ilustrações numéricas, haja vista a utilização do conceito de fatorial impossibilitar a geração de primos gêmeos grandes, ainda que tenha se utilizado recursos computacionais. Ademais, a Tabela 3.1 e os Exemplos 3.1, 3.7 e 3.2 são fundamentais para compreensão das demonstrações destes resultados.

4 NÚMEROS PRIMOS GÊMEOS E O PEQUENO TEOREMA DE FERMAT

Nesta seção será apresentado o Pequeno Teorema de Fermat (Teorema 4.1) um resultado que permite verificar se um número é ou não primo. Será considerado também, uma generalização para números primos gêmeos com base no trabalho de Rezgui (2017). A demonstração do Teorema 4.1 está embasada em alguns dos resultados apresentados em Oliveira (2019).

Teorema 4.1. *(Pequeno Teorema de Fermat). Seja p um número primo e $a \in \mathbb{Z}$, então, $a^p \equiv a$ mod p.*

Demonstração. Serão considerados dois casos: quando a é múltiplo de p e quando a não é múltiplo de p.

$1)$ Se a é múltiplo de p, então, $a \equiv 0$ mod p, logo, $a^p \equiv 0$ mod p e $a^p \equiv a$ mod p.

$2)$ Considera-se que a não é múltiplo de p. Assim, para mostrar que $a^p \equiv a$ mod p é suficiente mostrar que $a^{p-1} \equiv 1$ mod p, pois o $mdc(a, p) = 1$.

Para demonstrar que $a^{p-1} \equiv 1$ mod p considere o conjunto $A = \{a, 2a, 3a, ..., (p-1)a\}$.

$a)$ Será provado por absurdo que não há múltiplos de p em A.

Se existe, $k \in \{1, 2, 3, 4, ..., p-1\}$ tal que, $ka \equiv 0$ mod p, isso implica que $p \mid ka$. Note que, k é menor que p e assim, o $mdc(p, k) = 1$, então, $p \nmid k$, logo, $p \mid a$. Mas isso é absurdo pois por hipótese $p \nmid a$.

$b)$ Será utilizado novamente a redução ao absurdo para provar que em A não há dois números congruentes módulo p.

Se existe k_1 e $k_2 \in \{1, 2, 3, 4, ..., p-1\}$, com $k_1 \neq k_2$, então, $ak_1 \equiv ak_2$ mod p. Como, $mdc(a, p) = 1$ pela Proposição 2.2, tem-se que, $k_1 \equiv k_2$ mod p, logo, $k_1 = k_2$. Mas isso é absurdo, pois por hipótese $k_1 \neq k_2$.

$c)$ Dos resultados obtidos em a) e b) segue que, cada um dos números de $A = \{a, 2a, 3a, ..., (p-1)a\}$ é congruente com algum dos elementos em $\{1, 2, 3, ..., p-1\}$ módulo p, desta forma estabelece-se que,

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \text{ mod } p$$
$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \text{ mod } p.$$

Visto que $mdc((p-1)!, p) = 1$ pode-se utilizar a Proposição 2.2, para concluir que, $a^{p-1} \equiv 1$ mod p. □

Exemplo 4.1. *A recíproca do Teorema 4.1 não é válida, ou seja, existem a e p tais que* $a^p \equiv a$ *mod* p*, mas* p *não é primo. Considere por exemplo* $a = 2$ *e* $p = 341$.

De fato, note que, $2^{10} = 1024 = 3 \cdot 341 + 1$*, ou seja,* $2^{10} \equiv 1$ *mod* 341*, assim, elevando ambos os membros da congruência a trigésima quarta potência, chega-se a ,*

$$(2^{10})^{34} \equiv 1^{34} \textit{ mod } 341$$
$$2^{340} \equiv 1 \textit{ mod } 341.$$

Multiplicando ambos os membros da congruência por 2*, conclui-se que,*

$$2^{340} \cdot 2 \equiv 1 \cdot 2 \textit{ mod } 341$$
$$2^{341} \equiv 2 \textit{ mod } 341.$$

Contudo, $341 = 11 \cdot 31$ *e, portanto é composto.*

Para relacionar números primos gêmeos e o Pequeno Teorema de Fermat, é preciso considerar o Teorema 4.2, que mostra que para todo primo $q < p$ a recíproca é válida.

Teorema 4.2. *Um número* p *é primo se, e somente se, para todos os primos* q *menores que* p*, tem-se que* $q^{p-1} \equiv 1$ *mod* p*.*

Demonstração. ($\Rightarrow$) Para todo primo $q < p$, se p é primo, então, p não divide q, logo, a partir do Pequeno Teorema de Fermat (Teorema 4.1), obtém-se que $q^{p-1} \equiv 1 \bmod p$.

($\Leftarrow$) Se $q^{p-1} \equiv 1 \bmod p$, para todo q primo menor que p então, p é primo.

Note que, se q é um primo menor que p, então, p é maior que 2. Se $q^{p-1} \equiv 1 \bmod p$, então, $q \cdot q^{p-2} \equiv 1 \bmod p$. Pela Proposição 2.5, tem-se que tal congruência é verdadeira se, e somente se, $mdc(q, p) = 1$.

Assim, constata-se que p e q não tem divisores comuns maiores do que 1, para todo q primo menor que p. Logo, p é primo, pois se p fosse composto, tomando q como um dos fatores primos de p então, p e q teriam divisores comuns maiores do que 1. □

Na Tabela 4.1 será considerado $p = 51$ e todos os primos q menores que p, isto é, $q \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47\}$.

Tabela 4.1 – Ilustração do Teorema 4.2

$q < p$	$q^{p-1} \equiv 1 \bmod p$
$2 < 51$	$2^{51-1} \equiv 4 \bmod 51$
$3 < 51$	$3^{51-1} \equiv 9 \bmod 51$
$5 < 51$	$5^{51-1} \equiv 25 \bmod 51$
$7 < 51$	$7^{51-1} \equiv 49 \bmod 51$
$11 < 51$	$11^{51-1} \equiv 19 \bmod 51$
$13 < 51$	$13^{51-1} \equiv 16 \bmod 51$
$17 < 51$	$17^{51-1} \equiv 34 \bmod 51$
$19 < 51$	$19^{51-1} \equiv 4 \bmod 51$
$23 < 51$	$23^{51-1} \equiv 19 \bmod 51$
$29 < 51$	$29^{51-1} \equiv 25 \bmod 51$
$31 < 51$	$31^{51-1} \equiv 43 \bmod 51$
$37 < 51$	$37^{51-1} \equiv 43 \bmod 51$
$41 < 51$	$41^{51-1} \equiv 49 \bmod 51$
$43 < 51$	$43^{51-1} \equiv 13 \bmod 51$
$47 < 51$	$47^{51-1} \equiv 16 \bmod 51$

Fonte: O autor.

Ao determinar no MAXIMA os restos das congruências expressas na Tabela 4.1, constata-se que a congruência $q^{p-1} \equiv 1 \bmod p$ não é satisfeita para nenhum primo q menor que $p = 51$. Logo, o Teorema 4.2 mostra que 51 não é primo. Observe que, se uma congruência não fosse satisfeita já mostraria que $p = 51$ não é primo.

Uma relação muito útil entre os números primos gêmeos e o Pequeno Teorema de Fermat (Teorema 4.1) será apresentada a seguir conforme Aebi e Cairns (2008) e Rezgui (2017).

Teorema 4.3. *Se os números naturais $p, p+2$ são primos, então $2^{p+2} \equiv 3p + 8$ mod $p \cdot (p+2)$.*

Demonstração. Se p é primo, então, aplicando o Pequeno Teorema de Fermat 4.1 tem-se que,

$$2^p \equiv 2 \bmod p.$$

Desta forma, multiplicando ambos os membros da congruência por 2^2 e somando $3p$ em ambos os membros a congruência, obtém-se,

$$(2^p \cdot 2^2) + 3p \equiv (2 \cdot 2^2) + 3p \bmod p$$
$$2^{p+2} + 3p \equiv 8 + 3p \bmod p.$$

Sabendo que, $3p \equiv 0 \bmod p$, determina-se que,

$$2^{p+2} \equiv 8 + 3p \bmod p. \tag{4.1}$$

Se $p+2$ é primo, de forma análoga, e utilizando o Pequeno Teorema de Fermat (Teorema 4.1) tem-se que,

$$2^{p+2} \equiv 2 \bmod (p+2).$$

Assim, somando $3(p+2)$ em ambos os membros chega-se a

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

Como $3(p+2) \equiv 0 \bmod (p+2)$, tem- se, $2^{p+2} \equiv 2 + 3p + 6 \bmod (p+2)$ o que implica que,

$$2^{p+2} \equiv 8 + 3p \bmod (p+2). \tag{4.2}$$

O $mdc(p, p+2) = 1$, assim, pode-se agrupar as congruências (4.1) e (4.2), e usar a Proposição 2.4 para concluir que,

$$2^{p+2} \equiv 3p + 8 \bmod p \cdot (p+2).$$

□

O próximo exemplo ilustra o Teorema 4.3.

Exemplo 4.2. *Considere os primos $p = 11$ e $p + 2 = 13$. Assim, pode-se estabelecer que,*

$$\begin{aligned} 2^{11+2} = 2^{13} = 8192 &\equiv 41 \textit{ mod } 11 \cdot 13 \\ &\equiv 41 \textit{ mod } 143. \end{aligned}$$

Além disso,

$$\begin{aligned} 3 \cdot 11 + 8 \equiv 33 + 8 &\textit{ mod } 11 \cdot 13 \\ &\equiv 41 \textit{ mod } 143. \end{aligned}$$

Portanto a congruência é satisfeita.

Exemplo 4.3. *Será mostrado que a recíproca do Teorema 4.3 não é verdadeira, ou seja, serão encontrados valores $p, p+2$ que satisfazem a congruência, mas que não são primos gêmeos. Encontrar tais números, não é uma tarefa simples. Para encontrar tais valores, foi determinado no MAXIMA os restos r_1 da congruência $2^{p+2} \equiv r_1$ mod $p(p+2)$, os restos r_2 da congruência $3p + 8 \equiv r_2$ mod $p(p+2)$, a decomposição em fatores primos de n e também de $n+2$ tomando diferentes valores entre 3 e 600, conforme a Figura 4.1. Após isso, analisou-se os restos r_1 e r_2 de ambas as congruências e também a fatoração dos valores de n e $n+2$, desta forma ao comparar quais restos eram iguais, desconsiderou-se aqueles correspondentes a primos gêmeos conhecidos, como o par $(569, 571)$.*

Figura 4.1 – Restos da divisão de 2^{n+2} e $3n+8$ por $n(n+2)$ e decomposição de $n, n+2$ feitos no MAXIMA

```
(%i1) for n: 3 thru 600 do print
      (n, n+2, mod(2^n·2^2, n·(n+2)),
mod(3·n+8,n·(n+2)),  factor(n),  factor(n+2));

558  560  111136  1682  2 3^2 31  2^4 5 7
559  561  48248  1685  13 43  3 11 17

560  562  286624  1688  2^4 5 7  2 281
561  563  1691  1691  3 11 17  563

562  564  121408  1694  2 281  2^2 3 47
563  565  311347  1697  563  5 113

564  566  166408  1700  2^2 3 47  2 283

565  567  105218  1703  5 113  3^4 7

566  568  253584  1706  2 283  2^3 71

567  569  44384  1709  3^4 7  569

568  570  35104  1712  2^3 71  2 3 5 19
569  571  1715  1715  569  571

570  572  42376  1718  2 3 5 19  2^2 11 13
done
```

Fonte: O autor.

Assim, para $p = 561$ *e* $p+2 = 563$ *constata-se que,*

$$\begin{aligned} 2^{561+2} = 2^{563} &\equiv 1691 \ \textit{mod}\ 561 \cdot 563 \\ &\equiv 1691 \ \textit{mod}\ 315843 \end{aligned}$$

assim como,

$$\begin{aligned} 3 \cdot 561 + 8 &\equiv 1691 \ \textit{mod}\ 561 \cdot 563 \\ &\equiv 1691 \ \textit{mod}\ 315843. \end{aligned}$$

Perceba que 561 *satisfaz a congruência* $2^{p+2} \equiv 3p+8$ *mod* $p(p+2)$. *Contudo,* 561 *não é primo já que,* $561 = 3 \cdot 11 \cdot 17$ *conforme a sua decomposição expressa na Figura 4.1.*

Os Teoremas 4.4 e 4.5 podem ser demonstrados de modo análogo ao Teorema 4.3, como será visto adiante.

Teorema 4.4. *Se os números* p *e* $p+2$ *são primos, então,* $3^{p+1} \equiv 4p+9$ *mod* $p \cdot (p+2)$.

Demonstração. Se p é primo, então, aplicando o Pequeno Teorema de Fermat (Teorema 4.1) tem-se:

$$3^p \equiv 3 \bmod p.$$

Desse modo, multiplicando por 3 e somando $4p$ em ambos os membros da congruência , obtém-se,

$$(3^p \cdot 3) + 4p \equiv (3 \cdot 3) + 4p \bmod p$$
$$3^{p+1} + 4p \equiv 9 + 4p \bmod p.$$

Considerando que $4p \equiv 0 \bmod p$, determina-se que,

$$3^{p+1} \equiv 9 + 4p \bmod p. \tag{4.3}$$

Como p e $p+2$ são primos, então $(p+2) \geq 5$. Pode-se utilizar o Pequeno Teorema de Fermat (Teorema4.1) para obter,

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

Deste modo, somando $4(p+2)$ em ambos os membros chega-se a

$$3^{p+1} + 4(p+2) \equiv 1 + 4(p+2) \bmod (p+2).$$

Sabendo que, $4(p+2) \equiv 0 \bmod (p+2)$, tem- se, $3^{p+1} \equiv 1 + 4p + 8 \bmod (p+2)$ o que implica que,

$$3^{p+1} \equiv 9 + 4p \bmod (p+2). \tag{4.4}$$

Como $mdc(p, p+2) = 1$ pode-se utilizar a Proposição 2.4 para combinar as congruências (4.3) e (4.4), e concluir que,

$$3^{p+1} \equiv 4p + 9 \bmod p \cdot (p+2).$$

□

Exemplo 4.4. *Considere os primos $p = 5$ e $p + 2 = 7$ para ilustrar o Teorema 4.4 .*

Desta forma, tem-se que,

$$3^{5+1} = 3^6 = 729 \equiv 29 \textit{ mod } 5 \cdot 7$$
$$\equiv 29 \textit{ mod } 35$$

tal qual,

$$4 \cdot 5 + 9 \equiv 20 + 9 \textit{ mod } 5 \cdot 7$$
$$\equiv 29 \textit{ mod } 35.$$

Portanto a congruência $3^{p+1} \equiv 4p + 9$ mod $p \cdot (p+2)$ é satisfeita.

Exemplo 4.5. *A recíproca do Teorema 4.4 é inválida. De modo análogo ao utilizado no Exemplo 3.2, usando MAXIMA foi determinado que* $p = 89$ *e* $p + 2 = 91$ *satisfazem:*

$$\begin{aligned} 3^{89+1} = 3^{90} &\equiv 365 \textit{ mod } 89 \cdot 91 \\ &\equiv 365 \textit{ mod } 8099 \end{aligned}$$

e,

$$\begin{aligned} 4 \cdot 89 + 9 &\equiv 356 + 9 \textit{ mod } 89 \cdot 91 \\ &\equiv 365 \textit{ mod } 8099. \end{aligned}$$

Logo a congruência $3^{p+1} \equiv 4p + 9$ *mod* $p \cdot (p + 2)$ *é satisfeita, no entanto,* $91 = 13 \cdot 7$ *e, portanto é composto.*

Teorema 4.5. *Se* p *e* $p + 2$ *são primos, então,* $5^{p+2} \equiv 60p + 125$ *mod* $p \cdot (p + 2)$.

Demonstração. Se p é primo, então, aplicando o Pequeno Teorema de Fermat (Teorema 4.1) tem-se que,

$$5^p \equiv 5 \bmod p.$$

Desse modo, multiplicando por 5^2 e somando $60p$ em ambos os membros da congruência, obtém-se,

$$\begin{aligned} 5^p \cdot 5^2 + 60p &\equiv (5 \cdot 5^2) + 60p \bmod p \\ 5^{p+2} + 60p &\equiv 125 + 60p \bmod p. \end{aligned}$$

Como $60p \equiv 0 \bmod p$, determina-se que,

$$5^{p+2} \equiv 125 + 60p \bmod p. \tag{4.5}$$

Se $p + 2$ é primo, de forma análoga, utilizando o Pequeno Teorema de Fermat (Teorema 4.1) tem-se que,

$$5^{p+2} \equiv 5 \bmod (p + 2).$$

Desse modo, somando $60(p + 2)$ em ambos os membros chega-se a

$$5^{p+2} + 60(p + 2) \equiv 5 + 60(p + 2) \bmod (p + 2)$$

e como $60(p + 2) \equiv 0 \bmod (p + 2)$, tem- se, $5^{p+2} \equiv 5 + 60p + 120 \bmod (p + 2)$ o que implica que,

$$5^{p+2} \equiv 60p + 125 \bmod (p + 2). \tag{4.6}$$

Como $mdc(p, p+2) = 1$ pode-se usar a Proposição 2.4 para combinar as congruências (4.5) e (4.6) e concluir que,

$$5^{p+2} \equiv 60p + 125 \bmod p \cdot (p+2).$$

□

Exemplo 4.6. *Ao estabelecer os primos $p = 17$ e $p + 2 = 19$ verifica-se que as condições do Teorema 4.5 são atendidas.*

Assim, tem-se que,

$$\begin{aligned} 5^{17+2} = 5^{19} = 19073486328125 &\equiv 176 \textit{ mod } 17 \cdot 19 \\ &\equiv 176 \textit{ mod } 323. \end{aligned}$$

e,

$$\begin{aligned} 60 \cdot 17 + 125 &\equiv 1020 + 125 \textit{ mod } 17 \cdot 19 \\ &\equiv 1145 \textit{ mod } 323 \\ &\equiv 176 \textit{ mod } 323. \end{aligned}$$

Portanto a congruência $5^{p+2} \equiv 60p + 125$ mod $p \cdot (p+2)$ é satisfeita.

Exemplo 4.7. *A recíproca do Teorema 4.5 não é válida. Desta forma, de modo análogo ao utilizado nos Exemplos 3.2 e 3.4 usando o MAXIMA foi estabelecido $p = 125$ e $p + 2 = 127$, que satisfazem:*

$$\begin{aligned} 5^{125+2} = 5^{127} &\equiv 7625 \textit{ mod } 125 \cdot 127 \\ &\equiv 7625 \textit{ mod } 15875 \end{aligned}$$

e,

$$\begin{aligned} 60 \cdot 125 + 125 &\equiv 7500 + 125 \textit{ mod } 125 \cdot 127 \\ &\equiv 7625 \textit{ mod } 15875. \end{aligned}$$

Logo a congruência $5^{p+2} \equiv 60p + 125$ mod $p \cdot (p+2)$ é satisfeita, entretanto, $125 = 5^3$ e, portanto é composto.

O Teorema 4.6 que será demonstrado a seguir é um resultado mais forte do que os Teoremas 4.3, 4.4 e 4.5. Trata-se de uma congruência que utiliza o Pequeno Teorema de Fermat (Teorema 4.1) e permite um certo tipo de recíproca, que é o Teorema 4.7.

Teorema 4.6. *Para todo primo $q < p$, se p e $p+2$ são primos, então,*

$$2q^{p+1} \equiv p(q^2-1) + 2q^2 \textit{ mod } p(p+2).$$

Demonstração. Se p é primo, então, aplicando o Pequeno Teorema de Fermat (Teorema 4.1), tem-se,

$$q^p \equiv q \bmod p,$$

assim, multiplicando por $2q$ em ambos os membros da congruência, obtém-se, $2q^{p+1} \equiv 2q^2 \bmod p$ e, somando $p(q^2-1)$ em ambos os membros da congruência, estabelece-se que, $2q^{p+1} + p(q^2-1) \equiv 2q^2 + p(q^2-1) \bmod p$.

Sabe-se que, $p(q^2-1) \equiv 0 \bmod p$, logo,

$$2q^{p+1} \equiv 2q^2 + p(q^2-1) \bmod p. \tag{4.7}$$

Analogamente, se $p+2$ é primo e q é um primo menor que p, então, $q < p+2$, assim, aplicando o Pequeno Teorema de Fermat 4.1, tem-se,

$$q^{p+1} \equiv 1 \bmod p+2$$

desta forma, multiplicando por 2 em ambos os membros da congruência, obtém-se, $2q^{p+1} \equiv 2 \bmod p+2$ e, somando $(q^2-1)\cdot(p+2)$ em ambos os membros da congruência, determina-se que,

$$2q^{p+1} + (q^2-1)\cdot(p+2) \equiv 2 + (q^2-1)\cdot(p+2) \bmod p+2.$$

Sabe-se que, $(q^2-1)\cdot(p+2) \equiv 0 \bmod p+2$, logo,

$$2q^{p+1} \equiv 2 + q^2p + 2q^2 - p - 2 \equiv 2q^2 + p(q^2-1) \bmod p+2. \tag{4.8}$$

Como $mdc(p, p+2) = 1$ podemos utilizar a Proposição 2.4 para combinar as congruências (4.7) e (4.8), e concluir que, $2q^{p+1} \equiv p(q^2-1) + 2q^2 \bmod p(p+2)$. □

Na Tabela 4.2 será considerado o primo $p = 41$ e todos os primos q menores que 31, isto é, $q \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37\}$. Ao determinar no MAXIMA os restos das congruências apresentadas na Tabela 4.2, constata-se que a congruência $2q^{p+1} \equiv p(q^2-1) + 2q^2 \bmod p(p+2)$ é satisfeita para todos os primos menores que 41 mostrando a validade do Teorema 4.6.

Tabela 4.2 – Ilustração do Teorema 4.6

$q < p$	$2q^{p+1} \equiv r_1 \bmod p(p+2)$	$p(q^2-1)+2q^2 \equiv r_2 \bmod p(p+2)$
$2 < 41$	$2 \cdot 2^{41+1} \equiv 131 \bmod 41 \cdot 43$	$41(2^2-1)+2 \cdot 2^2 \equiv 131 \bmod 41 \cdot 43$
$3 < 41$	$2 \cdot 3^{41+1} \equiv 346 \bmod 41 \cdot 43$	$41(3^2-1)+2 \cdot 3^2 \equiv 346 \bmod 41 \cdot 43$
$5 < 41$	$2 \cdot 5^{41+1} \equiv 1034 \bmod 41 \cdot 43$	$41(5^2-1)+2 \cdot 5^2 \equiv 1034 \bmod 41 \cdot 43$
$7 < 41$	$2 \cdot 7^{41+1} \equiv 303 \bmod 41 \cdot 43$	$41(7^2-1)+2 \cdot 7^2 \equiv 303 \bmod 41 \cdot 43$
$11 < 41$	$2 \cdot 11^{41+1} \equiv 1636 \bmod 41 \cdot 43$	$41(11^2-1)+2 \cdot 11^2 \equiv 1636 \bmod 41 \cdot 43$
$13 < 41$	$2 \cdot 13^{41+1} \equiv 174 \bmod 41 \cdot 43$	$41(13^2-1)+2 \cdot 13^2 \equiv 174 \bmod 41 \cdot 43$
$17 < 41$	$2 \cdot 17^{41+1} \equiv 45 \bmod 41 \cdot 43$	$41(17^2-1)+2 \cdot 17^2 \equiv 45 \bmod 41 \cdot 43$
$19 < 41$	$2 \cdot 19^{41+1} \equiv 1378 \bmod 41 \cdot 43$	$41(19^2-1)+2 \cdot 19^2 \equiv 1378 \bmod 41 \cdot 43$
$23 < 41$	$2 \cdot 23^{41+1} \equiv 1550 \bmod 41 \cdot 43$	$41(23^2-1)+2 \cdot 23^2 \equiv 1550 \bmod 41 \cdot 43$
$29 < 41$	$2 \cdot 29^{41+1} \equiv 862 \bmod 41 \cdot 43$	$41(29^2-1)+2 \cdot 29^2 \equiv 862 \bmod 41 \cdot 43$
$31 < 41$	$2 \cdot 31^{41+1} \equiv 733 \bmod 41 \cdot 43$	$41(31^2-1)+2 \cdot 31^2 \equiv 733 \bmod 41 \cdot 43$
$37 < 41$	$2 \cdot 37^{41+1} \equiv 647 \bmod 41 \cdot 43$	$41(37^2-1)+2 \cdot 37^2 \equiv 647 \bmod 41 \cdot 43$

Fonte: O autor.

O Teorema 4.7 é quase uma recíproca do Teorema 4.6 com algumas condições acrescentadas.

Teorema 4.7. *Se p é primo ímpar e a congruência $2q^{p+1} \equiv p(q^2-1)+2q^2$ mod $p(p+2)$ é satisfeita para todo primo q menor que $p+2$, então, $p+2$ é primo.*

Demonstração. Da congruência $2q^{p+1} \equiv p(q^2-1)+2q^2 \bmod p(p+2)$ pode ser obtida a congruência

$$2q^{p+1} \equiv pq^2 - p + 2q^2 \bmod p+2,$$

ou seja, $2q^{p+1} \equiv q^2(p+2) - p \bmod p+2$ e como $q^2(p+2) \equiv 0 \bmod p+2$ obtém-se, $2q^{p+1} \equiv -p \bmod p+2$.

Perceba que, $-p = -1(p+2)+2$, e $-1(p+2) \equiv 0 \bmod p+2$ logo, $2q^{p+1} \equiv -1(p+2)+2 \bmod p+2$, isto é, $2q^{p+1} \equiv 2 \bmod p+2$.

Por hipótese $p+2$ também é ímpar, assim, $mdc(p+2,2) = 1$. Logo, pela Proposição 2.2 estabelece-se que,

$$q^{p+1} \equiv 1 \bmod p+2,$$

para todo primo q menor que $p+2$. Portanto, pelo Teorema 4.2 $p+2$ é primo. □

Na Tabela 4.3 será considerado o primo $p = 29$ e todos os primos q menores que $p+2 = 31$, isto é, $q \in \{2,3,5,7,11,13,17,19,23,29\}$.

Tabela 4.3 – Ilustração do Teorema 4.7

$q < p+2$	$2q^{p+1} \equiv r_1 \bmod p(p+2)$	$p(q^2-1)+2q^2 \equiv r_2 \bmod p(p+2)$
$2 < 31$	$2 \cdot 2^{29+1} \equiv 95 \bmod 29 \cdot 31$	$29(2^2-1)+2 \cdot 2^2 \equiv 95 \bmod 29 \cdot 31$
$3 < 31$	$2 \cdot 3^{29+1} \equiv 250 \bmod 29 \cdot 31$	$29(3^2-1)+2 \cdot 3^2 \equiv 250 \bmod 29 \cdot 31$
$5 < 31$	$2 \cdot 5^{29+1} \equiv 746 \bmod 29 \cdot 31$	$29(5^2-1)+2 \cdot 5^2 \equiv 746 \bmod 29 \cdot 31$
$7 < 31$	$2 \cdot 7^{29+1} \equiv 591 \bmod 29 \cdot 31$	$29(7^2-1)+2 \cdot 7^2 \equiv 591 \bmod 29 \cdot 31$
$11 < 31$	$2 \cdot 11^{29+1} \equiv 126 \bmod 29 \cdot 31$	$29(11^2-1)+2 \cdot 11^2 \equiv 126 \bmod 29 \cdot 31$
$13 < 31$	$2 \cdot 13^{29+1} \equiv 715 \bmod 29 \cdot 31$	$29(13^2-1)+2 \cdot 13^2 \equiv 715 \bmod 29 \cdot 31$
$17 < 31$	$2 \cdot 17^{29+1} \equiv 839 \bmod 29 \cdot 31$	$29(17^2-1)+2 \cdot 17^2 \equiv 839 \bmod 29 \cdot 31$
$19 < 31$	$2 \cdot 19^{29+1} \equiv 374 \bmod 29 \cdot 31$	$29(19^2-1)+2 \cdot 19^2 \equiv 374 \bmod 29 \cdot 31$
$23 < 31$	$2 \cdot 23^{29+1} \equiv 188 \bmod 29 \cdot 31$	$29(23^2-1)+2 \cdot 23^2 \equiv 188 \bmod 29 \cdot 31$
$29 < 31$	$2 \cdot 29^{29+1} \equiv 870 \bmod 29 \cdot 31$	$29(29^2-1)+2 \cdot 29^2 \equiv 870 \bmod 29 \cdot 31$

Fonte: O autor.

Ao determinar no MAXIMA os restos das congruências expressas na Tabela 4.3, constata-se que a congruência $2q^{p+1} \equiv p(q^2-1)+2q^2 \bmod p(p+2)$ é satisfeita para todos os primos menores que 31 mostrando a validade do Teorema 4.7.

5 SÉRIE DOS INVERSOS DOS PRIMOS GÊMEOS

Neste capítulo será apresentada a série dos inversos dos números primos gêmeos. Além disso, procura-se ilustrar numericamente e comparar o comportamento desta série, com a série dos inversos dos números naturais (série harmônica) e com a série dos inversos dos números primos.

Como foi discutido na introdução, a série dos inversos dos primos gêmeos é convergente para um valor finito aproximadamente $1,9021$ (Constante de Brun). O fato desta série ser convergente (Teorema 5.1) é o que instiga a estudá-la contrapondo-a com as outras séries, que são divergentes (Teoremas 5.2 e 5.3). A demonstração do Teorema 5.1 está fora do escopo do trabalho, todavia este resultado será ilustrado numericamente na Seção 5.1. A demonstração detalhada pode ser encontrada em Leveque (2014).

Teorema 5.1. *A soma dos recíprocos de todos os primos gêmeos converge para a constante de Brun, ou seja,*

$$\sum_{(p,p+2)\in\mathcal{P}_g} \frac{1}{p}+\frac{1}{p+2} = \left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\cdots = 1.9021605823...,$$

onde P_g é o conjunto de pares de primos gêmeos.

Antes de ilustrar a soma dos inversos dos primos gêmeos será considerado o comportamento das outras duas séries, a série harmônica e a série dos inversos dos primos. A demonstração do Teorema 5.2, está embasada em uma das provas apresentadas por Kifowit e Stamps (2006).

Teorema 5.2. *A série*

$$\sum_{k=1}^{\infty}\frac{1}{k} = 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}+\cdots$$

é divergente.

Demonstração. Note que:

$$\begin{aligned}
\frac{1}{3}+\frac{1}{4} &> \frac{1}{4}+\frac{1}{4} = \frac{1}{2};\\
\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8} &> \frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8} = \frac{1}{2};\\
\frac{1}{9}+\frac{1}{10}+\cdots+\frac{1}{15}+\frac{1}{16} &> \frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16} = \frac{1}{2}.\\
&\vdots
\end{aligned}$$

Assim, considerando, SH_{2^n} a soma parcial $1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots\frac{1}{2^n}$ da série harmônica tem-se:

$$
\begin{aligned}
SH_{2^0} &= 1 = 1+0\cdot\frac{1}{2};\\
SH_{2^1} &= 1+\frac{1}{2} = 1+1\cdot\frac{1}{2};\\
SH_{2^2} &= 1+\frac{1}{2}+\left(\frac{1}{3}+\frac{1}{4}\right) > 1+\frac{1}{2}+\frac{1}{2} = 1+2\cdot\frac{1}{2};\\
SH_{2^3} &= 1+\frac{1}{2}+\left(\frac{1}{3}+\frac{1}{4}\right)+\left(\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}\right) > 1+\frac{1}{2}+\frac{1}{2}+\frac{1}{2} = 1+3\cdot\frac{1}{2};\\
SH_{2^4} &= 1+\frac{1}{2}+\left(\frac{1}{3}+\frac{1}{4}\right)+\left(\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}\right)+\left(\frac{1}{9}+\frac{1}{10}+\cdots+\frac{1}{15}+\frac{1}{16}\right)\\
&\qquad > 1+\frac{1}{2}+\frac{1}{2}+\frac{1}{2}+\frac{1}{2} = 1+4\cdot\frac{1}{2};\\
&\vdots
\end{aligned}
$$

Generalizando é possível mostrar que,

$$SH_{2^n} > 1+n\cdot\frac{1}{2}.$$

Como as somas parciais SH_2^n são maiores que $1+n\cdot\frac{1}{2}$, concluímos que, a série é divergente, pois, dado qualquer número a direita, você consegue superá-lo com uma certa quantidade de termos da série harmônica. □

Após o estudo da série harmônica (Teorema 5.2), busca-se demonstrar a divergência da série dos inversos dos números primos (Teorema 5.3). A demonstração não é trivial, por tal razão, procurou-se apresentá-la com riqueza de detalhes. Esta bela demonstração está fundamentada em Angelidakis (2020).

Teorema 5.3. *Se $p_1, p_2, p_3, ...$ a sequência de números primos, então, a série*

$$\sum_{i=1}^{\infty}\frac{1}{p_i} = \frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+... \tag{5.1}$$

diverge.

Demonstração. Segue uma prova por contradição. Considere a sequência dos números primos em ordem crescente, isto é,

$$p_1 < p_2 < p_3 < ... < p_n < ...,$$

Supondo que a série (5.1) converge, então, pela definição formal de convergência existe um número natural k , tal que

$$\sum_{i=k+1}^{\infty}\frac{1}{p_i} < \frac{1}{2}. \tag{5.2}$$

A partir da constante k os números primos serão divididos em dois conjuntos:

Primos pequenos $= \{p_1, p_2, p_3, ..., p_{k-1}, p_k\}$ e *Primos grandes* $= \{p_{k+1}, p_{k+2}, p_{k+3}, ...\}$.

Considere também $N = 2^{2(k+1)}$. Ao analisar todos os números naturais de 1 a N, estes podem ser divididos em dois grupos:

$G =$ "números que são divisíveis por pelo menos um grande primo", e

$P =$ "números que são apenas divisíveis por pequenos primos".

Seja $N(g)$ o número de elementos de G e $N(p)$ o número de elementos de P. Note que, $N = N(g) + N(p)$.

A seguir, será estimado o valor de $N(p)$. Pelo Lema 2.1 tem-se que todo número natural n pode ser escrito como $n = a \cdot b^2$, com $a, b \in \mathbb{N}$ com a livre de quadrados ou $a = 1$.

Se $n \leq N$ e $n = a \cdot b^2$ é divisível apenas por pequenos primos, com $a, b \in \mathbb{N}$ e a livre de quadrados, isso significa que cada primo $p_1, \cdots, p_k$ ou aparece uma única vez na decomposição de fatores primos de a ou não aparece, ou seja, existem no máximo 2^k maneiras de formar a com os primos $p_1, ..., p_k$. Ademais, já que $n \leq N$ então, $b^2 < N$, logo $b < \sqrt{N}$ e assim, o número de formas em que pode ser escolhido b é menor que $\sqrt{N}$. Pelos comentários anteriores, o número de formas de escolher um elemento $n = a \cdot b^2$ divisível por pequenos primos, é menor que $2^k \cdot \sqrt{N}$. Logo,

$$\begin{aligned} N(p) &\leq 2^k \cdot \sqrt{N} \\ &\leq 2^k \cdot \sqrt{2^{2(k+1)}} \\ &\leq 2^k \cdot 2^{\frac{2k+2}{2}} \\ &\leq 2^k \cdot 2^{k+1} \\ &\leq 2^{2k+1} \\ &\leq 2^{2(k+1)} \cdot \frac{1}{2} = \frac{N}{2}. \end{aligned} \tag{5.3}$$

Por outro lado para estimar $N(g)$ deve-se considerar todos os números naturais de 1 a N que estão no conjunto G, ou seja, números que são divisíveis por pelo menos um grande primo. Ao considerar o conjunto G_{k+i} definido como o conjunto dos números que são divisíveis por p_{k+i}, tem-se que,

$$G \subseteq G_{k+1} \cup G_{k+2} \cup G_{k+3} \cup G_{k+4} \cup \cdots \cup G_{k+i} \cdots \tag{5.4}$$

Note que para qualquer número primo p, a quantidade de números naturais positivos menores ou iguais a N, que são múltiplos de p, é igual a $\left\lfloor \frac{N}{p} \right\rfloor$ que é menor que $\frac{N}{p}$.

Com isso, considerando $N(g_{k+i}) = |G_{k+i}|$ tem-se $N(g_{k+i}) = |G_{k+i}| \leq \dfrac{N}{p_{k+i}}$, e da expressão (5.4) obtém-se,

$$\begin{aligned} |G| &\leq |G_{k+1}| + |G_{k+2}| + |G_{k+3}| + |G_{k+4}| + \cdots + |G_{k+i}| + \cdots \\ N(g) &\leq \frac{N}{p_{k+1}} + \frac{N}{p_{k+2}} + \frac{N}{p_{k+3}} + \frac{N}{p_{k+4}} + ... \\ &\leq \sum_{i=k+1}^{\infty} \frac{N}{p_i} \\ &\leq N \cdot \sum_{i=k+1}^{\infty} \frac{1}{p_i}. \end{aligned}$$

Assim sendo, a partir da desigualdade (5.2) tem-se que,

$$N(g) < \frac{N}{2}. \tag{5.5}$$

Portanto, pode-se utilizar para $N(p)$ e $N(g)$ as estimativas superiores (5.3) e (5.5) para concluir que,

$$\begin{aligned} N(p) + N(g) &< \frac{N}{2} + \frac{N}{2} \\ &< \frac{2N}{2} \\ &< N, \end{aligned}$$

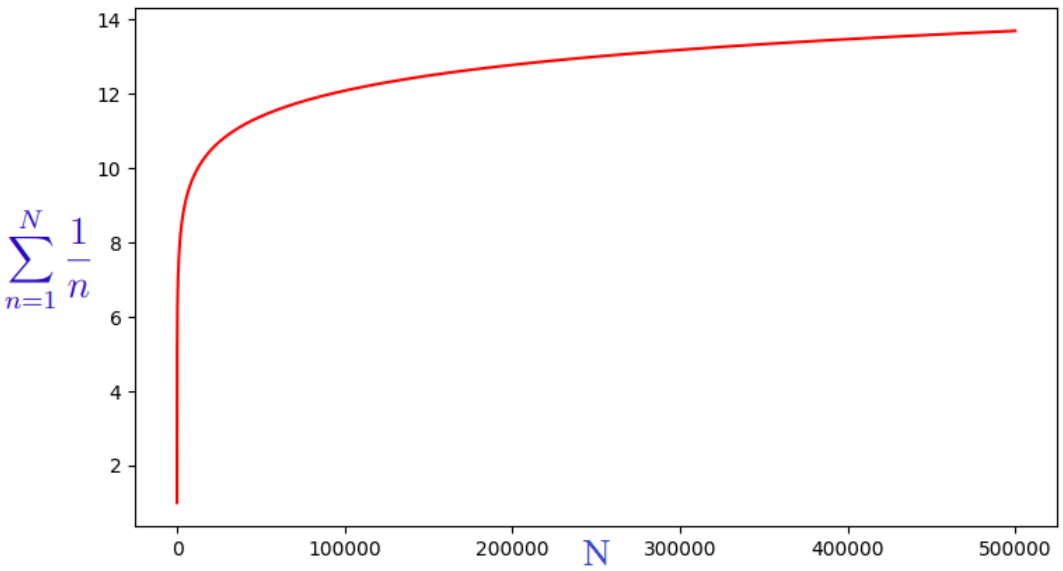
o que é absurdo pois $N(p) + N(g) = N$. □

5.1 ILUSTRAÇÕES NUMÉRICAS

No estudo da série harmônica é possível constatar que, a medida que o valor de n aumenta, a soma dos inversos dos naturais também aumenta. Entretanto, isto ocorre lentamente, conforme ilustra a Figura 5.1 programada em Python, usando o código descrito na Figura 5.2. Para se ter uma real ideia, a soma dos inversos dos primeiros 500 000 números naturais resulta em aproximadamente 13.7.

Por outro lado, ao explorar a série dos inversos dos primos, percebe-se que, ao passo que se acrescentam números primos, a soma dos inversos dos primos também cresce, conforme a Figura 5.3 programada em Python. Para se ter conhecimento, a soma dos inversos dos primos menores que 100 000 resulta em um valor aproximadamente igual a 2.5828.

Figura 5.1 – Somas Parciais da Série Harmônica



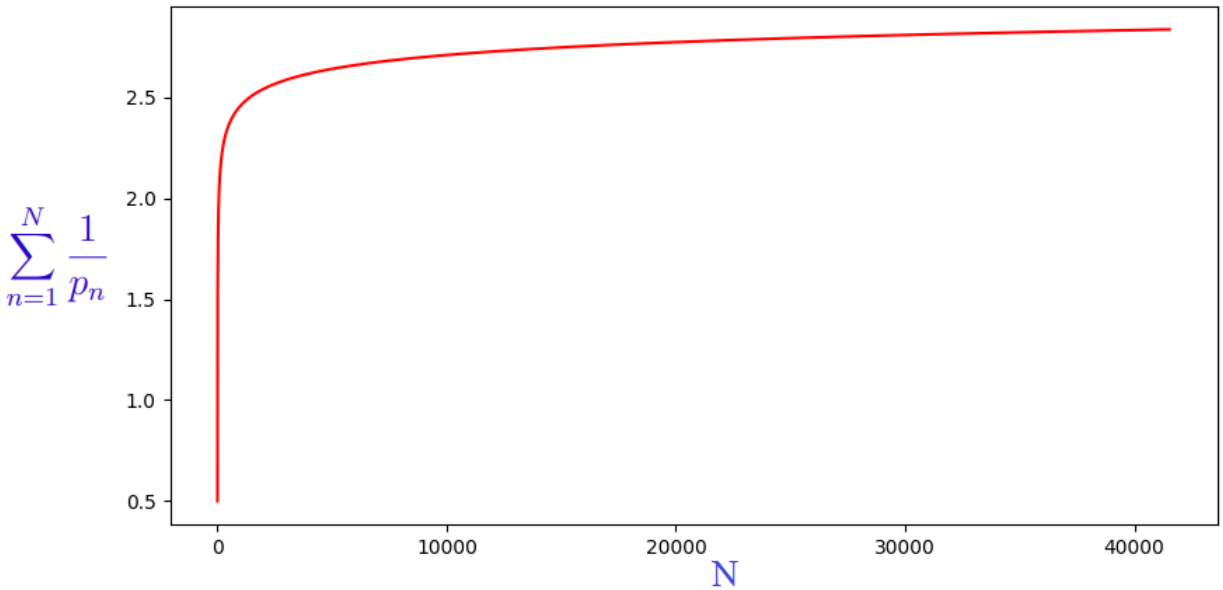
Fonte: O autor.

Figura 5.2 – Código para gerar a soma dos inversos dos naturais

```
soma = 0
for i in range(1,n):
    soma = soma + 1.0/i
```

Fonte: O autor.

Figura 5.3 – Somas Parciais da Série dos Inversos dos Primos



Fonte: O autor.

A soma ilustrada na Figura 5.3 foi obtida a partir do código fonte programado em Python descrito na Figura 5.4.

Figura 5.4 – Código para gerar a soma dos inversos dos primos

```
1 soma = 1.0/2 + 1.0/3
2 for p in range (1,n):
3     if (p)%(6)==1 or (p)%(6)==5:
4         if (2**(p-1))%(p)== 1:
5             if (math.factorial(p-1))%(p)==(p-1):
6                 soma=soma+1.0/p
```

Fonte: O autor.

Para compreender os métodos utilizados no programa é indispensável saber quais teoremas são empregados e em quais linhas estão inseridos.

Na linha 1 o comando soma = $1.0/2 + 1.0/3$, descreve a soma do inverso dos primeiros primos, ou seja, $\frac{1}{2}$ e $\frac{1}{3}$ isto é necessário, pois a caracterização dos primos da forma $6k+1$ ou $6k+5$ (Teorema 2.3) só é verdadeira para primos maiores que 3.

Na linha 2, mostra o intervalo entre 3 e n onde verifica-se se p satisfaz os teoremas citados.

Na linha 3 considera-se a caracterização dos primos da forma $6k+1$ ou $6k+5$, ou seja, Teorema 2.3.

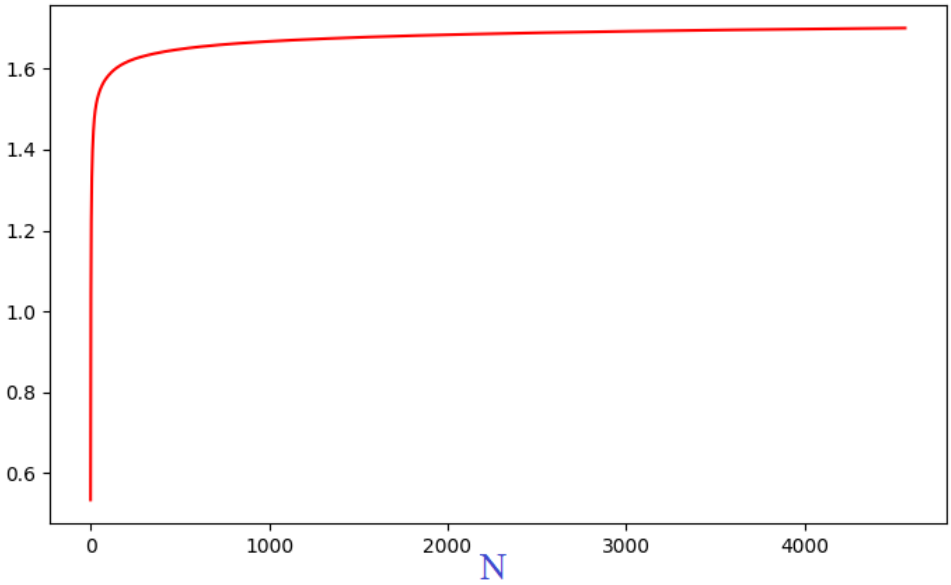
Na linha 4 utiliza-se o Teorema 4.1 ($a^{p-1} \equiv 1 \bmod p$) considerando $a = 2$, ou seja, $2^{p-1} \equiv 1 \bmod p$. Neste código poderia substituir a por qualquer valor inteiro maior que 2 que apresentaria o mesmo resultado.

Na linha 5 utiliza-se o Teorema 2.1 , isto é, $(p-1)! \equiv -1 \bmod p$. Justamente este teorema eliminará os contraexemplos gerados na linha 4.

Na linha 6, a variável soma armazena todas as somas que satisfazem todos os teoremas trabalhados.

A seguir será ilustrado numericamente o Teorema 5.1, conforme a Figura 5.5.

Figura 5.5 – Somas Parciais dos inversos dos primeiros N pares de primos Gêmeos



Fonte: O autor.

A soma ilustrada na Figura 5.5 foi obtida a partir do código fonte programado em Python que será apresentado a seguir.

Figura 5.6 – Código para gerar a soma dos inversos dos primos gêmeos

```
1 soma = 1.0/3 + 1.0/5
2 for p in range(1,n):
3    if p % 6 == 5:
4       if (2 ** (p + 2)) % (p * (p + 2)) == (3 * p + 8):
5          if (math.factorial(p - 1) * 4 + 4 + p) % (p * (p + 2)) == 0:
6           soma = soma + 1.0/p + 1.0/(p+2)
```

Fonte: O autor.

Para entender os procedimentos utilizados no código fonte explícito na Figura 5.6 é fundamental perceber quais teoremas são utilizados e em quais linhas estão inseridos.

Na linha 1 a variável soma = $1.0/3 + 1.0/5$, descreve a soma do primeiro par de inverso de gêmeos, ou seja, $\left(\frac{1}{3} + \frac{1}{5}\right)$, isto é necessário, pois a caracterização dos primos gêmeos da forma $6k - 1$ e $6k + 1$ (Teorema 2.3) só é válida para primos gêmeos maiores que 3, ou seja, o par$(3, 5)$ não satisfaz este teorema.

Na linha 2 se estabelece p no intervalo entre 1 e n.

Na linha 3 considera-se a caracterização dos primos gêmeos da forma $(6k - 1, 6k + 1)$, ou seja, Teorema 2.3.

Na linha 4 utiliza-se a congruência $2^{p+2} \equiv 3p+8 \mod p\cdot(p+2)$, assim dizendo Teorema 4.3 que relaciona o Pequeno Teorema de Fermat com os primos gêmeos. Este teorema poderia ser

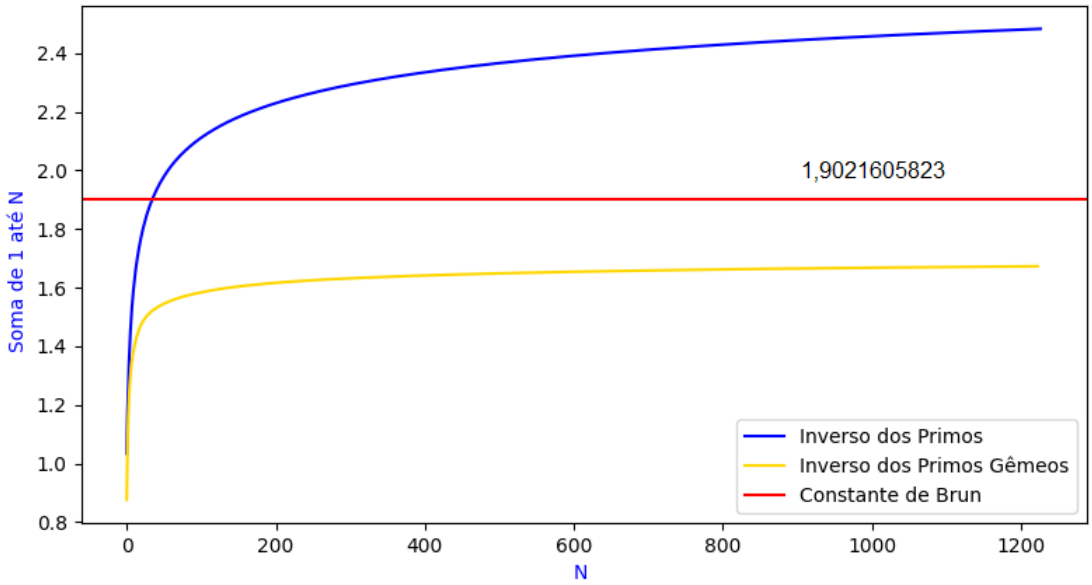
substituído pelos Teorema 4.4 e 4.5 e mesmo assim o código apresentaria resultado equivalente.

Na linha 5 utiliza-se o teorema que relaciona o Teorema de Wilson com os primos gêmeos, ou seja, Congruência de Clement (Teorema 2.2) expresso pela congruência

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

Após as investigações em relação as ilustrações das séries dos inversos dos primos e dos gêmeos, observa-se que nos gráficos das Figuras 5.3 e 5.5 as diferenças não ficam tão perceptíveis, assim, ao comparar ambas as séries em contraste com a constante de Brun, apresenta-se a seguinte representação gráfica feita também em Python.

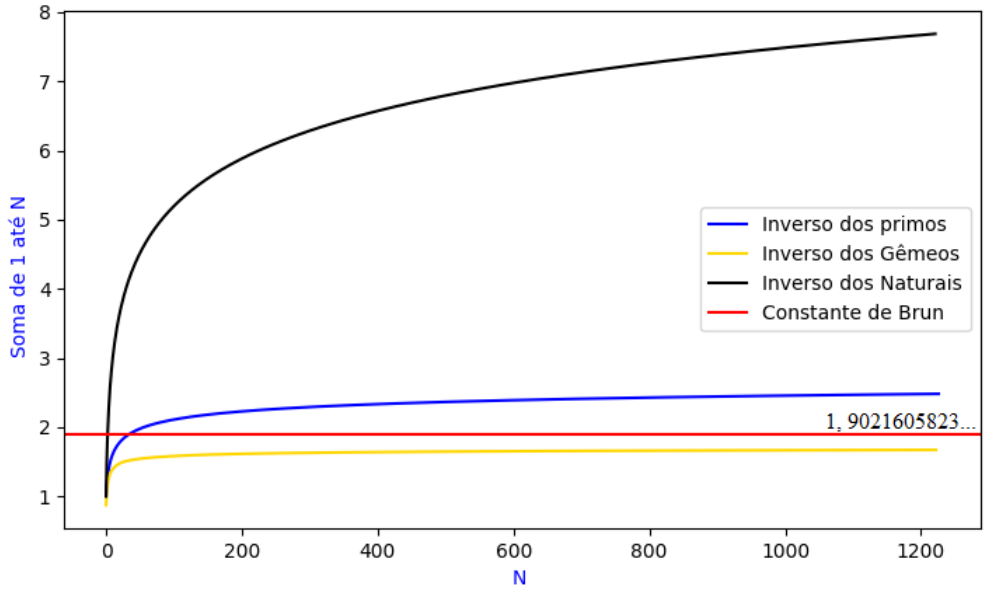
Figura 5.7 – Somas parciais até N-ésimo termo para a Série dos Inverso dos Primos e dos Primos Gêmeos



Fonte: O autor.

Nota-se na Figura 5.7 que a soma dos inversos dos primos ultrapassa rapidamente a constante de Brun, enquanto que a soma dos inversos dos primos gêmeos converge lentamente para a mesma. Além disso, ao representar as três séries, isto é, inverso dos primos, inversos dos primos gêmeos e a série harmônica, em comparação com a constante de Brun, tem-se a seguinte ilustração.

Figura 5.8 – Somas parciais para a Série dos Inversos dos Naturais, dos Primos e dos Primos Gêmeos



Fonte: O autor.

Percebe-se na Figura 5.8 que a soma dos inversos dos naturais e dos primos ultrapassam rapidamente a constante de Brun, enquanto que a soma dos inversos dos primos gêmeos converge de forma lenta.

É possível comprovar que a soma dos inversos dos 5 primeiros naturais já é suficiente para ultrapassar o valor da constante de Brun, isto é,

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}=2.08\overline{3}.$$

Além do que, a soma dos inversos dos 38 primeiros primos já é o bastante para exceder o valor da constante de Brun, ou seja,

$$\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{157}+\frac{1}{163}\approx 1.9056360330938213.$$

Em contrapartida, na abordagem dos primos gêmeos a soma dos 1224 primeiros pares não é suficiente para alcançar a constante de Brun, ou melhor,

$$\left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\cdots+\left(\frac{1}{99719}+\frac{1}{99721}\right)+\left(\frac{1}{99989}+\frac{1}{99991}\right)\approx 1.672799584827738.$$

Para atingir a 1.90 é necessário somar todos os primos gêmeos menores que 100 bilhões.

6 CONCLUSÕES

As propriedades de aritmética são bases dos conteúdos tanto do ensino fundamental quanto do ensino médio. Essas especificidades são fundamentais para o bom desenvolvimento do conhecimento matemático, especialmente quando auxiliado por um recurso computacional.

Este trabalho trouxe uma breve análise histórica acerca dos números primos gêmeos, salientando curiosidades desta admirável conjectura que ainda permanece sem solução.

Além disso, formalizou proposições de aritmética modular compreendidas durante o PROFMAT na disciplina de Aritmética, especialmente a Proposição 2.5 que denota a unicidade da solução da congruência $aX \equiv 1 \bmod m$ e a demonstração do Teorema 2.1 (Teorema de Wilson). A prova deste teorema serviu como alicerce para a Congruência de Clement (Teorema 2.2). Esta congruência foi um dos pontos chaves do estudo, tendo em vista, sua utilização na geração de primos gêmeos, bem como nas ilustrações apresentadas.

Outro ponto fundamental considerado, foi o Teorema 2.3 que abordou em sua validação propriedades de divisão euclidiana também transmitidas durante o PROFMAT, permitindo um filtro no programa para gerar primos gêmeos, uma vez que, só caracteriza os primos gêmeos na forma $6k - 1$ e $6k + 1$.

Ademais, esta pesquisa propiciou o estudo dos primos gêmeos e sua relação com os coeficientes binomiais. Nesta etapa, foi desenvolvida a Relação de Stifel (Lema 3.1), demonstração essencialmente algébrica também transmitida na disciplina de Matemática Discreta. Além disso, houve o estudo de caracterizações bem interessantes como os Teoremas 3.1 e 3.2. Nas demonstrações destes teoremas a Relação de Stifel (Lema 3.1), foi indispensável. Além do que o Teorema 3.2 é visualmente fantástico, visto que, o produto de primos gêmeos divide todas as linhas do triângulo de Pascal. Estes Teoremas não foram utilizados nas ilustrações numéricas das séries por incluírem números fatoriais em todos os termos, fato que tornou o programa lento e impossibilitou uma evolução neste sentido. Mesmo assim, a Tabela 3.1 foi uma ilustração de destaque por detalhar o processo principal utilizado na demonstração do Teorema 3.1 de forma clara e objetiva.

Ainda neste trabalho procurou-se destacar a demonstração do Teorema 4.1 (Pequeno Teorema de Fermat) , conceito tão abordado durante o PROFMAT e que funcionou como estrutura para as generalizações dos Teoremas 4.3, 4.4 e 4.5. Nesta mesma etapa, houve a apresentação de um resultado mais forte expresso nos Teoremas 4.6 e 4.7. No processo de provas destes teoremas, bem como nos contraexemplos explanados foi significativo o uso dos recursos computacionais assimilados no PROFMAT.

Outra perspectiva abordada neste trabalho foi o estudo das séries dos inversos dos números naturais, dos inversos dos números primos e dos inversos dos primos gêmeos. A

demonstração da divergência da série harmônica se apresentou de maneira simples, porém de fácil entendimento até mesmo aos que não são familiarizados com o estudo de séries. A prova da divergência da série dos inversos dos primos exibiu uma experiência bela e pouco comum, contudo, longe de ser trivial. Neste processo procurou-se esmiuçar os argumentos para tornar palpável a demonstração feita por contradição.

Além do mais, vale destacar que, as ilustrações explanadas neste trabalho apareceram através de tabelas desenvolvidas no próprio LATEX . Além do que, a utilização do MAXIMA foi substancial tanto para imprimir primos gêmeos, quanto para determinar contraexemplos como no Exemplo 4.3, onde mostrou-se que a recíproca do Teorema 4.3 não é válida para $p = 561$ e $p = 563$, conforme a decomposição em fatores primos expressos da Figura 4.1 .Tais execuções não seriam possíveis sem o fundamento básico da disciplina de Recursos Computacionais e das Orientações de TCC.

Outro conhecimento adquirido durante este estudo foi o aprendizado, ainda que de maneira básica, da programação por meio da linguagem Python. Este aprendizado permitiu gerar primos, primos gêmeos ou ilustrar as séries imprescindíveis neste processo. Até porque, um código fonte pronto, não mostra as falhas prévias, seja erros de sintaxe simples ou nome de variáveis incorretas para gerar uma simples soma de naturais.

Sob outra visão, constatou-se que, as referências em relação a Teoria dos Números em português são escassas. Fato este, que não impossibilitou a este trabalho de deixar algumas demonstrações aos estudantes futuros do PROFMAT.

Diante de todo estudo, espera-se dar continuidade ao aprendizado no estudo da Teoria dos Números, busca-se prosseguir no manuseio do LATEX nas aulas de ensino fundamental, ensino médio e técnico, objetiva-se utilizar o MAXIMA como facilitador nas atividades escolares, assim como empregar a linguagem de programação nas aulas de matemática e em projetos interdisciplinares. Por fim, melhorar a maneira de argumentar e justificar as propriedades matemáticas apresentadas aos alunos para assim, transmitir um pouco do conhecimento adquirido no PROFMAT para as salas de aula.

REFERÊNCIAS

AEBI, C.; CAIRNS, G. Catalan numbers, primes and twin primes. **Elemente der Mathematik(EM)**, n. 1, p. 11, 2008. 48

ANGELIDAKIS, H. **The Infinity of Primes**. 2020. Disponível em: <https://www.cantorsparadise.com/proofs-from-the-book-the-infinity-of-primes-4795fb4f01ac>. Acesso em: 10 abr. 2021. 58

CALDWELL, C. K. **The Top Twenty: Twin Primes**. 2020. Disponível em: <https://primes.utm.edu/top20/page.php?id=1#references>. Acesso em: 22 set. 2020. 13

HEFEZ, A. **Aritmética**. Rio de Janeiro, RJ, Brasil: SBM, 2016. v. 2. 284 p. 17, 18, 19

HOSCH, W. L. Twin prime conjecture. **Britannica Encyclopedia**, https://www.britannica.com/science/twin-prime-conjecture. Acesso em: 04 out. 2020, 2017. 11

KIFOWIT STEVEN J.; STAMPS, T. A. The harmonic series diverges again and again. **Prairie State College**, n. 1, p. 13, 2006. 57

LEVEQUE, W. J. **Fundamentals of Number Theory**. Estados Unidos da América: Courier Corporation, 2014. Edição Revisada. 288 p. 57

MORGADO, A. C.; CARVALHO, P. C. P. **Matemática Discreta**. Rio de Janeiro, RJ, Brasil: Sociedade Brasileira de Matemática, 2015. Edição 2. 282 p. 35

OLIVEIRA, F. E. **Sobre várias demonstrações do Pequeno Teorema de Fermat e as inter-relações entre as áreas da matemática**. 2019. Disponível em: <http://www.repositorio.ufc.br/bitstream/riufc/44231/1/2019_dis_fefoliveira.pdf>. Acesso em: 02 fev. 2021. 46

PANTOJA, P. Primos gêmeos e outras conjecturas. **Revista Escolar de la Olimpíada Iberoamericana de Matemática n.45**, n. 1, p. 11, 2012. 23

POLYMATH, D. **The "bounded gaps between primes" PolyMath Project - a retrospective**. 2014. Disponível em: <https://arxiv.org/abs/1409.8361>. Acesso em: 08 mar. 2021. 13

REZGUI, H. Conjecture of twin primes (still unsolved problem in number theory) an expository essay. **Surveys in Mathematics and its Applications**, v. 17, n. 12, p. 229–252, 2017. 46, 48

RIBENBOIM, P. **The Little Book of Bigger Primes**. Kingston, ON, Canadá: Springer, 2004. v. 2. 356 p. 11, 23

TALAPADTUR, P. The twin prime problem. **Resonance – Journal of Science Education.**, v. 7, n. 2, p. 86–90, 2002. 35

ZHANG, Y. Bounded gaps between primes. **Annals of Mathematics.**, v. 7, n. 179, p. 1121–1174, 2014. 12