Universidade Federal de São Paulo

Instituto de Ciência e Tecnologia

Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

Aspectos Aritméticos e Históricos de Certos Números Inteiros Especiais

Julio William Iotty Bulhões

Orientador: Prof. Dr. Robson da Silva

São José dos Campos
Julho, 2020

PROFMAT

Título: *Aspectos Aritméticos e Históricos de Certos Números Inteiros Especiais*
Dissertação apresentada ao Instituto de Ciência e Tecnologia da UNIFESP, campus São José dos Campos/SP, como parte dos requisitos exigidos para a obtenção do título de Mestre pelo Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT.

São José dos Campos
Julho, 2020

Iotty Bulhões, Julio william

Aspectos Aritméticos e Históricos de Certos Números Inteiros Especiais, Julio William Iotty Bulhões – São José dos Campos, 2020.

viii, 40f.

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

Arithmetic and Historical Aspects of Certain Special Numbers

1. Números Perfeitos. 2. Números de Mersenne. 3. Números de Fermat. 4. Números Amigáveis. 5. Número de Lucas.

UNIVERSIDADE FEDERAL DE SÃO PAULO

INSTITUTO DE CIÊNCIA E TECNOLOGIA

Mestrado Profissional em Matemática em Rede Nacional
PROFMAT

Chefe de departamento:

Prof. Dr. Eduardo Antonelli

Coordenador do Programa de Pós-Graduação:

Prof. Dr. Angelo Calil Bianchi

JULIO WILLIAM IOTTY BULHÕES

ASPECTOS ARITMÉTICOS E HISTÓRICOS DE CERTOS NÚMEROS INTEIROS ESPECIAIS

Presidente da banca: Prof. Dr. Robson da Silva

Banca examinadora:

Prof. Dr. Almir Cunha da Graça Neto

Profa. Dra. Elen Viviane Pereira Spreafico

Prof. Dr. Thadeu Alves Senne

Data da Defesa: 17 de Julho de 2020

"Se eu vi mais longe, foi por estar sobre ombros de gigantes."
Isaac Newton

AGRADECIMENTOS

Primeiro de tudo, gostaria de agradecer a Deus por me conceder a vida e a oportunidade de obter tal conhecimento. Gostaria, também de expressar minha imensa gratidão a todos os meus professores do curso por acrescentarem conhecimentos permanentes em minha vida e isso não tem preço. Agradeço ao meu orientador Professor Doutor Robson da Silva por todo tempo dedicado a me acompanhar durante as pesquisas além de seus ensinamentos. Agradeço aos meus pais por sempre me apoiarem e seus constantes dizeres sobre a importância dos estudos. Por fim, a minha família: minha esposa Carla e minhas filhas Marina e Isabel pelo apoio emocional e incondicional aos sacrifícios necessários para este fim.

RESUMO

Os estudos sobre números especiais não aparecem com frequência e não são muito aprofundados no Ensino Médio. Nessa dissertação serão apresentados os aspectos aritméticos de certos números especiais, incluindo os Números Perfeitos, Números de Mersenne, Números de Fermat, Números Amigáveis, Número de Lucas e os Números de Stirling. Adicionalmente, serão discutidos alguns aspectos históricos desses números. Objetivamos com esse estudo apresentar uma coleção de números especiais e demonstrações de algumas de suas propriedades mais importantes. As evoluções históricas desses números também serão apresentadas. Outros números serão abordados brevemente. Por fim, uma proposta didática para apresentar esses conceitos em duas formas distintas será apresentada.

Palavras-chave: 1. Números Perfeitos. 2. Números de Mersenne. 3. Números de Fermat. 4. Números Amigáveis. 5. Número de Lucas.

ABSTRACT

Special numbers do not appear frequently and are not very detailed in high school. In this work, the arithmetic aspects of certain special numbers are be presented, including the Perfect Numbers, Mersenne Numbers, Fermat Numbers, Friendly Numbers, Lucas Number, and Stirling Numbers. Additionally, historical aspects of these numbers are presented. With this study we aim to present a collection of special numbers and proofs of some of their most relevant properties. The historical developments of these numbers are also presented. Other numbers will be briefly covered. At the end, we present two different didactic schemes for teaching these concepts in class.

Keywords: 1. Perfect numbers. 2. Mersenne numbers. 3. Fermat numbers. 4. Amicable number. 5. Lucas number.

SUMÁRIO

INTRODUÇÃO 2

1 PRELIMINARES 3

2 NÚMEROS PERFEITOS 12

3 NÚMEROS DE MERSENNE 25

4 NÚMEROS DE FERMAT 28

5 NÚMEROS AMIGÁVEIS 31

6 NÚMEROS DE STIRLING 37

7 NÚMERO DE LUCAS 44

8 OUTROS NÚMEROS ESPECIAIS 50

9 PROPOSTA DIDÁTICA 53

10 CONCLUSÃO 58

REFERÊNCIAS BIBLIOGRÁFICAS 59

INTRODUÇÃO

Os números especiais representam uma importante parte da Teoria dos Números. Existem muitos tipos e cada um deles apresenta propriedades interessantes, algumas das quais serão aqui discutidas. Veremos alguns problemas que permanecem abertos até os dias de hoje, o que tem instigado matemáticos a expandir cada vez mais a fronteira da pesquisa nesta área.

Alguns números, como os perfeitos e os amigáveis, por exemplo, que serão objeto de estudo neste trabalho, iniciam-se basicamente na Grécia antiga e possuem conjecturas relacionadas à crenças e à religiosidade (Cap.1 de [1]). Como veremos, os números perfeitos têm uma importante ligação com os Números de Mersenne, o que tem incentivado as recentes descobertas de novos desses últimos números. A enorme quantidade de dígitos das descobertas recentes, que utilizam muitos recursos computacionais, indicam a dificuldade de se encontrar tais números. O Teste de Lucas-Lehmer será importante para determinar Números de Mersenne e consequentemente Números Perfeitos.

Veremos também que os Números de Fermat, mesmo sendo infinitos, ainda possuem um problema em aberto: decidir se existem ou não infinitos tais números que são primos. Mostraremos algumas propriedades, dentre elas a quantidade de dígitos desse tipo de número.

Apresentaremos também os Números de Stirling (Cap.2 de [28]). Pouco ou talvez não conhecido dos estudantes, possuem utilidade muito grande em partições de conjuntos. Veremos que eles se apresentam em dois tipos e sua relação com o Número de Bell.

A sequência de Fibonacci será de grande importância para introduzirmos o Número de Lucas. Veremos suas ligações e algumas propriedades. Dentre elas, podemos destacar sua relação com a proporção Áurea e poderemos encontrar um termo de sua sequência por meio dos índices de Fibonacci.

Com o objetivo de mostrar uma coleção de números especiais, definiremos outros números, como o curioso *Sexy Primes* [19], cujo nome estão relacionados ao fonema *six*, que tem relação à diferença entre primos.

Ao final, apresentaremos uma proposta didática para ser trabalhada com alunos do Ensino Básico. Tal proposta procura despertar nos estudantes a curiosidade e a vontade de solucionar problemas matemáticos cujos enunciados são simples. Com o intuito de tornar essa atividade didática mais completa e ao mesmo tempo acessível, desenvolvemos ferramentas (um blog e um perfil no Instagram) para reunir as informações sobre os números especiais aqui estudados. Essas ferramentas são apresentadas com maiores detalhes no Capítulo 9.

1

PRELIMINARES

Relembramos aqui alguns resultados elementares que serão muito úteis nos outros capítulos [3][28][29].

Teorema 1.1 (Soma dos n primeiros termos de uma progressão geométrica)**.** *Seja* $(a_1, a_2, \ldots, a_n, \ldots)$ *uma progressão geométrica com razão* $q \neq 1$*. Então a soma dos seus* n *primeiros termos é dada por:*

$$S_n = a_1 \cdot \frac{q^n - 1}{q - 1}$$

Demonstração. Seja

$$S_n = a_1 + a_2 + \cdots a_n.$$

Multiplicando por q a expressão S_n, obtemos:

$$\begin{aligned} S_n q &= q(a_1 + a_2 + \cdots + a_n) \\ &= qa_1 + qa_2 + \cdots + qa_n \\ &= qa_1 + qa_1 q + \cdots + qa_1 q^{n-1} \\ &= a_1(q + q^2 + \cdots + q^n). \end{aligned}$$

Segue que

$$qS_n - S_n = a_1(q + q^2 + \cdots + q^n) - a_1(1 + q + q^2 + \cdots + q^{n-1}).$$

Arrumando o segundo membro,

$$qS_n - S_n = a_1(q^n - 1).$$

Isolando S_n no primeiro membro, temos:

$$S_n = a_1 \frac{q^n - 1}{q - 1}.$$

□

Teorema 1.2 (Soma dos termos infinitos de uma progressão geométrica)**.** *Seja* $(a_1, a_2, \ldots, a_n, \ldots)$ *uma progressão geométrica com razão* $0 \leq q < 1$*. Então a soma dos seus termos é dada por*

$$S = \frac{a_1}{1 - q}.$$

Demonstração. Segue da fórmula do Teorema 1.1 que

$$S = \lim_{n\to\infty} a_1 \frac{q^n - 1}{q - 1} = \frac{a_1}{1 - q},$$

pois $0 \leq q < 1$, o que implica $q^n \to 0$ quando $n \to \infty$. □

Definição 1.3 (Divisibilidade)**.** *Dados dois números inteiros a e b, diremos que a divide b, escrevendo $a|b$, quando existir $c \in \mathbb{Z}$, tal que $b = ca$. Neste caso, diremos também que a é um divisor ou um fator de b ou, ainda, que b é um múltiplo de a ou que b é divisível por a. Caso contrário, escrevemos $a \nmid b$.*

Relembramos a seguir algumas das mais importantes propriedades de divisibilidade de inteiros, que serão muito úteis ao longo deste texto.

Proposição 1.4. *Se $a, b, c, d \in \mathbb{Z}$, $a|b$ e $c|d$ então $ac|bd$.*

Demonstração. Se $a|b$ e $c|d$ então $\exists f, g \in \mathbb{Z}$, tais que $b = fa$ e $d = gc$. Portanto, $bd = (fg)(ac)$, logo, $ac|bd$. □

Proposição 1.5. *Se $a, b, c \in \mathbb{Z}$ são tais que $a|b$ e $a|c$, então para todo $x, y \in \mathbb{Z}$*

$$a|(xb + yc).$$

Demonstração. Temos que $a|b$ e $a|c$. Isso implica que existem $f, g \in \mathbb{Z}$ tais que $b = fa$ e $c = ga$. Logo,

$$xb + yc = x(fa) + y(ga) = (xf + yg)a.$$

□

Proposição 1.6. *Sejam $a, b, c \in \mathbb{Z}$, tais que $a|(b \pm c)$. Então $a|b \iff a|c$.*

Demonstração. Suponha que $a|(b + c)$. Logo, existe $f \in \mathbb{Z}$ tal que $b + c = fa$. Também vamos supor que $a|b$, então existe $g \in \mathbb{Z}$ tal que $b = ga$. Juntando as igualdades, temos:

$$ga + c = fa,$$

de onde segue que $c = (f - g)a$, logo $a|c$. A implicação contrária é análoga. □

Proposição 1.7. *Se $a, b, c \in \mathbb{Z}$ são tais que $a|b$ e $a|c$, então para todo $x, y \in \mathbb{Z}$*

$$a|(xb + yc).$$

Demonstração. Se $a|b$ e $a|c$ isso implica que existem $f, g \in \mathbb{Z}$ tais que $b = fa$ e $c = ga$. Logo,

$$xb + yc = x(fa) + y(ga) = (xf + yg)a.$$

□

Teorema 1.8 (Divisão Euclidiana)**.** *Sejam a e b dois números inteiros com $b \neq 0$. Existem dois únicos números inteiros q e r tais que:*

$$a = bq + r,$$

com $0 \leq r < |b|$.

Demonstração. Considere o conjunto

$$A = \{x = a - by; y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\}).$$

Existência:
Tomando $n \in \mathbb{Z}$ suficientemente grande, temos que $n(-b) > -a$. Logo $a - nb > 0$, o que mostra que A é não vazio. O conjunto A é limitado inferiormente por 0. Logo, pelo Princípio da Boa Ordenação[1], temos que A possui um menor elemento $r = a - bq$. Sabemos que $r \geq 0$. Vamos mostrar que $r < |b|$. Suponhamos por absurdo que $r \geq |b|$. Portanto, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |b| + s$, logo $0 \leq s < r$. Mas isso contradiz o fato de r ser o menor elemento de A, pois $s = a - (q \pm 1)b \in A$, com $s < r$.
Unicidade:
Suponha que $a = bq + r = bq' + r'$, onde $q, q', r, r' \in \mathbb{Z}$, $0 \leq r < |b|$ e $0 \leq r' < |b|$. Assim, temos que $-|b| < -r \leq r' - r \leq r' < |b|$. Logo, $|r' - r| < |b|$. Por outro lado, $b(q - q') = r' - r$, o que implica que:

$$|b||q - q'| = |r' - r| < |b|,$$

o que só é possível se $q = q'$ e, consequentemente, $r = r'$. □

Definição 1.9 (Número Primo)**.** *Um número natural maior que* 1 *que só possui como divisores positivos* 1 *e ele próprio é chamado de número primo.*

Dados dois números primos p e q e um número inteiro m qualquer, decorrem da definição acima os seguintes fatos:

Proposição 1.10. *Se $p|q$, então $p = q$.*

Demonstração. De fato, como $p|q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Sendo p primo, tem-se que $p > 1$, o que acarreta $p = q$. □

Proposição 1.11. *Se $p \not| m$, então $(p, m) = 1$.*

Demonstração. De fato, se $(p, m) = c$, temos que $c|p$ e $c|m$. Portanto, $c = p$ ou $c = 1$. Mas $c \neq p$, pois $p \neq m$ e, consequentemente, $c = 1$. □

Definição 1.12 (Número composto)**.** *Um número maior que* 1 *e que não é primo será chamado de composto.*

[1] PBO: todo conjunto não-vazio de inteiros positivos possui um menor elemento

Portanto, se um número natural $n > 1$ é composto, existirá um divisor natural n_1 de n tal que $1 < n_1 < n$. Logo, existirá um número natural n_2 tal que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$.

Teorema 1.13 (Teorema Fundamental da Aritmética)**.** *Todo número natural maior que* 1 *ou é primo ou se escreve de modo único (desprezando-se a ordem de seus fatores) como um produto de número primos.*

Demonstração. Faremos a demonstração por indução. Para $n = 2$ temos um número primo. Consideremos válido para todo número natural menor que n. Vamos provar que o resultado é válido para n. Se n é primo, nada temos a demonstrar. Suponhamos então n composto. Logo, existem n_α e n_β tais que $n = n_\alpha \cdot n_\beta$, com $1 < n_\alpha < n$ e $1 < n_\beta < n$. Usando agora nossa hipótese de indução, então existem números primos $p_1, \cdots, p_r$ e $q_1, \cdots, q_s$ tais que $n = p_1 \cdots p_r q_1 \cdots q_s$, onde p_i e q_j são primos. Logo n é um produto de primos.

Provaremos agora a unicidade. Como $p_1 | q_1 \cdots q_s$, temos que $p_1 = q_j$ para algum j ao qual podemos supor que seja q_1 dentro de $q_1, \cdots, q_s$. Portanto:

$$p_2 \cdots p_r = q_2 \cdots q_s.$$

Como $p_2 \cdots p_r < n$, da hipótese de indução, temos que $r = s$ e os p_i e q_j são iguais aos pares. Portanto, segue a unicidade. □

Definição 1.14 (Máximo divisor comum)**.** *Sejam dois inteiros a e b, distintos ou não. Um número inteiro d será dito um divisor comum de a e b se $d|a$ e $d|b$. Se d é divisível por todo divisor comum de a e b será então o máximo divisor comum de a e b e será denotado por (a, b). Como o máximo divisor comum não depende da ordem então*

$$(a, b) = (b, a).$$

Definição 1.15. *Seja n um número natural. Denotemos por $\sigma(n)$ a soma de todos os seus divisores naturais.*

É comum, também definirmos essa função na forma:

$$\sigma(n) = \sum_{d|n} d,$$

onde d são todos os divisores positivos inteiros de n.

Proposição 1.16. *Seja $n \in \mathbb{N}$. Tem-se que $\sigma(n) = n + 1$ se, e somente se, n é um número primo.*

Demonstração. De fato, os únicos divisores naturais de n sendo primo é ele próprio e o 1, o que nos dá $\sigma(n) = n + 1$.

Como $n + 1 = \sigma(n)$, segue que $n > 1$ e que n e 1 são os únicos divisores de n. Portanto n é primo. □

Proposição 1.17. *Seja $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ a decomposição de n em fatores primos. Então,*

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{\alpha_r+1} - 1}{p_r - 1}.$$

Demonstração. Considere a igualdade:

$$(1 + p_1 + \cdots + p_1^{\alpha_1}) \cdots (1 + p_r + \cdots + p_r^{\alpha_r}) = \Sigma p_1^{\beta_1} \cdots p_r^{\beta_r},$$

onde o somatório do lado direito da igualdade é tomado sobre todas r-uplas $(\beta_1, \ldots, \beta_r)$ ao variar cada β_i no intervalo $0 \leq \beta_i \leq \alpha_i$, para $i = 0, \ldots, r$. Como tal somatório é a soma de todos os divisores de n, a fórmula para $\sigma(n)$ resulta aplicando a fórmula da soma de uma progressão geométrica a cada soma do lado esquerdo da igualdade acima. □

Definição 1.18 (Primo de Euler)**.** *Chamamos de Primo de Euler os números primos gerados pelo polinômio $P(n) = n^2 + n + 41$ com $n \in \mathbb{N} \cup \{0\}$.*

n	$P(n) = n^2 + n + 41$
0	$P(0) = 0^2 + 0 + 41 = 41$
1	$P(1) = 1^1 + 1 + 41 = 43$
2	$P(2) = 2^2 + 2 = 41 = 47$
3	$P(3) = 3^2 + 3 + 41 = 53$
$\cdots$	$\cdots$

Tabela 1: Primeiros Primos de Euler[30].

Teorema 1.19 (Função multiplicativa)**.** *A função $\sigma(n)$ é multiplicativa, isto é, se $(m, n) = 1$, então*

$$\sigma(mn) = \sigma(m)\sigma(n).$$

Demonstração. Consideremos m e n números inteiros relativamente primos. Pela definição, temos $\sigma(mn) = \sum_{d|mn} d$. Entretanto, uma vez que os números m e n são relativamente primos, cada divisor de mn pode ser escrito como produto de um divisor de n e um divisor de m. Assim, podemos escrever:

$$\sigma(mn) = \sum_{d|mn} d = \sum_{(d_1|m)(d_2|n)} d_1 d_2 = \sum_{d_1|m} \sum_{d_2|n} d_1 d_2 = \sum_{d_1|m} d_1 \cdot \sum_{d_2|n} d_2 = \sigma(m)\sigma(n).$$

Logo, σ é multiplicativa. □

Definição 1.20 (Deficiência de n [22])**.** *Seja $n \in \mathbb{N}$. A deficiência $D(n)$ é*

$$D(n) = 2n - \sigma(n).$$

Exemplo 1.21. *Alguns valores a deficiência de n são:*

- $D(1) = 2 \cdot 1 - 1 = 1$,
- $D(2) = 2 \cdot 2 - 3 = 1$,
- $D(4) = 2 \cdot 4 - 7 = 1$,
- $D(6) = 2 \cdot 6 - 12 = 0$,
- $D(10) = 2 \cdot 10 - 18 = 2$.

Definição 1.22 (Índice de Abundância [22])**.** *Definimos a função Índice de Abundância $I(n)$ com $n \in \mathbb{N}$ como*

$$I(n) = \frac{\sigma(n)}{n}.$$

Proposição 1.23. *Dada as Definições 1.20 e 1.22 temos a identidade $\frac{D(n)}{n} + I(n) = 2$.*

Demonstração. $\frac{D(n)}{n} + \frac{\sigma(n)}{n} = \frac{2n-\sigma(n)}{n} + \frac{\sigma(n)}{n} = \frac{2n}{n} = 2.$ □

Definição 1.24 (Aritmética dos restos)**.** *Seja m um número natural. Diremos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se*

$$a \equiv b \mod m.$$

Definição 1.25. *Quando a relação $a \equiv b \mod m$ for falsa, diremos que a e b são não congruentes, ou que são incongruentes módulo m. Então escrevemos $a \not\equiv b \mod m$.*

Exemplo 1.26. $15 \equiv 9 \pmod 2$*, já que ambos deixam resto* 1 *na divisão por* 2*.*

Proposição 1.27. *Suponha que $a, b, m \in \mathbb{Z}$, com $m > 1$. Tem-se que $a \equiv b \pmod m$ se, e somente se, $m|b - a$.*

Demonstração. Sejam $a = mq + r$, com $0 \leq r < m$ e $b = mq' + r'$, com $0 \leq r' < m$, as divisões euclidianas de a e b por m, respectivamente. Logo,

$$b - a = m(q' - q) + (r' - r).$$

Portanto, $a \equiv b \pmod m$ se, e somente se, $r = r'$, o que, em vista da igualdade acima, é equivalente a dizer que $m|b - a$ já que $|r - r'| < m$. □

Proposição 1.28. *Sejam $a, b, c, m \in \mathbb{Z}$ com $m > 1$. Temos que*

$$ac \equiv bc \pmod m \iff a \equiv b \pmod{\frac{m}{(c, m)}}$$

Demonstração. Como $\left(\frac{m}{(c,m)}, \frac{c}{(c,m)}\right) = 1$, temos que

$$ac \equiv bc \pmod{m} \iff m|(b-a)c \iff \frac{m}{(c,m)}|(b-a)\frac{c}{(c,m)}$$

$$\iff \frac{m}{(c,m)}|(b-a) \iff a \equiv b \pmod{\frac{m}{(c,m)}}.$$

□

Proposição 1.29. *Para todos $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m}$.*

Demonstração. Faremos a demonstração por indução. Para $n = 1$, temos

$$a \equiv b \pmod{m}.$$

Supomos o resultado verdadeiro para $n = k$. Provaremos para $n = k + 1$. Temos que

$$a^{k+1} - b^{k+1} = aa^k - ba^k + ba^k - bb^k = a^k(a-b) + b(a^k - b^k) \equiv 0 \pmod{m},$$

pois $a - b \equiv 0 \pmod{m}$, pelo caso base, e $a^k - b^k \equiv 0 \pmod{m}$ por hipótese de indução. Portanto $a^n \equiv b^n \pmod{m}$. □

Teorema 1.30 (Pequeno Teorema de Fermat)**.** *Se p é primo e $a \in \mathbb{Z}$, então*

$$a^p \equiv a \pmod{p}.$$

Além disso, se $p \nmid a$ então

$$a^{p-1} \equiv 1 \pmod{p}.$$

Demonstração. Faremos aqui a demonstração para as duas condições: $p|a$ e quando $p \nmid a$.

Se $p|a$, pela Proposição 1.27 então $p|a^p - a$.

Suponhamos que $p \nmid a$. Vamos considerar os conjuntos $\{1, 2, 3, \cdots, p-1\}$ e $\{a, 2a, 3a, \cdots, (p-1)a\}$. Temos que

- $a \not\equiv 0 \pmod{p}$;
- $2a \not\equiv 0 \pmod{p}$;
- $\cdots$;
- $(p-1)a \not\equiv 0 \pmod{p}$.

Pois $(p, a) = 1$ e $(p, p-1) = 1$.

Se $i, j \in \{1, 2, \cdots, p-1\}$ e $ia \equiv ja \pmod{p}$, concluímos $i \equiv j \pmod{p}$. Então $i = j$, pois $0 \leq |i - j| < p$. Isto significa que os números $a, 2a, \cdots, (p-1)a$ são incongruentes

dois a dois módulo p. Logo os inteiros $a, 2a, \cdots, (p-1)$ são congruentes, em alguma ordem, aos números $1, 2, \cdots, p-1$. Podemos concluir então que

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1) \equiv a \cdot 2a \cdot 3a \cdots (p-1)a \pmod{p},$$

ou seja

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

Como $(p, (p-1)!) = 1$ podemos cancelar na congruência acima o fator $(p-1)!$, o que resulta em

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

Relembramos a seguir algumas propriedades sobre o máximo divisor comum entre dois inteiros, aqui representado por (a, b).

Lema 1.31. *Sejam $a, b, n \in \mathbb{Z}$. Então $(a, b) = (a, b - na)$.*

Demonstração. Seja $d = (a, b - na)$. Como $d|a$ e $d|(b - na)$, segue que d divide $b = b - na + na$. Logo, d é um divisor comum de a e b. Além disso, se c é um divisor comum de a e $b - na$ então $c|d$. Provamos que $d = (a, b)$. □

Lema 1.32. *Sejam $a, b \in \mathbb{N}$, com $(a, b) = 1$ e $m, n, q, r \in \mathbb{N} \cup \{0\}$ tais que $m = nq + r$. Então:*

$$(a^m + b^m, a^n + b^n) = \begin{cases} (a^n + b^n, a^r + b^r), \text{ se } q \text{ é par}, \\ (a^n + b^n, a^r - b^r), \text{ se } q \text{ é ímpar}. \end{cases}$$

Demonstração. Se q é par, temos que $a^n + b^n | a^{nq} - b^{nq}$ e como

$$a^m + b^m = a^{nq+r} + b^{nq+r} = a^r(a^{nq} - b^{nq}) + b^{nq}(a^r + b^r),$$

segue do lema anterior que

$$(a^n + b^n, a^m + b^m) = (a^n + b^n, b^{nq}(a^r + b^r)).$$

Como $(a^n + b^n, b^{nq}) = 1$, temos que:

$$(a^n + b^n, a^m + b^m) = (a^n + b^n, a^r + b^r).$$

Se q é ímpar, $a^n + b^n | a^{nq} + b^{nq}$ e como $a^m + b^m = a^{nq+r} + b^{nq+r} = a^r(a^{nq} + b^{nq}) - b^{nq}(a^r - b^r)$, e $(a^n + b^n, b^{nq}) = 1$, decorre do Lema 1.31 que:

$$(a^n + b^n, a^m + b^m) = (a^n + b^n, a^r - b^r).$$

□

Definição 1.33 (Partição de conjuntos)**.** *Seja χ um conjunto não vazio. Uma partição de χ é uma coleção P de subconjuntos não vazios de χ dotada da seguinte propriedade: Todo elemento de χ pertence a um e apenas um dos elementos de P. Em outras palavras, uma coleção de conjuntos $P = \{\chi_1, \chi_2, \cdots, \chi_n\}$ é uma partição (finita) do conjunto χ, se as seguintes condições forem simultaneamente satisfeitas:*

- $\chi_i \neq \emptyset$, *para* $i = 1, 2, \ldots, n$;
- $\chi_i \subset \chi$, *para* $i = 1, 2, \ldots, n$;
- $\chi = \chi_1 \cup \chi_2 \cup \cdots \cup \chi_n$;
- $\chi_1, \chi_2, \ldots, \chi_n$ *são disjuntos, isto é,* $\chi_i \cap \chi_j = \emptyset$, *para* $i \neq j$, *com* $i, j = 1, 2, \ldots, n$.

Exemplo 1.34. *Se $\chi = \{1, 2, 3, 4, 5, 6, 7, 8\}$, então $P = \{\{1, 5\}, \{2\}, \{4, 6\}, \{3, 7, 8\}\}$ é uma partição de χ com quatro elementos. Veja Figura 1.*

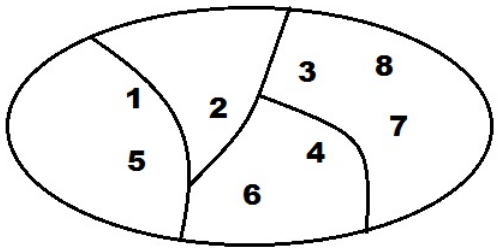

Figura 1: Exemplo de partição de um conjunto χ.

2

NÚMEROS PERFEITOS

Trataremos aqui de uma importante parte da Teoria dos Números, os números perfeitos. Mesmo sendo pouco, ou nunca, mencionado nas escolas de Ensino Básico, é de grande importância por envolver resultados significativos que começaram basicamente com estudos e pensamentos dos Pitagóricos na Grécia Antiga e passam por notáveis matemáticos, como Euler, Fermat, Mersenne, entre outros com conjecturas, teoremas e descobertas de novos números. Apresentaremos também, resultados recentes com novos números perfeitos descobertos, consequentemente, mostrar problemas ainda não resolvidos como infinitude e a existência de Números Perfeitos ímpares ao longo deste capítulo.

Já na Grécia Antiga, os Pitagóricos perceberam que o número 6 tinha uma importante propriedade: a soma de seus divisores positivos inteiros, excluindo ele próprio, era igual ao próprio 6 (Pág.3, Cap.1 de [1]), isto é:

$$6 = 1 + 2 + 3.$$

O mesmo acontece também com o número 28:

$$28 = 1 + 2 + 4 + 7 + 14.$$

Os números que possuem tal propriedade são chamados de números perfeitos.

Por muito tempo, os números perfeitos estavam ligados a crenças, casos religiosos. Santo Agostinho, certa vez, relacionou as ideias da Igreja Católica a respeito da criação do mundo por Deus em seis dias com o nosso primeiro número perfeito, 6 (Pág.3, Cap.1 de [1], Pág.219, Cap.10 de [9]) . Além disso, segundo comentários no Antigo Testamento, a perfeição do universo é representada pelo número 28 (Pág.219, Cap.10 de [9]), também perfeito, cujo valor é exatamente o número de dias que totaliza o ciclo lunar, acrescentando-se mais motivação à essa "conjectura religiosa".

O problema de saber quais e quantos são os números perfeitos motivou muita pesquisa. Discutiremos a seguir alguns dos resultados conhecidos.

Poderemos definir os Números Perfeitos por meio da função $\sigma(n)$. De fato, n perfeito é equivalente a

$$\sigma(n) - n = n,$$

ou seja,

$$\sigma(n) = 2n.$$

Portanto:

- $\sigma(6) = 1 + 2 + 3 + 6 = 2 \cdot 6$, número perfeito.
- $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 2 \cdot 28$, número perfeito.

Se $\sigma(n)$ for diferente de $2n$, temos, por definição, segundo Nicomachus (Pág.3, Cap.1 [1]):

- $\sigma(n) < 2n$: n será um número deficiente,
- $\sigma(n) > 2n$: n será um número abundante.

Iamblichus ($283 - 330$ d.C.) (Pág.4, Cap.1[1]) também fez uso dessas definições.

Exemplo 2.1.

$\sigma(15) = 1 + 3 + 5 + 15 = 24 < 30$, *portanto,* 15 *é deficiente,*

$\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28 > 24$, *portanto,* 12 *é abundante.*

Somente quatro números perfeitos eram conhecidos na Grécia Antiga. Nicomachus em *Introductio Arithmeticae* (por volta de 100 d.C.) listou os quatro primeiros números perfeitos (Pág.3, Cap.1 de [1]):

$$6, 28, 496, 8128.$$

Os estudos iniciais desses números produziram algumas conjecturas baseadas apenas nesses quatro números perfeitos conhecidos (já que na época, não se dispunha de tecnologia avançada para a obtenção de mais exemplos), incluindo:

- O n-ésimo número perfeito possui n dígitos. Acreditava-se que o índice n representa a quantidade de algarismos que o número perfeito possui. Exemplos: $n_1 = 6$ (apenas um algarismo), $n_2 = 28$ (possui 2 algarismos) e assim por diante;
- Os números perfeitos pares terminam, alternadamente, em 6 e 8.

Posteriormente, percebeu-se que ambas as conjecturas estão incorretas: não existe número perfeito de cinco dígitos, já que o quinto número perfeito é 33.550.336, obtido por um manuscrito anônimo do século XV, e o sexto número perfeito é 8.589.869.056. Observe que ambos terminam em 6, o que já exclui a segunda conjectura e a quantidade de dígitos do quinto para o sexto número perfeito exclui a primeira. Porém, percebemos que terminar em 6 ou 8, não necessariamente alternados, aparenta ser de fato uma propriedade dos números perfeitos pares. Também percebemos que, pelo fato de apenas o sexto número perfeito possuir tantos algarismos, nos faz pensar o quanto esses números são raros. E chegamos então, a uma grande questão matemática: existem infinitos números perfeitos?

Se quisermos responder a essa pergunta, seria interessante determinar a forma de tal número. Do início da era Matemática, tal problema foi parcialmente solucionado por Euclides em seu nono volume de *Os Elementos*, que dedica boa parte a construção de números pares perfeitos.

Euclides provou que se a soma

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^{k-1} = p,$$

que representa soma de uma progressão geométrica, que já era encontrada em textos antigos dos Pitagóricos, é um número primo, então

$$2^{k-1} \cdot p$$

é um número perfeito. Note que o primeiro fator é necessariamente par.

Exemplo 2.2.

$1 + 2 = 3$ *é primo e, portanto,* $2 \cdot 3 = 6$ *é um número perfeito,*

$1 + 2 + 4 = 7$ *é um número primo e, portanto* $4 \cdot 7 = 28$ *número perfeito.*

Euclides usou como argumento a fórmula da soma da progressão geométrica

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^{k-1} = 2^k - 1,$$

para chegar ao próximo resultado que estava relacionado com textos Pitagóricos antigos (Pág.220, Cap.10 de [9]). Se $2^k - 1$ é primo, com $k > 1$, então

$$n = 2^{k-1} \cdot (2^k - 1)$$

é um número perfeito.

Passaram-se cerca de dois mil anos até que Euler provasse a recíproca do Teorema de Euclides, ou seja, todo par perfeito é da forma $2^{k-1} \cdot (2^k - 1)$. Veremos agora o Teorema Euclides-Euler sobre os números perfeitos pares.

Teorema 2.3 (Euclides-Euler)**.** *Um número natural n é um número perfeito par se, e somente se, $n = (2^{k-1})(2^k - 1)$, onde $2^k - 1$ é um número primo.*

Demonstração. ($\Leftarrow$ Euclides) Tome $2^k - 1 = p$ um primo e considere $n = 2^{k-1}p$, com $(2^{k-1}, p) = 1$, note que se $k > 1$, isso sempre ocorre. Como σ é uma função multiplicativa, temos

$$\sigma(n) = \sigma(2^{k-1}p) = \sigma(2^{k-1})\sigma(p) = (2^k - 1)(p + 1) = (2^k - 1)2^k = 2n.$$

Portanto, n é um número perfeito.

($\Rightarrow$ Euler) Como n é par, temos que $n = 2^{k-1}b$, com $k > 1$ e b inteiro ímpar. Sendo a função σ, multiplicativa, segue que

$$\sigma(n) = \sigma(2^{k-1}) \cdot \sigma(b) = (2^k - 1) \cdot \sigma(b).$$

Como n é perfeito, então

$$\sigma(n) = 2n = 2^k \cdot b,$$

o que implica

$$2^k b = (2^k - 1) \cdot \sigma(b).$$

Daí temos que $(2^k - 1)|b$, pois 2^k e $(2^k - 1)$ são coprimos. Então, existe $c \in \mathbb{N}$ com $c < b$ tal que

$$b = c(2^k - 1). \tag{1}$$

Segue dessas duas últimas equações que

$$(2^k - 1)\sigma(b) = 2^k(2^k - 1)c.$$

Portanto,

$$\sigma(b) = 2^k c. \tag{2}$$

De (1) temos que c e b são divisores distintos de b tais que $c + b = 2^k c$. Concluímos que $c = 1$. De fato, suponha por absurdo que $c \neq 1$. Temos então que $\sigma(b) \geq 1 + c + b > c + b = 2^k c$. Dessa última relação e de (2) segue que

$$2^k c = c + b < \sigma(b) = 2^k c,$$

o que seria um absurdo.

Portanto, de (1) e (2) segue que $\sigma(b) = b + 1$. Logo b é primo. Temos então que $n = 2^{k-1}(2^k - 1)$ com $2^k - 1$ primo. □

Segue abaixo uma tabela com alguns números perfeitos com base no que vimos acima.

k	$2^k - 1$	$2^{k-1}(2^k - 1)$
2	3	6
3	7	28
5	31	496
7	127	8128
13	8191	33550336
17	131071	8589869056
19	524287	137438691328

Tabela 2: Alguns Números Perfeitos.

Apresentamos agora um resultado que nos diz que se $a^k - 1$ é primo, então devemos ter k primo e $a = 2$.

Lema 2.4. *Se $a^k - 1$ é primo, com $a > 0$ e $k \geq 2$, então $a = 2$ e k é também um primo.*

Demonstração. Fatorando $a^k - 1$, como produto de dois fatores, temos

$$a^k - 1 = (a - 1)(a^{k-1} + a^{k-2} + \cdots + a + 1).$$

Daí, temos que

$$a^{k-1} + a^{k-2} + \cdots + a + 1 \geq a + 1 > 1.$$

Por hipótese, como $a^k - 1$ é primo, então $(a-1) = 1$. Portanto, $a = 2$.

Agora, suponha k um número composto. Logo, podemos escrever $k = cd$, com $c, d > 1$. Com isso, temos

$$a^k - 1 = (a^c)^d - 1 = (a^c - 1)(a^{c(d-1)} + a^{c(d-2)} + \cdots + a^c + 1).$$

Note que qualquer fator da direita é maior do que 1, visto que $c, d > 1$ e $a > 1$. Isso contraria o fato de que $a^k - 1$ é primo. Portanto, k é primo. □

Ao longo do desenvolvimento do estudo dos Números Perfeitos, tivemos alguns equívocos. Por exemplo, a partir do Lema 2.4, acreditava-se que todo número na forma $2^p - 1$, com p primo, era primo. Foi então que Hudarilchus Regius (Pág.222, Cap.10 de [9]) em 1536, em sua obra *Utriusque Arithmetices*, mostrou que

$$2^{11} - 1 = 2047 = 23 \cdot 89.$$

Dos resultados acima já demonstrados, surge uma questão: existem infinitos primos da forma $2^p - 1$ com p primo? Caso provássemos isso, desencadearia em mais resultados expressivos, por exemplo, garantiríamos a existência de infinitos números perfeitos pares. Por ora, não se tem prova disso. Tendo como um problema em aberto atualmente.

Talvez, o caminho poderia ser provando que todos os números perfeitos (pares) terminam realmente em 6 ou 8.

Teorema 2.5. *Se n é um número perfeito par, então seu algarismo da unidade termina com 6 ou 8, o que equivale a $n \equiv 6 \pmod{10}$ ou $n \equiv 8 \pmod{10}$.*

Demonstração. Seja n um número perfeito par na forma $2^{k-1} \cdot (2^k - 1)$, com $2^k - 1$ primo. Para $k = 2$, temos $n = 6$ e o resultado se verifica. Se $k > 2$, podemos separar em dois casos: k tem a forma $4m + 1$ ou $4m + 3$, com $m \in \mathbb{N}$. No caso $k = 4m + 1$, temos

$$n = 2^{4m} \cdot (2^{4m+1} - 1) = 2^{8m+1} - 2^{4m} = 2 \cdot 16^{2m} - 16^m.$$

Note que $16^t \equiv 6 \pmod{10}$ para qualquer $t \in \mathbb{N}$. Substituindo tal congruência, temos

$$n \equiv 2 \cdot 6 - 6 \equiv 6 \pmod{10}.$$

No caso de $4m + 3$, temos

$$n = 2^{4m+2}(2^{4m+3} - 1) = 2^{8m+5} - 2^{4m+2} = 2 \cdot 16^{2m+1} - 4 \cdot 16^m,$$

o que nos dá

$$n \equiv 2 \cdot 6 - 4 \cdot 6 \equiv -12 \equiv 8 \pmod{10}.$$

Portanto, todo número perfeito par possui seu último algarismo 6 ou 8. □

Mas, e os números perfeitos ímpares? O Teorema 2.3 exibe a forma dos números perfeitos pares, e por ora, nada se pode afirmar sobre a existência dos perfeitos ímpares. Porém, conseguimos garantir que se tal número existe, esse não será primo. De fato, seja p um número primo. Supondo que p é perfeito, teríamos $\sigma(p) = 2p$, mas p só possui 1 e p como divisores naturais. Portanto, temos

$$\sigma(p) = p + 1 = 2p,$$

o que implica $p = 1$, o que é um absurdo já que p é primo.

Um outro caso, seria analisar os números quadrados perfeitos ímpares n^2, com n primo. Notemos que os divisores para esse quadrado perfeito mencionado são formados apenas por 1, n e n^2. Tendo n a forma $2k-1$, com $k \in \mathbb{N}$, temos

$$\sigma(n^2) = 1 + n + n^2.$$

Como, $n = 2k - 1$ ou ainda,

$$\sigma(n^2) = 1 + (2k-1) + (2k-1)^2 = 1 + 2k - 1 + 4k^2 - 4k + 1 = 4k^2 - 2k + 1 \neq 2n^2.$$

Resta agora pensarmos em números ímpares compostos. Listamos aqui a função σ de alguns desses números para observação.

Exemplo 2.6.

$\sigma(15) = 1 + 3 + 5 + 15 = 24 < 30$, *deficiente;*

$\sigma(21) = 1 + 3 + 7 + 21 = 32 < 42$, *deficiente;*

$\sigma(27) = 1 + 3 + 9 + 27 = 40 < 54$, *deficiente;*

$\sigma(33) = 1 + 3 + 11 + 33 = 48 < 66$, *deficiente.*

Note que a função σ dos primeiros ímpares compostos e não quadrados perfeitos são todos números deficientes, o que representa apenas uma conjectura. Descartes $(1596 - 1650)$ menciona que todo número perfeito é da forma de Euclides e que não há motivo para a não existência de números perfeitos ímpares (Pág.12, Cap.1 de [1]).

A partir de Descartes, começou-se a cogitar essa existência. Frenicle afirma que, se tal número existe, ele tem a forma pk^2, com p primo da forma $4n + 1$, com $n \in \mathbb{N}$ (Pág.12, Cap.1 de [1]). Um pouco depois, Sorli conjectura que $k = 1$ após testar em números ímpares grandes. Assim como Frenicle $(1604 - 1674)$, Euler também considerou sua existência, chegando a provar que se um número perfeito ímpar existe, então deve ter a forma $N = q^k \cdot n^2$, onde q é um primo de Euler e $(q, n) = 1$.

Proposição 2.7. *Se $N = q^k \cdot n^2$ é um número perfeito ímpar com q um primo de Euler, então*

$$(n^2, \sigma(n^2)) = \frac{D(n^2)}{\sigma(q^{k-1})} = \frac{\sigma(N/q^k)}{q^k}.$$

Demonstração. Seja $N = q^k n^2$ um número perfeito ímpar com q um primo de Euler. Sendo N perfeito, temos

$$\sigma(q^k)\sigma(n^2) = \sigma(N) = 2N = 2q^k n^2,$$

onde $(q, n) = 1$ e, lembremos, σ é uma função multiplicativa. Segue que $q|\sigma(n^2)$, pois $(q^k, \sigma(q^k)) = 1$. O que nos leva a

$$\frac{\sigma(n^2)}{q^k} = \frac{\sigma(N/q^k)}{q^k} = \frac{2n^2}{\sigma(q^k)}$$

é um inteiro. Consequentemente, definindo

$$A = \sigma(n^2),\ B = q^k,\ C = 2n^2,\ D = \sigma(q^k),$$

usando a identidade

$$\frac{A}{B} = \frac{C}{D} = \frac{C - A}{D - B}$$

temos que

$$\frac{\sigma(N/q^k)}{q^k} = \frac{D(n^2)}{\sigma(q^{k-1})},$$

sendo $D - B = \sigma(q^k) - q^K = 1 + q + \cdots + q^{k-1} = \sigma(q^{k-1})$. Então temos

$$(n^2, \sigma(n^2)) = \frac{D(n^2)}{\sigma(q^{k-1})}.$$

Segue que

$$\frac{\sigma(n^2)}{q^k} = \frac{2n^2}{\sigma(q^k)} = \frac{D(n^2)}{\sigma(q^{k-1})},$$

pelo fato de $(q^k, \sigma(q^k)/2) = 1$. Portanto, concluímos a demonstração. □

Fazendo-se uso da Proposição 2.7, seguem outras proposições importantes relacionadas à forma de um número perfeito ímpar.

Proposição 2.8. *Se $N = q^k n^2$ é um número perfeito ímpar com q primo de Euler, então $k = 1$ se, e somente se,*

$$\sigma(n^2) - n^2 = \left(\frac{q-1}{2}\right) \cdot D(n^2).$$

Demonstração. Seja $N = q^k n^2$ um número perfeito ímpar, com q um primo de Euler. Pela Proposição 2.7, temos

$$\frac{\sigma(n^2)}{q^k} = \frac{2n^2}{\sigma(q^k)} = \frac{D(n^2)}{\sigma(q^{k-1})}.$$

Supondo $k = 1$, obtemos

$$\frac{\sigma(n^2)}{q} = \frac{n^2}{\frac{q+1}{2}} = D(n^2).$$

Definimos

$$A' = \sigma(n^2), B' = q, C' = n^2, D' = \tfrac{q+1}{2}.$$

Reciprocamente, se a identidade

$$\frac{A'}{B'} = \frac{C'}{D'} = \frac{A' - C'}{B' - D'}$$

é válida, segue que

$$D(n^2) = \frac{\sigma(n^2) - n^2}{\frac{q-1}{2}},$$

o que implica

$$2\left(\sigma(n^2) - n^2\right)\Big) = (q-1) \cdot \left(2n^2 - \sigma(n^2)\right).$$

Assim,

$$2\sigma(n^2) - 2n^2 = 2qn^2 - 2n^2 - q\sigma(n^2) + \sigma(n^2).$$

Simplificando os termos semelhantes, obtemos

$$(q+1)\sigma(n^2) = 2qn^2,$$

o que implica

$$I(n^2) = \frac{\sigma(n^2)}{n^2} = \frac{2q}{q+1}.$$

Então segue que

$$I(q^k) = \frac{2}{I(n^2)} = \frac{q+1}{q},$$

com q primo de Euler. Concluímos que $k = 1$. □

Proposição 2.9. *Se $N = q^k n^2$ é um número perfeito ímpar, com q primo de Euler, então $k = 1$ se, e somente se,*

$$N = \left(\frac{q(q+1)}{2}\right) \cdot D(n^2).$$

Demonstração. Seja $N = q^k n^2$ um número perfeito ímpar, com q primo de Euler. Como todo número perfeito ímpar $N = q^k n^2$ pode ser escrito na forma

$$N = \left(\frac{q^k \sigma(q^k)}{2}\right) \cdot \frac{D(n^2)}{\sigma(q^{k-1})},$$

então a demonstração segue da Proposição 2.7. Note ainda que

$$\left(q^k, \sigma(q^{k-1})\right) = \left(\sigma(q^k), \sigma(q^{k-1})\right) = 1.$$

□

Proposição 2.10. *Se $N = q^k n^2$ é um número perfeito ímpar, com q um primo de Euler, então $k = 1$, se e somente se,*

$$N = \frac{n^2\sigma(n^2)}{D(n^2)}.$$

Demonstração. Suponha que $N = q^k n^2$ é um número perfeito ímpar com q um primo de Euler. Assumimos $k = 1$. Pela Proposição 2.7, temos

$$\frac{\sigma(n^2)}{q} = D(n^2)$$

o que implica

$$\frac{n^2\sigma(n^2)}{D(n^2)} = qn^2 = N.$$

Agora suponhamos que

$$q^k n^2 = N = \frac{n^2\sigma(n^2)}{D(n^2)}.$$

Logo,

$$\frac{\sigma(n^2)}{q^k} = D(n^2).$$

Contudo, pela Proposição 2.7, sabemos que

$$\frac{\sigma(n^2)}{q^k} = \frac{D(n^2)}{\sigma(q^{k-1})},$$

do qual segue que

$$\sigma(q^{k-1}) = 1.$$

Isso significa que $q^{k-1} = 1$, o que implica que $k - 1 = 0$, isto é, $k = 1$. □

Em 1991, Brent, Cohen e te Riele provaram que números ímpares perfeitos, se existirem, são maiores do que 10^{300} [22]. Em 2012, Ochem e Rao [22] modificaram seu método para mostrar que números ímpares perfeitos, se existirem, são maiores que 10^{1500}.

Listaremos na Tabela 3 abaixo os nove primeiros números perfeitos, lembrando que são 51 números perfeitos descobertos até o momento [8].

Para encerrar este capítulo, segue uma lista das contribuições relevantes historicamente, envolvendo os avanços matemáticos sobre os números perfeitos. Maiores detalhes podem ser encontrados em (Cap.1, [1]).

- Nicomachus, por volta de I d.C., separou os números pares em abundante, deficiente e perfeito. Também colocou em ordem os quatro primeiros e nos seus respectivos intervalos entre 1, 10,100,1000 e 10000, além da conjectura de terminar alternadamente em 6 e 8.

- Theon de Esmirna, por volta de 130 d.C, citou 6 e 28 como perfeitos, 12 como abundante e 8 como deficiente.

n	$\sigma(n)$
1	6
2	28
3	496
4	8128
5	33550336
6	8589869056
7	137438691328
8	2305843008139952128
9	2658455991569831744654692615953842176

Tabela 3: 9 primeiros Números perfeitos.

- Iamblichus $(283-330)$ repetiu as observações de Nicomachus sobre perfeito, abundante e deficiente, e afirmou que existe um e somente um número perfeito em sucessivos intervalos entre 1, 10,100,...

- Aurelius Augustinus $(354-430)$ relacionou a perfeição do número 6, com Deus e a criação do mundo em 6 dias.

- O mesopotâmio Thabit ben Korrah, em um manuscrito, atribuiu a Pitágoras e sua escola o emprego dos números perfeitos e amigáveis.

- Rabbi Josef b. Juhuda Ankin, no fim do século XII, recomendou o estudo de números perfeitos em um programa de educação em seu livro "Cura das Almas".

- Jordanus Nemorarius (?-1236) afirmou (Prop. $55, 56$, Livro VII) que todo múltiplo de um número perfeito ou abundante é abundante e todo divisor de um número perfeito é deficiente. E tentou provar uma afirmação errada de que todo número abundante é par.

- Fibonacci $(1170-1240)$ em sua obra Liber Abbaci de 1202, revisado em 1228, citou:

$$\frac{1}{2}2^2(2^2-1)=6.$$
$$\frac{1}{2}2^3(2^3-1)=28.$$
$$\frac{1}{2}2^5(2^5-1)=496.$$

  Excluindo o expoente 4, pois 2^4-1 não é primo. Então afirmou que por meio do processo acima, seriam encontrados infinitos números perfeitos.

- Nicolas Chuquet $(1445-1488)$ afirmou incorretamente que todo número perfeito terminava alternadamente em 6 e 8.

- Pietro Cataldi $(1548-1626)$ em 1588 descobriu o sexto e o sétimo números perfeitos.

- Girardus Ruffus $(1500-1550)$ afirmou que todo número perfeito é par, e contrariou Jordanus (todo ímpar é deficiente), provando que 45045 é abundante.

- Cardano $(1501-1576)$ afirmou que os números perfeitos eram da forma de Euclides e sempre terminam com 6 ou 8 e que só existe um perfeito entre duas potências de dez.

- René Descartes $(1596-1650)$ em uma carta enviada a Mersenne $(1588-1648)$ pensou que poderia provar que todo número perfeito par é escrito na forma de Euclides e que todo perfeito ímpar deve ser da forma ps^2, com p primo, além de dizer que não há motivos para não existir perfeito ímpar.

- Fermat $(1607-1665)$ produziu 3 proposições que chamou de base da descoberta dos números perfeitos:

  Se n é composto, então 2^n-1 é composto;
  Se n é primo, então 2^n-2 é divisível por $2n$;
  Nenhum primo divide 2^n-1 que não seja da forma $2kn+1$.

  Exemplo 2.11.

  $2^9-1=7\cdot 73$, *com* $n=9$ *composto implica* 511 *composto.*

  $2^3-2=2\cdot 3$ *como em sua segunda proposição.*

  $2^3-1=2\cdot 1\cdot 3+1$ *com* $k=1$.

- Mersenne $(1588-1648)$ afirmou que, dos 28 números exibidos por Bungus como números perfeitos, 20 eram imperfeitos e 8 perfeitos, além de desenvolver vários estudos sobre o termo 2^p-1 com p primo.

- Frenicle $(1605-1675)$ afirmou, em 1657, que a fórmula de Euclides daria todos os números perfeitos pares. Já os perfeitos ímpares, se existirem, são da forma pk^2, onde p é primo da forma $4n+1$, com $n\in\mathbb{N}$.

- Leibniz $(1646-1716)$ implicou incorretamente que 2^p-1 é um primo, se e somente se, p também for.

- Jacques Ozanam $(1640-1717)$ afirmou que existem infinitos números perfeitos e que todos são dados pela fórmula de Euclides, desde que o fator ímpar seja primo.

- Leonard Euler $(1707-1783)$ notou que 2^n-1 pode ser composto com n primo, por exemplo, $2^{11}-1=23\cdot 89$, contrariando alguns resultados antigos. Mas, o trabalho de maior importância está, sem dúvida, na recíproca do Teorema de Euclides, como já foi demonstrado neste capítulo.

A Tabela 4 mostra, em ordem, todos os números descobertos até o momento: ao todo são cinquenta e um [10]. Note que as últimas descobertas vêm do grupo de pesquisas GIMPS (Great Internet Mersenne Primes Search) que mantém o site www.mersenne.org com todos os resultados históricos e últimas descobertas:

Número Perfeito	Número de dígitos	Ano de descoberta	Quem descobriu
6	1	500 a.C.	Gregos antigos
28	2	500 a.C.	Gregos antigos
496	3	275 a.C.	Gregos antigos
8128	4	275 a.C.	Gregos antigos
33550336	8	1456	Anônimo
8589869056	10	1588	Pietro Cataldi
137438691328	12	1588	Pietro Cataldi
2305843008139952128	19	1772	Leonard Euler
$2^{60} \cdot (2^{61} - 1)$	37	1883	Ivan M. Pervushin
$2^{88} \cdot (2^{89} - 1)$	54	1911	R.E. Powers
$2^{106} \cdot (2^{107} - 1)$	65	1914	R.E. Powers
$2^{126} \cdot (2^{127} - 1)$	77	1876	E. Lucas
$2^{520} \cdot (2^{521} - 1)$	314	1952	Raphael M. Robinson
$2^{606} \cdot (2^{607} - 1)$	366	1952	Raphael M. Robinson
$2^{1278} \cdot (2^{1279} - 1)$	770	1952	Raphael M. Robinson
$2^{2202} \cdot (2^{2203} - 1)$	1327	1952	Raphael M. Robinson
$2^{2280} \cdot (2^{2281} - 1)$	1373	1952	Raphael M. Robinson
$2^{3216} \cdot (2^{3217} - 1)$	1937	1957	Hans Riesel
$2^{4252} \cdot (2^{4253} - 1)$	2561	1961	Alexander Hurwitz
$2^{4422} \cdot (2^{4423} - 1)$	2663	1961	Alexnder Hurwitz
$2^{9688} \cdot (2^{9689} - 1)$	5834	1963	Donald B. Gilles
$2^{9940} \cdot (2^{9941} - 1)$	5985	1963	Donald B. Gilles
$2^{11212} \cdot (2^{11213} - 1)$	6751	1963	Donald B. Gilles
$2^{19936} \cdot (2^{19937} - 1)$	12003	1971	Bryant Tuckerman
$2^{21700} \cdot (2^{21701} - 1)$	13066	1978	L. C. Noell/Laura Nickel
$2^{23208} \cdot (2^{23209} - 1)$	13973	1979	L.C. Noell
$2^{44496} \cdot (2^{44497} - 1)$	26790	1979	H.L. Nelson/D. Slowinski
$2^{86242} \cdot (2^{86243} - 1)$	51924	1982	D.Slowinski
$2^{110502} \cdot (2^{110503} - 1)$	66530	1988	W.Colquitt/L. Welsh
$2^{132048} \cdot (2^{132049} - 1)$	79502	1983	D.Slowinski
$2^{216090} \cdot (2^{216091} - 1)$	130100	1985	D.Slowinski
$2^{756838} \cdot (2^{756839} - 1)$	455663	1992	D.Slowinski/P. Gage
$2^{859432} \cdot (2^{859433} - 1)$	517430	1994	D.Slowinski/P.Gage
$2^{1257786} \cdot (2^{1257787} - 1)$	757263	1996	D.Slowinski/P. Gage
$2^{1398268} \cdot (2^{1398269} - 1)$	841842	1996	GIMPS/J. Armengaud
$2^{2976220} \cdot (2^{2976221} - 1)$	1791864	1997	GIMPS/G. Spence
$2^{3021376} \cdot (2^{30210377} - 1)$	1819050	1998	GIMPS/R. Clarkson
$2^{6972592} \cdot (2^{6972593} - 1)$	4197919	1999	GIMPS/N. Hajratwala
$2^{13466916} \cdot (2^{13466917} - 1)$	8107892	2001	GIMPS/M. Cameron
$2^{20996010} \cdot (2^{20996011} - 1)$	12640858	2003	GIMPS/M. Shafer
$2^{24036582} \cdot (2^{24036583} - 1)$	14471465	2004	GIMPS/J. Findley
$2^{25964950} \cdot (2^{25964951} - 1)$	15632458	2005	GIMPS/M. Nowak
$2^{30402456} \cdot (2^{30402457} - 1)$	18304103	2005	GIMPS/C. Cooper/S. Boone
$2^{32582656} \cdot (2^{32582657} - 1)$	19616714	2006	GIMPS/C. Cooper/S. Boone
$2^{37156666} \cdot (2^{37156667} - 1)$	22370543	2008	GIMPS/H. Elvenich
$2^{42643800} \cdot (2^{42643801} - 1)$	25674127	2009	GIMPS/O.M. Strindmo
$2^{43112608} \cdot (2^{43112609} - 1)$	25956377	2008	GIMPS/E. Smith
$2^{57885160} \cdot (2^{57885161} - 1)$	34850340	2013	GIMPS/C. Cooper
$2^{74207280} \cdot (2^{74207781} - 1)$	44677235	2016	GIMPS/C. Cooper
$2^{77232916} \cdot (2^{77232917} - 1)$	46498850	2017	GIMPS/Jon Pace
$2^{82589932} \cdot (2^{82589933} - 1)$	49724095	2018	GIMPS/P. Laroche

Tabela 4: cronologia.

3

NÚMEROS DE MERSENNE

Uma parte importante dos estudos dos números especiais e consequentemente da Teoria dos Números, os Números de Mersenne possuem relação direta com os números perfeitos que tratamos no Capítulo 2. Seu surgimento, incluindo seu próprio nome, é devido a um ilustre estudioso em Matemática e religioso Marin Mersenne $(1588 - 1648)$ (Pág.225, Cap.10 de [9]). De uma família de fazendeiros, Mersenne estudou em Paris com os jesuítas. Seu contato com o trabalho de Galileu por meio da Igreja despertou grande interesse pela ciência, correspondendo-se e mantendo encontros com célebres cientistas como: Descartes, Fermat, Pascal, Torricelli e o próprio Galileu. Dentre seus estudos, certamente o que deu maior contribuição à Matemática, está relacionado a Teoria dos Números conforme veremos abaixo.

Os Números de Mersenne são definidos por

$$M_n = 2^n - 1,$$

onde $n \in \mathbb{N}$. A Tabela 5 exibe os primeiros números de Mersenne.

M_n	$2^n - 1$	Número
M_1	$2^1 - 1$	1
M_2	$2^2 - 1$	3
M_3	$2^3 - 1$	7
M_4	$2^4 - 1$	15
M_5	$2^5 - 1$	31
M_6	$2^6 - 1$	63
M_7	$2^7 - 1$	127

Tabela 5: Números de Mersenne.

Note que alguns desses números são primos.

Definição 3.1. *Chamamos de primo de Mersenne todo número primo da forma* $M_n = 2^n - 1$*, com* $n \in \mathbb{N}$.

Esses números possuem características interessantes:

- Os Números de Mersenne são ímpares. Com efeito, visto que qualquer potência de 2 é par e ao subtrair a unidade, temos um número ímpar.
- É claro também que o único número de Mersenne par é o zero, já que $M_0 = 2^0 - 1 = 0$.

Além disso, mostraremos aqui um resultado muito importante relacionado aos primos de Mersenne:

Teorema 3.2. *Se $2^n - 1$ é primo, então n é primo.*

A demonstração desse Teorema se encontra no Lema 2.4.

Uma curiosidade histórica sobre Mersenne aparece no prefácio de sua obra *Cogitata Physica-Mathematica* (1644), em que ele afirma (Pág.225, Cap.10 de [9]) que M_p é primo para

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$$

e composto para os outros primos menores do que 257. Para os recursos disponíveis à época, calcular por exemplo $2^{257} - 1$, ou até mesmo $2^{67} - 1$, não era tarefa simples para finalidade de confirmações desses resultados. Porém, em 1772, Euler, usando o Teorema 2.3, verificou todos primos até 46339 e acabou encontrando o oitavo número perfeito

$$n_8 = 2^{30}(2^{31} - 1).$$

Observe que o fator $2^{31} - 1$ é um primo de Mersenne, o M_{31}.

Muitos matemáticos, durante muito tempo, acreditaram que todo número da forma de Mersenne era primo com n primo. Todavia, como mencionamos acima, Hudalricus Regius, em 1536, mostrou que $2^{11} - 1$ era composto conforme mostramos no capítulo 2, ver (2).

Como vimos na Tabela 3 contendo os números perfeitos no capítulo 2, percebemos a quantidade de números descobertos nos últimos anos, números com grande quantidade de algarismos e isso se deve ao emprego de recursos tecnológicos e algoritmos. O Teste de Lucas-Lehmer a seguir possui grande utilidade para esta finalidade. O critério utiliza uma base de algoritmo para testar se $2^p - 1$ é primo ou não para grandes valores de p.

Teorema 3.3 (Teste de Lucas-Lehmer)**.** *Seja S_k a sequência definida por $S_k = (2 + \sqrt{3})^{2^k} + (2 - \sqrt{3})^{2^k}$ para $k \in \mathbb{N}$. Para $n > 2$, $M_n = 2^n - 1$ é primo se, e somente se, S_{n-2} é múltiplo de M_n.*

Demonstração. ($\Rightarrow$) Suponha, por absurdo, que $M_n | (2 + \sqrt{3})^{2^{n-2}} + (2 - \sqrt{3})^{2^{n-2}}$ e que M_n seja composto, com um fator primo p tal que $p^2 \leq M_n$. Assim, temos:
$(2 + \sqrt{3})^{2^{n-2}} + (2 - \sqrt{3})^{2^{n-2}} \equiv 0 \pmod{p} \Leftrightarrow (2 + \sqrt{3})^{2^{n-2}} \equiv -(2 - \sqrt{3})^{2^{n-2}} \pmod{p}$.
Como $(2 + \sqrt{3})(2 - \sqrt{3}) = 1$, ou seja, $2 - \sqrt{3} = (2 + \sqrt{3})^{-1}$, podemos reescrever a equação $(2 + \sqrt{3})^{2^{n-2}} \equiv -\frac{1}{(2+\sqrt{3})^{2^{n-2}}} \pmod{p} \Leftrightarrow (2 + \sqrt{3})^{2^{n-2}} \equiv -1 \pmod{p}$, o que significa que a ordem de $2 + \sqrt{3}$ módulo p é igual a 2^n. Absurdo, pois $\sigma(M_n) = p^2 - 1 < 2^n$, logo se S_{n-2} é múltiplo de M_n então M_n é primo.

($\Leftarrow$) Supondo M_n primo, temos:

$(1 + \sqrt{3})^{M_n} \equiv 1 + (\sqrt{3})^{M_n} \equiv 1 + 3^{\frac{M_n - 1}{2}}\sqrt{3} \equiv 1\left(\frac{3}{M_n}\right)\sqrt{3} \equiv 1 - \sqrt{3} \pmod{M_n}$, já que pela reciprocidade quadrática $\left(\frac{3}{M_n}\right) = -\left(\frac{M_n}{3}\right) = -\left(\frac{-2}{3}\right) = -1$.

Note ainda que $(1 + \sqrt{3})^2 = 2(2 + \sqrt{3})$. Assim, temos:

$[(1+\sqrt{3})^2]^{2^{n-1}} = 2^{2^{n-1}}(2+\sqrt{3})^{2^{n-1}} \Leftrightarrow (1+\sqrt{3})^{2^n} = 2^{2^{n-1}}(2+\sqrt{3})^{2^{n-1}}(1+\sqrt{3})^{M_n+1} = 2 \cdot 2^{\frac{M_n-1}{2}}(2+\sqrt{3})^{2^{n-1}} \Leftrightarrow -2 \equiv 2\left(\frac{2}{M_2}\right)(2+\sqrt{3})^{2^{n-1}} \pmod{M_n}$. Segue que

$-1 \equiv \left(\frac{2}{M_n}\right)(2+\sqrt{3})^{2^{n-1}} \pmod{M_n} \Leftrightarrow -1 \equiv (2+\sqrt{3})^{2^n-1} \pmod{M_n}$, uma vez que $\left(\frac{2}{M_n}\right) = (-1)^{\frac{M_n^2-1}{8}} = 1$.

Usando a igualdade $(2+\sqrt{3})(2-\sqrt{3}) = 1$, concluímos que
$(2+\sqrt{3})^{2^{n-1}} \cdot (2-\sqrt{3})^{2^{n-2}} \equiv -(2-\sqrt{3})^{2^{n-2}} \pmod{M_n} = (2+\sqrt{3})^{2^{n-1}} \cdot \frac{1}{(2+\sqrt{3})^{2^{n-2}}} \equiv -(2-\sqrt{3})^{2^{n-2}} \pmod{M_n}$,
que é o mesmo que
$(2+\sqrt{3})^{2^{n-2}} \equiv -(2-\sqrt{3})^{2^{n-2}} \pmod{M_n} = (2+\sqrt{3})^{2^{n-2}} + (2-\sqrt{3})^{2^{n-2}} \equiv 0 \pmod{M_n}$.

Portanto, $M_n|(2+\sqrt{3})^{2^{n-2}} + (2-\sqrt{3})^{2^{n-2}}$, ou seja, S_{n-2} é múltiplo de M_n. □

Finalizamos este capítulo apresentando uma recorrência para o cálculo de S_k do teste acima.

Proposição 3.4. *Seja a sequência* $S_k = (2+\sqrt{3})^{2^k} + (2-\sqrt{3})^{2^k}$. *Então* S_k *satisfaz:* $S_0 = 4$ *e* $S_{k+1} = S_k^2 - 2$.

Demonstração. Para $k = 0$, temos

$$S_0 = (2+\sqrt{3})^{2^0} + (2-\sqrt{3})^{2^0} \Leftrightarrow S_0 = 2+\sqrt{3}+2-\sqrt{3} \Leftrightarrow S_0 = 4.$$

De maneira análoga, para S_{k+1} temos:

$$\begin{aligned} S_{k+1} &= (2+\sqrt{3})^{2^{k+1}} + (2-\sqrt{3})^{2^{k+1}} = (2+\sqrt{3})^{2^k \cdot 2} + (2-\sqrt{3})^{2^k \cdot 2} \\ &= [(2+\sqrt{3})^{2^k}]^2 + [(2-\sqrt{3})^{2^k}]^2 + 2(2+\sqrt{3})^{2^k}(2-\sqrt{3})^{2^k} - 2(2+\sqrt{3})^{2^k}(2-\sqrt{3})^{2^k} \\ &= [(2+\sqrt{3})^{2^k} + (2-\sqrt{3})^{2^k}]^2 - 2[(2+\sqrt{3})(2-\sqrt{3})]^{2^k} \\ &= [(2+\sqrt{3})^{2^k} + (2-\sqrt{3})^{2^k}]^2 - 2 \cdot 1^{2^k} = [(2+\sqrt{3})^{2^k} + (2-\sqrt{3})^{2^k}]^2 - 2 = S_k^2 - 2. \end{aligned}$$

□

Exemplo 3.5. *Seja* $M_3 = 2^3 - 1 = 7$ *e* $S_{3-2} = S_1 = S_0^2 - 2 = 4^2 - 2 = 14$. *Portanto* $M_3|S_1$.

Exemplo 3.6. *Seja* $M_5 = 2^5 - 1 = 31$ *e* $S_{5-2} = S_3 = S_3^2 - 2 = 194^2 - 2 = 37634$. *Portanto* $M_5|S_3$.

Os Números Primos de Mersenne representam também um problema em aberto da Matemática, pois ainda não se sabe se existem infinitos tais números primos. Ao concluirmos o capítulo 2, mencionamos o site GIMPS que possui relevantes contribuições principalmente recentes sobre os resultados de suas pesquisas em relação a esses números. Consequentemente seu resultado influencia diretamente na busca de números perfeitos como já mencionamos aqui por meio da forma do próprio. Recentemente, em dezembro de 2018, foi encontrado o quinquagésimo primeiro número primo de Mersenne. Também foi constatado que tal número possui 24.862.048 de algarismos. Novamente, chamamos a atenção para o quão poucos e ao mesmo tempo quão grandes são esses números especiais.

4

NÚMEROS DE FERMAT

Pierre de Fermat foi um advogado francês que viveu entre 1601 e 1665. Fermat obteve contribuições importantes para a Teoria dos Números, incluindo uma família de números especiais que leva seu nome, os chamados Números de Fermat. Em 1640, Fermat escreveu para Mersenne dizendo acreditar que todos os números da forma abaixo eram primos (Pág.164, Cap.8 de [3]).

$$F_n = 2^{2^n} + 1, n = 0, 1, 2, ...,$$

onde F_n denota o n-ésimo número de Fermat.

A Tabela 6 abaixo apresenta os primeiros termos dessa sequência em que Fermat acreditava serem todos primos.

F_n	$2^{2^n} + 1$
F_0	$2 + 1 = 3$
F_1	$2^2 + 1 = 5$
F_2	$2^4 + 1 = 17$
F_3	$2^8 + 1 = 257$
F_4	$2^{16} + 1 = 65537$

Tabela 6: Números de Fermat.

Em 1732, Leonhard Euler mostrou que

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417.$$

Vamos mostrar este fato sem fazer uso de recursos computacionais, como na época de Euler. Inicialmente, note que $641 = 1 + 640 = 1 + 64 \cdot 10 = 1 + 2^6 \cdot 10 = 1 + 2^7 \cdot 5$. Ou seja, a expressão acima é da forma: $1 + ab$, onde $a = 2^7$ e $b = 5$. Para estes valores de a e b, temos que $1 + ab - b^4 = 1 + (a - b^3)b = 1 + 3b$, isto é,

$$1 + 2^7 5 - 5^4 = 1 + (2^7 - 5^3)5 = 1 + 3 \cdot 5 = 2^4.$$

E isso implica

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 2^4 \cdot (2^7)^4 + 1 = 2^4 a^4 + 1.$$

Trocando 2^4 por $1+ab-b^4$, temos

$$\begin{aligned} F_5 &= (1+ab-b^4)a^4+1 \\ &= (1+ab)a^4+(1-a^4b^4) \\ &= (1+ab)a^4+(1-a^2b^2)(1+a^2b^2) \\ &= (1+ab)a^4+(1+a^2b^2)(1+ab)(1-ab) \\ &= (1+ab)[a^4+(1-ab)(1+a^2b^2)], \end{aligned}$$

como $(1+ab)=641$, provamos que $641|F_5$.

Até o momento não se sabe se existem mais primos de Fermat além dos que estão na Tabela 6 e também disponível em [23]. Vejamos agora uma importante propriedade desses números.

Proposição 4.1. *Para $m \neq n$, temos $(F_m, F_n) = (2^{2^m}+1, 2^{2^n}+1) = 1$.*

Demonstração. Sem perda de generalidade, vamos supor $m > n$. Nesse caso, m pode ser escrito na forma $m = nq+r$, com $q > 0$ inteiro.

$$(2^{2^m}+1, 2^{2^n}+1) = (2^{2^{nq+r}}+1, 2^{2^n}+1) = (2^{2^{nq+r}}+1^{2^{nq+r}}, 2^{2^n}+1^{2^n}),$$

como $(2,1)=1$, pelo Lema 1.32 segue que $(F_m, F_n) = (2^{2^m}+1, 2^{2^n}+1) = 1, m \neq n$. □

Uma curiosidade sobre os Números de Fermat é apresentada na próxima proposição.

Proposição 4.2. *Para todo $n \geq 1$,*

$$F_n = F_0 \cdot F_1 \cdot F_2 \cdots F_{n-1} + 2.$$

Demonstração. Faremos a demonstração por indução. Para $n = 1$, temos

$$F_1 = F_0 + 2 = (2^{2^0}+1)+2 = 5.$$

Suponha que o resultado seja válido para F_{k-1}, ou seja,

$$F_{k-1} = F_0 \cdot F_1 \cdots F_{k-2} + 2.$$

Segue que

$$F_{k-1} - 2 = F_0 \cdot F_1 \cdots F_{k-2}.$$

Usando essa última igualdade, temos

$$F_0 \cdot F_1 \cdot F_2 \cdots F_{k-1} + 2 = (F_{k-1}-2) \cdot F_{k-1} + 2.$$

Mas, como $F_{k-1} = 2^{2^{k-1}} + 1$, temos que

$$\begin{aligned}(2^{2^{k-1}} + 1 - 2) \cdot (2^{2^{k-1}} + 1) + 2 &= (2^{2^{k-1}} - 1) \cdot (2^{2^{k-1}} + 1) + 2 \\ &= (2^{2^{k-1}})^2 - 1 + 2 \\ &= 2^{2 \cdot 2^{k-1}} + 1 = 2^{2^k} + 1 = F_k.\end{aligned}$$

□

Outra curiosidade sobre os Números de Fermat: Gauss provou que um polígono regular de n lados pode ser construído com régua e compasso se n é um produto de potência de 2 e primos ímpares distintos na forma F_n, e afirmou que a construção é impossível se n não é como esse produto (Pág.375, Cap.15 de [1]).

Proposição 4.3. *A quantidade de dígitos do n-ésimo número de Fermat é dado pela fórmula*

$$D(n) = \left\lfloor [log(2^{2^n} + 1)] + 1 \right\rfloor \approx \left\lfloor log(2^{2^n}) + 1 \right\rfloor = 1 + \lfloor 2^n log 2 \rfloor .$$

Para $n = 0, 1, 2, 3...$ os números de dígitos em F_n são, portanto, $1, 1, 2, 3, 5$, 10, 20, 39, $78, 155, ...$[14].

Demonstração. Considere $F_n = 2^{2^n} + 1$ um número de Fermat e considere também que todo número na base decimal pode ser escrito na forma:

$$F_m = \alpha_{n-1} \cdot 10^{n-1} + \alpha_{n-2} \cdot 10^{n-2} + ... + \alpha_1 \cdot 10 + \alpha_0 \cdot 10^0.$$

Como o número de dígitos é representado pelo maior expoente, então temos

$$D(m) = n - 1 + 1 = n,$$

segue que

$$10^{n-1} \leq 2^{2^m} + 1 \implies n - 1 \leq \log(2^{2^m} + 1).$$

□

Lembramos também que as contribuições de Fermat ao mundo da Matemática não se resume só a esse número especial, O Pequeno Teorema de Fermat e o Teorema de Fermat são igualmente conhecidos e estudados na Teoria dos Números, porém esse conteúdo foge do escopo deste trabalho e portanto não os mencionaremos.

5

NÚMEROS AMIGÁVEIS

Nesse capítulo, trataremos de mais um curioso e especial grupo de números, os chamados Números Amigáveis, abordando sua definição, exemplos, propriedades e resultados.

Definição 5.1. *Dois números são chamados de amigáveis se a soma dos divisores próprios de um desses números é exatamente igual ao outro e vice-versa.*

Exemplo 5.2. *Tome os números* 220 *e* 284*. Temos que*
$\sigma(220) - 220 = 1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284.$
$\sigma(284) - 284 = 1 + 2 + 4 + 71 + 142 = 220.$
Portanto, os números 220 *e* 284 *são amigáveis.*

Historicamente, Segundo Iamblichus (Pág.38, Cap.1 de [1]), "certos homens impregnados de opiniões equivocadas pensavam que o número perfeito era chamado de amor pelos Pitagóricos por conta da união de diferentes elementos e afinidades que nele existem; pois eles chamam outros números, pelo contrário, números amigáveis, adotando virtudes e qualidades sociais nos números, como 220 e 284, pois cada parte tem o poder de gerar a outra, de acordo com a regra da amizade, como afirmava Pitágoras. Quando perguntado o que é um amigo, ele respondeu, "outro eu", que é mostrado nesses números, Aristóteles definiu um amigo em sua ética."

Existem textos que afirmam possuir dúvidas em relação ao uso do termo amigáveis e incluindo o próprio conceito aos Pitagóricos, isso porque há uma estreita relação entre números perfeitos e amigáveis, já que todo número perfeito é amigável (a soma de seus divisores é igual a ele mesmo quando excluído o próprio).

Alguns textos, também na busca do surgimento desses números, sugerem seu uso em textos religiosos. Por exemplo, em Gênesis, em que há uma relação direta entre os primeiros números amigáveis conhecidos: o 220 e o 284. Nos versículos $32 : 14 - 16$ de Gênesis, na Bíblia Sagrada em que Jacob presenteia, como gesto de amizade, seu irmão Esaú com 220 animais: "E Jacob passou a noite naquele lugar. De tudo o que possuía, Jacob escolheu um presente para seu irmão Esaú: duzentas cabras e vinte bodes, duzentas ovelhas e vinte cordeiros, trinta camelos de leite, com suas crias, quarenta vacas e dez touros, vinte jumentas e dez jumentinhos". O argumento então é que Jacob usou os números amigáveis 220 (de sua parte) como um talismã para conquistar a amizade do seu irmão.

Ainda mais, conta-se que existia algo como talismãs gravados com esses números que eram vendidos na Idade Média. Conta-se que o uso do amuleto promovia o amor. Outra curiosidade diz respeito a um numerologista árabe que registrou a prática de se gravar 220

em uma fruta e 284 em outra. Logo, comia-se a primeira fruta e oferecia-se a segunda para uma outra pessoa como forma de afrodisíaco matemático.

Contudo, apesar desses relatos, não se sabe precisamente quando se deu o surgimento dos números amigáveis. O que existe na verdade são registros das descobertas de alguns pares e seus respectivos descobridores (ver Tabela 7).

Par	Descobridor
$220, 284$	Conhecido na Antiguidade
$1184, 1210$	Paganini
$17296, 18416$	Fermat
$9363584, 9437056$	Descartes

Tabela 7: Relação Números Amigáveis e seus descobridores.

Como podemos imaginar, não era tarefa simples encontrar pares de números amigáveis. De fato, esses pares são raros, visto que crescem rapidamente. Sem os recursos computacionais atuais, esta tarefa torna-se extenuante.

Assim como os outros números especiais já apresentados aqui, ficam as mesmas perguntas: Será que existe um fórmula para descobrir esses números? Quantos são? São infinitos? Existem pares de números amigáveis ímpares?

Muitos matemáticos ao longo da história se interessaram pelo tema, incluindo Descartes, Van Scooten, Fermat e Leonhard Euler. Alguns matemáticos árabes da época medieval já tinham descoberto dois pares que foram redescobertos por Fermat e Descartes.

Segue um pouco da história dessas buscas:

- Por volta do Século XIII, os números 17296 e 18416 foram descobertos pelos árabes e redescobertos por Fermat em 1636.

- No Século IX o árabe Thabit ben Korrah criou uma regra (Proposição 5.3 abaixo) que leva seu nome e é da forma: se

$$\begin{cases} p = 3 \cdot 2^n - 1, \\ q = 3 \cdot 2^{n-1} - 1, \\ r = 9 \cdot 2^{2n-1} - 1 \end{cases}$$

  são primos maiores do que 2, então $2^n pq$ e $2^n r$ são amigáveis.

- Um terceiro par foi descoberto por Descartes: 9363584 e 9437056.

- Leonhard Euler foi o primeiro a estudar sistematicamente esse tipo de número e inclusive a existência de ímpares bem como os números perfeitos. Tentou estabelecer métodos para descobri-los. E encontrou 60 desses.

- Em 1866 foi encontrado um par cujo valor seria mais simples, 1184 e 1210. O autor da descoberta foi um menino de 16 anos chamado Niccolò Paganini (Pág.139, Cap.4 de [18]).

Proposição 5.3 (Regra de Thabit)**.** *Se*

$$p = 3 \cdot 2^n - 1, q = 3 \cdot 2^{n-1} - 1, r = 9 \cdot 2^{2n-1} - 1$$

são primos maiores que 2*, então* $2^n pq$ *e* $2^n r$ *são amigáveis.*

Demonstração. Usaremos a Proposição 1.16, o Teorema 1.19 e a soma dos divisores próprios de n, dada por $\sigma(n) - n$, para provar que $\sigma(2^n pq) - 2^n pq = 2^n r$ e $\sigma(2^n r) - 2^n r = 2^n pq$. Temos que

$$\begin{aligned}
\sigma(2^n pq) - 2^n pq &= \sigma(2^n)\sigma(p)\sigma(q) - 2^n pq \\
&= (2^{n+1} - 1)3 \cdot 2^n 3 \cdot 2^{n-1} - 2^n(3 \cdot 2^n - 1)(3 \cdot 2^{n-1} - 1) \\
&= 9 \cdot 2^{2n-1}(2^{n+1} - 1) - 2^n(9 \cdot 2^{2n-1} - 3 \cdot 2^n - 3 \cdot 2^{n-1} + 1) \\
&= 9 \cdot 2^{3n} - 9 \cdot 2^{3n-1} + 3 \cdot 2^{2n} + 3 \cdot 2^{2n-1} - 2^n \\
&= 18 \cdot 2^{3n-1} - 9 \cdot 2^{2n-1} - 9 \cdot 2^{3n-1} + 6 \cdot 2^{2n-1} + 3 \cdot 2^{2n-1} - 2^n \\
&= 9 \cdot 2^{3n-1} - 2^n \\
&= 2^n(9 \cdot 2^{2n-1} - 1) \\
&= 2^n r.
\end{aligned}$$

e

$$\begin{aligned}
\sigma(2^n r) - 2^n r &= \sigma(2^n)\sigma(r) - 2^n r \\
&= (2^{n+1} - 1)(r + 1) - 2^n r \\
&= (2^{n+1} - 1)9 \cdot 2^{2n-1} - 2^n(9 \cdot 2^{2n-1} - 1) \\
&= 2^n(9 \cdot 2^{2n-1} - 9 \cdot 2^{n-1} + 1) \\
&= 2^n(9 \cdot 2^{2n-1} - 6 \cdot 2^{n-1} - 3 \cdot 2^{n-1} + 1) \\
&= 2^n(9 \cdot 2^{2n-1} - 3 \cdot 2^n - 3 \cdot 2^{n-1} + 1) \\
&= 2^n(3 \cdot 2^n - 1)(3 \cdot 2^{n-1} - 1) \\
&= 2^n pq.
\end{aligned}$$

□

Desde a época de Euler, muitos pares de números amigáveis foram descobertos e publicados, o que responde uma de nossas perguntas anteriores: a existência de pares de amigáveis ímpares ([13]). Observando rapidamente os pares amigáveis ímpares conhecidos, percebemos que a falta do fator 2 é compensada de certa maneira pelo fator 3, pois todos amigáveis ímpares o possuem.

Teorema 5.4 (Regra de Euler para Números Amigáveis)**.** *Sejam m e n dois inteiros positivos com $1 \leq m \leq n-1$. Se*

$$\begin{cases} p = 2^n \cdot (2^{n-m}+1) - 1, \\ q = 2^m \cdot (2^{n-m}+1) - 1, \\ r = 2^{n+m} \cdot (2^{n-m}+1)^2 - 1, \end{cases}$$

são todos primos, então o par $(2^n \cdot p \cdot q, 2^n \cdot r)$ é de números amigáveis.

Demonstração. Para facilitar a demonstração da Regra de Euler para Números Amigáveis, usaremos $\xi = 2^{n-m}+1$. Assim, queremos provar que se

$$\begin{cases} p = 2^n \cdot \xi - 1, \\ q = 2^m \cdot \xi - 1, \\ r = 2^{n+m} \cdot \xi^2 - 1, \end{cases}$$

Fazendo-se uso do Teorema 1.1 e da Proposição 1.16, temos que

$$\begin{aligned} \sigma(2^n pq) &= \sigma(2^n)\sigma(p)\sigma(q) \\ &= (2^{n+1}-1) \cdot 2^n \xi \cdot 2^m \xi \\ &= (2^{n+1}-1) \cdot 2^{n+m} \cdot \xi^2. \end{aligned}$$

$$\begin{aligned} \sigma(2^n r) &= \sigma(2^n)\sigma(r) \\ &= (2^{n+1}-1) \cdot 2^{n+m} \cdot \xi^2. \end{aligned}$$

$$\begin{aligned} 2^n pq + 2^n r &= 2^n(pq+r) \\ &= 2^n[(2^n \cdot \xi - 1)(2^m \cdot \xi - 1) + 2^{n+m} \cdot \xi^2 - 1] \\ &= 2^{2n+m}\xi^2 - 2^{n+m}\xi - 2^{2n}\xi + 2^{2n+m}\xi^2 \\ &= (2^{n+1}-1)2^{n+m}\xi^2. \end{aligned}$$

Pela Definição 5.1, temos que $\sigma(2^n pq) - 2^n pq = 2^n r$. Portanto, $\sigma(2^n pq) = 2^n r + 2^n pq$, o mesmo acontece com $\sigma(2^r) - 2^n r = 2^n pq$, tendo $\sigma(2^n r) = 2^n pq + 2^n r$. Logo, $2^n pq$ e $2^n r$ são pares amigáveis com p, q, r primos. □

Note que, se $n - m = 1$ na Regra de Euler, então teremos a Regra de Thabit. Vamos mostrar este fato. Para isso, usaremos $n - m = 1$. Logo, temos

$$\begin{cases} p = 2^m \cdot (2^1+1) - 1 = 3 \cdot 2^n - 1, \\ q = 2^m \cdot (2^1+1) - 1 = 3 \cdot 2^m - 1, \\ r = 2^{n+m} \cdot (2^1+1)^2 - 1 = 9 \cdot 2^{n+m} - 1. \end{cases}$$

Como $n - m = 1 \Leftrightarrow m = n - 1$, basta substituir o valor de m na expressão de r e chegaremos em

$$r = 9 \cdot 2^{n+n-1} - 1 = 9 \cdot 2^{2n-1} - 1,$$

conforme Regra de Thabit.

Apesar de Thabit e Euler viverem em épocas diferentes, Thabit já conhecia o primeiro par de números amigáveis 220 e 284 [12] e estudou métodos para obter outros pares, descobrindo regras parecidas com a de Euclides para números perfeitos e composição de números amigáveis. Composição esta também estabelecida por Euler, que descreveu métodos de construção numéricas através de exemplos, [12], como:

$$69615 = 32 \cdot 7 \cdot 13 \cdot 5 \cdot 7.$$

$$87633 = 32 \cdot 7 \cdot 13 \cdot 107.$$

Note que os primeiros fatores são os mesmos e que 32 é uma potência de 2 conforme suas regras.

Proposição 5.5. *Sejam $p = t + 2^n$, $q = t - 2^{n-1}$, $t = 1 + 2 + 2^2 + \cdots + 2^n$ e $r = (2^{n+1} + 2^{n-2}) \cdot 2^{n+1} - 1$, com $n \geq 2$. Se p, q e r são primos, então $2^n pq$ e $2^n r$ são amigáveis.*

Demonstração. Para p, temos

$$\begin{aligned} p &= t + 2^n \\ &= 1 + 2 + 2^2 + \cdots 2^n + 2^n \\ &= (2^{n+1} - 1) + 2^n \\ &= (2 \cdot 2^n - 1) + 2^n \\ &= 2 \cdot 2^n + 2^n - 1 \\ &= (2 + 1) \cdot 2^n - 1 \\ &= 3 \cdot 2^n - 1. \end{aligned}$$

Para q, temos

$$\begin{aligned} q &= t - 2^{n-1} \\ &= 1 + 2 + 2^2 + \cdots 2^n - 2^{n-1} \\ &= (2^{n+1} - 1) - 2^{n-1} \\ &= 2^2 \cdot 2^{n-1} - 2^{n-1} - 1 \\ &= (2^2 - 1) \cdot 2^{n-1} - 1 \\ &= 3 \cdot 2^{n-1} - 1. \end{aligned}$$

Para r, temos

$$\begin{aligned} r &= (2^{n+1} + 2^{n-2}) \cdot 2^{n+1} - 1 \\ &= 2^{2n+2} + 2^{2n-1} - 1 \\ &= (2^3 + 1) \cdot 2^{n-1} - 1 \\ &= 9 \cdot 2^{n-1} - 1. \end{aligned}$$

O resultado agora segue pela regra de Thabit. □

Dessa forma, temos os três termos apenas dependendo de n, conforme dito anteriormente. Observemos na tabela seguinte com os primeiros valores de n que os resultados encontrados usando-se tal regra não garantem pares de números amigáveis.

Valores para (n, p, q, r)	Pares gerados $(2^n pq, 2^n r)$
$(2, 11, 5, 71)$	$(220, 284)$
$(3, 23, 11, 287)$	287 não é primo.
$(4, 47, 23, 1151)$	$(17296, 18416)$
$(5, 95, 47, 4607)$	95 e 4607 não são primos.
$(6, 191, 95, 18431)$	18431 não é primo.
$(7, 383, 191, 73727)$	$(9363584, 9437056)$

Tabela 8: Tabela com os primeiros pares da Regra de Thabit.

Na Tabela 8, podemos analisar os pares obtidos por meio da Regra de Thabit. Fica evidente o que já mencionamos anteriormente, não garantimos que o par encontrado é amigável. O que podemos garantir é que podemos encontrar pares amigáveis usando essa regra. Observe, por exemplo, que a segunda linha da tabela não satisfaz a condição de r primo, já que $287 = 7 \cdot 41$ um número composto. Portanto, o par gerado com certeza não será amigável. Segundo Burton (Pág.510, Cap.10 de [26]), até o momento não há regra conhecida para encontrar todos os pares de números amigáveis e, hoje, mais de 50.000 pares amigáveis são conhecidos, alguns deles têm por volta de 320 dígitos.

6

NÚMEROS DE STIRLING

Neste capítulo, trataremos dos Números de Stirling. Mesmo sendo pouco conhecido, principalmente pelos estudantes no Brasil, esse número especial possui uma importância muito grande em combinatória, sendo seu nome relacionado ao matemático escocês James Stirling $(1692 - 1770)$.

Os Números de Stirling são classificados em dois tipos: os de primeiro tipo e os de segundo tipo.

Os Números de Stirling do primeiro tipo são usados para o cálculo das permutações de n elementos com k ciclos disjuntos, também conhecidos por Ciclos de Stirling. Já o do segundo tipo, também é conhecido como Número de Partições de Stirling.

Os Números de Stirling também são separados da seguinte maneira: com sinal e sem sinal. Trataremos disso ainda neste capítulo.

Diretamente relacionado aos Números de Stirling do segundo tipo está o Número de Bell, que permite contar o número de partições possíveis de um conjunto finito. Este último leva esse nome em homenagem ao matemático Eric Temple Bell $(1883 - 1960)$.

Definição 6.1 (Fórmula recursiva do Número de Stirling do primeiro tipo sem sinal)**.** *Denotamos por $C(n.k)$ o número de partições de n elementos em k ciclos não vazios. Este número é recursivamente definido por*

$$C(n,k) = C(n-1,k-1) + (n-1)C(n-1,k).$$

Por definição:

- $C(n,n) = 1$, para $n \geq 1$;
- $C(0,0) = 1$, para $n \geq 1$;
- $C(n,0) = 0$, para $n \geq 1$.

A seguir, apresentaremos um exemplo do Número de Stirling do primeiro tipo sem sinal em que encontraremos o número de maneiras de se permutar um conjunto com 5 elementos em 2 ciclos não-vazios.

A Figura 2 representa uma partição possível de um conjunto de 5 elementos $\{a,b,c,d,e\}$ em 2 ciclos. Note que inverter os círculos como na Figura 3 produz a mesma partição, ou seja, $\{a,b,c\}\{d,e\} = \{d,e\}\{a,b,c\}$.

Note que, na Figura 4, as rotações não mudam as partições (permutações circulares), ou seja, $\{a,b,c\}\{d,e\} = \{c,a,b\}\{d,e\}$.

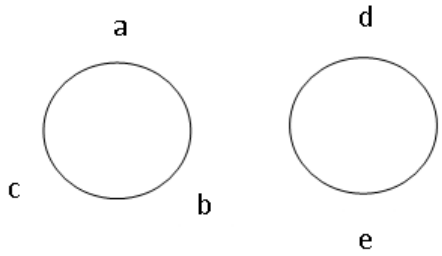

Figura 2: Exemplo de partição do conjunto $\{a, b, c, d, e\}$.

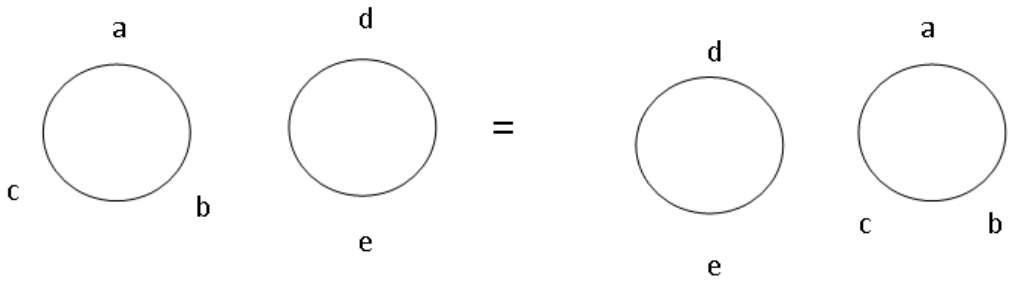

Figura 3: Círculos idênticos.

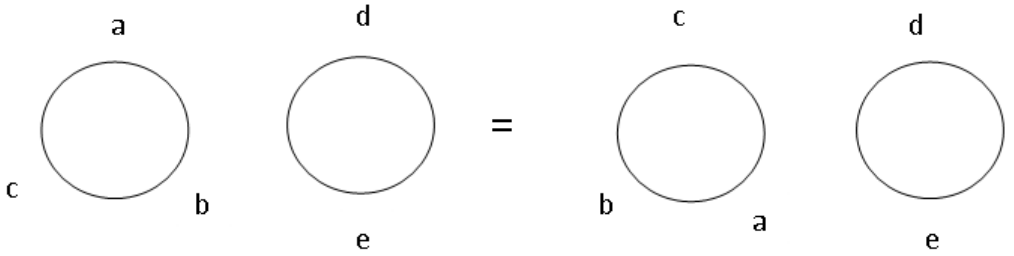

Figura 4: Rotações no círculo.

O que faremos a partir de agora é escrever as partições em relação às figuras levando-se em consideração suas combinações da seguinte forma: a partição da Figura 5 será escrita como $\{a, b, c\}\{d, e\}$. Isso ajudará na determinação de todos os resultados possíveis de uma partição.

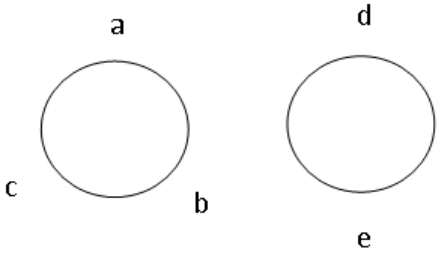

Figura 5: {a,b,c}{d,e}.

Observamos pelas Figuras 5 e 6 que $\{a, b, c\}\{d, e\}$ é o mesmo que $\{c, a, b\}\{d, e\}$.

Faremos, então, uma lista com todas as partições possíveis de $C(5, 2)$, o que corresponde a um total de 50 permutações.

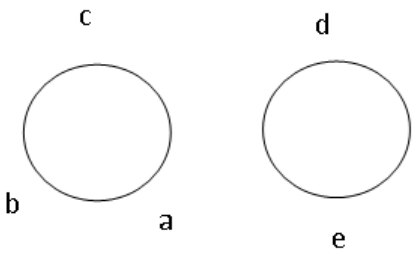

Figura 6: {c,a,b}{d,e}.

$\{a,b,c\}\{d,e\}$	$\{a,c,b\}\{d,e\}$	$\{a,b,d\}\{c,e\}$	$\{a,d,b\}\{c,e\}$	$\{a,b,e\}\{c,d\}$
$\{a,e,b\}\{d,c\}$	$\{a,c,d\}\{b,e\}$	$\{a,d,c\}\{b,e\}$	$\{a,c,e\}\{b,d\}$	$\{a,e,c\}\{b,d\}$
$\{a,d,e\}\{b,c\}$	$\{b,c,e\}\{a,d\}$	$\{b,e,c\}\{a,d\}$	$\{b,d,e\}\{a,c\}$	$\{b,e,d\}\{a,c\}$
$\{c,d,e\}\{a,b\}$	$\{c,e,d\}\{a,b\}$	$\{a,b,c,d\}\{e\}$	$\{a,b,d,c\}\{e\}$	$\{a,c,d,b\}\{e\}$
$\{a,c,b,d\}\{e\}$	$\{a,b,c,e\}\{d\}$	$\{a,b,e,c\}\{d\}$	$\{a,c,b,e\}\{d\}$	$\{a,c,e,b\}\{d\}$
$\{a,e,b,c\}\{d\}$	$\{a,e,c,b\}\{d\}$	$\{a,b,d,e\}\{c\}$	$\{a,b,e,d\}\{c\}$	$\{a,d,b,e\}\{c\}$
$\{b,c,d\}\{a,e\}$	$\{a,e,b,d\}\{c\}$	$\{a,e,d,b\}\{c\}$	$\{a,d,e,c\}\{b\}$	$\{a,d,c,e\}\{b\}$
$\{a,d,c,e\}\{b\}$	$\{a,e,c,d\}\{b\}$	$\{a,e,d,c)\{b\}$	$\{a,c,e,d\}\{b\}$	$\{a,c,d,e\}\{b\}$
$\{b,c,d,e\}\{a\}$	$\{b,c,e,d\}\{a\}$	$\{b,d,c,e\}\{a\}$	$\{b,d,e,c\}\{a\}$	$\{b,e,c,d\}\{a\}$
$\{b,e,d,c\}\{a\}$	$\{a,d,b,c\}\{e\}$	$\{a,d,c,b\}\{e\}$	$\{a,e,d\}\{b,c\}$	$\{b,d,c\}\{a,e\}$

Tabela 9: Lista da combinação Stirling C(5,2).

Vamos calcular $C(5,2)$ usando a fórmula apresentada na Definição 6.1. Substituindo os valores na fórmula, temos:

$$C(5,2) = C(4,1) + 4C(4,2).$$

Porém,

$$C(4,2) = C(3,1) + 3C(3,2)$$

e, ainda,

$$C(3,2) = C(2,1) + 2C(2,2).$$

Mas, por definição, conforme visto acima $C(2,2) = 1$, e

$$C(2,1) = C(1,0) + 1C(1,1). \tag{3}$$

Também por definição, temos $C(1,0) = 0$ e $C(1,1) = 1$. Substituindo esses valores em (3), temos:

$$C(2,1) = 1,$$

consequentemente:

$$C(3,2) = C(2,1) + 2C(2,2) = 1 + 2 \cdot 1 = 3.$$

Olhando agora para $C(3,1)$, temos:

$$C(3,1) = C(2,0) + 2C(2,1),$$

que, por definição, $C(2,0) = 0$ e $C(2,1) = 1$ já determinado anteriormente. Logo,

$$C(3,1) = 2.$$

Substituindo os resultados em $C(4,2)$, temos:

$$C(4,2) = 2 + 3 \cdot 3 = 11. \tag{4}$$

Falta apenas determinar $C(4,1)$: $C(4,1) = (3,0) + 3C(3,1)$. Novamente, por definição, $C(3,0) = 0$ e $C(3,1) = 2$, já encontrado. Portanto,

$$C(4,1) = 0 + 3 \cdot 2 = 6. \tag{5}$$

Finalmente por (4) e (5), temos

$$C(5,2) = C(4,1) + 4C(4,2) = 6 + 4 \cdot 11 = 50.$$

Definição 6.2 (Números de Stirling do primeiro tipo com sinal)**.** *Os números Stirling do primeiro tipo, denotados por $s(n,k)$, são dados por*

$$\sum_{k=0}^{n} s(n,k)x^k = x(x-1)(x-2)\cdots(x-n+1)$$

ou seja, são os coeficientes da expansão.

$$s(n,k) = (-1)^{n-k}C(n.k).$$

O que leva a uma conexão muito simples entre os números Stirling sem sinal e com sinal do primeiro tipo.

Exemplo 6.3. *Calculando $s(n,k)$ com $n = 5$ e $k = 2$ para o Número de Stirling do primeiro tipo com sinal.*

$$s(5,2) = (-1)^{5-2}C(5,2) = -1 \cdot 50 = -50.$$

A razão pela qual os Números de Stirling do primeiro tipo recebem sinais é devido à sua relação com os Números de Stirling do segundo tipo. Em múltiplas identidades e teoremas simétricos, os dois tipos de Números de Stirling aparecem. Existem vários tipos de problemas combinatórios que são resolvidos com o uso dos Números de Stirling.

Exemplo 6.4. *De quantas maneiras você pode distribuir quatro crianças e cinco adultos em duas mesas circulares idênticas, de modo que cada mesa tenha pelo menos uma criança e um adulto?*

***Solução**. Dividimos o problema em dois problemas separados, organizando quatro crianças em duas mesas e cinco adultos em duas mesas. A resposta final será apenas o produto dos dois números, pelo princípio multiplicativo. Como temos* $s(4,2) = 11$ *e* $|s(5,2)| = 50$*, nossa resposta final é* $11 \cdot 50 = 550$*.*

De fato, $s(4,2) = (-1)^{4-2}C(4,2) = 1 \cdot 11$ *e* $|s(5,2)| = C(5,2) = |(-1)^{5-2}| \cdot 50 = 50$*. Note que usamos o módulo pois essas contagens são positivas.*

Trataremos agora dos Números de Stirling do segundo tipo, aos quais fazemos partições mas não em grupos circulares.

Definição 6.5 (Números de Stirling e Números de Bell)**.** *Seja* $S(n,k)$ *o número de partições de* $\{1,2,...,n\}$ *em* k *subconjuntos não vazios.* $S(n,k)$ *é chamado de Número de Stirling do segundo tipo. Seja* $B(n)$ *o total de números de partições do conjunto* $\{1,2,...,n\}$*.* $B(n)$ *é chamado de Número de Bell.*

Os Números de Stirling e de Bell não são dados por fórmulas fechadas que envolvam fatoriais, coeficientes binomiais, etc, embora existam fórmulas que usem somatórios e funções geradoras para essas quantidades [28]. No entanto, os Números de Stirling satisfazem uma recursão que pode ser usada para calcular $S(n,k)$ e $B(n)$ muito rapidamente.

Teorema 6.6 (Recursão para Números de Stirling do segundo tipo)**.** *Para todo* $n > 0$ *e* $k > 0$*,*

$$S(n,k) = S(n-1,k-1) + k(n-1,k),$$

tendo como condições iniciais $S(0,0) = 1$*,* $S(n,0) = 0$ *para* $n > 0$ *e* $S(0,k) = 0$ *para* $k > 0$*. Além disso* $B(0) = 1$ *e* $B(n) = \sum_{k=1}^{n} S(n,k)$ *para* $n > 0$*.*

Demonstração. Sejam $n, k > 0$ e Ω o conjunto das partições de $\{1,2,3,\ldots,n\}$ em k subconjuntos não-vazios. Seja $\Omega' = \{E \in \Omega : \{n\} \in \Omega\}$ e $\Omega'' = \{E \in \Omega : \{n\} \notin \Omega\}$. Note que o conjunto Ω é a união disjunta de Ω' e Ω'', uma vez que Ω' consiste nas partições definidas de modo que n está em um subconjunto por si só, enquanto Ω'' consiste nas partições definidas de forma que n está em um subconjunto com alguns outros elementos. Para construir uma partição típica $E \in \Omega'$, primeiro escolhemos uma partição arbitrária de conjuntos E_0 de $\{1,2,...,n-1\}$ em $k-1$ subconjuntos vazios de qualquer uma das $S(n-1,k-1)$ maneiras. Em seguida, adicionamos $\{n\}$ a E_0 para obter E. Para criar uma partição típica $E \in \Omega''$, primeiro escolhemos uma partição arbitrária E_1 de $\{1,2,...,n-1\}$ em k subconjuntos não-vazios de qualquer uma das $S(n-1,k)$ maneiras. Então, escolhemos um desses subconjuntos não-vazios e adicionamos n como um novo membro desse conjunto não-vazio. Pelas regras de soma e produto, temos

$$S(n,k) = |\Omega| = |\Omega'| + |\Omega''| = S(n-1,k-1) + kS(n-1,k).$$

As condições iniciais são imediatas das definições (observe que $E = \emptyset$ é o conjunto exclusivo partição de $X = \emptyset$). A fórmula para $B(n)$ segue a regra da soma. □

Exemplo 6.7. *Particionar um conjunto de cinco elementos em três subconjuntos não-vazios Grupo* 1*:* $\{1, 2, 3\}$

Grupo 2*:* $\{4\}$

Grupo 3*:* $\{5\}$

Escrevemos então $\{1, 2, 3\}\{4\}\{5\}$ *Note que, se particionarmos na forma*

Grupo 1*:*$\{5\}$

Grupo 2*:* $\{1, 2, 3\}$

Grupo 3*:* $\{4\}$

obtemos o mesmo grupo anterior, ou seja, $\{1, 2, 3\}\{4\}\{5\}$ *e* $\{5\}\{1, 2, 3\}\{4\}$ *são as mesmas partições.*

Listaremos na Tabela 10 *todas as partições possíveis enumeradas por* $S(5, 3)$*.*

$\{1,2,3\}\{4\}\{5\}$	$\{1,2,4\}\{3\}\{5\}$	$\{1,2,5\}\{3\}\{4\}$	$\{1,3,4\}\{2\}\{5\}$	$\{1,3,5\}\{2\}\{4\}$
$\{1,4,5\}\{2\}\{3\}$	$\{2,3,4\}\{1\}\{5\}$	$\{2,3,5\}\{1\}\{4\}$	$\{2,4,5\}\{1\}\{3\}$	$\{3,4,5\}\{1\}\{2\}$
$\{1,2\}\{3,4\}\{5\}$	$\{1,3\}\{2,4\}\{5\}$	$\{1,4\}\{2,3\}\{5\}$	$\{1,2\}\{3,5\}\{4\}$	$\{1,3\}\{2,5\}\{4\}$
$\{1,5\}\{2,3\}\{4\}$	$\{1,2\}\{4,5\}\{3\}$	$\{1,4\}\{2,5\}\{3\}$	$\{1,5\}\{2,4\}\{3\}$	$\{1,3\}\{4,5\}\{2\}$
$\{1,4\}\{3,5\}\{2\}$	$\{1,5\}\{3,4\}\{2\}$	$\{2,3\}\{4,5\}\{1\}$	$\{2,4\}\{3,5\}\{1\}$	$\{2,5\}\{3,4\}\{1\}$

Tabela 10: Partições do Exemplo 6.7.

Temos, então, um total de 25 *partições.*

Mais uma vez, pensamos em alguma fórmula direta ou recursiva desses resultados. Porém, precisamos definir:

$S(0, 0) = 1$;

$S(n, 0) = 0$ para $n \geq 1$;

$S(n, n) = 1$ para $n \geq 1$.

Exemplo 6.8. *Encontrar todas as partições de* $S(5, 3)$*. Aplicando-se a fórmula recursiva, temos*

$$S(5, 3) = S(4, 2) + 3S(4, 3). \tag{6}$$

Calculando, separadamente, $S(4, 2)$*, temos*

$$S(4, 2) = S(3, 1) + 2S(3, 2), \tag{7}$$

mas

$$S(3, 2) = S(2, 1) + 2S(2, 2). \tag{8}$$

Por definição, temos que $S(2, 2) = 1$ *e* $S(2, 1) = S(1, 0) + 1S(1, 1) = 0 + 1 = 1$*. Substituindo em* (8)*, temos*

$$S(3, 2) = 1 + 2 \cdot 1 = 3, \tag{9}$$

e temos que

$$S(3,1) = S(2,0) + 1S(2,1) = 0 + 1 \cdot 1 = 1. \tag{10}$$

Substituindo (10) *e* (9) *em* (7)*, temos*

$$S(4,2) = 1 + 2 \cdot 3 = 7. \tag{11}$$

Calculando agora $S(4,3)$*, temos*

$$S(4,3) = S(3,1) + 3S(3,3). \tag{12}$$

De (10) *e por definição* $S(3,3) = 1$*, temos*

$$S(4,3) = S(3,1) + 3S(3,3) = 2 + 3 \cdot 1. \tag{13}$$

Finalmente, substituindo (11) *e* (13) *em* (6) *concluímos que*

$$S(5,3) = S(4,2) + 3S(4,3) = 7 + 3 \cdot 6 = 25.$$

Definição 6.9 (Número de Bell)**.** *Os números inteiros* B_n *podem ser definidos pela soma*

$$B_n = \sum_{k=0}^{n} S(n,k),$$

em que $S(n,k)$ *é um número Stirling do segundo tipo.*

Portanto temos o número de maneiras pelas quais um conjunto de n elementos pode ser particionado em subconjuntos não vazios.

$(1, 1, 2, 5, 15, 52, 203, 877, 4140, 21147, 115975, 678570, 4213597, 27644437, \ldots)$[27].

7

NÚMERO DE LUCAS

Assim como vimos em outros capítulos, este também recebe o nome do matemático que introduziu esse tipo de número, os chamados Números de Lucas, em homenagem ao matemático francês François Édouard Anatole Lucas $(1842 - 1891)$.

Lucas teve grande importância na Teoria dos Números, não só com o estudo de seu número especial, que vamos tratar aqui, mas com contribuições de seu teorema, o Teorema de Lucas, e o famoso jogo Torre de Hanói.

O Número de Lucas surgiu da tentativa de generalizar a famosa sequência de Fibonacci, interesse de seus estudos. Veremos que estes números possuem características, relações e propriedades muito interessantes.

Lembraremos aqui, brevemente, a sequência de Fibonacci, cujos termos são chamados de números de Fibonacci, que possuem propriedades aritméticas interessantes e são constantemente objetos de estudos até os dias de hoje, ver por exemplo [16], [24], [25].

$$(1, 1, 2, 3, 5, 8, 13, 21, 34, ..)$$

Sabemos que, para determinar algum elemento da sequência f_n com $n \in \mathbb{N}$, basta somar os dois termos antecedentes a ele, isto é

$$f_n = f_{n-1} + f_{n-2}, \tag{14}$$

com $f_1 = f_2 = 1$ e n representa o termo geral a ser obtido.

Novamente, fica evidente que, para obtermos termos de índices muito maiores que os primeiros, seria bom termos uma fórmula para o termo geral.

Proposição 7.1. *O n-ésimo termo da sequência de Fibonacci é dado por*

$$f_n = \frac{1}{\sqrt{5}} \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}} \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Demonstração. O polinômio característico da relação de recorrência (14) é dado por

$$\lambda^2 - \lambda - 2 = 0,$$

o que implica

$$\lambda = \frac{-(-1) \pm \sqrt{(-1)^2 - 4 \cdot 1 \cdot (-1)}}{2 \cdot 1} = \frac{1 \pm \sqrt{5}}{2}.$$

Então, $\lambda_1 = \frac{1+\sqrt{5}}{2}$ e $\lambda_2 = \frac{1-\sqrt{5}}{2}$.

Como a Equação (14) é uma relação de recorrência que depende dos valores iniciais, uma possível solução é da forma

$$a_n = C_1 \cdot \lambda_1^n + C_2 \cdot \lambda_2^n,$$

em que $a_n = a_{n-1} + a_{n-2}$ e C_1 e C_2 são constantes reais.

Substituindo as raízes do polinômio característico encontrado, temos

$$a_n = C_1 \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n + C_2 \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Usando agora o problema de valores iniciais, temos:

- Quando $a_0 = 0$ e $a_1 = 1$, temos os Números de Fibonacci;
- Quando $a_0 = 2$ e $a_1 = 1$, temos os Números de Lucas.

Finalizando a fórmula explícita para os Números de Fibonacci, temos

$$a_0 = C_1 \cdot \left(\frac{1+\sqrt{5}}{2}\right)^0 + C_2 \cdot \left(\frac{1-\sqrt{5}}{2}\right)^0 = 0,$$

que nos dá $C_1 + C_2 = 0$ equivalente à $C_1 = -C_2$.

Agora, para $a_1 = 1$,

$$a_1 = C_1 \cdot \left(\frac{1+\sqrt{5}}{2}\right)^1 + C_2 \cdot \left(\frac{1-\sqrt{5}}{2}\right)^1 = 1.$$

Desta última equação, podemos substituir C_1 por $-C_2$, daí

$$-C_2 \cdot \left(\frac{1+\sqrt{5}}{2}\right) + C_2 \cdot \left(\frac{1-\sqrt{5}}{2}\right) = C_2 \cdot \left(\frac{-1-\sqrt{5}}{2}\right) + C_2 \cdot \left(\frac{1-\sqrt{5}}{2}\right) = 1.$$

Colocando C_2 em evidência, pois é o fator comum

$$C_2 \left[\frac{-1-\sqrt{5}}{2} + \frac{1-\sqrt{5}}{2}\right] = 1.$$

Segue que

$$C_2[\sqrt{5}] = 1,$$

então $C_2 = \frac{-1}{\sqrt{5}}$. Logo $C_1 = \frac{1}{\sqrt{5}}$. Portanto, a fórmula que nos permite calcular o n-ésimo termo da sequência de Fibonacci é

$$f_n = \frac{1}{\sqrt{5}} \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}} \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

□

Os primeiros termos da sequência de Lucas são, [15],

$$(2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, 843, ...)$$

Note que cada termo a partir do terceiro é a soma dos dois termos antecedentes, como na sequência de Fibonacci. Isso facilita encontrar a fórmula para o n-ésimo termo, pois o polinômio característico e a resolução da respectiva equação característica são exatamente as mesmas encontradas anteriormente. Podemos partir para o problema do valor inicial [24],[25],

$$L_n = L_{n-1} + L_{n-2},$$

com $L_1 = 1$ e $L_2 = 3$, sendo L_n é o termo geral da Sequência de Lucas.

Proposição 7.2. *O n-ésimo termo da sequência de Lucas é dado por*

$$L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Demonstração. Com base na demonstração da Proposição 7.1, temos que a solução para a recorrência que define L_n é dada por

$$a_n = \alpha \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n + \beta \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Podemos adotar $a_0 = 2$ e $a_1 = 1$ como os primeiros termos da Sequência de Lucas para resolver o problema de valores iniciais,

$$a_0 = \alpha + \beta = 2,$$

que equivale à $\beta = 2 - \alpha$, e

$$a_1 = \alpha \cdot \left(\frac{1+\sqrt{5}}{2}\right) + \beta \cdot \left(\frac{1-\sqrt{5}}{2}\right) = 1.$$

Substituindo $\beta = 2 - \alpha$ na equação anterior, temos

$$\alpha \cdot \left(\frac{1+\sqrt{5}}{2}\right) + (2-\alpha) \cdot \left(\frac{1-\sqrt{5}}{2}\right) = 1.$$

Desenvolvendo a equação, segue que

$$\begin{aligned} \alpha \cdot \left(\frac{1+\sqrt{5}}{2}\right) + (1-\sqrt{5}) - \alpha\left(\frac{1-\sqrt{5}}{2}\right) &= 1, \\ \alpha \cdot \left(\frac{1+\sqrt{5}}{2}\right) + \alpha \cdot \left(\frac{-1+\sqrt{5}}{2}\right) &= 2 - 1 - \sqrt{5}, \\ \alpha \cdot \sqrt{5} &= \sqrt{5}. \end{aligned}$$

Logo, $\alpha = 1$ e substituindo em $\beta = 2 - \alpha$, obtemos $\beta = 2 - 1 = 1$. Portanto, $\alpha = 1$ e $\beta = 1$, que nos dá a fórmula fechada para os Números de Lucas na forma

$$L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

□

Conseguimos observar que entre os números de Lucas existem números primos, os quais chamados de Primos de Lucas [17]. Segue a sequência com os primeiros primos

$$(2, 3, 7, 11, 29, 47, 199, 521, 2207, 3571, 9349, 3010349, ...)$$

Algo que se torna extremamente interessante em relação ao Números de Lucas é sua forte ligação com a Proporção Áurea e suas potências. Lembrando que a Proporção Áurea é definida por

$$\phi = \frac{1+\sqrt{5}}{2} \approx 1,618.$$

A Tabela 11 mostra a relação $\phi^n \approx L_n$, para alguns valores de $n \geq 0$.

n	ϕ^n	L_n
2	2, 61803...	3
3	4, 2358...	4
4	6, 853...	7
5	11, 0901...	11
6	17, 9420...	18
7	29, 0301...	29

Tabela 11: $\phi^n \approx L_n$.

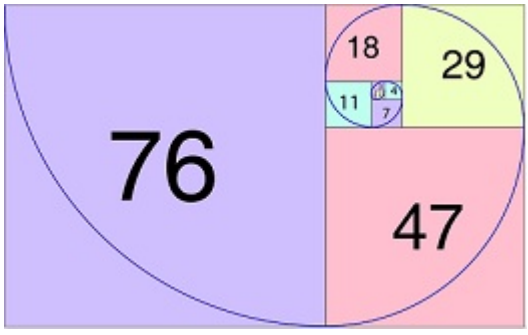

Figura 7: Espiral com Número de Lucas.

Os números de Lucas estão relacionados aos números de Fibonacci por muitas identidades. Apresentamos algumas delas a seguir.

Proposição 7.3. *Para todo $n \geq 2$,*

$$L_n = f_{n-1} + f_{n+1}.$$

Demonstração. A demonstração é feita por indução. Inicialmente, notemos que

$$L_2 = f_1 + f_3 = 0 + 1 = 1$$

e

$$L_3 = f_2 + f_4 = 1 + 2 = 3.$$

Suponhamos que a identidade seja válida para todo inteiro de 2 até k, com $k > 2$, ou seja, $L_k = f_{k-1} + f_{k+1}$. Provaremos que $L_{k+1} = f_k + f_{k+2}$.

Adicionando-se membro a membro as equações de L_k e L_{k-1}, obtemos

$$L_k + L_{k-1} = f_{k-1} + f_{k+1} + f_{k-2} + f_k.$$

Por definição, temos que $L_k + L_{k-1} = L_{k+1}$, $f_{k-1} + f_{k-2} = f_k$ e $f_k + f_{k+1} = f_{k+2}$, Então segue imediatamente que

$$L_{k+1} = f_k + f_{k+2}.$$

□

A Figura 8 representa essa última relação. Observe que estão alinhados os índices da sequência, a sequência de Fibonacci e a sequência de Lucas. Escolhido $L_n \geq L_1$, seu valor será a soma dos termos antecessor e sucessor de f_n, justamente como dado pela Proposição 7.3.

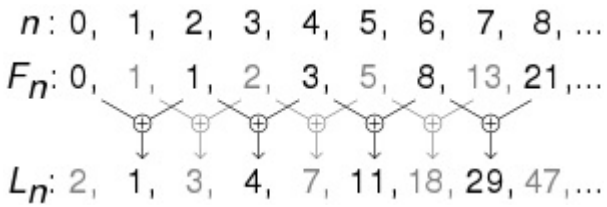

Figura 8: Ilustração da relação demonstrada na proposição 7.3.

Proposição 7.4. *Para todo $n \geq 1$,*

$$f_n \cdot L_{n+1} + f_{n+1} \cdot L_n = 2 \cdot f_{2n+1}.$$

Demonstração. Fazendo indução em k, com $k \in \mathbb{N}$, temos, para $k = 0$:

$$f_0 \cdot L_1 + f_1 \cdot L_0 = 0 \cdot 1 + 1 \cdot 2 = 2 = 2 \cdot f_1.$$

Para $k = 1$, obtemos

$$2 \cdot f_3 = f_1 \cdot L_2 + f_2 \cdot L_1 = 1 \cdot 3 + 1 \cdot 1 = 2 \cdot 2 = 4.$$

Assumimos que $2 \cdot f_{2k+1} = f_k \cdot L_{k+1} + f_{k+1} \cdot L_k$ seja verdadeiro. Provaremos a afirmação para $k+1$. De fato:

$$\begin{aligned} f_{k+1} \cdot L_{k+2} + f_{k+2} \cdot L_{k+1} &= f_{k+1}(L_{k+1} + L_k) + (f_{k+1} + f_k)L_{k+1} \\ &= f_{k+1} \cdot L_{k+1} + f_{k+1} \cdot L_k + f_{k+1} \cdot L_{k+1} + f_k \cdot L_{k+1} \\ &= 2 \cdot f_{k+1} \cdot L_{k+1} + (f_{k+1} \cdot L_k + f_k \cdot L_{k+1}) \\ &= 2 \cdot f_{2k+2} + 2 \cdot f_{2k+1} \\ &= 2 \cdot (f_{2k+2} + f_{2k+1}) \\ &= 2 \cdot f_{2k+3}. \end{aligned}$$

□

Proposição 7.5. *Para $n \geq 0$,*

$$f_{2n} = L_n f_n.$$

Demonstração. A demonstração é feita por indução. Para $k = 0$, temos

$$f_{2\cdot 0} = f_0 = L_0 \cdot f_0 = 0 \cdot 2 = 0.$$

Para $k = 1$, temos

$$f_{2\cdot 1} = f_2 = L_1 \cdot f_1 = 1 \cdot 1 = 1.$$

Assumimos agora que $f_{2k} = L_k \cdot f_k$. Provaremos para $k+1$. De fato, pela hipótese de indução e pela Proposição 7.4 segue que

$$\begin{aligned} f_{k+1} \cdot L_{k+1} &= (f_k + f_{k-1})(L_k + L_{k-1}) \\ &= f_k \cdot L_k + f_k \cdot L_{k-1} + f_{k-1} \cdot L_k + f_{k-1} \cdot L_{k-1} \\ &= f_{2k} + 2 \cdot f_{2k-1} + f_{2k-2} \\ &= (f_{2k} + f_{2k-1}) + (f_{2k-1} + f_{2k-2}) \\ &= f_{2k+1} + f_{2k} = f_{2k+2}. \end{aligned}$$

□

8

OUTROS NÚMEROS ESPECIAIS

Neste capítulo, apresentaremos outros números especiais. Faremos aqui uma breve apresentação de cada um com sua definição e exemplos. A finalidade é difundir outros casos também interessantes e atuais.

Definição 8.1 (Primo Especial)**.** *Um número primo é chamado de especial se o mesmo pode ser expresso como a soma de três inteiros, sendo dois primos consecutivos e o um.*

Exemplo 8.2. *Usaremos dois primos especiais para representar a definição anterior.*

- $13 = 5 + 7 + 1$,
- $19 = 11 + 7 + 1$.

Observe que o 2 nunca entrará nessa soma, pois obrigatoriamente $3 + 2 + 1 = 6$ que não é primo e é justamente nosso primeiro número perfeito.

Definição 8.3 (Primo de Mersenne Duplo)**.** *Seja um número de Mersenne $M_p = 2^p - 1$ primo. Chamamos de Primo de Mersenne Duplo se M_{M_p} for primo também.*

Exemplo 8.4. *Tomemos $p = 2$, então $M_2 = 2^2 - 1 = 3$, segue imediatamente que $M_3 = 2^3 - 1 = 7$.*

Segue abaixo uma pequena tabela com alguns valores de p.

p	$M_p = 2^p - 1$	$M_{M_p} = 2^{2^p-1} - 1$	Resultado
2	3	primo	7
3	7	primo	127
5	31	primo	2147483647

Tabela 12: Primo de Mersenne Duplo.

Observe que esses primeiros valores são todos Primos de Mersenne Duplos. Porém, nem todos valores de p resultam nessa forma, por exemplo, para $p = 11$ não obtemos tal resultado, pois em sua decomposição encontramos o fator 47.

Definição 8.5 (Primos Sensuais)**.** *Chamamos de Primos Sensuais (Sexy primes) os pares de números primos cuja diferença é exatamente* 6*.*

Exemplo 8.6. *Temos aqui uma lista de pares menores do que* 400 *que obedecem tal regra [19].* $(5, 11), (7, 13), (11, 17), (13, 19), (17, 23), (23, 29), (31, 37), (37, 43), (41, 47), (47, 53), (53, 59), (61, 67), (67, 73), (73, 79), (83, 89), (97, 103), (101, 107), (103, 109), (107, 113), (131, 137), (151, 157), (157, 163), (167, 173), (173, 179), (191, 197), (193, 199), (223, 229), (227, 233), (233, 239), (251, 257), (257, 263), (263, 269), (271, 277), (277, 283), (307, 313), (311, 317), (331, 337), (347, 353), (353, 359), (367, 373), (373, 379), (383, 389)$.

O termo "sexy" na verdade representa uma paronomásia em relação ao número 6 em inglês "six". Um detalhe importante é que o maior par de números sensuais foi descoberto recente em outubro de 2019 por P. Kaiser e possui 50539 dígitos[20]. Esses são os pares:

$$p = (520461 \cdot 2^{55931} + 1) \cdot (9856939289 \cdot (520461 \cdot 2^{55931} - 1)^2 - 3) - 1,$$
$$p + 6 = (520461 \cdot 2^{55931} + 1) \cdot (9856939289 \cdot (520461 \cdot 2^{55931} - 1)^2 - 3) + 5.$$

Ainda não se sabe se existem infinitos tais pares de primos.

Definição 8.7 (Primos Gêmeos)**.** *São pares de primos cuja a diferença entre eles é* 2*.*

Exemplo 8.8. *Uma breve sequência de pares de primos gêmeos, [21], inclui*

$$(3,5),(5,7),(11,13),(17,19),(29,31),(41,43),(59,61),(71,73),(101,103),(107,109).$$

Historicamente, existe uma busca pela infinitude de pares de primos gêmeos, permanecendo um problema em aberto até o momento.

Definição 8.9 (Números da sorte)**.** *Chamamos de Número da sorte (Lucky Number) o número que obedece a um processo de crivo específico que elimina números com base em sua posição no conjunto restante, em vez de seu valor (ou posição no conjunto inicial de números naturais).*

Exemplo 8.10. *Usaremos os primeiros* 30 *números inteiros positivos.*

$$1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16$$
$$17-18-19-20-21-22-23-24-25-26-27-28-29-30.$$

O crivo consiste no seguinte: como o primeiro número após o 1 *é o* 2*, então eliminamos todos os múltiplos de* 2 *(ou seja, os números pares) da lista, restando apenas*

$$1-3-5-7-9-11-13-15-17-19-21-23-25-27-29.$$

Agora, como o próximo número depois do 1 *é o* 3*, eliminaremos todos os números restantes que ocupam a posição múltiplo de* 3*, restando*

$$1-3-7-9-13-15-19-21-25-27.$$

Após o 3 *temos* 7*, logo eliminaremos todos os que ocupam a posição, múltipla de* 7*, restando*

$$1-3-7-9-13-15-21-25-27.$$

Por fim, eliminamos todos que ocupam a posição múltipla de 9*, obtendo*

$$1-3-7-9-13-15-21-25.$$

Obtemos então, a sequência de números da sorte entre os 30 *inteiros positivos.*

Definição 8.11 (Primos Primos)**.** *Os Primos Primos (cousin Primes) são pares de números primos cuja diferença entre eles é* 4*.*

Exemplo 8.12. *Os pares abaixo são da forma* $(p; p+4)$*.*

$$(3,7),(7,11),(13,17),(19,23),(37,41),(43,47),(67,71),(79,83),(97,101).$$

Duas propriedades importantes sobre esses pares:

- 7 é o único primo a fazer par com outros primos.
- Quaisquer que sejam três números consecutivos $(n, n+4, n+8)$ um deles sempre será divisível por 3, logo $n = 3$ é o único caso em que os três são primos.

9 PROPOSTA DIDÁTICA

No presente capítulo, faremos duas propostas didáticas com respeito ao foco do curso, a Rede Nacional de Ensino Básico.

- Proposta I - Blog
  Conhecendo a importância dos recursos de multimídia e levando em consideração o relevante acesso dos jovens às redes sociais, seja na necessidade de obtenção de conhecimento ou em busca de coisas interessantes, a proposta é de um blog que será alimentado ao longo do tempo com aspectos históricos e aritméticos dos números especiais aqui mencionados, com a finalidade de despertar o interesse de estudantes. Juntamente com o blog, será criado também um perfil no Instagram que será diretamente ligado ao blog, de maneira que atraia o interesse por meio de um desafio ou de uma pergunta atraente como "Você sabia?". Ao ler o conteúdo principal de forma resumida, poderá acessar o conteúdo detalhado, mais completo, que estará no blog.

  A princípio é algo direcionado ao nosso público alvo, os estudantes de nosso país, mas seu alcance poderá ser mundial, pois os motores de busca como Google sugere buscas de sites em outros países.

  O blog, já construído, se chama https://numerosespeciais.blogspot.com/. Nele encontramos esses conteúdos e sua ligação será o perfil do instagram numeros_especiais, no qual serão postadas curiosidades. Lembramos que o objetivo é ter o maior alcance possível em rede nacional e definimos os números especiais, bem como suas propriedades.

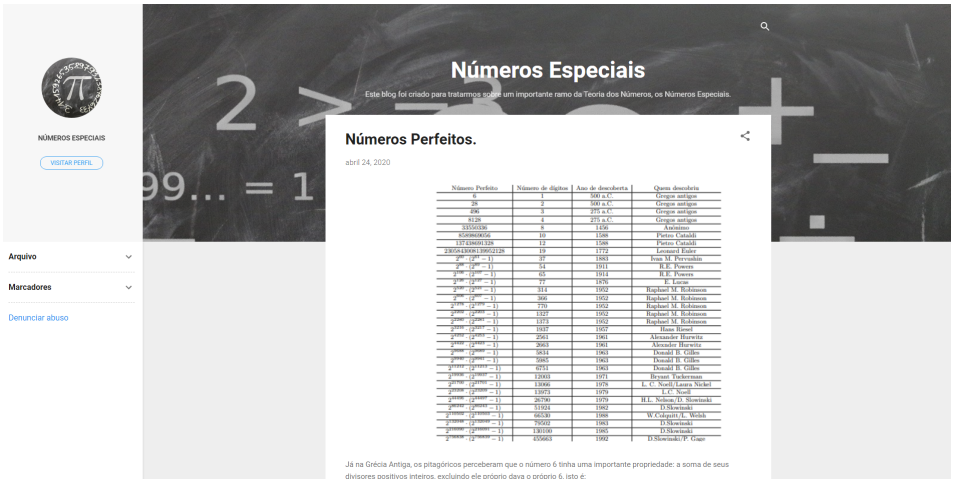

Figura 9: Blog Números Especiais.

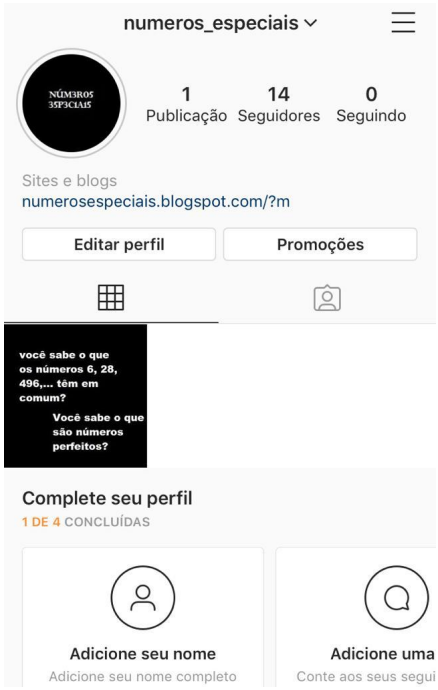

Figura 10: Perfil no Instagram numeros_especiais.

- Proposta II - Plano de aula
  A segunda proposta será de aplicação de aulas especiais, já que o conteúdo em si não aparece nos livros didáticos ou apostilas. Pretende-se usar dois tempos de aulas regulares, tendo um total cem minutos. O plano de aula será dividido nas seguintes partes:

  1- Introdução ao conteúdo (aproximadamente 25 minutos).
  Escolhido o número especial a ser trabalhado, podemos perguntar aos alunos que tipo de número seria, qual sua definição e, durante os primeiros minutos, eles poderão pesquisar no celular se estivermos em sala de aula, ou nos computadores da escola, se forem levados ao laboratório de informática (incluindo o blog). A partir daí, podemos contar um pouco de sua história, as primeiras menções e sua definição.

  2 - Desenvolvimento (aproximadamente 50 minutos).
  Nesta parte da aula, serão explanados alguns resultados, aos quais os próprios alunos poderão fazer testes por substituições diretas em fórmulas e construir pequenas tabelas para, em seguida, haver uma reflexão do comportamento da sequência construída, e podemos aproveitar o momento para que eles façam conjecturas. Dependendo do ano escolar que for trabalhado, muitos conceitos usados nas demonstrações já são de conhecimento como: somas de PGs, divisibilidade, Teorema Fundamental da Aritmética, etc. É possível desenvolver juntos tais demonstrações e, enfim, atingir resultados historicamente já construídos.

3 - Conclusão (aproximadamente 25 minutos).

Pretende-se que os alunos, dentro de suas reflexões, percebam o crescimento de tal sequência, a relação de paridade dos valores encontrados, e também o quão raros são esses resultados, e questionem sobre sua infinitude, bem como se fazem parte dos problemas abertos da Matemática atual, podendo o professor intervir nesses questionamentos num debate, apresentando resultados mais atualizados.

Exemplo 9.1 (Aula sobre Números Perfeitos)**.** *Aqui estará um roteiro para uma aula sobre Números Perfeitos.*

Dentro da proposta, começaremos a aula apresentando um importante ramo da Teoria dos Números: Os Números Especiais. É importante nesse momento que o aluno entenda que a Matemática apresenta mais ramos que os presentes em seus materiais. A partir daí, uma pergunta mais específica, se já ouviram falar de números perfeitos. Sem dizer seu significado, proporemos:

Atividade 9.2. *Fazer a soma dos divisores naturais dos números de* 1 *a* 10 *e observar quais deles têm a seguinte propriedade: a soma de seus divisores representa seu dobro. Espera-se que aluno conclua que somente o* 6 *obedece tal propriedade.*

Já podemos então apresentar os Números Perfeitos e a função $\sigma(n) = 2n$.

Atividade 9.3. *Qual seria o próximo número perfeito? Para que não se perca muito tempo, poderíamos criar um intervalo numérico fazendo uso de um software como Excel, por exemplo: "Está entre* 20 *e* 30*". Espera-se que o aluno encontre o resultado:* 28*.*

Como os números crescem rapidamente, podemos nesse momento sugerir que façam uma pesquisa por celular ou computador se estivermos no laboratório de informática da escola.

Atividade 9.4. *Pesquisar a sequência dos Números Perfeitos na internet. Sugestão: https://oeis.org/.*

A seguir, um exemplo de pesquisa.

Observando-se a sequência apresentada, esperam-se indagações sobre a infinitude, a existência de perfeitos ímpares, o algarismo da unidade dos números da sequência se alternarem em 6 e 8, existência de apenas um número perfeito por ordem de grandeza, desde quando é sabido da existência de números perfeitos.

Completando-se essa parte, faz-se necessária a introdução de seus aspectos históricos, e continua-se a pesquisa.

Atividade 9.5. *Pesquisar a história dos números perfeitos.*
Sugestão: https://numerosespeciais.blogspot.com/2020/04/numeros-perfeitos.html

Entendido e estudado a parte histórica, podemos então desenvolver os aspectos aritméticos construindo, por exemplo, o Teorema de Euclides-Euler e usar como atividade para determinar outros termos.

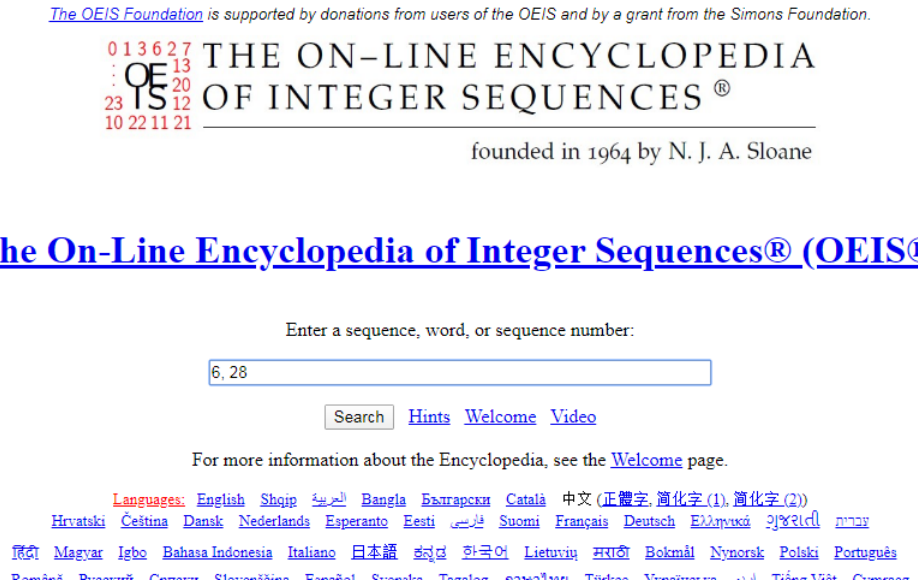

Figura 11: Pesquisa OEIS.

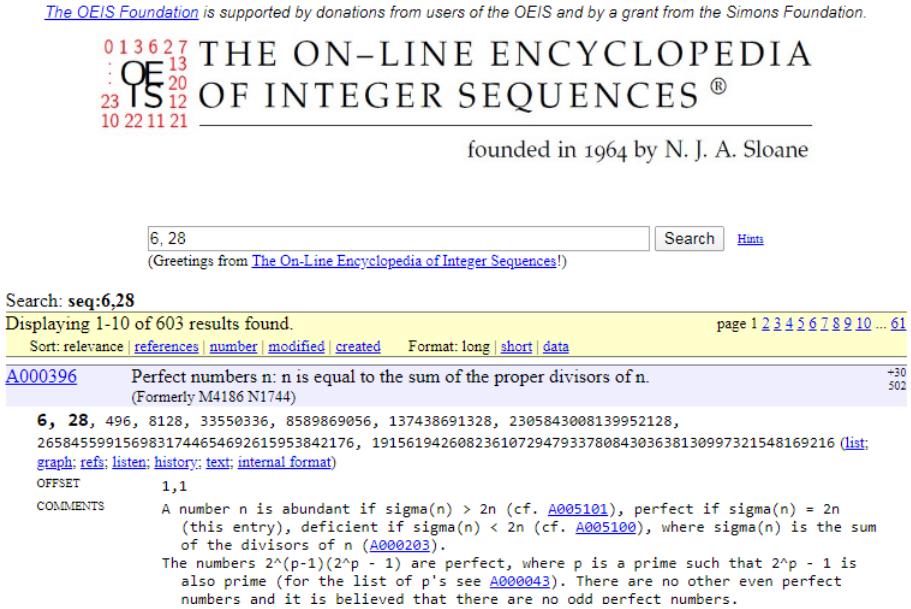

Figura 12: Resultado pesquisa OEIS.

Atividade 9.6. *Determine os seis primeiros números perfeitos usando o Teorema Euclides-Euler* $n = (2^{p-1})(2^p - 1)$*, em que* $2^p - 1$ *é um número primo (podendo-se usar calculadora).*

Este é um bom momento para mencionar os Números de Mersenne, já que o destacamos na atividade anterior, e reafirmar a necessidade de $2^p - 1$ ser primo.

Atividade 9.7. *Pesquisar sobre os Números de Mersenne. Sugestão:*

https://www.mersenne.org/.

A partir daqui, podemos concluir a aula expondo a questão da ordem de grandeza dos últimos números encontrados, e incentivá-los a apresentar como um problema aberto da Matemática.

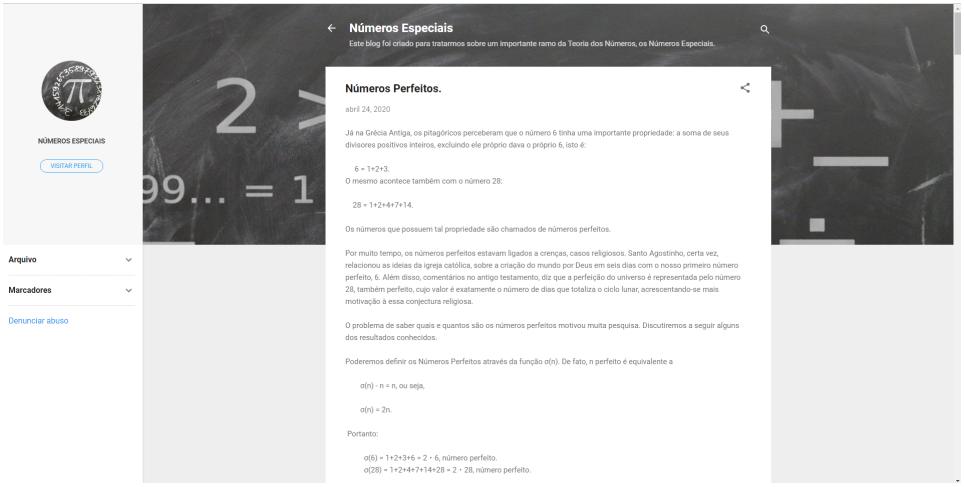

Figura 13: Blog Números Especiais.

Figura 14: https://www.mersenne.org/.

1

CONCLUSÃO

Vimos aqui a importância de certos números especiais, suas propriedades, suas histórias, algumas curiosidades, suas demonstrações. Portanto, ao apresentar sua importância aritmética, pretende-se difundir e despertar a curiosidade aos estudantes, de forma que entendam a relevância desse importante ramo da Teoria dos Números, e quem sabe, torná-los futuros contribuintes com mais resultados para avançarmos. Os problemas em aberto servem como incentivo e desafio para mostrar que a Matemática não está totalmente pronta e desenvolvida, tanto que apresentamos resultados que foram provados há séculos e outros, como os números perfeitos e primos sensuais, obtidos recentemente.

Uma das contribuições mais relevantes deste trabalho, acreditamos, é o de termos exposto tanto a evolução histórica quanto os resultados matemáticos de importantes famílias de números. Foram mencionados resultados obtidos ao longo dos séculos e também alguns recentes, que demandaram o uso de recursos computacionais.

Não podemos deixar de mencionar a existência de mais categorias de números especiais para além daqueles apresentados aqui. A lista é extensa, mas acreditamos que, com base nos números aqui, apresentados já temos uma boa base para o desenvolvimento da proposta didática em sala de aula, o que será enormemente ajudado pelo site e pelo blog, uma vez que não encontramos muitas referências sobre este assunto em língua portuguesa.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] L. E. Dickson, History of the Theory of Numbers, Vol. I: Divisibility and Primality. Dover Publications, 2005.

[2] G. H. Hardy, E. M. Wright, An Introduction to the Theory of Numbers, 6 Ed. Oxford University Press, 2008.

[3] Hefez, A., Aritmética, Coleção PROFMAT, SBM, 2014.

[4] Martinez, F. B., Moreira, C. G., Saldanha, N., Tengan, E., Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro, IMPA, 2010.

[5] P. Ribenboim, My numbers, my friends. Springer, 2000.

[6] P. Ribenboim, The Little Book of Bigger Primes, 2 Ed. Springer, 2004.

[7] S. Shokranian, Uma breve história da Teoria dos Números no século vinte. Editora Ciência Moderna, 2010.

[8] https://oeis.org/A000396, acessado no dia 27/07/2019.

[9] David M. Burton, Elementary Number Theory. Allyn and Bacon, 1980.

[10] http://clubes.obmep.org.br/blog/wp-content/uploads/2016/02/PERFEITOS_final.pdf, acessado em 14/08/2019.

[11] https://www.mersenne.org/, acessado em 02/08/2019.

[12] Leonhard Euler, Sobre Números Amigáveis, Volume 9, Arquivo para História da Teoria dos Números e Lógica, edufrn.

[13] https://oeis.org/A063990/b063990.txt acessado em 07/12/2019.

[14] https://oeis.org/A057755, acessado no dia 02/01/2020.

[15] https://oeis.org/A000032, acesssado no dia 03/01/2019.

[16] https://oeis.org/A000045,acesssado no dia 03/01/2019.

[17] https://oeis.org/A005479, acessado no dia 03/01/2019.

[18] James J. Tattersall, Elementary Number Theory in Nine Chapters, Cambrigde University Press, 1999.

[19] https://oeis.org/A023201, acessado em 19/01/2020.

[20] https://www.mersenneforum.org/showpost.php?p=527198&postcount=37, acessado em 20/01/2020.

[21] https://oeis.org/A077800, acessado em 20/01/2020.

[22] http://www.lirmm.fr/ ochem/opn/opn.pdf, acessado em 02/08/2019.

[23] https://oeis.org/A019434/list, acessado 22/01/2020.

[24] "Sequências de Fibonacci, Lucas e Pell". Dissertação PROFMAT Paulo Henrique Joca de Sá Barreto - UFCA Juazeiro do Norte - 2019. https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?id=170172257

[25] "Números de Fibonacci e números de Lucas". Dissertação PROFMAT, Bruno Astrolino e Silva - USP São Carlos - 2017. https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?id=73922

[26] David M. Burton, The History of Mathematics an introduction. 7ª edição, The McGraw-Hill Companies 1999.

[27] https://oeis.org/A000110. Acessado em 20/03/2020.

[28] Nicholas A. Loehr, bijective Combinatorics, CRC Press Taylor Francis Group, 2011.

[29] Elon L. Lima, Paulo Cezar P. Carvalho, Eduardo Wagner, Augusto César Morgado, A Matemática do Ensino Médio. Volume 2, Coleção do Professor de Matemática, SBM.

[30] https://oeis.org/A005846. Acessado em 11/04/2020.