Universidade do Estado do Rio de Janeiro
Centro de Tecnologia e Ciências
Instituto de Matemática e Estatística

Victor Gomes Cerqueira

Sobre números perfeitos e quase perfeitos

Rio de Janeiro
2023

Victor Gomes Cerqueira

Sobre números perfeitos e quase perfeitos

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, da Universidade do Estado do Rio de Janeiro.

Orientador: Prof. Dr. Ruben Lizarbe Monje

Rio de Janeiro

2023

CATALOGAÇÃO NA FONTE

UERJ / REDE SIRIUS / BIBLIOTECA CTC-A

C416 Cerqueira, Victor Gomes.
Sobre números perfeitos e quase perfeitos/ Victor Gomes Cerqueira. – 2023.
76 f.: il.

Orientador: Ruben Lizarbe Monje
Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade do Estado do Rio de Janeiro, Instituto de Matemática e Estatística.

1. Teoria dos números - Teses. I. Monje, Ruben Lizarbe. II. Universidade do Estado do Rio de Janeiro. Instituto de Matemática e Estatística. III. Título

CDU 511

Patricia Bello Meijinhos CRB7/5217 - Bibliotecária responsável pela elaboração da ficha catalográfica

Victor Gomes Cerqueira

Sobre números perfeitos e quase perfeitos

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, da Universidade do Estado do Rio de Janeiro.

Aprovada em 28 de março de 2023.
Banca Examinadora:

Prof. Dr. Ruben Lizarbe Monje (Orientador)
Instituto de Matemática e Estatística – UERJ

Prof. Dr. Guido Gerson Espiritu Ledesma
Instituto de Matemática e Estatística - UERJ

Prof. Dr. Hernan Maycol Falla Luza
Universidade Federal Fluminense - UFF

Rio de Janeiro
2023

DEDICATÓRIA

À minha mãe Vânia, à minha esposa Patrícia e à minha filha Alice e meu filho Arthur (que está sendo gerado no ventre de minha esposa).

AGRADECIMENTOS

À Deus, meu refúgio e fortaleza, pelo dom da vida, pela sabedoria advinda do alto e por adestrar minhas mãos nas horas em que achei que não fosse conseguir.

À minha mãe Vânia, por todo amor, dedicação e por nunca medir esforços para me proporcionar bons estudos.

À minha esposa Patrícia, por acreditar em minha capacidade mesmo nos meus momentos de fraqueza e me encorajar a chegar até o final.

À minha filha Alice, minha inspiração a prosseguir, por quem sempre darei o meu melhor e deixarei meu legado.

Ao Professor Doutor Ruben, meu orientador, por todo profissionalismo e apoio, pela sua humildade cativante, por sua paciência e pelos ensinamentos.

Aos amigos mais chegados que irmãos, Gilson e Fabrício, com quem dividimos momentos de angústia e também de alegrias nessa caminhada durante o PROFMAT e que muito me ajudaram e incentivaram nos momentos de dificuldade.

Bendito seja o Senhor, minha rocha, que adestra as minhas mãos para a peleja e os meus dedos para a guerra. Salmos 144.1

RESUMO

CERQUEIRA, Victor Gomes. **Sobre números perfeitos e quase perfeitos**. 2023. 76 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Instituto de Matemática e Estatística, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2023.

Este trabalho foi idealizado visando mostrar que a matemática é uma ciência em constante evolução e que, desta maneira, desperta e aguça a curiosidade de todos que se debruçam a desvendá-la. Inicialmente, apresentamos noções básicas de divisibilidade mostrando suas principais propriedades, passando pelos números primos com todo o seu mistério e estudos desenvolvidos. Posteriormente falamos de uma classe de números especiais, a saber, os números perfeitos e números quase perfeitos, apresentando estudos bem recentes que estão sendo desenvolvidos, bem como questões em aberto a respeito do tema. Assim, procuramos despertar nos professores e alunos leitores o interesse pelo assunto e mostrar que eles podem fazer parte deste processo de descobertas a respeito do tema.

Palavras-chave: Números perfeitos. Números quase perfeitos. .

ABSTRACT

CERQUEIRA, Victor Gomes. **About perfect and near perfect numbers**. 2023. 76 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Instituto de Matemática e Estatística, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2023.

This work was conceived with the aim of showing that mathematics is a science in constant evolution and that, in this way, it awakens and sharpens the curiosity of all those who dedicate themselves to unraveling it. Initially, we present basic notions of divisibility showing its main properties, going through prime numbers with all their mystery and developed studies. Later we talk about a class of special numbers, namely, perfect numbers and near perfect numbers, presenting very recent studies that are being developed, as well as open questions about the subject. Thus, we seek to awaken interest in the subject in teachers and student readers and show that they can be part of this process of discoveries on the subject.

Keywords: Perfect numbers. Near perfect numbers. .

LISTA DE ILUSTRAÇÕES

SUMÁRIO

INTRODUÇÃO

Os números e o procedimento de contagem foram desenvolvidos a partir da necessidade do homem primitivo em saber quantos membros possuía o seu clã ou até quantos animais possuía seu rebanho. Acredita-se que as primeiras técnicas de contagem utilizavam o princípio da correspondência biunívoca, fazendo uso de riscos ou traços no barro ou em pedras. Desta maneira, com o desenvolvimento da comunicação através de sons e do consequente desenvolvimento da escrita, ao longo do tempo, foram utilizados símbolos para representar números. Neste processo histórico do estudo de maneiras de quantificar coisas e, consequentemente, do desenvolvimento dos números, temos na obra "Os Elementos", de Euclides (360 a.C – 295 a.C) os conceitos de números pares, números impares, números primos e números compostos e podemos considerar Pierre de Fermat (1601-1605) como o fundador da moderna teoria dos números. Assim, até os dias atuais os estudos sobre teoria dos números continuam despertando o interesse de muitos estudiosos do tema, mostrando que a matemática está em constante evolução sendo, portanto, uma ciência viva. Podemos afirmar que a natureza está impregnada de conceitos matemáticos.

Iniciamos este trabalho mostrando os conceitos básicos de divisibilidade com seus principais teoremas e definições que servirão de base para os assuntos tratados em seguida. Falaremos em seguida sobre os números primos e a incansável busca por uma fórmula que defina o padrão de ocorrência de tais números por matemáticos como Pierre de Fermat, Leonhard Euler (1707 – 1783), Marin Mersenne (1588-1648) entre outros além de algumas proposições que tratam do assunto. A partir do capítulo 4 trataremos sobre uma classe de números especiais, a saber, os números perfeitos que apesar de serem atribuídos aos matemáticos pitagóricos, foi na obra "Os Elementos" de Euclides, citada anteriormente, que essa classe de números ganhou notoriedade quando Euclides estabelece uma fórmula para encontrá-los. Outro tipo de números especiais, relacionados com os números perfeitos e estudados recentemente são os números quase perfeitos. O conceito destes números serão apresentados ao leitor bem como os teoremas recém enunciados com suas demonstrações e servirão de inspiração para que professores de matemática do ensino fundamental e médio estimulem seus alunos a participarem desta evolução da matemática com questionamentos e ideias que possam contribuir cada vez mais e tornar o estudo da matemática mais atraente. Desta maneira, ao ser apresentado em sala de aula, podemos fornecer aos estudantes o lado investigativo da matemática despertando nos mesmos o interesse pelo assunto e inserindo o aluno no processo de aprendizagem, modificando a maneira como a matemática tradicionalmente é ensinada. O objetivo deste trabalho é dar subsídios para os professores de matemática do ensino fundamental e médio para trabalharem os conceitos apresentados com seus alunos além de estimular nos mesmos o interesse pela matemática, dada como uma ciência em constante evolução, mostrando que seus alunos

podem e devem fazer parte deste processo de construção do conhecimento. Dessa forma, desconstruir o pensamento errôneo de que a matemática é apenas uma mera repetição de fórmulas.

1 NÚMEROS NATURAIS

As origens dos números naturais vêm da necessidade de contar objetos, iniciando, portanto, do número um. O uso de numerais representando os números naturais permitiu aos povos antigos desenvolverem técnicas e sistemas capazes de armazenar grandes números, como os babilônicos e os egípcios. Uma construção através de uma estrutura simples do conjunto dos números naturais, foi fornecida no século XIX por Giuseppe Peano (1858-1932), chamada de Axiomas de Peano.

1.1 Axioma de Peano

Giuseppe Peano (1858-1932) elaborou 4 axiomas, conhecidos como axiomas de Peano que sintetizam as propriedades fundamentais dos números naturais de onde surgem todas as afirmações que se podem concluir sobre os naturais. Vejamos a seguir os axiomas de Peano, segundo o autor Elon Lages Lima [1], em uma linguagem mais simples e acessível:

1. Todo número natural possui um único sucessor, que também é um número natural;
2. Números naturais diferentes possuem sucessores diferentes. Números que têm o mesmo sucessor são iguais;
3. Existe um único número natural que não é sucessor de nenhum outro. Este número é representado pelo símbolo 1 e chamado de"número um".
4. Se um conjunto de números naturais contém o número 1 e, além disso, contém o sucessor de cada um de seus elementos, então esse conjunto coincide com $\mathbb{N}$, isto é, contém todos os números naturais.

A seguir, veremos algumas propriedades dos naturais, mas antes apresentaremos as definições não formais da adição e da multiplicação dos números naturais, bem como a relação de ordem. Ao leitor que queira verificar as definições formais, recomendamos o livro Fundamentos de Aritmética de Hygino H. Domingues [2], o livro Elementos de Aritmética de Abramo Hefez [3] e o livro Teoria elementar dos números de Edgard de Alencar Filho [4].

Soma dos números naturais: Dados $n, p \in \mathbb{N}$, definimos a soma $n + p$ da seguinte forma recursiva:

1. $s(n) := n + 1$;
2. $n + (p + 1) := (n + p) + 1$.

Multiplicação dos números naturais: Dados $n, p \in \mathbb{N}$, definimos o produto $n \cdot p$ da seguinte forma recursiva:

1. $n \cdot 1 := n$;
2. $n \cdot (p+1) := n \cdot p + n$.

Relação de ordem: Dados $n, p \in \mathbb{N}$ dizemos que m é menor do que n e denotamos por $m < n$ se existe $p \in \mathbb{N}$ tal que $n = m + p$. Também dizemos que que m é menor ou igual do que n e denotamos por $m \leq n$ se $m < n$ ou $m = n$. Analogamente podemos definir as relações maior ($>$) e maior ou igual ($\geq$) de dois números naturais.

Eis as propriedades dos números naturais:

1. *Associatividade da adição:* Dados $m, n, p \in \mathbb{N}$, temos $m + (n + p) = (m + n) + p$.
   Prova: Se $p = 1$; $m + (n + 1) = (m + n) + 1$. Supomos válido para $p = k$, isto é, $m + (n + k) = (m + n) + k$. Provaremos que é válido para $p = k + 1$, ou seja, $m+(n+(k+1)) = (m+n)+(k+1)$. Assim, $m+(n+(k+1)) = m+((n+k)+1) = (m + (n + k)) + 1 = ((m + n) + k) + 1 = (m + n) + (k + 1)$.

2. *Comutatividade da adição:* Dados $m, n \in \mathbb{N}$, temos $m + n = n + m$.
   Prova: para $n = 1$, temos que $m + 1 = 1 + m$. (m e 1 são comutáveis que pode ser demonstrado por indução em n). Supomos válido para $n = k$, isto é, $m+k = k+m$. Provaremos que é válido para $n = k+1$, ou seja, $m + (k+1) = (k+1) + m$. Assim, $m+(k+1) = (m+k)+1 = (k+m)+1 = k+(m+1) = k+(1+m) = (k+1)+m$.

3. *Distributividade da multiplicação:* Dados $m, n, p \in \mathbb{N}$, temos $m \cdot (n+p) = m \cdot n + m \cdot p$.
   Prova: Pela definição é válido para $p = 1$, isto é, $m \cdot (n+1) = m \cdot n + m \cdot 1$. Supomos válido para $p = k$, ou seja, $m \cdot (n + k) = m \cdot n + m \cdot k$. Provemos ser válido para $n = k+1$: $m \cdot (n+(k+1)) = m \cdot ((n+k)+1) = m \cdot (n+k)+m = (m \cdot n+m \cdot k)+m = m \cdot n + (m \cdot k + m \cdot 1) = m \cdot n + m \cdot (k + 1)$.

4. *Comutatividade da multiplicação:* Dados $m, n \in \mathbb{N}$, temos $m \cdot n = n \cdot m$.
   Prova: Para $n = 1$, temos $m \cdot 1 = 1 \cdot m$. Supomos válido para $n = k$, ou seja, $m \cdot k = k \cdot m$. Vamos provar que é válido para $n = k+1$:$m \cdot (k+1) = m \cdot k + m \cdot 1 = k \cdot m + 1 \cdot m = (k + 1) \cdot m$.

5. *Associatividade da multiplicação:* Dados $m, n, p \in \mathbb{N}$, temos $m \cdot (n \cdot p) = (m \cdot n) \cdot p$.
   Prova: para $p = 1$, temos que $m \cdot (n \cdot 1) = m \cdot n = (m \cdot n) \cdot 1$. Supomos válido para $p = k$, isto é, $m \cdot (n \cdot k) = (m \cdot n) \cdot k$. Provaremos que é válido para $p = k + 1$, ou seja, $m \cdot (n \cdot (k + 1)) = (m \cdot n) \cdot (k + 1)$. Assim, $m \cdot (n \cdot (k + 1)) = m \cdot ((n \cdot k) + n) = (m \cdot (n \cdot k)) + m \cdot n = ((m \cdot n) \cdot k) + m \cdot n = (m \cdot n) \cdot (k + 1)$.

6. *Lei do corte para adição:* Dados $m, n, p \in \mathbb{N}$ e $m + p = n + p$, logo $m = n$.
   Prova: Para $p = 1$, $m + 1 = n + 1$, logo $m = n$. Temos que $s(m) = m + 1$, mas pela hipótese $s(m) = n + 1$. Mas $s(n) = n + 1$, assim m e n têm os mesmo sucessores. Pela identidade da sucessão, $m = n$. Vamos supor válido para $p = k$, ou seja, $m + k = n + k$, logo $m = n$. Vamos mostrar que também é válido para $p = k + 1$: $m + (k + 1) = n + (k + 1)$. Mas, $s(m + k) = s(n + k)$, implica que $m + k = n + k$ e pela hipótese indutiva $m = n$.

7. *Recíproca da Lei do corte para adição:* Dados $m, n, p \in \mathbb{N}$ e $m = n$, logo $m+p = n+p$.
   Prova: É válido para $p = 1$, ou seja, $m = n$, logo $s(m) = s(n)$, ou seja, $m+1 = n+1$. Vamos supor válido para $p = k$, ou seja, $m = n$, então $m+k = n+k$. Vamos mostrar que é válido para $p = k + 1$: $m + (k + 1) = (m + k) + 1 = (n + k) + 1 = n + (k + 1)$.

8. *Lei do corte para multiplicação:* Dados $m, n, p \in \mathbb{N}$ e $m \cdot p = n \cdot p$, logo $m = p$.
   Prova: É válido para $p = 1$, ou seja, $m \cdot 1 = n \cdot 1$, então $m = n$. Vamos supor válido para $p = k$, ou seja, $m \cdot k = n \cdot k$. Vamos mostrar que é válido para $p = k + 1$, vejamos $m \cdot (k + 1) = m \cdot k + m \cdot 1 = n \cdot k + n \cdot 1 = n \cdot (k + 1)$, então $m = n$.

9. *Transitividade da relação de ordem:* Dados $m, n, p \in \mathbb{N}$ tais que $m < n$ e $n < p$ tem-se que $m < p$.
   Prova: Vamos fazer $n = m+k_1$ e $p = n+k_2$. Então $p = m+k_1+k_2 = m+(k_1+k_2)$, implicando em $m < p$.

10. *Tricotomia:* Dados $m, n \in \mathbb{N}$ ocorre uma, e somente uma, das três possibilidades: $m = n$; ou $m < n$; ou $m > n$.

    Prova: Primeiro provaremos que só uma das três possibilidades verifica. Se tivéssemos $m < n$ e $m = n$, então seria $m = m + p$, donde $m + 1 = m + p + 1$ e, cortando m, concluiríamos que $1 = p + 1$, um absurdo, pois 1 não é sucessor de p. Portanto $m < n$ (e analogamente, $n < m$) é incompatível com $m = n$. Do mesmo modo, se tivéssemos $m < n$ e $n < m$, então teríamos $n = m + p$ e $m = n + k$, do que resultaria $n = n + k + p$, logo $n + 1 = n + k + p + 1$ e, cortando n, concluiríamos que $1 = k + p + 1$, um absurdo.
    Vamos verificar a tricotomia pelo Princípio da indução, provando que $I = \mathbb{N}$, considerando o conjunto $I = \{n \in \mathbb{N} |\ m = n$; ou $m < n$; ou $m > n\}$. Vamos provar que $1 \in I$ para todo $n \in \mathbb{N}$, temos a dicotomia: $n = 1$ ou $n \neq 1$, onde $n \neq 1$ implica que $n > 1$, logo a tricotomia não vale se, e somente se, $n > 1$ implica $n \neq 1$, pois neste caso, $n = 1$ ou $n > 1$, é uma dicotomia equivalente a anterior. Mas se $n > 1$ implica que $1 + p = n$ para algum $p \in \mathbb{N}$, logo $n = 1 + p = s(p)$ para o mesmo p. Portanto n é sucessor de p, o que implica, pelos axiomas de Peano, que $n \neq 1$. Agora, vamos provar que para todo $a \in I$, $s(a) \in I$. Tome $n \in \mathbb{N}$, se $n = 1$, pelos

axiomas de Peano, temos que $s(a) \neq 1$, logo $s(a) > n$ que é a única possibilidade. Se $n \neq 1$, então $n = s(c) = c + 1$ para algum $c \in \mathbb{N}$ (também pelos axiomas de Peano), pela propriedade do corte, temos que $n < a + 1$, $n = a + 1$ e $n > a + 1$, são respectivamente, equivalentes a $c < a$, $c = a$ e $c > a$. Como $a \in I$, estas três últimas possibilidades são tricotômicas, de modo que $n < a + 1$, $n = a + 1$ e $n > a + 1$, também serão. Portanto, concluímos que $s(a) = a = 1 \in I$.

11. *Monotonicidade:* Se $m, n \in \mathbb{N}$ são tais que $m < n$, então

$$m + p < n + p \text{ e } m \cdot p < n \cdot p,$$

para qualquer $p \in \mathbb{N}$.
Prova: Tomando $n = m + k$, temos

(a) $n + p = (m + k) + p = (m + p) + k$, logo $m + p < n + p$;

(b) $n \cdot p = (m + k) \cdot p = m \cdot p + k \cdot p$, logo $m \cdot p < n \cdot p$

12. *Lei do corte para desigualdades:* Dados $m, n, p \in \mathbb{N}$, de modo que $m + p < n + p$ ou que $m \cdot p < n \cdot p$, então ocorre em ambas que $m < n$.
Prova: Como $m + p < n + p$, pela definição de ordem, existe um q natural tal que $m + p + q = n + p$. Pela comutatividade da adição, $m + q + p = n + p$. Pela lei do corte da adição, $m + q = n$, e pela relação de ordem entre dois números, $m < n$.

Sabemos da tricotomia que dados m, n naturais temos: $m = n$ ou $m < n$ ou $n < m$. Então, caso $m = n$, logo $m \cdot p = n \cdot p$ (não atende nossa hipótese). Caso $n < m$, logo pela monotonicidade temos que $n \cdot p < m \cdot p$, para qualquer p natural (também não atende a nossa hipótese). Logo $m < n$, pois as outras duas possibilidades são incompatíveis com a nossa hipótese e pela tricotomia uma das três comparações é verdade.

A seguir, vamos provar uma outra versão do quarto axioma de Peano, conhecido como princípio da indução.

Teorema 1.1 (Princípio da Indução Finita)**.** *Seja $a \in \mathbb{N}$ e seja $P(n)$ uma sentença aberta em n. Suponha que:*

1. *$P(a)$ é verdadeira, e que;*
2. *Para todo $n \geqslant a$, $P(n)$ implica $P(n+1)$ seja verdadeira, então, $P(n)$ é verdade para todo $n \geqslant a$.*

Demonstração. Se $a = 1$, então segue do axioma (ou princípio) da indução. Suponha que $a > 1$, nesse caso definimos o seguinte conjunto

$$A = \{1, \ldots, a - 1\} \cup \{n \in \mathbb{N} | \, P(n) \text{ é verdadeira}\}.$$

Podemos ver $1 \in A$. Também, pelo item 2. podemos ver que se $n \in A$, então $n+1 \in A$. Portanto pelo axioma da indução podemos concluir que $A = \mathbb{N}$. □

Exemplo 1.1. Vamos usar o método da indução finita para provar que a soma:

$$S_n = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{n \cdot (n+1)} = \frac{n}{n+1}$$

é verdadeira para todo natural $n \geqslant 1$.

Resolução: Para $n = 1$ a afirmação é verdadeira, pois: $S_1 = \frac{1}{2} = \frac{1}{1+1}$. Suponhamos que a afirmação seja verdadeira para $n = k$, ou seja,

$$S_k = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{k \cdot (k+1)} = \frac{k}{k+1}$$

e vamos provar que a afirmação é verdadeira para $n = k+1$, ou seja,

$$S_{k+1} = \frac{k+1}{k+1+1} = \frac{k+1}{k+2}.$$

De fato,

$$S_{k+1} = \underbrace{\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{k \cdot (k+1)}}_{S_k} + \frac{1}{(k+1) \cdot (k+2)} = S_k + \frac{1}{(k+1) \cdot (k+2)}.$$

Por hipótese de indução, temos:

$$S_{k+1} = \frac{k}{k+1} + \frac{1}{(k+1) \cdot (k+2)} = \frac{k^2 + 2 \cdot k + 1}{(k+1) \cdot (k+2)} = \frac{(k+1)^2}{(k+1) \cdot (k+2)} = \frac{k+1}{k+2}$$

Portanto, com base no Princípio de Indução Matemática, podemos afirmar que $S_n = \frac{n}{n+1}$, para todo natural $n \geqslant 1$.

Teorema 1.2 (Princípio da Boa Ordenação)**.** *Todo subconjunto A não vazio dos números naturais possui um menor elemento.*

Demonstração. Vamos analisar dois casos: Primeiro caso, se $1 \in A$, então 1 seria o menor elemento de A.
No outro caso teríamos que $1 \notin A$. Definimos o seguinte conjunto

$$M = \{n \in \mathbb{N} \,|\, 1 \notin A, \ldots, n \notin A, \}.$$

Temos que $1 \in M$, pois $1 \notin A$, logo, $M \neq \emptyset$. Como $A \neq \emptyset$, então $M \neq \mathbb{N}$. Logo M não verifica as hipótese do Princípio da Indução e portanto existe $m \in M$ tal que $(m+1) \notin M$, isto é, $1 \notin A, \ldots, m \notin A$ e $(m+1) \in A$. Assim, concluímos que $m+1$ é o menor elemento de A. □

Exemplo 1.2. Usando o Princípio da Boa Ordenação, mostre que

$$S_n = \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n\cdot(n+1)} = \frac{n}{n+1}$$

para todo natural $n \geqslant 1$.

Resolução: Seja $F = \{n \in \mathbb{N} : S_n \neq \frac{n}{n+1}\}$. Desejamos mostrar que $F = \emptyset$. Em efeito, suponha por contradição que $F \neq \emptyset$. Assim, pelo Princípio da Boa Ordenação 1.2, existe $a \in F$ tal que a é o menor elemento de F. Como $a \in F$ temos que $S_a \neq \frac{a}{a+1}$ e $a > 1$, pois $S_1 = \frac{1}{2} = \frac{1}{1+1}$, o que implica que $1 \notin F$. Sendo a o menor elemento de F então $(a-1) \notin F$, isto é,

$$S_{a-1} = \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{(a-1)\cdot a} = \frac{a-1}{a}.$$

Assim, temos:

$$S_a = S_{a-1} + \frac{1}{a\cdot(a+1)} = \frac{a-1}{a} + \frac{1}{a\cdot(a+1)} = \frac{(a-1)\cdot(a+1)+1}{a\cdot(a+1)} = \frac{a}{a+1}.$$

Mas isso contradiz $S_a \neq \frac{a}{a+1}$. Portanto $F = \emptyset$ e concluímos que não existe $n \in \mathbb{N}$ tal que $S_n \neq \frac{n}{n+1}$, ou seja, $S_n = \frac{n}{n+1}$, para todo natural $n \geqslant 1$.

Teorema 1.3 (Princípio da Indução Forte)**.** *Seja a proposição $P(n)$ para cada natural $n \geqslant n_0$, com n_0 natural, que satisfaz as condições:*

1. *$P(n_0)$ é verdadeira, e que;*
2. *para todo $k > n_0$, tem-se para cada m natural tal que $n_0 \leqslant m < k$, se $P(m)$ é verdadeira, então $P(k)$ também é verdadeira.*

Então, $P(n)$ é verdadeira para todo $n \geqslant n_0$.

Demonstração. Seja $A = \{n \in \mathbb{N} |\ n \geqslant n_0$ e $P(n)$ é falsa$\}$. Por verificar que $A = \emptyset$. Em efeito, suponha por contradição que $A \neq \emptyset$, então pelo Princípio da Boa Ordenação (Teorema 1.2) temos que existe a o menor elemento de A, o que garante $a \in A$ ($a \geqslant n_0$ e $P(a)$ falsa). Como $P(n_0)$ é verdadeira, então $n_0 \notin A$, logo como $a \in A$ temos que $a \neq n_0$. De $a \geqslant n_0$ e $a \neq n_0$, concluímos que $a > n_0$. Como a é o menor elemento de A, devemos ter $P(m)$ verdadeira para todo m com $n_0 \leqslant m < a$. Aplicando o Item 2. concluímos que $P(a)$ é verdadeira, logo, $a \notin A$, gerando uma contradição. Logo, $A = \emptyset$, isto é, $P(n)$ é verdadeira para todo $n \geqslant n_0$. □

Exemplo 1.3. Considere a sequência de Fibonacci

$$1, 1, 2, 3, 5, 8, 13, 21, \ldots$$

onde cada elemento, a partir do terceiro, é a soma dos dois anteriores.

Se denotarmos por $F(n)$ o n-ésimo termo desta sequência, podemos defini-la por:

$$F(1) = 1$$
$$F(2) = 1$$
$$F(n) = F(n-2) + F(n-1), \text{ se n}\geqslant 3.$$

Mostre que $F(n) < \left(\frac{7}{4}\right)^n$, para todo natural $n \geqslant 1$.

Resolução: Vamos a tentar solucionar pelos dois princípios vistos:

1. *Utilizando o Princípio da Indução Finita:* Seja $P(n)$ a afirmativa: $F(n) < \left(\frac{7}{4}\right)^n$, $n \geq 1$. Temos que P(1) e P(2) são verdadeiras pois $F(1) < \frac{7}{4}$ e $F(2) = 1 < \left(\frac{7}{4}\right)^2$. Seja $k \geqslant 2$ e suponhamos que $P(k)$ seja válida, isto é, $F(k) < \left(\frac{7}{4}\right)^k$. Devemos mostrar que $F(k+1) < \left(\frac{7}{4}\right)^{(k+1)}$. Como $k+1 \geqslant 3$ então
   $F(k+1) = F(k-1) + F(k)$ e não fica claro como obter a desigualdade desejada a partir da hipótese de indução. Observe que $F(k-1) \leqslant F(k)$ e então

$$\begin{aligned} F(k+1) &= F(k-1) + F(k) \\ &\leqslant F(k) + F(k) \\ &< 2 \cdot \left(\frac{7}{4}\right)^k \\ &= \frac{8}{7} \cdot \left(\frac{7}{4}\right)^{(k+1)} \end{aligned}$$

   que é uma cota maior que a desejada. Então podemos concluir que nem sempre podemos resolver usando este princípio.

2. *Utilizando o Princípio da Indução Forte:* Já vimos que $P(1)$ e $P(2)$ são verdadeiras. Seja $k \geqslant 2$ e suponhamos $P(m)$ verdadeira para todo natural m, $1 \leqslant m \leqslant k$. Precisamos mostrar que $P(k+1)$ é verdadeira, ou seja, $F(k+1) < \left(\frac{7}{4}\right)^{(k+1)}$. Como $F(k+1) = F(k-1) + F(k)$ e, por hipótese de

indução, $F(k) < \left(\frac{7}{4}\right)^k$ e $F(k-1) < \left(\frac{7}{4}\right)^{(k-1)}$, então

$$\begin{aligned} F(k+1) &= F(k-1) + F(k) \\ &< \left(\frac{7}{4}\right)^{k-1} + \left(\frac{7}{4}\right)^k \\ &= \frac{4}{7} \cdot \left(\frac{7}{4}\right)^k + \left(\frac{7}{4}\right)^k \\ &= \frac{11}{7} \cdot \left(\frac{7}{4}\right)^k \\ &< \frac{7}{4} \cdot \left(\frac{7}{4}\right)^k = \left(\frac{7}{4}\right)^{k+1} \end{aligned}$$

Exemplo 1.4. Dois termos da sequência de Fibonacci são primos entre si.

Resolução: Na resolução deste exercício vamos considerar o conceito de mdc que será apresentado de maneira mais detalhada no capítulo 2, seção 2.3. Vamos mostrar, pelo princípio da indução, que $\text{mdc}(F_{n+1}; F_n) = 1$. De fato, para $n = 1$, temos que $\text{mdc}(F_2, F_1) = \text{mdc}(1, 1) = 1$. Suponhamos que o resultado seja válido para algum n, isto é, $\text{mdc}(F_{n+1}, F_n) = 1$. Assim,

$$\text{mdc}(F_{n+2}, F_{n+1}) = \text{mdc}(F_{n+2} - F_{n+1}, F_{n-1}) = \text{mdc}(F_n, F_{n+1}) = 1,$$

o que demonstra o resultado.

Exemplo 1.5. Para $n \geqslant 1$, $F_{n-1} \cdot F_{n+1} - F_n^2 = (-1)^n$ *(Identidade de Cassini).*

Resolução: Provando por indução em n. De fato, para $n = 1$, temos $F_0 \cdot F_2 - F_1^2 = 0 \cdot 1 - 1^2 = -1$. Suponhamos que seja válida para algum $n \geqslant 1$. Provemos que também é válida para $n + 1$.

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

2 DIVISIBILIDADE

Veremos a seguir como se dá a divisão entre dois números naturais, através do algoritmo de Euclides, e as propriedades do máximo divisor comum (MDC) e do mínimo múltiplo comum (MMC), além de importantes proposições.

2.1 Divisão no conjunto dos números naturais

Dados dois números naturais a e b, dizemos que a *divide* b ou que a é um *divisor* de b ou ainda que b é um *múltiplo* de a e escrevemos $a \mid b$, se existir $c \in \mathbb{N}$, com $b = a \cdot c$. Caso contrário, escrevemos $a \nmid b$. O elemento $c \in \mathbb{N}$ tal que $b = a \cdot c$, é indicado por $c = \dfrac{b}{a}$ e é chamado de *quociente de* b *por* a.

A título de exemplo, temos que:

1. $2 \mid 10$, pois $10 = 2 \cdot 5$;
2. $1 \mid a$, para todo $a \in \mathbb{N}$, pois $a = 1 \cdot a$.

A seguir veremos algumas propriedades básicas de divisibilidade em $\mathbb{N}$. Para as proposições a seguir, adotaremos $a, b \in \mathbb{N}$ e $c \in \mathbb{N}$.

Proposição 2.1.

1. $a \mid a$, para todo $a \in \mathbb{N}$. (reflexiva).

2. Se $a \mid b$ e $b \mid a$ então $a = b$ (anti-simétrica).

3. Se $a \mid b$ e $b \mid c$, então $a \mid c$ (transitiva).

Estas três propriedades nos dizem que "$\mid$" é uma relação de equivalência sobre $\mathbb{N}$.

Demonstração.

1. Vem da igualdade: $a = a \cdot 1$.
2. De fato, por hipótese, $b = a \cdot c$ e $a = b \cdot d$. Daí $a = a(c \cdot d)$. Como vale a lei do cancelamento nos naturais temos que $c \cdot d = 1$ e portanto $c = d = 1$. Logo $a = b$ também neste caso.
3. Como $b = a \cdot r$ e $c = b \cdot s$, com $r, s \in \mathbb{N}$, temos que $c = a(r \cdot s)$. Concluímos que $a \mid c$.

□

Proposição 2.2. *Se $a \mid b$ e $a \mid c$, então $a \mid (b \cdot x + c \cdot y)$, para todo x e $y \in \mathbb{N}$. Em particular, se $a \mid b$, então $a \mid b.x$, para todo $x \in \mathbb{N}$.*

Demonstração. Por hipóteses temos que $b = a \cdot r$ e $c = a \cdot s$ para alguns $r, s \in \mathbb{N}$. Decorre que $b \cdot x = a \cdot r \cdot x$ e $c \cdot y = a \cdot s \cdot y$. Donde $b \cdot x + c \cdot y = a \cdot r \cdot x + a \cdot s \cdot y = a(r \cdot x + s \cdot y)$. □

Proposição 2.3. *Se $c \mid a$, $c \mid b$ e $a < b$, então $c \mid (b - a)$. Neste caso $\dfrac{b-a}{c} = \dfrac{b}{c} - \dfrac{a}{c}$.*

Demonstração. Por hipótese $a = c \cdot r$, $b = c \cdot s$ e $b = a + u$, com $u = b - a$. Logo temos $c \cdot s = c \cdot r + u$ e daí $u = c \cdot s - c \cdot r = c(s - r)$. Logo $c \mid u$ e como $u = b - a$, a propriedade está provada. □

Proposição 2.4. *Seja $b = a + c$ e suponhamos $d \mid a$. Então: $d \mid b$ se,e somente se, $d \mid c$.*

Demonstração. Primeiro suponha que $d \mid b$. Por verificar que $d \mid c$. Como $d \mid a$, $d \mid b$ e $a < b$, podemos aplicar a proposição anterior e concluir que $d \mid c$.

Reciprocamente, agora suponha que $d \mid c$. Como $d \mid a$ podemos aplicar a Proposição 2.2 para concluir que $d \mid a + c$, isto é, $d \mid b$. Isso finaliza a prova.

□

Proposição 2.5. *Se $a \mid b$, então $a \leqslant b$.*

Em particular, se $a \mid 1$, então $a = 1$.

Demonstração. De fato, se $a \mid b$, existe $c \in \mathbb{N}$ tal que $b = a \cdot c$, então $a \leqslant b$, pois $c \geqslant 1$. Em particular, se $a \mid 1$, então $a \leqslant 1$ e segue que $a = 1$. □

2.2 Algoritmo da divisão ou de Euclides

Teorema 2.6 (Algoritmo da divisão ou de Euclides)**.** *Sejam $a, b \in \mathbb{N}$, com $a > b$. Então*

1. *ou $b \mid a$;*
2. *ou existe um único par de números $q, r \in \mathbb{N}$, de maneira que $a = b \cdot q + r$, com $r < b$.*

Demonstração. Primeiro provaremos a existência. Se $b \mid a$, então segue o Item 1. Suponha que $b \nmid a$ e considere o conjunto S formado pelos números naturais da forma $a, a - b, a - 2 \cdot b, \ldots, a - n \cdot b, \ldots$. Como S não é vazio podemos aplicar o Princípio da Boa Ordenação e garantir que S possui um menor elemento $r = a - b \cdot q$. Portanto $a = bq + r$. Como r é menor elemento de S temos que $a \leq b(q + 1)$. Logo $r \leq b$ e finalmente como $b \nmid a$ concluímos que $r < b$.

Agora provaremos a unicidade. Suponhamos $a = b \cdot q + r = b \cdot q_1 + r_1$, onde $r < b$ e $r_1 < b$. Admitamos que se pudesse ter $r \neq r_1$, e digamos $r > r_1$. Levando em conta

que tanto r como r_1 são menores que b podemos concluir que $r - r_1 < b$. Mas então da igualdade $b \cdot q + r = b \cdot q_1 + r_1$ decorre que $b \cdot q + (r - r_1) = b \cdot q_1$ e portanto $b \mid (r - r_1)$. Donde $b \leqslant (r - r_1)$, o que é absurdo. Logo $r = r_1$ e portanto $q = q_1$. □

Exemplo 2.1. Na divisão euclidiana de 802 por b, o quociente é 14 e o resto r. Determine b e r.

Resolução: Por hipótese, $802 = b \cdot 14 + r$ com $r < b$. Daí $0 \leqslant 802 - 14 \cdot b = r < b$. Assim, $14 \cdot b \leqslant 802$ e $802 < 15 \cdot b$. Os valores possíveis para esse sistema de desigualdades são $b = 54, 55, 56$ ou 57 e respectivamente $r = 46, 32, 18$ ou 4.

Exemplo 2.2. Na divisão euclidiana de a por b, o quociente é 106 e o resto 304. Qual o maior número de que se pode aumentar dividendo e divisor sem que o quociente se altere?

Resolução: Por hipótese $a = b \cdot 106 + 304$, com $304 < b$. Acrescentando x ao dividendo e ao divisor, se 106 é o quociente da divisão de $a + x$ por $b + x$, então $(b + x) \cdot 106 \leqslant a + x < (b + x) \cdot 107$. Subtraindo $106 \cdot b + x$ de cada um dos termos, fica $105 \cdot x \leqslant 304 < b + 160 \cdot x$. A última desigualdade se verifica para todo x pois $304 < b$. Assim basta estudar $105 \cdot x \leqslant 304$ que fornece as soluções $x = 0, 1$ ou 2. Logo, a resposta é $x = 2$.

2.3 Máximo divisor comum

Definição 2.1. *Sejam $a, b \in \mathbb{N}$. Um número $d \in \mathbb{N}$ se diz máximo divisor comum de a e b, se:*

1. *$d \mid a$ e $d \mid b$;*
2. *Se c é um número natural tal que $c \mid a$ e $c \mid b$, então $c \mid d$.*

Exemplo 2.3. Sejam $a = 6$ e $b = 8$. Os divisores de 6 e 8 são respectivamente $1, 2, 3, 6$ e os $1, 2, 4, 8$. Daí segue que os divisores comuns de 6 e 8 são $1, 2$. Observemos que $2 \mid 6$ e $2 \mid 8$; se $c \mid 6$ e $c \mid 8$, então $c = 1$ ou $c = 2$ e portanto $c \mid 2$. Logo concluímos que 2 é máximo divisor comum de 6 e 8.

Observação 1.

- Primeiro vejamos a unicidade do máximo divisor comum. Em efeito, sejam d e e máximos divisores comuns de a e b. Como $e \mid a$ e $e \mid b$ e d é máximo divisor de a e b temos que $e \mid d$. Analogamente podemos obter que $d \mid e$, o que implica que $d = e$.

  A partir de agora, o máximo comum divisor de a e b é denotado por $\text{mdc}(a, b)$.

- Note que se c é divisor de a e b, então $c \mid \text{mdc}(a, b)$. Portanto

$$c \leq \text{mdc}(a, b),$$

  isso significa que $\text{mdc}(a, b)$ representa o maior divisor de a e b.

- Da definição decorre diretamente que $\text{mdc}(a, b) = \text{mdc}(b, a)$.

Quanto à existência de máximo divisor comum, separaremos em alguns casos. A seguir mostraremos os primeiros casos.

Proposição 2.7. *Para qualquer a, b, c naturais, temos que:*

1. $\text{mdc}(a, 1) = 1$.
2. *Se $a \mid b$, então* $\text{mdc}(a, b) = a$, *isto é,* $\text{mdc}(a, ac) = a$.

Demonstração. De fato:

1. Segue imediato do fato que o único divisor comum de a e 1 é 1.
2. Por hipótese $a \mid a$ e $a \mid b$. E se $c \mid a$ e $c \mid b$, é imediato que $c \mid a$. Logo concluímos que $a = \text{mdc}(a, b)$.

□

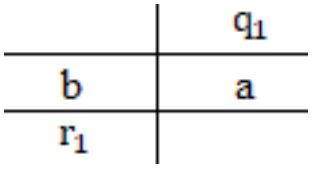
Proposição 2.8 (Lema de Euclides)**.** *Se $a = b \cdot q + r$ e $d = \text{mdc}(a, b)$, então $d = \text{mdc}(b, r)$. Em particular, se $r \mid b$, então* $\text{mdc}(a, b) = r$.

Demonstração. Como $d = \text{mdc}(a, b)$, então $d \mid a$ e $d \mid b$. Desta última relação resulta que $d \mid b \cdot q$. Logo $d \mid (a - b \cdot q)$, ou seja, $d \mid r$. Por outro lado, se $c \mid b$ e $c \mid r$, então $c \mid (b \cdot q + r)$ devido a Proposição 2.2 ; como $b \cdot q + r = a$, então $c \mid a$ e $c \mid b$, o que implica $c \mid d$, já que $d = \text{mdc}(a, b)$. Assim concluímos que $d = \text{mdc}(b, r)$. □

Para provar a existência do máximo divisor comum, aplicaremos sucessivamente, a partir de a e b, o algoritmo da divisão da seguinte maneira:

Se $b \mid a$, então $\text{mdc}(a, b) = b$. Caso contrário teríamos $a = b \cdot q_1 + r_1$, com $r_1 < b$. Se $r_1 \mid b$ então $\text{mdc}(a, b) = \text{mdc}(b, r_1) = r_1$. Caso contrário teríamos $b = r_1 \cdot q_2 + r_2$, com $r_2 < r_1$. Se $r_2 \mid r_1$, então $\text{mdc}(a, b) = \text{mdc}(b, r_1) = \text{mdc}(r_2, r_1) = r_2$. Podemos continuar com este processo e à medida que o resto diminui em cada etapa, podemos concluir que

Figura 1 - Algoritmo de Euclides



	q_1
b	a
r_1	

Figura 2 - Algoritmo de Euclides (continuação)

	q_1	q_2
b	a	r_1
r_1	r_2	

ele termina. Assim chegamos na seguinte sequência:

$$\begin{aligned}
a &= b \cdot q_1 + r_1, \text{ com } r_1 < b,\\
b &= r_1 \cdot q_2 + r_2, \text{ com } r_2 < r_1,\\
r_1 &= r_2 \cdot q_3 + r_3, \text{ com } r_3 < r_2,\\
\vdots &= \vdots\\
r_{n-2} &= r_{n-1} \cdot q_n + r_n, \text{ com } r_n < r_{n-1},\\
r_{n-1} &= r_n \cdot q_{n+1}.
\end{aligned}$$

Como consequência das proposições anteriores, obtém-se então o seguinte:

$$r_n = \text{mdc}(r_{n-1}, r_n) = \text{mdc}(r_{n-2}, r_{n-1}) = \cdots = \text{mdc}(b, r_1) = \text{mdc}(a, b).$$

Ou seja:

$$r_n = \text{mdc}(a, b).$$

Figura 3 - Algoritmo de Euclides para calcular o mdc(a, b)

	q_1	q_2	q_3	...	q_{n+1}	q_n	q_{n+1}
b	a	r_1	r_2	...	r_{n-2}	r_{n-1}	$r_n = (a, b)$
r_1	r_2	r_3	r_4	...	r_n		

Figura 4 - Algoritmo de Euclides para o Exemplo 2.4

	3	2	2	2
41	12	5	2	(1)
5	2	1	0	

O algoritmo acima é sintetizado e feito da seguinte maneira prática:

- *Primeiro passo:* Inicialmente, efetuamos a divisão $b = a \cdot q_1 + r_1$ e colocamos os números envolvidos na Figura 1.
- *Segundo passo:* A seguir, continuamos efetuando a divisão $a = r_1 \cdot q_2 + r_2$ e colocamos os números envolvidos na Figura 2.
- *Terceiro passo:* Prosseguindo, enquanto for possível, teremos finalmente a Figura 3.

Exemplo 2.4. Vamos encontrar o $\text{mdc}(41, 12)$

Resolução:

$$41 = 12 \cdot 3 + 5$$
$$12 = 5 \cdot 2 + 2$$
$$5 = 2 \cdot 2 + 1$$
$$2 = 1 \cdot 2$$

Logo, $\text{mdc}(41, 12) = 1$. Utilizando o algoritmo explicado teremos a Figura 4.

Definição 2.2. *Dois números naturais a e b se dizem primos entre si se* $\text{mdc}(a, b) = 1$. *Neste caso diz-se também que a e b são coprimos.*

Exemplo 2.5. Dois números consecutivos a e $a + 1$ são sempre primos entre si.

Resolução: De fato, é claro que $1 \mid a$ e $1 \mid (a + 1)$. Agora, se $c \mid a$ e $c \mid (a + 1)$, então $c \mid (a + 1 - a)$. Portanto $c \mid 1$. Assim concluímos que $\text{mdc}(a, a + 1) = 1$.

Proposição 2.9. *Se* $d = \text{mdc}(a, b)$, *então* $\text{mdc}(s \cdot a, s \cdot b) = s \cdot d$, *para todo* $s \in \mathbb{N}$.

Demonstração. Multipliquemos por s cada uma das igualdades obtidas pelo algoritmo da

divisão no processo das divisões sucessivas que leva a d, a partir de a e b:

$$\begin{aligned}
s \cdot a &= (s \cdot b) \cdot q_1 + s \cdot r_1 \\
s \cdot b &= (s \cdot r_1) \cdot q_2 + s \cdot r_2 \\
&\vdots \\
s \cdot r_{n-2} &= (s \cdot r_{n-1}) \cdot q_n + s \cdot r_n \\
s \cdot r_{n-1} &= (s \cdot r_n) \cdot q_{n+1}
\end{aligned}$$

As Proposições 2.7 e 2.8 nos garantem então que:

$$s \cdot d = s \cdot r_n = \text{mdc}(s \cdot r_{n-1}, s \cdot r_n) = \cdots = \text{mdc}(s \cdot b, s \cdot r_1) = \text{mdc}(s \cdot a, s \cdot b).$$

□

Corolário 2.1. *Se $a, b \in \mathbb{N}$ e $d = \text{mdc}(a, b)$, então $\text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, ou seja, $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si.*

Demonstração. Como $d = \text{mdc}(a, b) = \text{mdc}(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}) = d \cdot \text{mdc}(\frac{a}{d}, \frac{b}{d})$ podemos concluir que $\text{mdc}(\frac{a}{d}, \frac{b}{d}) = 1$. □

Corolário 2.2. *Se $a \mid b \cdot c$ e $\text{mdc}(a, b) = 1$, então $a \mid c$.*

Demonstração. Da hipótese $\text{mdc}(a, b) = 1$ decorre, levando em consideração a Proposição 2.9, que $\text{mdc}(a \cdot c, b \cdot c) = c$. Como $a \mid b \cdot c$ por hipótese e obviamente $a \mid a \cdot c$, então $a \mid \text{mdc}(a \cdot c, b \cdot c)$, ou seja, $a \mid c$. □

Corolário 2.3. *Se a e b são divisores de c e $\text{mdc}(a, b) = 1$, então $a \cdot b \mid c$.*

Demonstração. De $\text{mdc}(a, b) = 1$ e usando a Proposição 2.9, temos que $\text{mdc}(a \cdot c, b \cdot c) = c$. Mas $a \cdot b \mid a \cdot c$, pois $b \mid c$ e $a \cdot b \mid b \cdot c$ já que $a \mid c$. Logo $a \cdot b \mid \text{mdc}(a \cdot c, b \cdot c)$, isto é, $a \cdot b \mid c$. □

2.4 Mínimo múltiplo comum

Definição 2.3. *Um número m se diz mínimo múltiplo comum de $a, b \in \mathbb{N}$, se:*

1. *$a \mid m$ e $b \mid m$, isto é, m é múltiplo de a e b;*
2. *Se $a \mid n$ e $b \mid n$ então $m \mid n$, isto é, todo múltiplo de a e b é também múltiplo de m.*

Observação 2.

- Note que também temos unicidade para o mínimo múltiplo comum como no caso do máximo comum divisor. O mínimo múltiplo comum de a e b, se existe, é denotado por $\text{mmc}(a, b)$.

- Note que se n é múltiplo comum de a e b, então $\text{mmc}(a, b) \mid n$. Portanto

$$\text{mmc}(a, b) \leq n,$$

  isso significa que $\text{mmc}(a, b)$ representa o menor múltiplo comum de a e b.

- Também temos da definição que $\text{mmc}(a, b) = \text{mmc}(b, a)$.

Quanto à existência do mínimo múltiplo comum, consideremos inicialmente o seguinte resultado.

Proposição 2.10. *Para qualquer a, b, c naturais, temos que:*

1. $\text{mmc}(a, 1) = a$.
2. *Se $a \mid b$, então* $\text{mmc}(a, b) = b$, *isto é,* $\text{mmc}(a, ac) = ac$.

Demonstração. De fato:

1. Segue imediato da definição.
2. Por hipótese $a \mid b$ e $b \mid b$. E se $a \mid n$ e $b \mid n$, é imediato que $b \mid n$. Logo concluímos que $b = \text{mmc}(a, b)$.

□

Para os demais casos, a garantia de existência é dada pela proposição a seguir:

Proposição 2.11. *Para quaisquer $a, b \in \mathbb{N}$, se $d = \text{mdc}(a, b)$, então*

$$m = \frac{a \cdot b}{d}$$

é o mínimo múltiplo comum de a e b.

Demonstração. Notemos primeiro que como $d \mid (a \cdot b)$, pois $d \mid a$ e $d \mid b$, então $m \in \mathbb{N}$. Como, $a \cdot \frac{b}{d} = \frac{a \cdot b}{d} = m$, então $a \mid m$. Analogamente, se mostra que $b \mid m$. Seja n um múltiplo de a e de b. Portanto $n = a \cdot r$ e $n = b \cdot s$, com $r, s \in \mathbb{N}$. De $a \cdot r = b \cdot s$ temos que $\frac{a}{d} \cdot r = \frac{b}{d} \cdot s$. Daí segue que $\frac{a}{d} \mid \frac{b}{d} \cdot s$. Usando o fato que $\text{mdc}(\frac{a}{d}, \frac{b}{d}) = 1$ temos que $\frac{a}{d} \mid s$. Assim, $s = \frac{a}{d} \cdot k$ para algum $k \in \mathbb{N}$. Como $n = b \cdot s$, obtemos que $n = b \cdot \frac{a}{d} \cdot k = \frac{a \cdot b}{d} \cdot k = m \cdot k$, ou seja $m \mid n$. Portanto concluímos que $m = \text{mmc}(a, b)$. □

Corolário 2.4. *Se a e b são primos entre si, então* $\text{mmc}(a, b) = a \cdot b$.

Demonstração. De fato, como $d = \text{mdc}(a, b) = 1$, então $\text{mmc}(a, b) = \frac{a \cdot b}{1} = a \cdot b$. □

Proposição 2.12. *Se* $m = \text{mmc}(a, b)$*, então* $\text{mmc}(s \cdot a, s \cdot b) = s \cdot m$*, para qualquer* $s \in \mathbb{N}$.

Demonstração. Segue de aplicar a Proposição 2.11 da seguinte maneira:

$$\text{mmc}(s \cdot a, s \cdot b) = \frac{s \cdot a \cdot s \cdot b}{\text{mdc}(s \cdot a, s \cdot b)} = \frac{s^2 \cdot a \cdot b}{s \cdot \text{mdc}(a, b)} = s \cdot \frac{a \cdot b}{\text{mdc}(a, b)} = s \cdot \text{mmc}(a, b).$$

□

3 NÚMEROS PRIMOS

A história dos números primos se desenrola desde a Grécia antiga até os dias atuais. Neste capítulo, mostraremos as tentativas de vários matemáticos, como Euclides, Fermat e Mersenne de encontrar um padrão que fornecesse a lista de todos os (infinitos) números primos. Veremos importantes proposições sobre o tema, a conjectura de Goldbach além do pequeno teorema de Fermat e suas implicações.

Definição 3.1. *Seja $n > 1$ um número natural. Dizemos n é um número primo, ou simplesmente primo, se seus únicos divisores são e e n. Caso contrário dizemos que n é composto.*

Observação 3.

- Os primeiros números primos são $2, 3, 5, 7, 11, 13, 17$.
- Os primeiros números compostos são $4, 6, 8, 9, 10, 12$.
- Observe que 1 não é primo nem composto.

Proposição 3.1. *Sejam $p, a, b \in \mathbb{N}$.*

1. *Se p é primo, então* $\text{mdc}(a, p) = 1$ *ou* $\text{mdc}(a, p) = p$.
2. *Se p é primo e $p \mid a \cdot b$, então $p \mid a$ ou $p \mid b$.*

Demonstração.

1. Se $d = \text{mdc}(a, p)$, então $d \mid p$. Pela definição de primo temos que $d = 1$ ou $d = p$.
2. Se $p \mid a$, nada há que demonstrar. Suponhamos agora que $p \nmid a$. Pelo Item 1. temos que $\text{mdc}(a, p) = 1$ ou $\text{mdc}(a, p) = p$. Se $\text{mdc}(a, p) = p$, então $p \mid a$, isso é uma contradição. Logo $\text{mdc}(a, p) = 1$. Finalmente usando o Corolário 2.2 concluímos que $p \mid b$.

□

Proposição 3.2. *Seja $a \in \mathbb{N}$, com $a > 1$. Então, o elemento mínimo de*

$$S = \{x \in \mathbb{N} \mid x > 1 \text{ e } x \mid a\}$$

é um número primo.

Em particular, todo natural composto possui um divisor primo.

Demonstração. Note que $S \neq \emptyset$, pois $a \in S$. Seja p o mínimo de S. Pela definição $p > 1$, por verificar que p é primo. Suponha o contrário que p é composto, isto é, $p = b \cdot c$, com $1 < b < p$. Como $b \mid p$ e $p \mid a$ temos que $b \mid a$. Portanto $b \in S$, isso contradiz a minimalidade de p. Assim concluímos que p é primo. □

Uma aplicação da proposição anterior seria o seguinte exemplo.

Exemplo 3.1. Prove que se a e b são primos entre si, então $a \cdot b$ e $a + b$ também são primos entre si.

Resolução: Suponhamos que $\text{mdc}(a \cdot b, a + b) = d > 1$. Então d admite um divisor primo p que, por sua vez, também é divisor de $a \cdot b$ e $a + b$. Se $p \mid a \cdot b$, então $p \mid a$ ou $p \mid b$. Supondo $p \mid a$, como $p \mid (a + b)$, então $p \mid b$, pois $b = (a + b) - a$. Logo, $p \mid \text{mdc}(a, b)$ o que é absurdo pois $\text{mdc}(a, b) = 1$. Portanto $\text{mdc}(a \cdot b, a + b) = 1$

Proposição 3.3. *Sejam p primo e $a_1, \ldots, a_n \in \mathbb{N}$.*

1. *Se $p \mid a_1 \cdots a_n$, então existe um índice k, com $1 \leqslant k \leqslant n$, tal que $p \mid a_k$.*

2. *Se $a_1, a_2, \ldots, a_n$ são todos primos e se $p \mid a_1 \cdots a_n$ então $p = a_k$, para algum índice k, com $1 \leqslant k \leqslant n$.*

Demonstração.

1. A prova é por indução sobre n. Para $n = 1$ segue imediato. Suponha por indução que vale para n. Por verificar para $n + 1$. Em efeito, se $p \mid a_1 \ldots a_{n+1}$, fazendo $a = a_1 \ldots a_n$ e $b = a_{n+1}$ e aplicando a Proposição 3.1 para os valores de p, a e b temos que $p \mid a$ ou $p \mid b$. Se $p \mid b$ então $p \mid a_{n+1}$, a proposição está demonstrada, e se, ao invés, $p \mid a$ então $p \mid a_1 \ldots a_n$, então a hipótese de indução assegura que $p \mid a_k$, com $1 \leqslant k \leqslant n$. Em qualquer dos dois casos, p divide um dos naturais $a_1, \ldots, a_{n+1}$.

2. Com efeito, pelo Item 1. existe um índice k, com $1 \leqslant k \leqslant n$, tal que $p \mid q_k$, e como os únicos divisores positivos de q_k são 1 e q_k, segue que $p = 1$ ou $p = q_k$. Mas $p > 1$ porque p é primo. Logo, $p = q_k$.

□

Teorema 3.4. *Para todo número natural $a > 1$, existem números primos $p_1 \leq p_2 \leq \ldots \leq p_r$, com $r \geqslant 1$, de maneira que $a = p_1 \cdot p_2 \cdots p_r$.*

Além disso, a decomposição em produto de fatores primos é única, isto é, se também $a = q_1 \cdot q_2 \cdots q_s$, com $q_1 \leq q_2 \leq \cdots \leq q_s$ e $s \geqslant 1$, onde os q_i são igualmente primos, então $r = s$ e $p_i = q_i$ para cada i.

Demonstração. Primeiro vamos provar a existência de que todo número natural maior que 1 se pode escrever como produto de fatores primos. A prova vai ser feita pelo Princípio da Indução Forte sobre a. Se $a = 2$, então segue a afirmação já que 2 é primo. Supondo-se por indução sua veracidade para todo $m \in \mathbb{N}$ com $1 < m < a$. Por verificar para a. Em

efeito, se $a = p$ é um número primo, a afirmação seria correta. Caso contrário a seria composto, logo pela Proposição 3.2 existe p divisor primo de a, isto é $a = p \cdot m$, com $1 < m < a$. Pelo hipótese indutiva m é produto de primos. Portanto a é produto de primos.

Agora vamos provar a unicidade do produto de fatores primos. Suponha

$$a = p_1 \cdot p_2 \dots p_r = q_1 \cdot q_2 \dots q_s,$$

com $p_1, p_2, p_3, \dots, p_r, q_1, q_2, q_3 \dots q_s$ primos. A demostração é por indução sobre r. Suponhamos que $r = 1$, logo $a = p_1$. Por outro lado como $q_1 \mid q_1 \cdot q_2 \dots q_s$ temos que $q_1 \mid p_1$, logo $p_1 = q_1$. Portanto $s = 1$ e $a = p_1 = q_1$. Suponhha que é verdade para r, vamos verificar para $r + 1$. Temos $p_1 \mid q_1 \cdot q_2 \cdot q_3 \dots q_s$ de onde concluímos, aplicando o Item 2. da Proposição 3.3, que existe k $(1 \leqslant k \leqslant s)$ tal que $p_1 = q_k \geqslant q_1$. Da mesma forma $q_1 \mid p_l$ para algum l $(1 \leqslant l \leqslant r)$ e segue $q_1 = p_l \geqslant p_1$. Assim $p_1 = q_1$. Agora, de $p_1 \cdot p_2 \cdots p_{r+1} = q_1 \cdot q_2 \cdots q_s$ segue $p_2.p_3 \dots p_{r+1} = q_2.q_3 \dots q_s$. Pela hipótese indutiva concluímos $r+1 = s$ e $p_2 = q_2 \dots, p_{r+1} = q_{r+1}$. Junto com $p_1 = q_1$, isto dá a afirmação. □

Considerando o Teorema 3.4 e agrupando os fatores primos repetidos, na fatoração de um número composto, e ordenando os primos em ordem crescente, temos o seguinte enunciado.

Teorema 3.5 (Teorema Fundamental da Aritmética)**.** *Todo natural $n > 1$ admite uma única decomposição da forma:*

$$n = p_1^{k_1} \cdot p_2^{k_2} \dots p_r^{k_r}$$

onde, para $i = 1, 2, \dots, r$, cada k_i é um natural e cada p_i é um primo, com $p_1 < p_2 < \cdots < p_r$, denominada decomposição canônica do natural $n > 1$.

Exemplo 3.2. A decomposição canônica do natural $n = 17460$ é dada pela igualdade:

$$1760 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2$$

Proposição 3.6. *Seja $n = p_1^{k_1} \cdot p_2^{k_2} \dots p_r^{k_r}$ a decomposição canônica de um natural n. Se a é um divisor de n, então*

$$a = p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_r^{\beta_r}$$

onde $0 \leqslant \beta_i \leqslant k_i$, para $i = 1, 2, \dots, r$.

Demonstração. Seja a um divisor de n e seja p^β a potência de um primo p que figura na decomposição de a em fatores primos. Como $p^\beta \mid n$, segue que p^β divide algum $p_i^{k_i}$ por ser primo com os demais $p_j^{k_j}$, e, consequentemente $p = p_i$ e $\beta \leqslant k_i$. □

Observação 4. Conhecidas as decomposições canônicas de dois naturais a e b, e usando a proposição anterior podemos concluir que o $\text{mdc}(a, b)$ é o produto dos fatores primos

comuns às duas decomposições canônicas tomados cada um com o menor expoente, e o $\text{mmc}(a, b)$ é o produto dos fatores primos comuns e não comuns às duas decomposições canônicas tomados cada um ao maior expoente.

Vejamos um exemplo a título de explicação.

Exemplo 3.3. Vamos calcular o $\text{mdc}(280, 300)$ e o $\text{mmc}(280, 300)$.

Resolução: Temos que $280 = 2^3 \cdot 5 \cdot 7$ e $300 = 2^2 \cdot 3 \cdot 5^2$. Logo,
$\text{mdc}(280, 300) = 2^2 \cdot 5 = 20$ e $\text{mmc}(280, 300) = 2^3 \cdot 3 \cdot 5^2 \cdot 7 = 4200$.

Como aplicação, vamos calcular alguns máximos divisores comuns que nos ajudaram nos capítulos seguintes sobre números perfeitos e quase perfeitos.

Proposição 3.7. $\text{mdc}(2^{t-1}, (2^t - 2^k - 1)) = 1$.

Demonstração. 2^{t-1} é uma potência de base 2, logo só aparece 2 em sua decomposição em fatores primos. Por outro lado, $(2^t - 2^k - 1)$ é um número ímpar, e em sua decomposição em fatores primos não aparece o número 2. Concluímos, portanto que os números acima são relativamente primos. □

Proposição 3.8. $\text{mdc}(2^{p-1}, (2^p - 1)^2) = 1$.

Demonstração. 2^{p-1} é uma potência de base 2, logo só aparece 2 em sua decomposição em fatores primos. Por outro lado, $2^p - 1$ é um número ímpar, que quando elevado a 2 continuará a ser ímpar, logo, em sua decomposição em fatores primos não aparece o número 2. Concluímos, portanto que os números acima são relativamente primos. □

Proposição 3.9. *Sejam q um número primo ímpar, a e b números naturais. Então*

1. $\text{mdc}(2^{a+1} - 1, 2^{a+1} + 1) = 1$
2. $\text{mdc}(1 + q + \cdots + q^b, q^b) = 1$

Demonstração.

1. Seja $d = \text{mdc}(2^{a+1} - 1, 2^{a+1} + 1)$, logo $d \mid 2^{a+1} - 1$ e $d \mid 2^{a+1} + 1$. Portanto $d \mid (2^{a+1} + 1) - (2^{a+1} - 1) = 2$. Como os números $2^{a+1} - 1$ e $2^{a+1} + 1$ são ímpares concluímos que $d = 1$.

2. Por indução sobre b, temos para $b = 1$ a proposição é válida pois $\text{mdc}(1 + q, q) = 1$ uma vez que dois números consecutivos são coprimos. Suponha que

$$\text{mdc}(1 + q + \cdots + q^b, q^b) = 1$$

é verdade. Por verificar que $\text{mdc}(1 + q + \cdots + q^{b+1}, q^{b+1}) = 1$. De fato, seja $d = \text{mdc}(1 + q + \cdots + q^{b+1}, q^{b+1})$. Como $d \mid q^{b+1}$ e $d \mid 1 + q + \cdots + q^{b+1}$ temos que

$d \mid 1 + q + \cdots + q^b$. Agora vejamos que $d \neq q^{b+1}$ e portanto $d \mid q^b$. Suponha por contradição que $d = q^{b+1}$. Logo $1+q+\cdots+q^{b+1} = kq^{b+1}$, simplificando e agrupando temos que $1 = q^{b+1}(k-(k-1)q)$. Isso é uma contradição. Assim podemos concluir que $d = \text{mdc}(1 + q + \cdots + q^b, q^b)$ e portanto $d = 1$.

□

Teorema 3.10 (de Euclides)**.** *Há um número infinito de primos.*

Demonstração. Suponhamos que exista um primo p_n maior que todos os demais primos $2, 3, 5, 7, \ldots$, e considere o natural

$$P = p_1 \cdot p_2 \cdot p_3 \ldots p_n + 1$$

Como $P > 1$, o Teorema Fundamental da Aritmética permite afirmar que P tem pelo menos um divisor primo p. Mas $p_1, p_2, \ldots, p_n$ são os únicos primos, de modo que p deve, necessariamente, ser igual a um desses n primos. Assim sendo: $p \mid P$ e $p \mid p_1 \cdot p_2 \cdot p_3 \ldots p_n$, o que implica $p \mid P - p_1 \cdot p_2 \cdot p_3 \ldots p_n$ ou $p \mid 1$ o que é absurdo, porque $p > 1$ e o único divisor positivo de 1 é o próprio 1. Logo, qualquer que seja o primo p_n existe um primo maior que p_n, isto é, o conjunto $\{2, 3, 5, 7, 11, 13, \ldots\}$ dos primos é infinito. □

Proposição 3.11. *Para todo $n \in \mathbb{N}$ existe um $k_n \in \mathbb{N}$ tal que os números consecutivos*

$$k_n + 1, k_n + 2, k_n + 3, \ldots, k_n + n$$

são todos compostos.

Em particular, existem primos consecutivos p e q com $q > p$ tais que $q - p > n$

Demonstração. Dado $n \in \mathbb{N}$, escolhemos $k_n = (n+1)! + 1$. Como $2, 3, 4, \ldots, (n+1)$ todos dividem $(n+1)!$, obtemos

$$2 \mid (n+1)! + 2 = k_n + 1,$$

$$3 \mid (n+1)! + 3 = k_n + 2,$$

$$\vdots$$

$$n \mid (n+1)! + n = k_n + (n-1),$$

$$(n+1) \mid (n+1)! + (n+1) = k_n + n,$$

mostrando que todos estes números são compostos. □

Proposição 3.12. *Seja $n \in \mathbb{N}$, com $n \geqslant 2$. Se n é composto, então n admite pelo menos um fator primo $p \leqslant \sqrt{n}$.*

Demonstração. Como n é composto, então existem naturais a e b tais que $n = a \cdot b$, onde $1 < a < n$ e $1 < b < n$. Supondo $a \leqslant b$ temos $a^2 \leqslant a \cdot b = n$. Pela Proposição 3.2 existe

Figura 5 - Crivo de Eratóstenes

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

p primo tal que $p \mid a$. Como $p \mid a$ e $a \mid n$, então $p \mid n$ e temos também que $p \leqslant a \leqslant \sqrt{n}$. Logo, n possui um divisor primo $p \leqslant \sqrt{n}$. □

A proposição anterior nos fornece um processo que permite conhecer se um natural $n > 1$ é primo ou é composto, onde basta dividir n sucessivamente pelos primos que não excedem $\sqrt{n}$.

Exemplo 3.4. Vamos verificar se o natural $n = 509$ é primo ou composto. Para o natural $n = 509$, temos que $22 < \sqrt{509} < 23$, de modo que os primos que não excedem $\sqrt{509}$ são 2,3,5,7,11,13,17 e 19, e como 509 não é divisível por nenhum deles, segue que 509 é primo.

É fácil perceber que este processo é trabalhoso e pouco prático, principalmente quando pensamos em naturais muito grandes.

3.1 Crivo de Eratóstenes

A construção de uma tabela de primos que não excedem um natural n faz-se pelo processo conhecido como Crivo de Eratóstenes, que consiste em escrever na ordem natural todos os naturais desde 2 até n e, em seguida, eliminam-se todos os números compostos que são múltiplos dos primos p tais que $p \leqslant \sqrt{n}$, isto é, $2p, 3p, 4p, \ldots$

Exemplo 3.5. Construir uma tabela de primos menores que 100. Os primos p tais que $p \leqslant \sqrt{100} = 10$ são 2, 3, 5 e 7. Logo, vamos escrever, na ordem natural, todos naturais desde 2 até 100 e, em seguida, eliminar todos os naturais compostos que são múltiplos de 2, 3, 5 e 7, ver Figura 5.

Os naturais não eliminados 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 e 97 são todos os primos menores que 100.

3.2 Polinômios que resultam em primos

Os números primos não aparecem regularmente na sequência dos números naturais, e, por isso, algumas fórmulas que fornecem primos foram construídas como por exemplo:

$$p(n) = n^2 + n + 41, \text{ (Fórmula de Euler)}$$

que fornece primos para $n = 0, 1, 2, \ldots, 39$. Porém, para $n = 40$ e $n = 41$ os números obtidos são compostos:

$$p(40) = 40^2 + 40 + 41 = 40\dot{(}40 + 1) + 41 = 40 \cdot 41 + 41 = 41 \cdot (40 + 1) = 41 \cdot 41$$

$$p(41) = 41^2 + 41 + 41 = 41 \cdot (41 + 1) + 41 = 41 \cdot 42 + 41 = 41 \cdot (42 + 1) = 41 \cdot 43$$

Outros polinômios que fornecem primos são:

$p(n) = 2n^2 + 29$, para $0 \leqslant n \leqslant 28$,
$p(n) = n^2 + n + 17$, para $0 \leqslant n \leqslant 16$,
$p(n) = 3n^2 + 3 \cdot n + 23$, para $0 \leqslant n \leqslant 21$.

3.3 Primos Gêmeos

Definição 3.2. *Chamam-se primos gêmeos dois naturais ímpares e consecutivos que são ambos primos.*

Como exemplos de pares de primos gêmeos temos: 3 e 5, 5 e 7, 11 e 13, 15 e 17, 29 e 31.

Não se sabe até hoje se há um número infinito de pares de primos gêmeos, mas sabemos que existem 27.412.679 primos gêmeos com 10 dígitos ou menos.

O maior primo gêmeo conhecido foi calculado em setembro de 2016 e é formado por primos com 388.342 dígitos, ver [5].

Um fato interessante é a existência de apenas um terno naturais ímpares e consecutivos que são todos primos: 3, 5 e 7.

3.4 Conjectura de Goldbach

No século XVIII o matemático Christian Goldbach conjecturou que todo natural par maior que 4 pode ser expresso como soma de dois primos ímpares.

Vamos ver alguns exemplos:

$$6 = 3 + 3,$$
$$8 = 3 + 5,$$
$$10 = 3 + 7 = 5 + 5,$$
$$12 = 5 + 7,$$
$$14 = 13 + 11,$$
$$16 = 3 + 13 = 5 + 11,$$

Esta Conjectura data de 7 de junho de 1742 em uma carta escrita para Leonhard Euler. Este, por sua vez, respondeu em outra carta que estava absolutamente certo que essa conjectura era verdadeira, mas que não era capaz de demonstrá-la. Até os dias atuais ninguém conseguiu demonstrar tal conjectura, sendo portanto um dos problemas mais antigos de Teoria do Números ainda em aberto.

Em 2012 e 2013, o matemático peruano Harald Helfgott publicou dois trabalhos alegando ter comprovado incondicionalmente a conjectura fraca de Goldbach, ver [6], [7] e [8]. A conjectura fraca de Goldbach afirma que: *Todo número ímpar maior que 7 pode ser expresso como soma de três números primos ímpares.* Ou de forma equivalente: *Todo número ímpar maior que 5 pode ser expresso como soma de três números primos.* (Sendo que é possível usar o mesmo número primo mais de uma vez nessa soma.)

Observação 5. Um grande número de problemas interessantes relacionados com os números primos permanecem sem solução tais como os quatro Problemas de Landau:

1. A própria conjectura de Goldbach que enunciamos acima;
2. A conjectura dos números primos gêmeos: Há infinitos números primos p tais que $(p + 2)$ também é um número primo?
3. A conjectura de Legendre: Sempre existe um número primo entre dois quadrados perfeitos?
4. A conjectura de que há infinitos números primos p tais que $(p - 1)$ é um quadrado perfeito. Dizendo de outra forma, há infinitos números primos da forma $n^2 + 1$?

Há também muitas proposições sobre os números primos cuja demonstração requer recursos muito elevados, ou seja, para os quais não existe uma demonstração elementar. Como exemplo podemos citar:

1. Em toda progressão aritmética:

$$a, a + r, a + 2 \cdot r, a + 3 \cdot r, \ldots$$

Figura 6 - Fatoração de Fermat

1	$21 + 1 = 22$
2	$22 + 3 = 25 = 5^2$
3	$25 + 5 = 30$
4	$30 + 7 = 37$
5	$37 + 9 = 46$
6	$46 + 11 = 57$
7	$57 + 13 = 70$
8	$70 + 15 = 85$
9	$85 + 17 = 102$
10	$102 + 19 = 121 = 11^2$

onde a e r são naturais primos entre si, há um número infinito de primos. (Dirichlet);

2. Para todo natural $n > 3$, entre n e $2(n-1)$ existe, pelo menos, um primo. (Tschebischeff).

3.5 Método de Fatoração de Fermat

Dado um natural ímpar n, a decomposição de n num produto de dois fatores primos distintos pode ser obtida pelo método de fatoração de Fermat, da seguinte maneira: Constrói-se uma tabela com $\frac{n-1}{2}$ linhas, obtidas pela adição sucessiva de inteiros ímpares consecutivos a n. Se a r-ésima linha aparece o quadrado perfeito t^2, então $n = (t+r)\cdot(t-r)$.

Exemplo 3.6. Vamos ver um exemplo para quando $n = 21$, com $\frac{21-1}{2} = 10$ linhas, ver Figura 6.

Vemos que na segunda linha da Figura 6 aparece 5^2 e na décima linha aparece 11^2,

sendo assim, podemos escrever:

$$21 = (5+2)\cdot(5-2) = 7\cdot 3,$$
$$21 = (11+10)\cdot(11-10) = 21\cdot 1.$$

São estas as duas únicas maneiras de decompor o natural ímpar 21 num produto de dois fatores distintos, pois, todas as outras são variações destas.

3.6 Pequeno Teorema de Fermat

Importante observar que por volta de 500 anos antes de Cristo, os chineses já se utilizavam do fato de que se p é primo, então $p \mid 2^p - 2$. Porém, coube a Pierre de Fermat, no século XVII, generalizar este resultado e formular um pequeno e importante teorema, que enunciaremos a seguir, porém, antes disso, veremos um lema que será utilizado na demonstração do Pequeno Teorema de Fermat.

Lema 3.1. *Seja p um número primo. Os números $\binom{p}{i}$, onde $0 < i < p$, são todos divisíveis por p.*

Demonstração. O resultado vale trivialmente para $i = 1$. Podemos, então, supor $1 < i < p$. Neste caso, $i! \mid p\cdot(p-1)\ldots(p-i+1)$. Como $\text{mdc}(i!, p) = 1$ decorre que $i! \mid p\cdot(p-1)\ldots(p-i+1)$, e o resultado se segue pois

$$\binom{p}{i} = p\cdot\frac{(p-1)\ldots(p-i+1)}{i!}$$

□

Teorema 3.13 (Pequeno Teorema de Fermat)**.** *Dado um número primo p, tem-se que $p \mid a^p - a$, para todo $a \in \mathbb{N}$.*

Demonstração. Vamos fazer a indução sobre a. O resultado vale para $a = 1$ pois $p \mid 0$. Supondo o resultado válido para a, vamos prová-lo para $a+1$. Pela fórmula do Binômo de Newton

$$(a+1)^p - (a+1) = a^p - a + \binom{p}{1}\cdot a^{p-1} + \cdots + \binom{p}{p-1}\cdot a.$$

Pelo Lema 3.1 e pela hipótese de indução, o segundo membro da igualdade acima é divisível por p. Sendo assim, o resultado segue. □

Exemplo 3.7. Vamos provar que dado um número qualquer $n \in \mathbb{N}$, tem-se que n^9 e n, quando escritos na base 10, têm o mesmo algarismo da unidade.

Resolução: A afirmação acima é equivalente a $10 \mid n^9 - n$. Como n^9 e n tem a mesma paridade, então, $n^9 - n$ é par, ou seja, $2 \mid n^9 - n$. Por outro lado,

$$n^9 - n = n \cdot (n^4 - 1)(n^4 + 1) = (n^5 - n)(n^4 + 1).$$

Logo, pelo Pequeno Teorema de Fermat 3.13, temos que $5 \mid n^9 - n$. Temos então que $10 \mid n^9 - n$.

Corolário 3.1. *Se p é um número primo e se a é um número natural não divisível por p, então $p \mid a^{p-1} - 1$.*

Demonstração. Pelo Pequeno Teorema de Fermat 3.13 temos que $p \mid a^p - a$ que é equivalente a dizer que $p \mid a \cdot (a^{p-1} - a)$ e como $\text{mdc}(a, p) = 1$, segue-se, imediatamente que $p \mid a^{p-1} - 1$. □

3.7 Primos de Fermat

Definição 3.3. *Todo número da forma:*

$$F_n = 2^{2^n} + 1, \ \textit{com } n \geqslant 0,$$

é um número de Fermat. Se F_n é primo, diz-se que é um primo de Fermat.

Em 1640, Fermat escreveu os cinco primeiros números de Fermat: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65537$ e neste mesmo ano conjecturou que F_n é primo para todo $n \geqslant 0$. Entretanto em 1732, Leonhard Euler mostrou que

$$F_5 = 2^{2^5} + 1 = 4.294.967.297 = 641 \cdot 6.700.417,$$

portanto composto.

Até hoje, não se conseguiu encontrar um primo de Fermat diferente dos cinco primeiros. Sabe-se que para $5 \leqslant n \leqslant 16$ cada número de Fermat é composto e ainda não foi provado se o número de primos de Fermat é finito ou não. A respeito dos números de Fermat é provado o seguinte teorema.

Teorema 3.14. *Se F_n e F_m são dois números de Fermat, com $m > n \geqslant 0$, então o* $\text{mdc}(F_n, F_m) = 1$.

Demonstração. Seja $d = \text{mdc}(F_n, F_m)$. Como os números de Fermat são naturais ímpares, segue-se que d também é um natural ímpar. Temos, então

$$\frac{F_m - 2}{F_n} = \frac{2^{2^m} - 1}{2^{2^n} + 1} = \frac{(2^{2^n})^{2^{m-n}} - 1}{2^{2^n} + 1}$$

Para facilidade na escrita, vamos denotar 2^{2^n} por x e 2^{m-n} por k, então

$$\frac{F_m - 2}{F_n} = \frac{x^k - 1}{x + 1} = x^{k-1} - x^{k-2} + \cdots - 1,$$

de modo que $F_n \mid F_m - 2$. Como $d \mid F_n$, segue-se que $d \mid F_m - 2$. Mas, $d \mid F_m$ e, portanto, $d \mid 2$. E como d é um natural ímpar concluímos que $d = 1$. □

Apresentaremos uma relação de recorrência, que funciona como uma propriedade dos números de Fermat.

Proposição 3.15. *Todo número de Fermat é igual ao produto de seus anteriores somados a 2.*

Demonstração. Para $n = 1$ temos: $F_1 = 5$ e $F_0 + 2 = 3 + 2 = 5$. Portanto, é válida para $n = 1$. Supondo válida para um $n = k - 1$, vamos provar para $n = k$. Em efeito, $F_0 \ldots F_{n-1} + 2 = (F_{n-1} - 2) \cdot F_{n-1} + 2 = (2^{2^{n-1}} + 1 - 2) \cdot (2^{2^{n-1}} + 1) + 2 = 2^{2^n} + 1 = F_n$ □

Para estimular a investigação e o gosto pelo assunto vamos apenas enunciar outras relações de recorrência conhecidas e interessantes dos números de Fermat e deixaremos, em seguida, algumas perguntas ainda em aberto:

1. $F_n = (F_{n-1} - 1)^2 + 1$ para $n \geqslant 1$;
2. $F_n = F_{n-1} + 2^{n-1} \cdot F_0 \ldots F_{n-2}$;
3. $F_n = F_{n-1}^2 - 2 \cdot (F_{n-2} - 1)^2$;
4. $F_{n+k} - 1 = (F_n - 1)^{2^k}$.

Todas estas propriedades podem ser demonstradas por indução finita.

1. Para $n > 4$, todo F_n é composto?
2. Existem infinitos primos de Fermat?
3. Existem infinitos números de Fermat compostos?
4. Existe algum número de Fermat que não tem como fator um quadrado perfeito?

3.8 Primos de Mersenne

Definição 3.4. *Chama-se número de Mersenne todo número da forma*

$$M_n = 2^n - 1$$

com $n \geq 2$. Se M_n é primo, diz-se que é um primo de Mersenne.

Em 1644, em suas pesquisas, Mersenne conjecturou que: *Todo número da forma*

$$M_p = 2^p - 1,$$

com p primo, é primo para $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ *e é composto para os outros primos menores que* 257.

Segue uma lista dos primeiros primos de Mersenne.

n	M_n
2	3
3	7
5	31
7	27
13	8.191
17	131.071
19	524.287
31	2.147.483.647

Sabe-se que a conjectura de Mersenne estava errada ao incluir os primos 67 e 257 e ao excluir os primos 19, 61, 89 e 107. Em 21 de dezembro de 2018 foi encontrado o 51º primo de Mersenne com mais de 24 milhões de dígitos, ver [9].

Vamos ver uma caracterização de um primo de Mersenne.

Teorema 3.16. *Seja* $p \geq 2$. *Se* $M_p = 2^p - 1$ *é primo de Mersenne, então p também é primo.*

Demonstração. Suponhamos $p \geqslant 2$ e $2^p - 1$ primo. Se o número natural p fosse composto, então teríamos $p = r \cdot s$, com $r > 1$ e $s > 1$, o que implica $2^p - 1 = 2^{r \cdot s} - 1 = (2^r)^s - 1$, ou seja,

$$2^p - 1 = (2^r - 1) \cdot (2^{r \cdot (s-1)} + 2^{r \cdot (s-2)} + \cdots + 2^r + 1).$$

Como $r > 1$, os dois fatores do segundo membro são ambos maiores que 1, isto é, $2^p - 1$ é um inteiro composto, o que contraria a hipótese. Logo, p é primo. □

Observação 6. O recíproco do Teorema 3.16 é falso, isto é, k primo não implica $2^k - 1$ também primo. Assim, por exemplo, 11 é primo e no entanto $2^{11} - 1$ é composto, pois, temos $2^{11} - 1 = 2047 = 23 \cdot 89$.

3.9 Aritmética dos restos

Nesta seção trabalharemos com o conjunto dos números inteiros $\mathbb{Z}$.

Definição 3.5. *Se a e b são naturais, dizemos que a é congruente a b módulo $m (m > 0)$ se $a - b = k \cdot m$ para algum $m \in \mathbb{Z}$, que ainda escreveremos $m \mid (a - b)$. Denotamos isso por $a \equiv b \pmod{m}$. Se $m \nmid (a - b)$ dizemos que a é incongruente a b módulo m e denotamos $a \not\equiv b \pmod{m}$.*

Exemplo 3.8. $24 \equiv 3 \pmod{7}$, pois $7 \mid (24 - 3)$; $15 \equiv 7 \pmod{8}$, pois $8 \mid (15 - 7)$; $21 \equiv 3 \pmod{6}$, pois $6 \mid (21 - 3)$.

Proposição 3.17. *Se a e b são naturais, temos que $a \equiv b \pmod{m}$ se, e somente se, existir um natural k tal que $a = b + k \cdot m$.*

Demonstração. Se $a \equiv b \pmod{m}$, então $m \mid (a - b)$ o que implica na existência de um natural k tal que $a - b = k \cdot m$, isto é, $a = b + k \cdot m$. A recíproca vem da existência de um k, satisfazendo $a = b + k \cdot m$, temos $k \cdot m = a - b$, ou seja, que $m \mid (a - b)$, isto é $a \equiv b \pmod{m}$. □

Proposição 3.18. *Se a, b, m e d são naturais, as sentenças são verdadeiras:*

1. $a \equiv a \pmod{m}$ *(reflexiva);*
2. *Se* $a \equiv b \pmod{m}$, *então* $b \equiv a \pmod{m}$ *(simétrica);*
3. *Se* $a \equiv b \pmod{m}$ *e* $b \equiv c \pmod{m}$, *então* $a \equiv c \pmod{m}$*(transitiva).*

Demonstração.

1. Como $m \mid 0$, então $m \mid (a - a)$, o que implica $a \equiv a \pmod{m}$.
2. Se $a \equiv b \pmod{m}$, então $a = b + k_1 \cdot m$ para algum natural k_1. Logo $a = b - k_1 \cdot m$, o que implica, pela Proposição 3.17, $b \equiv a \pmod{m}$.
3. Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então existem naturais k_1 e k_2 tais que $a - b = k_1 \cdot m$ $b - d = k_2 \cdot m$. Somando-se, membro a membro, estas últimas equações, obtemos $a - c = (k_1 + k_2) \cdot m$, o que implica $a \equiv c \pmod{m}$.

□

Teorema 3.19. *Se a, b, c e m são naturais tais que $a \equiv b \pmod{m}$, então*

1. $a + c \equiv b + c \pmod{m}$*;*
2. $a - c \equiv b - c \pmod{m}$*;*
3. $a \cdot c \equiv b \cdot c \pmod{m}$.

Demonstração.

1. Como $a \equiv b \pmod{m}$, temos que $a - b = k \cdot m$e, portanto, como $a - b = (a + c) - (b + c)$ temos $a + c \equiv b + c \pmod{m}$.
2. Como $(a - c) - (b - c) = a - b$ e, por hipótese, $a - b = k \cdot m$ temos que $a - c \equiv b - c \pmod{m}$.

3. Como $a - b = k \cdot m$ então $a \cdot c - b \cdot c = c \cdot k \cdot m$ o que implica $m \mid (a \cdot c - b \cdot c)$ e, portanto, $a \cdot c \equiv b \cdot c \pmod{m}$.

□

Teorema 3.20. *Se a, b, c, d e m são naturais tais que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então*

1. $a + c \equiv b + d \pmod{m}$;
2. $a - c \equiv b - d \pmod{m}$;
3. $a \cdot c \equiv b \cdot d \pmod{m}$.

Demonstração.

1. De $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$ temos $a - b = k \cdot m$ e $c - d = k_1 \cdot m$. Somando-se membro a membro obtemos $(a + c) - (b + d) = (k + k_1) \cdot m$.
2. Basta subtrair membro a membro $a - b = k \cdot m$ e $c - d = k_1 \cdot m$ obtendo $(a - b) - (c - d) = (a - c) - (b - d) = (k - k_1) \cdot m$ o que implica $a - c \equiv b - d \pmod{m}$.
3. Multiplicamos ambos os lados de $a - b = k \cdot m$ por c e ambos os lados de $c - d = k_1 \cdot m$ por b, obtendo $a \cdot c - b \cdot c = c \cdot k \cdot m$ e $b \cdot c - b \cdot d = b \cdot k_1 \cdot m$. Agora, basta somarmos membro a membro estas últimas igualdades obtendo $a \cdot c - b \cdot c + b \cdot c - b \cdot d = a \cdot c - b \cdot d = (c \cdot k + b \cdot k_1) \cdot m$ o que implica $a \cdot c \equiv b \cdot d \pmod{m}$.

□

Proposição 3.21. *Sejam $a, b, c, m \in \mathbb{N}$, com $c \neq 0$ e $m > 1$. Temos que $a \cdot c \equiv b \cdot c \pmod{m}$, se e somente se $a \equiv b \pmod{\frac{m}{\text{mdc}(c,m)}}$.*

Demonstração. Podemos supor, sem perda de generalidade, que $b \cdot c \geqslant a \cdot c$. Como $\dfrac{m}{mdc(c,m)}$ e $\dfrac{c}{mdc(c,m)}$ são primos entre si, temos que

$$\begin{aligned} a \cdot c \equiv b \cdot c \pmod{m} &\iff m \mid (b-a) \cdot c \iff \frac{m}{\text{mdc}(c,m)} \mid (b-a) \cdot \frac{c}{\text{mdc}(c,m)} \\ &\iff \frac{m}{mdc(c,m)} \mid (b-a) \iff a \equiv b \pmod{\frac{m}{\text{mdc}(c,m)}}. \end{aligned}$$

□

Corolário 3.2. *Sejam $a, b, m \in \mathbb{N}$, com $m > 1$. Se $a + b \equiv 0 \pmod{m}$, então, para todo $n \in \mathbb{N}$, tem-se que $a^{2n} \equiv b^{2n} \pmod{m}$ e $a^{2n+1} + b^{2n+1} \equiv 0 \pmod{m}$.*

Demonstração. O resultado é válido para $n = 0$. Podemos ainda supor, sem perda de generalidade, que $a \geqslant b$. Como $a + b \equiv 0 \pmod{m}$, segue que $m \mid a + b$ e, portanto, $m \mid (a + b) \cdot (a - b)$. Como $(a + b) \cdot (a - b) = a^2 - b^2$, segue-se que $a^2 \equiv b^2 \pmod{m}$. Temos então que $a^{2n} \equiv b^{2n} \pmod{m}$ para todo $n \in \mathbb{N}$.
Por outro lado, como $a^{2n+1} + b^{2n+1} = (a + b) \cdot (a^{2n} - b \cdot a^{2n-1} + \cdots - b^{2n-1} \cdot a + b^{2n})$, e $m \mid a + b$, segue-se que $m \mid a^{2n+1} + b^{2n+1}$ e ,portanto, $a^{2n+1} + b^{2n+1} \equiv 0 \pmod{m}$. □

Observação 7. Com a notação de congruências, o Pequeno Teorema de Fermat 3.13 se enuncia da seguinte maneira: Se p é um número primo e $a \in \mathbb{N}$, então $a^p \equiv a \pmod{p}$. Além disso, se $p \nmid a$, então $a^{p-1} \equiv 1 \pmod{p}$.

4 NÚMEROS ABUNDANTES, DEFICIENTES E PERFEITOS

Um número se diz perfeito se for igual à soma de seus divisores próprios, deficiente se ultrapassa a soma de seus divisores próprios e abundante se for menor que que a soma de seus divisores próprios, onde divisores naturais próprios de um número natural n são todos os divisores naturais de n, exceto o próprio n. Neste capítulo veremos proposições importantes sobre esse três tipos de números.

4.1 Quantidade de divisores de um número natural

Considerando um natural n cuja decomposição canônica é da forma

$$n = p_1^{k_1} \cdot p_2^{k_2} \dots p_r^{k_r},$$

temos que os divisores naturais de n, são da forma:

$$d = p_1^{h_1} \cdot p_2^{h_2} \dots p_r^{h_r},$$

onde $0 \leqslant h_1 \leqslant k_1$, $0 \leqslant h_2 \leqslant k_2$, $\dots$, $0 \leqslant h_r \leqslant k_r$. Temos $k+1$ maneiras de escolher o expoente h_1, k_2+1 maneiras de escolher o expoente h_2, $\dots$ k_r+1 maneiras de escolher o expoente h_r e, portanto, o número total de maneiras de escolher os expoentes $h_1, h_2, \dots, h_r$ é dado pelo produto:

$$(k_1+1) \cdot (k_2+1) \dots (k_r+1)$$

Assim sendo, o número $d(n)$ de divisores do natural $n > 1$ é dado pela fórmula:

$$d(n) = (k_1+1) \cdot (k_2+1) \dots (k_r+1)$$

Exemplo 4.1. O número de divisores naturais do número $n = 756 = 2^2 \cdot 3^3 \cdot 7$ é:

$$d(756) = (2+1) \cdot (3+1) \cdot (1+1) = 3 \cdot 4 \cdot 2 = 24.$$

Estes 24 divisores de 756 são os naturais d da forma:

$$d = 2^{h_1} \cdot 3^{h_2} \cdot 7^{h_3},$$

onde $h_1 = 0, 1, 2$, $h_2 = 0, 1, 2, 3$ e $h_3 = 0, 1$.

4.2 Soma dos divisores de um número natural

Seja n um número natural maior que 1. Vamos denotar por $\sigma(n)$ a soma de todos os seus divisores, de modo que $\sigma(1) = 1$.

Proposição 4.1. *Seja $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_r^{\alpha_r}$, onde $p_1, p_2, \dots p_r$ são números primos e $\alpha_1, \alpha_2, \dots \alpha_r$ são naturais maiores que zero. 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. Considerando a igualdade $(1 + p_1 + \cdots + p_1^{\alpha_1}) \dots (1 + p_r + \cdots + p_r^{\alpha_r}) = \sum p_1^{\beta_1} \dots p_r^{\beta_r}$ onde o somatório do lado direito da igualdade é tomado sobre todas as r-uplas $(\beta_1, \dots, \beta_r)$ ao variar de cada β_i no intervalo $0 \leqslant \beta_i \leqslant \alpha_i$, para $i = 0, \dots r$. Como tal somatório, representa 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. □

Observação 8. É claro que $\sigma(n) = 1 + n + \cdots \geqslant n + 1$, para todo $n \geqslant 2$. Veremos a seguir que $\sigma(n)$ assume o menor valor quando n é primo.

Proposição 4.2. *$\sigma(n) = n + 1$ se e somente se n é primo.*

Demonstração. Como $\sigma(n) = n + 1$, indica que n possui apenas dois divisores, a saber, 1 e o próprio n. Logo, pela definição de número primo, n é primo. Por outro lado, se n é primo, seus divisores são 1 e ele mesmo. Logo $\sigma(n) = n + 1$. □

Também podemos obter outra caracterização de um número primo.

Proposição 4.3. *Seja $n, k \in \mathbb{N}$. Então*

$$\sigma(n^k) \geq 1 + n + \cdots + n^k,$$

e $\sigma(n^k) = 1 + n + \cdots + n^k$ se e somente se n é primo.

Demonstração. Se $\sigma(n^k) = 1 + n + \cdots + n^k$, indica que n^k possui $k + 1$ divisores, o que só acontece se n for primo, como visto no início da seção 4.1. Por outro lado, se $n = p$, com p primo, $\sigma(p^k) = (1 + p) \cdot (1 + p) \dots (1 + p) = (1 + p)^k = 1 + p + \cdots + p^k$. Sendo n composto, $\sigma(n^k) > 1 + n + \cdots + n^k$.

□

Observação 9. A função $f : \mathbb{N} \to \mathbb{N}$ diz-se uma *função aritmética multiplicativa* se

$$f(r \cdot s) = f(r) \cdot f(s),$$

para todo par de naturais r e s tais que o $\text{mdc}(r, s) = 1$.

Vejamos que σ é uma função aritmética multiplicativa.

Proposição 4.4. *As seguintes afirmações são válidas.*

1. *Se $n = p^k$, com p primo e $k \geq 0$, então $\sigma(n) = 1 + \cdots + p^k$.*

2. *Se $\text{mdc}(r, s) = 1$, com $r, s \in \mathbb{N}$, então $\sigma(r \cdot s) = \sigma(r) \cdot \sigma(s)$.*

Demonstração.

1. Se p é primo, então $\sigma(p^k) = \dfrac{p^{k+1} - 1}{p - 1} = 1+p+p^2+\ldots+p^k$, pois $1+p+p^2+\ldots+p^k$ representa a soma dos termos de um progressão geométrica finita com primeiro termo igual a 1, razão igual a p e $k + 1$ termos.

2. Seja $n = r \cdot s$. Escrevendo a decomposição em fatores primos de $r = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_t^{\alpha_t}$ e $s = q_1^{\beta_1} \cdot q_2^{\beta_2} \ldots q_u^{\beta_u}$, com p_i e q_j primos distintos dois a dois respectivamente. Como $mdc(r, s) = 1$, significa que r e s não possuem fator comum. Logo a decomposição única é fatores primos de n é

$$p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_t^{\alpha_t} \cdot q_1^{\beta_1} \cdot q_2^{\beta_2} \ldots q_u^{\beta_u}.$$

   Então

$$\begin{aligned} \sigma(n) = \sigma(r \cdot s) &= \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_t^{\alpha_t+1} - 1}{p_t - 1} \cdot \frac{q_1^{\beta_1+1} - 1}{q_1 - 1} \cdots \frac{q_u^{\beta_u+1} - 1}{q_u - 1} \\ &= \sigma(r) \cdot \sigma(s) \end{aligned}$$

□

Vejamos alguns exemplos como aplicação.

Exemplo 4.2.

1. $\sigma(3) = \dfrac{3^2 - 1}{3 - 1} = 4$;

2. $\sigma(6) = \sigma(2 \cdot 3) = \dfrac{2^2 - 1}{2 - 1} \cdot \dfrac{3^2 - 1}{3 - 1} = 12$;

3. $\sigma(18) = \sigma(2 \cdot 3^2) = \dfrac{2^2 - 1}{2 - 1} \cdot \dfrac{3^3 - 1}{3 - 1} = 39$;

4. $\sigma(28) = \sigma(2^2 \cdot 7) = \dfrac{2^3 - 1}{2 - 1} \cdot \dfrac{7^2 - 1}{7 - 1} = 56$;

4.3 Números Perfeitos e Imperfeitos

Definição 4.1. *Um número $n \in \mathbb{N}$ chama-se:*

- *deficiente se a soma de seus divisores próprios é inferior a ele;*
- *abundante ou excessivo se a soma de seus divisores próprios é superior a ele;*
- *perfeito se se for igual à soma de seus divisores naturais próprios.*
- *imperfeito se não é perfeito.*

Divisores naturais próprios de um número natural n são todos os divisores naturais de n, exceto o próprio n.

Portanto, ao compararmos um número natural n com a soma de seus divisores, $\sigma(n)$, podemos ter três situações distintas e excludentes:

- $2n > \sigma(n)$: o número n é deficiente;
- $2n < \sigma(n)$: o número n é abundante;
- $2n = \sigma(n)$: o número n é perfeito.

Exemplo 4.3.

- $n = 1$; $\sigma(1) = 1 < 2 \cdot 1$ e $n = 2$; $\sigma(2) = 3 < 2 \cdot 2$. Portanto, 1 e 2 são primeiros números deficientes.
- $n = 12$; $\sigma(12) = 28$; $\sigma(4) > 2 \cdot 12$. Portanto, 12 é abundante e é o primeiro número natural abundante.
- $n = 6$; $\sigma(6) = 12$; $\sigma(6) = 2 \cdot 6$. Portanto, 6 é perfeito e é o primeiro número natural perfeito.

Observação 10. Todo número primo é deficiente.

Primeiro vamos classificar os números com um só primo na fatoração.

Proposição 4.5. *Se $n = p^k$, com $k \geq 0$, então n é deficiente.*

Demonstração. Claramente $1 = p^0$ é deficiente. A prova será feita por indução sobre k. Se $k = 1$, então n é primo. Portanto n é deficiente. Suponha por hipótese indutiva que $n = p^k$ é deficiente. Por verificar p^{k+1} é deficiente. Em efeito, usando a Proposição 4.4 temos que

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

Pela hipótese indutiva $2n - \sigma(n) > 0$ e $p \geq 2$ podemos concluir que $2p^{k+1} - \sigma(p^{k+1}) > 0$. Portanto p^{k+1} é deficiente. □

Agora vamos classificar os números com só dois primos diferentes na fatoração.

Proposição 4.6. *Seja $n = p \cdot q$, com p, q primos e $p \leq q$. Então temos duas alternativas*

1. *n é perfeito se e somente se $p = 2$ e $q = 3$.*

2. *n é deficiente se e somente se $p \neq 2$ ou $q \neq 3$.*

Demonstração. Se $p = q$, então pela Proposição 4.5 temos que $n = p^2$ é deficiente. Podemos assumir que $p < q$. Então

$$2n - \sigma(n) = pq - p - q - 1.$$

Temos duas possibilidades para analisar $p = 2$ ou $p > 2$. Se $p = 2$, então $2n - \sigma(n) = q - 3$. Portanto n é perfeito se e somente se $q = 3$ ou n é deficiente se e somente se $q > 3$. A outra possibilidade seria $p > 2$, neste caso teríamos

$$2n - \sigma(n) = q(p-1) - (p+1) \geq 2q - (p+1) > 0.$$

Portanto n é deficiente, isso prova a proposição. □

Proposição 4.7. *O número $2^k \cdot 3$ é abundante para todo $k \geq 2$.*

Demonstração. Considernado $n = 2^k \cdot 3$, basta fazer o seguinte cálculo:

$$\begin{aligned} \sigma(n) - 2 \cdot n &= \frac{2^{k+1} - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} - 2 \cdot 2^k \cdot 3 \\ &= (2^{k+1} - 1) \cdot 4 - 6 \cdot 2^k \\ &= 2 \cdot 2^k - 4 > 0 \end{aligned}$$

para todo $k \geqslant 2$. Logo n é abundante.

□

Proposição 4.8. *Seja $n = 2^k \cdot p$, com $p > 3$ primo e $k \geq 2$. Então temos só uma das seguintes alternativas.*

1. *n é deficiente se e somente se $p > 2^{k+1} - 1$.*

2. *n é abundante se e somente se $p < 2^{k+1} - 1$.*

3. *n é perfeito se e somente $p = 2^{k+1} - 1$.*

Demonstração. Sendo $n = 2^k \cdot p$, temos $\sigma(n) = \dfrac{2^{k+1}-1}{2-1} \cdot \dfrac{p^2-1}{p-1} = (2^{k+1}-1) \cdot (p+1)$. Calculando

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

1. Assim n é deficiente, se e somente se $\sigma(n) - 2 \cdot n < 0$ se e somente se $2^{k+1} - 1 < p$.
2. n é abundante, se e somente se $\sigma(n) - 2 \cdot n > 0$ se e somente se $2^{k+1} - 1 > p$.
3. n é perfeito, se e somente se $\sigma(n) - 2 \cdot n = 0$ se e somente se $2^{k+1} - 1 = p$.

□

Proposição 4.9. *Seja $n = 2^k \cdot p^l$, com $p \geq 3$ primo, $k \geq 1$ e $l \geq 2$. Então temos só uma das seguintes alternativas.*

1. *n é deficiente se e somente se $p > 2^{k+1}$.*
2. *n é abundante se e somente se $2^{k+1} > p$.*

Demonstração. Primeiro vamos calcular

$$\begin{aligned}(\sigma(n) - 2n) \cdot (p-1) &= \left(\frac{2^{k+1}-1}{2-1} \cdot \frac{p^{l+1}-1}{p-1} - 2 \cdot 2^k \cdot p^l\right) \cdot (p-1) \\ &= (2^{k+1}-1) \cdot (p^{l+1}-1) - 2^{k+1} \cdot p^l \cdot (p-1) \\ &= 2^{k+1} \cdot p^l - 2^{k+1} - p^{l+1} + 1.\end{aligned}$$

Assim

$$(\sigma(n) - 2n) \cdot (p-1) = p^l \cdot (2^{k+1} - p) - 2^{k+1} + 1. \tag{4.1}$$

1. Sendo n deficiente, temos $(\sigma(n) - 2n) \cdot (p-1) < 0$. Pela equação (4.1) concluímos $p^l \cdot (2^{k+1} - p) - 2^{k+1} + 1 < 0$. Mas $2^{k+1} - p$ deve ser negativo, para que a desigualdade se mantenha, uma vez que $p^l \cdot (2^{k+1} - p)$ representa uma quantidade maior que $2^{k+1} + 1$, pois $p \geq 3$ e $l \geq 2$, e por isso, $p > 2^{k+1}$. Por outro lado, se $p > 2^{k+1}$, então $(\sigma(n) - 2n) \cdot (p-1) = p^l \cdot (2^{k+1} - p) - 2^{k+1} + 1$ será negativo.
2. Sendo n abundante temos $(\sigma(n) - 2n) \cdot (p-1) > 0$. Pela equação (4.1) concluímos $p^l \cdot (2^{k+1} - p) - 2^{k+1} + 1 > 0$. Mas $2^{k+1} - p$ deve ser positivo para que a desigualdade se mantenha, uma vez que $p^l \cdot (2^{k+1} - p)$ representa uma quantidade maior que $2^{k+1} + 1$, pois $p \geq 3$ e $l \geq 2$, e por isso, $p < 2^{k+1}$. Por outro lado, se $p < 2^{k+1}$, então $(\sigma(n) - 2n) \cdot (p-1) = p^l \cdot (2^{k+1} - p) - 2^{k+1} + 1$ será positivo, uma vez que $(2^{k+1} - p)$ será positivo e $p^l \cdot (2^{k+1} - p)$ será maior que $2^{k+1} - 1$.

□

Proposição 4.10. *Sejam $2 < p < q$ primos. Então, para todos os $k, l \in \mathbb{N}$, o número*

$$n = p^k \cdot q^l$$

é deficiente.

Demonstração. Se $n = p^k \cdot q^l$, $3 \leq p$ e $5 \leq q$, então

$$\sigma(n) = \frac{p^{k+1}-1}{p-1} \cdot \frac{q^{l+1}-1}{q-1} < \frac{p^{k+1}}{p-1} \cdot \frac{q^{l+1}}{q-1} = n \cdot \frac{p}{p-1} \cdot \frac{q}{q-1} \leqslant \frac{3 \cdot 5}{2 \cdot 4} \cdot n < 2n,$$

o que mostra que n é um número deficiente. □

A seguir está uma lista dos números deficientes, abundantes e perfeitos que existem entre 1 a 100.

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

Em geral, podemos classificar números com 3 ou mais fatores primos sob certas condições no menor primo que aparece na fatoração.

Proposição 4.11. *Sejam $5 \leqslant p < q < r$ primos. Então, para todos os $m, n, s \in \mathbb{N}$, o número*

$$n = p^n \cdot q^m \cdot r^s$$

é deficiente.

Demonstração. Calculando

$$\sigma(n) = \frac{p^{n+1}-1}{p-1} \cdot \frac{q^{m+1}-1}{q-1} \cdot \frac{r^{s+1}-1}{s-1} < \frac{p^{n+1}}{p-1} \cdot \frac{q^{m+1}}{q-1} \cdot \frac{r^{s+1}}{r-1} = n \cdot \frac{p}{p-1} \cdot \frac{q}{q-1} \cdot \frac{r}{r-1}$$
$$\leq \frac{5 \cdot 7 \cdot 11}{4 \cdot 6 \cdot 10} \cdot n = \frac{77}{48} n < 2n.$$

Segue a proposição.

□

Proposição 4.12. *Sejam* $\frac{\sqrt[k]{2}}{\sqrt[k]{2}-1} \leqslant p_1 < p_2 < \cdots < p_k$ *primos. Então, para todos os* $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$*, o número*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

é deficiente.

Demonstração. Calculando

$$\begin{aligned}\sigma(n) &= \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdots \frac{p_k^{\alpha_k+1}-1}{p_k-1} < \frac{p_1^{\alpha_1+1}}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}}{p_2-1} \cdots \frac{p_k^{\alpha_k+1}}{p_k-1} \\ &= n \cdot \frac{p_1}{p_1-1} \cdot \frac{p_2}{p_2-1} \cdots \frac{p_k}{p_k-1} < \left(\frac{\frac{\sqrt[k]{2}}{\sqrt[k]{2}-1}}{\frac{\sqrt[k]{2}}{\sqrt[k]{2}-1}-1} \right)^k \cdot n = 2n.\end{aligned}$$

□

Assim chegamos a conclusão que a maioria dos números são deficientes.

5 NÚMEROS PERFEITOS

Um número n é dito perfeito, se for igual à soma dos seus divisores próprios, ou ainda, se a soma de todos os divisores for igual ao dobro de n. Os números perfeitos despertam até hoje a curiosidade de muitos pesquisadores do assunto. Veremos neste capítulo que os números perfeitos fornecidos pela fórmula de Euclides (que viveu e morreu por volta de 300 a.C), são todos pares. A existência ou não dos números perfeitos ímpares ainda é uma pergunta sem resposta, mas sabe-se que se existe, possui mais de 200 dígitos.

5.1 Números perfeitos pares

Teorema 5.1 (Teorema de Euclides)**.** *Se $2^k - 1$ for um número natural primo, então o número natural $n = 2^{k-1} \cdot (2^k - 1)$ é um número perfeito.*

Demonstração. Seja $p = 2^k - 1$ um primo maior que 2. Consideremos o número natural $n = 2^{k-1} \cdot p$. Como o $\text{mdc}(2^{k-1}, p) = 1$ e $\sigma(n)$ é uma função aritmética multiplicativa, temos:

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

Logo, por definição, n é um número perfeito. □

Teorema 5.2 (Teorema de Euler)**.** *Se n é um número perfeito par, então*

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

para algum número natural k tal que $2^k - 1$ é um número primo.

Demonstração. Suponhamos que n é um número perfeito par. Então, n pode ser escrito da forma $n = 2^{k-1} \cdot m$, onde m é um natural ímpar e $k \geqslant 2$. Como o $\text{mdc}(2^{k-1}, m) = 1$ e $\sigma(n)$ é uma função aritmética multiplicativa, temos

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

Por outro lado, como n é um número perfeito, temos $\sigma(n) = 2 \cdot n = 2^k \cdot m$. Portanto $2^k \cdot m = (2^k - 1) \cdot \sigma(m)$. Assim temos que $(2^k - 1) \mid 2^k \cdot m$. Mas, o $\text{mdc}(2^k - 1, 2^k) = 1$, o que implica $(2^k - 1) \mid m$, isto é, $m = (2^k - 1) \cdot M$. Substituindo este valor de m em $2^k \cdot m = (2^k - 1) \cdot \sigma(m)$ e cancelando o fator comum $2^k - 1$, obtemos

$$\sigma(m) = 2^k \cdot M.$$

Como m e M são ambos divisores de m (com $M < m$), temos

$$2^k \cdot M = \sigma(m) \geqslant m + M = 2^k \cdot M$$

o que implica $\sigma(m) = m + M$. Assim sendo, m e M são os únicos divisores naturais de m, e isto significa que m é primo e $M = 1$. Então $m = (2^k - 1) \cdot M = 2^k - 1$ é um primo, e por ser

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

o teorema fica demonstrado. □

Este teorema é o recíproco do Teorema 5.1 e foi demonstrado cerca de 2000 anos depois de Euclides. Então podemos concluir o seguinte teorema.

Teorema 5.3 (Teorema de Euclides-Euler)**.** *Um número natural n é um número perfeito par se, e somente se, $n = 2^{p-1} \cdot (2^p - 1)$, onde $2^p - 1$ é um primo de Mersenne.*

Os dez menores números perfeitos são os seguintes:

Posição	Número perfeito
1	6
2	28
3	496
4	8.128
5	33.550.336
6	8.589.869.056
7	137.438.691.328
8	2.305.843.008.139.952.128
9	2.658.455.991.569.831.744.645.692.615.953.842.176
10	191.561.942.608.236.107.294.793.378.084.303.638.130.997.321.548.169.216

Observação 11. Pela lista podemos ver que os números perfeitos conhecidos são pares. Quanto à questão da existência ou não de números perfeitos ímpares, é um dos problemas em aberto que ainda hoje permanece sem solução.

5.2 Algumas propriedades importantes

Teorema 5.4. *Todo número perfeito par termina em 6 ou 8.*

Demonstração. Seja n um número perfeito par. Pelo Teorema 5.2, temos $n = 2^{k-1} \cdot (2^k - 1)$, onde $2^k - 1$ é primo. E, pelo Teorema 3.16, sendo $2^k - 1$ primo, k também é primo. Se

$k = 2$, então $n = 6$, e a proposição é verdadeira. Suponhamos, pois, $k > 2$. Todo primo maior que 2 é da forma $4 \cdot m + 1$ ou $4 \cdot m + 3$. Se k é da forma $4 \cdot m + 1$, então

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

Por ser $16^l \equiv 6 \pmod{10}$, qualquer que seja o número natural l, segue-se que $n \equiv 2 \cdot 6 - 6 = 6 \pmod{10}$, isto é $n = 10 \cdot h + 6$ e, portanto, n termina em 6.

Analogamente, se k é da forma $4 \cdot m + 3$, então

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

De novo usando $16^l \equiv 6 \pmod{10}$, segue-se que $n \equiv 2 \cdot 6 - 4 \cdot 6 \equiv -12 \equiv 8 \pmod{10}$, isto é, $n = 10 \cdot j + 8$ e, portanto, n termina em 8. □

Proposição 5.5. *Um quadrado perfeito é um número imperfeito.*

Demonstração. Seja $n = s^2$ um quadrado perfeito. Suponha que s se decomponha da forma $s = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. A soma dos divisores de n será dada por

$$\sigma(n) = (1 + p_1 + \cdots + p_1^{2 \cdot \alpha_1}) \cdot (1 + p_2 + \cdots + p_2^{2 \cdot \alpha_2}) \cdots (1 + p_k + \cdots + p_k^{2 \cdot \alpha_k}).$$

Como cada um dos fatores acima é um número ímpar, temos que $\sigma(n)$ é ímpar. Portanto n é imperfeito já que $\sigma(n) \neq 2 \cdot n$. □

Vale ressaltar que um quadrado perfeito pode ser deficiente ou abundante. Para isso, usando a Proposição 4.9 na forma de quadrado perfeito, podemos obter a seguinte proposição.

Proposição 5.6. *Sejam $p \geq 3$ primo, $k \geq 1$ e $l \geq 1$. Se $n = 2^{2k} \cdot p^{2l}$ é um quadrado perfeito, então temos só uma das seguintes alternativas.*

1. *n é deficiente se e somente se $p > 2^{2k+1}$.*
2. *n é abundante se e somente se $2^{2k+1} > p$.*

Temos mais algumas propriedades sobre números perfeitos.

Proposição 5.7. *Se $n = 2^{p-1}(2^p - 1)$ é um número perfeito par, então o produto de seus divisores é n^p.*

Demonstração. Denotaremos por $P = 2^p - 1$ o primo de Mersenne. Neste caso os divisores de n são do tipo $2^i P^j$, com $0 \leqslant i \leqslant p - 1$ e $0 \leqslant j \leqslant 1$. Assim o produto dos divisores de

n denotado por T será

$$\begin{aligned} T &= (2^0P^0)(2^1P^0)\cdots(2^{p-1}P^0)(2^0P^1)(2^1P^1)\cdots(2^{p-1}P^1) \\ &= 2^{1+2+\ldots(p-1)} \cdot 2^{1+2+\ldots(p-1)} \cdot P^p \\ &= 2^{\frac{p(p-1)}{2}+\frac{p(p-1)}{2}}P^p = 2^{p(p-1)}P^p = (2^{p-1}\cdot P)^p \\ &= n^p. \end{aligned}$$

Isso prova a proposição. □

Proposição 5.8. *A soma dos recíprocos dos divisores de um número perfeito é 2.*

Demonstração. Seja n o número perfeito e $a_1, a_2, a_3, \ldots, a_r$ seus divisores. Observe que os conjuntos $\{a_1, a_2, a_3, \ldots, a_r\}$ e $\left\{\frac{n}{a_1}, \frac{n}{a_2}, \frac{n}{a_3}, \ldots, \frac{n}{a_r}\right\}$ são iguais, isto é, para cada divisor a_i de n existe um $1 \leqslant j \leqslant r$ tal que $a_i = \frac{n}{a_j}$. Logo,

$$\begin{aligned} \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_r} &= \frac{1}{n}\left(n\frac{1}{a_1} + n\frac{1}{a_2} + \cdots + n\frac{1}{a_r}\right) \\ &= \frac{1}{n}\left(a_1 + a_2 + \cdots + a_r\right) \\ &= \frac{1}{n}\cdot 2n = 2. \end{aligned}$$

Isso completa a prova da proposição. □

Ainda não foi descoberto nenhum número perfeito ímpar. Mas sabe-se que.

Corolário 5.1. *Se existe um número perfeito ímpar, então possui pelo menos três fatores primos distintos.*

Demonstração. Segue diretamente das Proposições 4.5, 4.6, 4.7, 4.8 e 4.9 e 4.10. □

6 NÚMEROS QUASE PERFEITOS

Um número é quase perfeito quando ele é igual à soma de seus divisores próprios, exceto um deles, conhecido como divisor redundante. Veremos adiante, proposições bem interessantes de estudos bem recentes sobre o tema e esperamos que possa incentivar o leitor, seja professores, alunos de graduação além de todos estudiosos e entusiastas do assunto. O que será desenvolvido adiante é baseado nos estudos de Pollack e Shevelev [10] e de X.Z REN e Y.G CHEN [11].

Definição 6.1. *Chamamos um número natural n de quase perfeito, se ele for igual à soma de todos os seus divisores próprios, exceto por um deles. Chamamos este divisor ausente de redundante.*

De acordo com a notação acima definida, um número natural n é quase perfeito se

$$\sigma(n) = 2n + d,$$

onde d é o divisor redundante de n.

A seguir todos os números quase perfeitos que existem entre 1 e 100.

Número quase perfeito	divisor redundante
12	4
18	3
20	2
24	12
40	10
56	8
88	4

Algumas importantes observações.

Observação 12.

1. Todo número quase perfeito não é perfeito.
2. Todo número quase perfeito é abundante.
3. Observamos que os divisores redundantes ímpares, são extremamente raros. Veremos mais adiante que os números ímpares quase perfeitos (apenas um é conhecido) possuem divisores redundantes ímpares e são quadrados perfeitos.

Para um dado $k \geqslant 1$, considere o conjunto P_k de primos da forma $2^t - 2^k - 1$, onde $t \geqslant k + 1$. Vejamos alguns exemplos desses números.

Exemplo 6.1.

k	t	$2^t - 2^k - 1$	Tipo de número
1	2	1	não é primo
1	3	5	primo
1	4	13	primo
1	5	29	primo
2	3	3	primo
2	4	11	primo
2	5	27	não é primo
2	6	59	primo

Pelo exemplo acima podemos ver que alguns elementos do conjunto P_k não são primos, mas vamos considerar apenas os primos que fazem parte do conjunto considerado.

Teorema 6.1 (Versão de Euclides para números quase perfeitos)**.** *Um número*

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

onde $2^t - 2^k - 1 \in P_k$*, é um número quase perfeito com divisor redundante* $d = 2^k$*.*

Demonstração. Considerando que $2^t - 2^k - 1$ é um primo e sabendo que 2^{t-1} é uma potência de base 2, logo só aparece 2 em sua decomposição em fatores primos podemos concluir que $\text{mdc}(2^{t-1}, 2^t - 2^k - 1) = 1$. Então $\sigma(n) = \sigma(2^{t-1}) \cdot \sigma(2^t - 2^k - 1) = (2^t - 1)(2^t - 2^k)$, logo

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

Portanto n é quase perfeito com divisor redundante 2^k. □

Como exemplo de números quase perfeitos desta forma temos os seguintes.

t	k	$2^{t-1} \cdot (2^t - 2^k - 1)$	divisor redundante 2^k
3	2	12	4
3	1	20	2
4	3	56	8
4	2	88	4
4	1	104	2

Observação 13. Existem, porém, números quase perfeitos que não podem ser expressos na forma $2^{t-1} \cdot P$, com $P \in P_k$. O inteiro 650 é um exemplo disso, seu divisor redundante é 2 e ele não pode ser expresso na forma acima.

Do Teorema 6.1, podemos provar o recíproco dele.

Teorema 6.2. *Sejam $k, t \in \mathbb{N}$ e $t \geqslant k+1$. Se $n = 2^{t-1} \cdot (2^t - 2^k - 1)$ é um número quase perfeito com divisor redundante $d = 2^k$, então $2^t - 2^k - 1$ é primo.*

Demonstração. Considerando que $n = 2^{t-1} \cdot (2^t - 2^k - 1)$ é um número quase perfeito com divisor redundante $d = 2^k$, sendo $k \geqslant 1$ e $t \geqslant k+1$, temos que $\sigma(n) - 2n = 2^k$. Na prova do Teorema 6.1, vimos que $\text{mdc}(2^{t-1}, 2^t - 2^k - 1) = 1$, portanto

$$\begin{aligned}
\sigma(2^{t-1}) \cdot \sigma(2^t - 2^k - 1) - 2 \cdot 2^{t-1} \cdot (2^t - 2^k - 1) &= 2^k; \\
(2^{t-1}) \cdot \sigma(2^t - 2^k - 1) &= 2^k + 2^t \cdot (2^t - 2^k - 1); \\
\sigma(2^t - 2^k - 1) &= \frac{2^k + 2^t \cdot (2^t - 2^k - 1)}{2^t - 1} = 2^t - 2^k.
\end{aligned}$$

Pela definição de números primos, sabemos que a soma dos divisores de um número primo é igual ao próprio número somado à unidade. Como $\sigma(2^t - 2^k - 1) = 2^t - 2^k$ equivale a $(2^t - 2^k - 1) + 1$, podemos concluir que $2^t - 2^k - 1$ é um número primo. □

Note que das Proposições 4.6, 4.7, 4.8, 4.9 e 4.10 podemos concluir que um número n quase perfeito formado por dois fatores primos é da forma $n = 2^k \cdot p^l$, com $p \geq 3$ primo. A seguir, classificamos esses números.

6.1 Classificação dos números quase perfeitos com dois fatores primos

Veremos números quase perfeitos da forma $n = 2^k \cdot m$, onde m é um número par perfeito.

Proposição 6.3. *Seja m um número perfeito par. Então $n = 2^k \cdot m$ é quase perfeito se e somente se ou $k = 1$ ou $k = p$, onde p é um primo de modo que 2^{p-1} é a maior potência de 2 que divide m.*

Demonstração. De acordo com o Teorema 5.3, $m = 2^{p-1} \cdot (2^p - 1)$, com p e $2^p - 1$ primos. Temos $n = 2^k \cdot m = 2^k \cdot 2^{p-1} \cdot (2^p - 1) = 2^{p+k-1} \cdot (2^p - 1)$. Então

$$\begin{aligned}
\sigma(n) - 2n &= \frac{2^{p+k-1+1}}{2-1} \cdot \frac{(2^p - 1)^2 - 1}{2^p - 1 - 1} - 2^{k+p} \cdot (2^p - 1), \\
&= (2^{p+k} - 1) \cdot 2^p - 2^{p+k} \cdot (2^p - 1), \\
&= 2^p \cdot (2^k - 1).
\end{aligned}$$

Que será um divisor redundante de n se e somente se $k = 1$ ou $k = p$.

□

Observação 14. Se p e $2^p - 1$ são números primos, então

$$n = 2^p(2^p - 1) = 2^p(2^{p+1} - 2^p - 1),$$

é um número quase perfeito com divisor redundante 2^p.

Segue uma lista (em formato de tabela) com números dessa forma.

p	$2^p \cdot (2^{p+1} - 2^p - 1)$	Divisor redundante (2^p)
2	12	4
3	56	8
5	992	32
7	16.256	128

Observamos que para primos maiores do que 5, o cálculo do divisor redundante fica muito trabalhoso. Podemos encontrar uma lista maior desses números em [12] e [13].

A recíproca da Proposição 6.3 também é válida. Passamos a enunciar e provar.

Proposição 6.4. *Se $n = 2^p \cdot m$ é quase perfeito com divisor redundante $d = 2^p \cdot (2^p - 1)$, então m é um par perfeito. Sendo p um primo de modo que 2^{p-1} é a maior potência de 2 que divide m.*

Demonstração. Primeiro escrevemos $m = 2^{p-1}x$, com x um numero ímpar. Como $2^p - 1$ é divisor de n, portanto de m. Temos que $x = (2^p - 1) \cdot c$, com x um numero ímpar. Assim $n = 2^{2p-1} \cdot x = 2^{2p-1} \cdot (2^p - 1) \cdot c$. Podemos calcular

$$\begin{aligned}
\sigma(n) &= 2n + d, \\
\sigma(2^{2p-1} \cdot x) &= 2^{2p} \cdot x + 2^p \cdot (2^p - 1), \\
\sigma(2^{2p-1}) \cdot \sigma(x) &= 2^{2p} \cdot (2^p - 1) \cdot c + 2^p \cdot (2^p - 1), \\
(2^p - 1)(2^p + 1) \cdot \sigma((2^p - 1) \cdot c) &= 2^{2p} \cdot (2^p - 1) \cdot c + 2^p \cdot (2^p - 1), \\
(2^p + 1) \cdot \sigma((2^p - 1) \cdot c) &= 2^p \cdot (2^p c + 2^p).
\end{aligned}$$

Se $c = 1$, então $\sigma(2^p - 1) = 2^p$. Logo $2^p - 1$ é primo. Portanto m é par perfeito. Se $c > 1$, então $\sigma((2^p - 1) \cdot c) \geq 1 + (2^p - 1) + c + (2^p - 1) \cdot c = (2^p + 1) \cdot c$. Logo $(2^p + 1) \cdot \sigma((2^p - 1) \cdot c) \geq (2^p + 1)(2^p + 1) \cdot c > 2^p \cdot (2^p + 1) \cdot c$. Isso é uma contradição. □

A seguinte proposição não conseguimos provar mas acreditamos que seja verdade.

Proposição 6.5. *Se $n = 2 \cdot m$ é quase perfeito com divisor redundante $d = 2^p$, então m é um par perfeito. Sendo p um primo de modo que 2^{p-1} é a maior potência de 2 que divide m.*

Outro tipo de número quase perfeito com dois fatores primos é o seguinte.

Proposição 6.6. *Se $2^p - 1$ um primo de Mersenne, então $n = 2^{p-1} \cdot (2^p - 1)^2$ é quase perfeito com divisor redundante $d = 2^p - 1$.*

Demonstração. Considerando $2^p - 1$ um primo de Mersenne, calculamos $\sigma(n) - 2n = (2^p - 1) \cdot ((2^p - 1)^2 + (2^p - 1) + 1) - 2^p \cdot (2^p - 1)^2 = 2^p - 1$ □

Segue uma lista (em formato de tabela) com números dessa forma.

p	$n = 2^{p-1} \cdot (2^p - 1)^2$	Divisor redundante $(2^p - 1)$
2	18	3
3	196	7
5	15.376	31
7	1.032.256	127

Fazendo uso dessa proposição podemos construir números quase perfeitos pares que são quadrados perfeitos.

Observação 15. O número $15376 = 124^2 = 2^4 \cdot 31^2$ é um quadrado perfeito e é um quase perfeito da forma $2^{5-1} \cdot (2^5 - 1)^2$ com divisor redundante 31, já que

$$\sigma(15376) = \frac{2^5 - 1}{2 - 1} \cdot \frac{31^3 - 1}{31 - 1} = 30783 = 2 \cdot 15376 + 31.$$

No caso de números ímpares quase perfeitos que são quadrados perfeitos, veremos na última seção deste capítulo. Agora, vamos provar a recíproca da Proposição 6.6.

Proposição 6.7. *Se $n = 2^{p-1} \cdot (2^p - 1)^2$ é quase perfeito com divisor redundante $d = 2^p - 1$ e p é primo, então $2^p - 1$ é primo.*

Demonstração. Seja $x = 2^p - 1$ um numero ímpar. Logo $n = 2^{p-1}x^2$. Se n é quase perfeito com divisor redundante $d = 2^p - 1$, então

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

Levando em consideração a Proposição 4.3 temos que x é primo. □

Usando o Teorema 6.1, Proposição 6.3 e Proposição 6.6 temos a construção de três tipos de números quase perfeitos com dois fatores primos.

- *Tipo 1:* $n = 2^{t-1} \cdot (2^t - 2^k - 1)$, onde $2^t - 2^k - 1$ é primo e 2^k é um divisor redundante.

- *Tipo 2:* $n = 2^{2p-1} \cdot (2^p - 1)$, onde p e $2^p - 1$ são primos e $2^p \cdot (2^p - 1)$ é um divisor redundante.
- *Tipo 3:* $n = 2^{p-1} \cdot (2^p - 1)^2$, onde p e $2^p - 1$ são primos e $2^p - 1$ é um divisor redundante.

Essas construções foram feitas por Pollack e Shevelev em [10].

Observação 16. Note que o número 40 é quase perfeito com divisor redundante 10. E também podemos ver que o número 40 não é do tipo 1, não é do tipo 2 e não é do tipo 3.

Entre os 39 primeiros números quase perfeitos listados em [12], exceto para o número 40, temos:

	Números quase perfeitos
Tipo 1	12, 20, 56, 88, 104, 368, 464, 992, 1.504, 1.888, 1.952, 16.256, 24.448, 28.544, 30.592, 32.128, 98.048, 122.624, 128.768, 130.304, 507.392
Tipo 2	24, 224, 15.872
Tipo 3	18, 196, 15.376
Que possuem 3 fatores primos distintos	234, 650, 3.724, 5.624, 9.112, 11.096, 13.736, 17.816, 77.744, 174.592, 396.896

Assim podemos enunciar o seguinte teorema que classifica os números quase perfeitos com dois fatores primos.

Teorema 6.8. *Todos os números quase perfeitos com 2 fatores primos distintos são do tipo 1, 2 e 3, junto com o 40.*

Antes de provar o teorema acima, vamos provar alguns lemas técnicos.

Lema 6.1. *Se $n = 2^a \cdot q$ é um número quase perfeito com divisor redundante $d = 2^s \cdot q$, onde q é um primo ímpar, então $n=40$ ou n é do tipo 2.*

Demonstração. Visto que $n = 2^a \cdot q$ é um número quase perfeito com divisor redundante $d = 2^s \cdot q$ temos que $\sigma(n) = 2 \cdot n + d$, colocando os valores de n e d obtemos que

$$(2^{a+1} - 1) \cdot (q + 1) = 2^{a+1} \cdot q + 2^s \cdot q.$$

Reduzindo a expressão e agrupando temos

$$(2^s + 1) \cdot q = 2^{a+1} - 1. \tag{6.1}$$

Como a igualdade no lado esquerdo é ímpar, isso implica que o lado direito também é ímpar, portanto $s \geqslant 1$. Aplicando o Algoritmo da Divisão para $a+1$ e s temos que existem únicos inteiros k e r com $0 \leqslant r < s$ tais que $a+1 = k \cdot s + r$. Assim podemos calcular

$$2^{a+1} - 1 = 2^{k \cdot s + r} - 1 \equiv (-1)^k \cdot 2^r - 1 \pmod{2^s + 1}. \tag{6.2}$$

Dado que $(2^s+1) \cdot q = 2^{a+1} - 1$ e (6.2), segue que $2^s + 1 \mid (-1)^k \cdot 2^r - 1$. Por outro lado temos que $|(-1)^k \cdot 2^r - 1| \leqslant 2^r + 1 < 2^s + 1$, assim concluímos que $(-1)^k \cdot 2^r - 1 = 0$. Isto implica que $k = 2m$ para algum $m \in \mathbb{N}$ e $r = 0$. Substituindo esses valores em (6.1) e agrupando adequadamente obtemos

$$q = (2^s - 1) \cdot \frac{2^{2m \cdot s} - 1}{2^{2s} - 1} \text{ e } a + 1 = 2m \cdot s. \tag{6.3}$$

Visto que q é um primo ímpar, segue-se que ou $2^s - 1 = 1$ ou $2^{2sm} - 1 = 2^{2s} - 1$. Portanto $s = 1$ ou $m = 1$. Se $s = 1$, então $a + 1 = 2m$. Novamente, substituindo esses valores em (6.1) obtemos $3q = (2^m - 1) \cdot (2^m + 1)$. Dado que $\text{mdc}(2^m - 1, 2^m + 1) = 1$ e $q \geqslant 3$, segue-se que $m = 2$, $q = 5$ e $a = 3$. Portanto $n = 40$. No caso de $m = 1$, substituindo em (6.3) temos $q = 2^s - 1$ é um primo ímpar e $a = 2s - 1$. Consequentemente $n = 2^{2s-1} \cdot (2^s - 1)$ é do tipo 2. Isso acaba com a prova do lema. □

Lema 6.2. *Sejam q um número primo ímpar, a e b números naturais com $b \geqslant 2$. Se $n = 2^a \cdot q^b$ é um número quase perfeito com divisor redundante d, então $q^b \nmid d$.*

Demonstração. A prova será feita por contradição, ou seja, assumiremos que $d = 2^s \cdot q^b$, com $0 \leqslant s \leqslant a - 1$. Dado que n é quase perfeito temos que $\sigma(n) = 2n + d$, segue-se que

$$(2^{a+1} - 1) \cdot (1 + q + \cdots + q^b) = (2^{a+1} + 2^s) \cdot q^b. \tag{6.4}$$

Se b for par, então $(1 + q + \cdots + q^b)$ é ímpar. Assim, de (6.4) deduzimos que $s = 0$. Substituindo em (6.4) temos

$$(2^{a+1} - 1) \cdot (1 + q + \cdots + q^b) = (2^{a+1} + 1) \cdot q^b. \tag{6.5}$$

Visto que $\text{mdc}(2^{a+1} - 1, 2^{a+1} + 1) = 1$ e $\text{mdc}(1 + q + \cdots + q^b, q^b) = 1$, segue-se que

$$2^{a+1} - 1 = q^b \text{ e } 1 + q + \cdots + q^b = 2^{a+1} + 1,$$

Pois como $\text{mdc}(2^{a+1} - 1, 2^{a+1} + 1) = 1$ então $2^{a+1} - 1 \neq 2^{a+1} + 1$ e como $\text{mdc}(1 + q + \cdots + q^b, q^b) = 1$, então não podem ser iguais entre eles. Assim,

$$2^{a+1} + 1 = 2^{a+1} - 1 + 2 = q^b + 2 < 1 + q + \cdots + q^b = 2^{a+1} + 1,$$

já que $b \geq 2$ e $q \geq 3$. Isso é uma contradição.

Se b é ímpar, então $1 + q + \cdots + q^b$ é par. Assim, o lado esquerdo (1º membro) da equação (6.4) é par. Assim, $s \geqslant 1$. De (6.4) temos que $2^s \mid (1 + q + \cdots + q^b)$ (pois ambos serão pares) e $(2^{a+1}-1)\cdot(1+q+\cdots+q^{b-1})=(2^s+1)\cdot q^b$. Por $(2^{a+1}-1)\cdot(1+q+\cdots+q^b) = (2^s+1)\cdot q^b$ e $\text{mdc}(q^b, 1+q+\cdots+q^b) = 1$, $1+q+\cdots+q^{b-1} \mid 2^s+1$ (ambos são ímpares) e daqui tiramos que $2^s + 1 \geqslant 1 + q + \cdots + q^{b-1}$. Dividiremos em 2 casos de acordo com o valor de b.

Caso 1: $b \equiv 1 \pmod 4$. Dado que $1+q+\cdots+q^b = (1+q)\cdot(1+q^2+q^4+\cdots+q^{b-1})$ e $1+q^2+q^4+\cdots+q^{b-1} \equiv \frac{b+1}{2} \not\equiv 0 \pmod 2$, segue de (2.2) que $2^s \mid 1+q$. Assim, por $b \geqslant 3$, temos $2^s + 1 \leqslant q + 2 < 1 + q + \cdots + q^{b-1}$, uma contradição com $1 + q + \cdots + q^b \mid 2^s + 1$.

Caso 2: $b \equiv 3 \pmod 4$. Dado que $1+q+\cdots+q^b=(1+q)\cdot(1+q+q^4+q^5+\cdots+q^{b-3}+q^{b-2})$ e $4 \nmid (1+q^2)$, segue de $2^s \mid (1+q+\cdots+q^b)$ que $2^{s-1} \mid (1+q+q^4+q^5+\cdots+q^{b-3}+q^{b-2})$. Assim, por $1 + q + \cdots + q^b \mid 2^s + 1$ e $b \geqslant 3$,

$$q \cdot 2^{s-1} \leqslant q \cdot (1 + q + q^4 + q^5 + \cdots + q^{b-3} + q^{b-2}) \leqslant 2^s + 1 - 1 = 2^s,$$

uma contradição com q sendo um primo ímpar. □

Considerando os lemas anteriores, passamos a provar o Teorema 6.8.

Demostração do Teorema 6.8. Seja $n = p^a q^b$ um número quase perfeito com divisor redundante d, onde p e q são dois primos com $p < q$ e a, b dois inteiros positivos. Então, $\sigma(n) = 2n + d$, portanto n é abundante. Pela Proposição 4.7, Proposição 4.8, Proposição 4.9 e Proposição 4.10 concluímos que $p = 2$ e $q \geq 3$. Consequentemente, $d = 2^s \cdot q^t$, com $0 \leqslant s \leq a$ e $0 \leqslant t \leq b$. Assim, $\sigma(n) = 2n + d$ torna-se

$$(2^{a+1} - 1) \cdot (1 + q + \cdots + q^b) = 2^{a+1} \cdot q^b + 2^s \cdot q^t. \tag{6.6}$$

Dividimos em 3 casos de acordo com o valor de b.

- Caso 1: $b = 1$. Então $t \in \{0, 1\}$. Se $t = 0$, então, por (6.6) deduzimos que $q = 2^{a+1} - 2^s - 1$ é um primo ímpar e $d = 2^s$. Assim, $n = 2^a \cdot (2^{a+1} - 2^s - 1)$ é do tipo 1. Se $t = 1$, então $n = 2^a \cdot q$ é um número quase perfeito com divisor redundante $d = 2^s \cdot q$. Aplicando o Lema 6.1 concluímos que $n = 40$ ou n é do tipo 2.

- Caso 2: $b = 2$. Então, $q^2 \nmid d$, pelo Lema 6.2. Assim $t \in \{0, 1\}$. Novamente usando $b = 2$ temos que $1 + q + q^2$ é ímpar. Assim, o lado direito da equação (6.6) é ímpar e deduzimos que $s = 0$. Se $t = 0$, então por (6.6) obtemos

$$(2^{a+1} - 1) \cdot (1 + q + q^2) = 2^{a+1} \cdot q^2 + 1.$$

Reduzindo a expressão chegamos $(2^{a+1} - q) \cdot (1 + q) = 2$. Isso é uma contradição com os valores de q. Consequentemente $t = 1$. Por (6.6) obtemos

$$(2^{a+1} - 1) \cdot (1 + q + q^2) = 2^{a+1} \cdot q^2 + q.$$

Reduzindo novamente a expressão chegamos $q = 2^{a+1} - 1$ é um primo ímpar. Portanto, $n = 2^a \cdot (2^{a+1} - 1)^2$ é do tipo 3.

- Caso 3: $b \geqslant 3$. Então, $0 \leqslant t \leqslant b - 1$, pelo Lema 6.2. A igualdade (6.6) pode ser reescrita como

$$(2^{a+1} - q) \cdot (1 + q + \cdots + q^{b-1}) = 1 + 2^s \cdot q^t. \tag{6.7}$$

Se $q \leq 2^a$, então o lado esquerdo da equação (6.7) é maior ou igual a

$$2^a \cdot (1 + q + \cdots + q^{b-1}).$$

Como $b \geqslant 3$ e $q^b \nmid d$ temos que o lado direito da equação (6.7) é menor ou igual a $1 + 2^a \cdot q^{b-1} < 2^a \cdot (1 + q + \cdots + q^{b-1})$. Isso é uma contradição. Consequentemente, $q > 2^a$. Dado que o lado esquerdo da equação (6.7) é pelo menos

$$(1 + q + \cdots + q^{b-1}) > 1 + q^2 \geqslant 1 + 2^a \cdot q \geqslant 1 + 2^s \cdot q,$$

temos $t \geqslant 2$. Por (6.7) temos que $q \mid 2^{a+1} - 1$, uma contradição com $q \geqslant 2^a$.

□

Agora veremos algumas generalizações no caso de um número quase perfeito com três fatores primos.

6.2 Uma generalização para números quase perfeitos com 3 fatores primos

Em 2015, Yanbin Li e Qunying Liao [14] publicaram um artigo onde forneciam 2 condições equivalentes para todos os números quase perfeitos pares da forma

$$2^k \cdot p_1 \cdot p_2 \text{ e } 2^k \cdot p_1^2 \cdot p_2, \text{ com } p_1, p_2 \text{ primos e } p_1 < p_2.$$

A seguir mostraremos os teoremas e suas respectivas provas dadas pelos autores citados.

6.2.1 Números quase perfeitos da forma $2^k \cdot p_1 \cdot p_2$

Lema 6.3. *Seja* $n = p_1^{k_1} \dots p_i^{k_i} \dots p_r^{k_r}$, *com* p_i *sendo primos distintos,* $\sigma(n) = 2n + d$, $\sigma(p_i^k) = p_i^k + \dots + p_1 + 1$ *e* $\sigma(n) = \prod_{i=1}^{r} \sigma(p_i^k) = \sigma(p_i^k) \cdot \sigma(\frac{n}{p_i^k})$. *Então*

1. *Se* $p_i \mid d$, *então* $p_i \mid \sigma(\frac{n}{p_i^{k_i}})$
2. *Se* $p_i \nmid d$, *então* $p_i \mid \sigma(\frac{n}{p_i^{k_i}}) - d$

Demonstração. 1. Suponha $p_i \mid d$, $2n + d = \sigma(n) = \sigma(p_i^k) \cdot \sigma(\frac{n}{p_i^k})$. Como $p_i \mid n$ e $p_i \mid d$, temos que $p_i \mid 2n + d$, logo $p_i \mid \sigma(n)$, ou seja, $p_i \mid \sigma(p_i^k) \cdot \sigma(\frac{n}{p_i^k})$. Como p_i é um primo, então $p_i \mid \sigma(p_i^k)$ ou $p_i \mid \sigma(\frac{n}{p_i^k})$. Mas, $\sigma(p_i^k) = p_i^k + p_i^{k+1} + \dots + 1$. Vejamos que $p_i \nmid \sigma(p_i^k)$. Suponha que $p_i \mid \sigma(p_i^k)$, então $\sigma(p_i^k) = k \cdot p_i = p_i^k + \dots + p_i + 1$. Com isso, $1 = p_i \cdot (k - p_i^{k-1} - \dots - 1)$, o que é uma contradição. Como $p_1 \nmid \sigma(p_i^k)$, então $p_i \mid \sigma(\frac{n}{p_i^k})$.

2. Suponha $p_1 \nmid d$, $\sigma(n) = \sigma(p_i^k) \cdot \sigma(\frac{n}{p_i^k})$. Somando $-\sigma(p_i^k) \cdot d$ a ambos os membros da equação, teremos

$$\begin{aligned}
\sigma(n) - \sigma(p_i^k) \cdot d &= \sigma(p_i^k) \cdot [\sigma(\frac{n}{p_i^k}) - d] \\
2 \cdot n + d - (p_i^k + \dots + 1) \cdot d &= \sigma(p_i^k) \cdot [\sigma(\frac{n}{p_i^k}) - d]; \\
2 \cdot n - (p_i^k + \dots + p_i) \cdot d &= \sigma(p_i^k) \cdot [\sigma(\frac{n}{p_i^k}) - d]; \\
2 \cdot n - p_i \cdot (p_i^{k-1} + \dots + 1) \cdot d &= \sigma(p_i^k) \cdot [\sigma(\frac{n}{p_i^k}) - d].
\end{aligned}$$

Como $p_i \mid n$, então $p_i \mid 2 \cdot n - p_i \cdot (p_i^{k-1} + \dots + 1) \cdot d$. Logo, $p_i \mid \sigma(p_i^k) \cdot [\sigma(\frac{n}{p_i^k}) - d]$, então $p_i \mid \sigma(p_i^k)$ ou $p_i \mid \sigma(\frac{n}{p_i^k}) - d$. Como sabemos que $p_i \nmid \sigma(p_i^k)$, é verdadeiro que $\sigma(\frac{n}{p_i^k}) - d$.

□

Teorema 6.9. *Seja* k *um número inteiro positivo. Suponha que ambos* p_1 *e* p_2 *sejam primos ímpares com* $p_1 < p_2$. *Então,* $n = 2^k \cdot p_1 \cdot p_2$ *é um quase perfeito se, e somente se, uma das seguintes condições são verdadeiras:*

1. $p_1 = \frac{2^{k+1}-1+t}{2^l+1-t}$, *onde* $t = \frac{2^{k+1}-1}{p_2}$ *e* $1 \leqslant l \leqslant k-1$. *Nesse caso, o divisor redundante é* $2^l \cdot p_1 \cdot p_2$.
2. $p_1 = 2^{k+1}-1+\frac{2^k-2^{l-1}}{t}$, *onde* t *é determinado pela equação* $p_2 = (2^{k+1}-1)\cdot(2\cdot t+1)-2^l$, $1 \leqslant l \leqslant k$. *Nesse caso, o divisor redundante é* $2^l \cdot p_1$.

3. $p_2 = 2^{k+1} - 1 + \frac{2^{2k+1} - 2^k - 2^{l-1}}{t}$, *onde* $t = \frac{p_1 - (2^{k+1} - 1)}{2}$ *e* $1 \leqslant l \leqslant k$. *Nesse caso, o divisor redundante é* 2^l.

Demonstração.

1. Começaremos provando a suficiência da primeira condição. Partindo do pressuposto que $p_1 = \frac{2^{k+1} - 1 + t}{2^l + 1 - t}$,onde $t = \frac{2^{k+1} - 1}{p_2}$ e $1 \leqslant l \leqslant k - 1$, temos:

$$(2^l + 1 - t) \cdot p_1 = 2^{k+1} - 1 + t$$
$$(2^l + 1) \cdot p_1 = 2^{k+1} - 1 + t + p_1 \cdot t$$

e $p_2 \cdot t = 2^{k+1} - 1$, logo $p_2 = \frac{2^{k+1} - 1}{t}$. Note que $n = 2^k \cdot p_1 \cdot p_2$, portanto

$$\begin{aligned}\sigma(n) &= (2^{k+1} - 1) \cdot (1 + p_1) \cdot (1 + p_2) \\ &= 2^{k+1} + 2^{k+1} \cdot p_2 - 1 - p_1 + 2^{k+1} \cdot p_2 + 2^{k+1} \cdot p_1 \cdot p_2 - p_2 - p_1 \cdot p_2\end{aligned}$$

$$\begin{aligned}\sigma(n) - 2 \cdot n =& 2^{k+1} + 2^{k+1} \cdot p_2 - 1 - p_1 + 2^{k+1} \cdot p_2 + 2^{k+1} \cdot p_1 \cdot p_2 - p_2 - p_1 \cdot p_2 \\ & - 2 \cdot 2^k \cdot p_1 \cdot p_2 \\ =& 2^{k+1} + 2^{k+1} \cdot p_1 + 2^{k+1} \cdot p_2 - 1 - p_1 - p_2 - p_1 \cdot p_2 \\ =& 2^{k+1} \cdot (1 + p_1 + p_2) - (1 + p_1 + p_2) - p_1 \cdot p_2 \\ =& (2^{k+1} - 1) \cdot (1 + \frac{2^{k+1} - 1}{t} + p_1) - p_1 \cdot \frac{2^{k+1} - 1}{t} \\ =& (2^{k+1} - 1) \cdot (\frac{t + 2^{k+1} - 1 + p_1 \cdot t}{t}) - p_1 \cdot (\frac{2^{k+1} - 1}{t}) \\ =& (2^{k+1} - 1) \cdot (\frac{2^l + 1}{t}) \cdot p_1 - p_1 \cdot (\frac{2^{k+1} - 1}{t}) \\ =& (\frac{2^{k+1} - 1}{t}) \cdot p_1 \cdot (2^l + 1 - 1) \\ =& 2^l \cdot p_1 \cdot p_2\end{aligned}$$

Note que $1 \leqslant l \leqslant k - 1$, logo $2^l \cdot p_1 \cdot p_2 \mid n$ e $2^l \cdot p_1 \cdot p_2 \neq n$. Portanto, da definição de números quase perfeitos, $n = 2^k \cdot p_1 \cdot p_2$ é um quase perfeito com divisor redundante $2^l \cdot p_1 \cdot p_2$.

Reciprocamente, supondo $n = 2^k \cdot p_1 \cdot p_2$ é um quase perfeito com divisor redundante d, primeiro vamos concluir que $2^l \cdot p_2$ $(1 \leqslant l \leqslant k)$. Por contradição, considerando $d = 2^l \cdot p_2$ e pelo Lema 6.3, temos $p_2 \mid \sigma(2^k p_1) = (2^{k+1} - 1) \cdot (p_1 + 1)$. Note que $p_1 < p_2$ e $mdc(p_2, p_1 + 1) = 1$, portanto $p_2 \mid (2^{k+1} - 1)$. Tomando $2^{k+1} - 1 = k \cdot p_2$,

então

$$2^l \cdot p_2 = d = \sigma(n) - 2n = (2^{k+1} - 1) \cdot (p_1 + 1) \cdot (p_2 + 1) - 2^{k+1} \cdot p_1 \cdot p_2$$
$$= p_2 \cdot [(2^{k+1} - 1) + (t - 1) \cdot (p_1 + 1) + 1]$$

por isso $2^l = 2^{k+1} - 1 + (t - 1) \cdot (p_1 + 1) + 1$. Mas de $1 \leqslant l \leqslant k$, temos $2^{k+1} - 1 + (t - 1) \cdot (p_1 + 1) + 1 \geqslant 2^{k+1} > 2^l$, o que é uma contradição.
Portanto o divisor redundante deve ser da forma 2^l, $2^l \cdot p_1$, com $(1 \leqslant l \leqslant k)$ ou $2^l \cdot p_1 \cdot p_2$ com $(1 \leqslant b \leqslant k - 1)$. Supondo $d = 2^l \cdot p_1 \cdot p_2$ com $(1 \leqslant l \leqslant k - 1)$, então, do Lema 6.3, $p_2 \mid \sigma(2^k \cdot p_1) = (2^{k+1} - 1) \cdot (p_1 + 1)$. Note que $mdc(p_2, p_1 + 1) = 1$, portanto $p_2 \mid (2^{k+1} - 1)$. Tomando $2^{k+1} - 1 = t \cdot p_2$, então

$$2^l \cdot p_1 \cdot p_2 = d = \sigma(n) - 2n = t \cdot p_2 \cdot (p_1 + 1) \cdot (p_2 + 1) - (k \cdot p_2 + 1) \cdot p_1 \cdot p_2.$$

Com isso, $(2^l + 1) \cdot p_1 = k \cdot (p_1 + p_2 + 1)$. Portanto $\frac{2^{k+1}-1+t}{2^l+1-t}$.

2. Agora, provaremos a suficiência da segunda condição. Partindo do pressuposto que $p_1 = 2^{k+1} - 1 + \frac{2^k - 2^{l-1}}{t}$, onde $p_2 = (2^{k+1} - 1) \cdot (2 \cdot t + 1) - 2^l$, com $1 \leqslant l \leqslant k$, $p_1 = \frac{t \cdot (2^{k+1}-1) + 2^k - 2^{l-1}}{t}$. Note que $n = 2^k \cdot p_1 \cdot p_2$, portanto

$$\begin{aligned}\sigma(n) - 2n =& (2^{k+1} - 1) \cdot (p_1 + 1) \cdot (p_2 + 1) - 2 \cdot 2^k \cdot p_1 \cdot p_2 \\ =& (2^{k+1} \cdot p_1 + 2^{k+1} - p_1 - 1) \cdot (p_2 + 1) \\ & - 2^{k+1} \cdot p_1 \cdot p_2 (2^{k+1} - 1) \cdot (1 + p_1 + p_2) - p_1 \cdot p_2.\end{aligned}$$

Substituindo os valores de p_1 e de p_2 pressupostos anteriormente e fazendo $2^{k+1} - 1 = c$, teremos

$$c \cdot [1 + \frac{t \cdot c + 2^k - 2^{l-1}}{t} + c \cdot (2 \cdot t + 1) - 2^l - (2 \cdot t + 1) \cdot \frac{t \cdot c + 2^k - 2^{l-1}}{t}] + p_1 \cdot 2^l = p_1 \cdot 2^l.$$

Note que $1 \leqslant l \leqslant k$, logo $2^l \cdot p_1 \mid n$, e, $2^l \cdot p_1 \neq n$. Portanto, pela definição de números quase perfeitos, $n = 2^k \cdot p_1 \cdot p_2$ é um quase perfeito com divisor redundante $2^l \cdot p_1$.

Reciprocamente, supondo que $d = 2^l \cdot p_1$, com $(1 \leqslant l \leqslant k)$, então, do Lema 6.3 temos $p_1 \mid \sigma(2^k \cdot p_2) = (2^{k+1} - 1) \cdot (p_2 + 1)$, portanto, $p - 1 \mid (2^{k+1} - 1)$ ou $p_1 \mid (p_2 + 1)$. Se $p_1 \mid (2^{k+1} - 1)$, então $2^{k+1} - 1 = t \cdot p_1$, logo

$$\begin{aligned}2^l \cdot p_1 = d = \sigma(n) - 2n =& t \cdot p_1 \cdot (p_1 + 1) \cdot (p_2 + 1) - (t \cdot p_1 + 1) \cdot p_1 \cdot p_2, \\ =& p_1 \cdot [2^{k+1} + (t - 1) \cdot (p_2 + 1)].\end{aligned}$$

Com isso $2^l = 2^{k+1} + (t-1)\cdot(p_2+1)$. Note que $1 \leqslant l \leqslant k$, portanto

$$2^{k+1} + (t-1)\cdot(p_2+1) \geqslant 2^{k+1} > 2^l,$$

o que é uma contradição. Portanto $p_1 \nmid (2^{k+1}-1)$, então temos que $p_1 \mid (p_2+1)$. Logo $p_2 = 2\cdot t\cdot p_1 - 1$. Então, de

$$\begin{aligned} 2^l \cdot p_1 = d = \sigma(n) - 2n =& (2^{k+1}-1)\cdot(p_1+1)\cdot 2\cdot t\cdot p_1 - 2^{k+1}\cdot p_1\cdot(2\cdot t\cdot p_1 - 1), \\ =& 2\cdot p_1[t\cdot(2^{k+1}-1-p_1) + 2^k] \end{aligned}$$

Teremos então $p_1 = 2^{k+1} - 1 + \frac{2^k - 2^{l-1}}{t}$.

3. Agora, provaremos a suficiência da terceira condição. Partindo do pressuposto que $p_2 = 2^{k+1} - 1 + \frac{2^{k+1} - 2^k - 2^{l-1}}{t}$, $t = \frac{p_1 - (2^{k+1}-1)}{2}$, $1 \leqslant\ l \leqslant k$, teremos

$$p_2 = 2^{k+1} - 1 + \frac{2^k\cdot(2^{k+1}-1) - 2^{l-1}}{t},$$

e $p_1 = 2\cdot t + (2^{k+1}-1)$. Note que $n = 2^k\cdot p_1\cdot p_2$, portanto

$$\begin{aligned} \sigma(n) - 2n =& (2^{k+1}-1)\cdot(1+p_1+p_2) - p_1\cdot p_2, \\ =& (2^{k+1}-1)\cdot(1+2\cdot t + 2^{k+1} - 1 + p_2) - (2\cdot t + 2^{k+1} - 1)\cdot p_2. \end{aligned}$$

Fazendo $2^{k+1} - 1 = c$, temos

$$c\cdot(1+2\cdot t + c + p_2) - (2\cdot t + c)\cdot p_2 = c + c^2 + 2\cdot t\cdot(c - p_2),$$

substituindo p_2 pelo pressuposto anteriormente, teremos $c + c^2 - 2^{k+1}\cdot c + 2^l$. Voltando com $c = 2^{k+1} - 1$ teremos

$$2^{k+1} - 1 + (2^{k+1}-1)^2 - 2^{k+1}\cdot(2^{k+1}-1) + 2^l = 2^l.$$

Portanto, pela definição de números quase perfeitos $n = 2^k\cdot p_1\cdot p_2$ é um quase perfeito com divisor redundante 2^l.

Reciprocamente, supondo que $d = 2^l$, com $1 \leqslant l \leqslant k$, então $p_2 \nmid d$. Pelo Lema 6.3, temos $p_2 \mid (\sigma(2^k\cdot p_1) - d = (2^{k+1}-1)\cdot(p_1+1) - 2^l$. Assim

$$(2^{k+1}-1)\cdot(p_1+1) - 2^l = 2\cdot t\cdot p_2,$$

o seja, $2 \cdot t \cdot p_2 + 2^l = (2^{k+1} - 1) \cdot (p_1 + 1)$. Então,

$$\begin{aligned} 2^l = d = \sigma(n) - 2n =& (2 \cdot t \cdot p_2 + 2^l) \cdot (p_2 + 1) - 2^{k+1} \cdot p_1 \cdot p_2, \\ =& p_2 \cdot [2 \cdot t \cdot (p_2 + 1) + 2^l - 2^{k+1} \cdot p_1] + 2^l. \end{aligned}$$

Consequentemente

$$\begin{aligned} & 2 \cdot t \cdot (p_2 + 1) + 2^l - 2^{k+1} \cdot p_1 = 0 \\ & 2 \cdot t \cdot p_2 + 2 \cdot t + 2^l - 2^{k+1} \cdot p_1 = 0. \end{aligned}$$

Mas, $2 \cdot t \cdot p_2 + 2^l = (2^{k+1} - 1) \cdot (p_1 + 1)$, então $(2^{k+1} - 1) \cdot (p_1 + 1) + 2 \cdot t - 2^{k+1} \cdot p_1 = 0$. Assim, $p_1 = 2^{k+1} - 1 + 2^t$. Por outro lado, substituindo $p_1 = 2^{k+1} - 1 + 2^t$ na equação $2 \cdot t \cdot p_2 + 2 \cdot t + 2^l - 2^{k+1} \cdot p_1 = 0$, teremos

$$\begin{aligned} 2 \cdot t \cdot p_2 =& 2^{k+1} \cdot (2^{k+1} - 1 + 2 \cdot t) - 2 \cdot t - 2^l, \\ p_2 =& \frac{2^{k+1} \cdot (2^{k+1} - 1 + 2 \cdot t) - 2 \cdot t - 2^l}{2 \cdot t}, \\ =& 2^{k+1} - 1 + \frac{2^{2 \cdot k+1} - 2^k - 2^{l-1}}{t}. \end{aligned}$$

Assim, finalizamos a prova do Teorema 6.9.

□

6.2.2 Números quase perfeitos da forma $2^k \cdot p_1^2 \cdot p_2$

Teorema 6.10. *Seja k um inteiro positivo. Suponha que ambos p_1 e p_2 sejam primos ímpares com $p_1 < p_2$. Então, $n = 2^k \cdot p_1^2 \cdot p_2$ é quase perfeito se e somente se uma das sentenças for verdadeira.*

1. *Existe algum l e q, tais que $1 \leqslant l \leqslant k$, $0 \leqslant q \leqslant 2$, e o divisor redundante*

$$d = 2^l \cdot p_1^q = (2^{k+1} - 1) \cdot (p_1^2 + p_1 + 1) - t \cdot p_2,$$

onde $t = p_1^2 - (2^{k+1} - 1) \cdot (p_1 + 1)$.

2. *Existe algum l, tal que $1 \leqslant l \leqslant k$, e o divisor redundante*

$$d = 2^l \cdot p_2 = (2^{k+1} - 1) \cdot (p_2 + 1) - 2 \cdot t \cdot p1,$$

onde $2 \cdot t = p_1 \cdot p_2 - (2^{k+1} - 1) \cdot (p_1 + p_2 + 1)$.

3. *Existe algum l e q, tais que $1 \leqslant l \leqslant k$, $1 \leqslant q \leqslant 2$, e $2^l \cdot p_1^q = (2^{k+1}-1)\cdot(p_1+1)+t-p_1^2$, onde $t = \frac{(2^{k+1}-1)\cdot(p_1^2+p_1+1)}{p_2}$. Neste caso, o divisor redundante é $d = 2^l \cdot p_1^q \cdot p_2$*

Demonstração.

1. Começaremos provando a suficiência da primeira condição. Partindo do pressuposto que temos

$$t \cdot p_2 + d + t = (2^{k+1} - 1) \cdot (p_1^2 + p_1 + 1) + p_1^2 - (2^{k+1} - 1) \cdot (p_1 + 1) = 2^{k+1} \cdot p_1^2,$$

Note que $n = 2^k \cdot p_1^2 \cdot p_2$, então

$$\begin{aligned}\sigma(n) - 2n =&(2^{k+1} - 1) \cdot (p_1^2 + p_1 + 1) \cdot (p_2 + 1) - 2^{k+1} \cdot p_1^2 \cdot p_2\\ =&(t \cdot p_2 + d) \cdot (p_2 + 1) - 2^{k+1} \cdot p_1^2 \cdot p_2\\ =&p_2 \cdot [t \cdot (p_2 + 1) + d - 2^{k+1} \cdot p_1^2] + d\\ =&p_2 \cdot 0 + d = d.\end{aligned}$$

e, como $d = 2^l \cdot p_1^q$, com $(1 \leqslant l \leqslant k,\ 0 \leqslant q \leqslant 2)$, podemos obter $d \mid n$ e $d \neq n$. Assim, da definição de números quase perfeitos sabemos que $n = 2^k \cdot p_1^2 \cdot p_2$ é quase perfeito com divisor redundante $d = 2^l \cdot p_1^q$.

Reciprocamente, se $d = 2^l \cdot p_1^q$, com $(1 \leqslant l \leqslant k,\ 0 \leqslant q \leqslant 2)$, então $p_2 \nmid d$. Pelo Lema 6.3, temos $p_2 \mid (\sigma(2^k \cdot p_1^2) - d) = (2^{k+1} - 1) \cdot (p_1^2 + p_1 + 1) - d$. Assim

$$(2^{k+1} - 1) \cdot (p_1^2 + p_1 + 1) - d = t \cdot p_2.$$

Note que n é quase perfeito com divisor redundante d, portanto

$$\begin{aligned}d =&\sigma(n) - 2n\\ =&[(2^{k+1} - 1) \cdot (p_1^2 + p_1 + 1) - d] \cdot (p_2 + 1) + d \cdot (p_2 + 1) - 2^{\alpha+1} \cdot p_1^2 \cdot p_2\\ =&t \cdot p_2 \cdot (p_2 + 1) + d \cdot (p_2 + 1) - 2^{k+1} \cdot p_1^2 \cdot p_2\\ =&p_2 \cdot [t \cdot (p_2 + 1) + d - 2^{k+1} \cdot p_1^2] + d.\end{aligned}$$

Mas, $t \cdot (p_2 + 1) + d - 2^{k+1} \cdot p_1^2 = 0$, portanto $t \cdot p_2 = 2^{k+1} \cdot p_1^2 - t - d$. Da equação $2^{k+1}-1\cdot(p_1^2+p_1+1)-d = t\cdot p_2$, concluímos que $2^{k+1}\cdot p_1^2 - t = (2^{k+1}-1)\cdot(p_1^2+p_1+1)$. Consequentemente $t = p_1^2 - (2^{k+1} - 1) \cdot (p_1 + 1)$.

2. Começaremos provando a suficiência da segunda condição. Note que $n = 2^k \cdot p_1^2 \cdot p_2$,

então

$$\begin{aligned}\sigma(n)-2n=d=&2^l\cdot p_2=(2^{k+1}-1)\cdot(p_2+1)-2\cdot t\cdot p_1\\ =&(2^{k+1}-1)\cdot(p_1^2+p_1+1)\cdot(p_2+1)-2^{k+1}\cdot p_1^2\cdot p_2\\ =&(2^{k+1}-1)(\cdot(p_2+1)-(2^{k+1}-1)\cdot(p_2+1)\cdot(p_1^2+p_1+1)+2^{k+1}\cdot p_1^2\cdot p_2\\ =&p_1\cdot p_2-(2^{k+1}-1)\cdot(p_1+p_2+1).\end{aligned}$$

Reciprocamente, se $d=2^l\cdot p_2$, com $(1\leqslant l\leqslant k)$, então $p_1\nmid d$. Do Lema 6.3, temos $p_1\mid(\sigma(2^k\cdot p_2)-d)=(2^{k+1}-1)\cdot(p_2+1)-2^l\cdot p_2$. Logo, $2^k\cdot p_2=(2^{k+1}-1)\cdot(p_2+1)-2\cdot t\cdot p_1$. Assim, de

$$\begin{aligned}2^l\cdot p_2=&d\\ =&\sigma(n)-2n\\ =&[(2^{k+1}-1)\cdot(p_2+1)-2^l\cdot p_2]\cdot(p_1^2+p_1+1)+2^l\cdot p_2\cdot(p_1^2+p_1+1)\\ &-2^{k+1}\cdot p_1^2\cdot p_2\\ =&p1[2\cdot t\cdot(p_1^2+p_1+1)+2^l\cdot p_2\cdot(p_1+1)-2^{k+1}\cdot p_1\cdot p_2]+2^l\cdot p_2\end{aligned}$$

Mas, sabemos que $2\cdot t\cdot(p_1^2+p_1+1)+2^l\cdot p_2\cdot(p_1+1)-2^{k+1}\cdot p_1\cdot p_2=0$ e da equação $(2^{k+1}-1)\cdot(p_2+1)-2^l\cdot p_2=2\cdot t\cdot p_1$, concluímos que

$$[(2^{k+1}-1)\cdot(p_2+1)-2^l\cdot p_2]\cdot(p_1+1)+2\cdot t+2^l\cdot p_2\cdot(p_1+1)-2^{k+1}\cdot p_1\cdot p_2=0.$$

Consequentemente $(2^{k+1}-1)\cdot(p_2+1)\cdot(p_1+1)+2\cdot t-2^{k+1}\cdot p_1\cdot p_2=0$. Portanto $(2^{k+1}-1)\cdot(p_1+p_2+1)+2\cdot t-p_1\cdot p_2=0$. Então $2\cdot t=p_1\cdot p_2-(2^{k+1}-1)\cdot(p_1+p_2+1)$.

3. Começaremos provando a suficiência da terceira condição. Seja $n=2^k\cdot p_1^2\cdot p_2$ um número quase perfeito com divisor redundante $d=2^l\cdot p_1^q=(2^{k+1}-1)\cdot(p_1+1)+t-p_1^2$, então $\sigma(n)-2n=d$, onde $d=2^l\cdot p_1^q$. Então

$$\begin{aligned}(2^{k+1}-1)\cdot(p_1^2+p_1+1)\cdot(p_2+1)-2^{k+1}\cdot p_1^2\cdot p_2=&[(2^{k+1}-1)\cdot(p_1+1)+t-p_1^2]\cdot p_2\\ =&(2^{k+1}-1)\cdot(p_1+1)\cdot p_2+k\cdot p_2\\ &-p_1^2\cdot p_2.\end{aligned}$$

Logo, $t\cdot p_2=2^{k+1}\cdot(p_1^2+p_1+1)-(p_1^2+p_1+1)$, portanto

$$t=\frac{(2^{k+1}-1)\cdot(p_1^2+p_1+1)}{p_2}.$$

Reciprocamente, se $d=2^l\cdot p_1^q\cdot p_2$, com $(1\leqslant l\leqslant k,\ 1\leqslant q\leqslant 2)$, então $p_2\mid d$. Do

Lema 6.3, temos $p_2 \mid \sigma(2^k \cdot p_1^2) = (2^{k+1} - 1) \cdot (p_1^2 + p_1 + 1)$. Tem-se

$$(2^{k+1} - 1) \cdot (p_1^2 + p_1 + 1) = t \cdot p_2.$$

Note que $2^l \cdot p_1^q \cdot p_2 = \sigma(n) - 2n = t \cdot p_2 \cdot (p_2 + 1) - 2^{k+1} \cdot p_1^2 \cdot p_2$. Temos

$$t \cdot (p_2 + 1) - 2^{k+1} \cdot p_1^2 = 2^l \cdot p_1^q.$$

Assim, da equação $(2^{k+1} - 1) \cdot (p_1^2 + p_1 + 1) = t \cdot p_2$, sabemos que

$$(2^{k+1} - 1) \cdot (p_1^2 + p_1 + 1) = 2^{k+1} \cdot p_1^2 - k + 2^l \cdot p_1^q.$$

Desta forma $2^l \cdot p_1^q = (2^{k+1} - 1) \cdot (p_1 + 1) + t - p_1^2$.

□

6.3 Números quase perfeitos ímpares

Sobre números quase perfeitos ímpares temos a seguinte proposição.

Proposição 6.11. *Todo número ímpar quase perfeito é um quadrado perfeito.*

Demonstração. Seja $n = p_1^{a_1} \cdot p_2^{a2} \cdots p_k^{a_k}$ a decomposição em fatores primos do número natural n. A soma de todos os divisores de n é a soma das parcelas deste tipo:

$$(1 + p_1 + p_1^2 + \cdots + p_1^{a1}) \cdot (1 + p_2 + p_2^2 + \cdots + p_2^{a2}) \ldots (1 + p_k + p_k^2 + \cdots + p_k^{ak}). \tag{6.8}$$

Se n é ímpar, cada p_i também será ímpar e então o fator correspondente em (6.8) é dado por uma soma de $(a_i + 1)$ números ímpares. Podemos concluir que se o expoente a_i é par, o fator correspondente em (6.8) é ímpar. Se o expoente a_i é ímpar, o fator correspondente em (6.8) é par. Se n é ímpar quase perfeito, a soma dos seus divisores, $\sigma(n)$, deve ser igual a $2n + d$, com d sendo seu divisor redundante. Como os p_i são ímpares, d só pode ser ímpar, o que implica que $\sigma(n) = 2n + d$ também é ímpar. Portanto os a_i serão todos pares. Consequentemente n é um quadrado perfeito.

□

Observação 17. Por enquanto, temos um único exemplo de número ímpar quase perfeito, que é o número 173369889, encontrado por Donovan Johnson em 15 de fevereiro de 2012, para mais detalhes veja [12]. De fato,

$$173369889 = 3^4 \cdot 7^2 \cdot 11^2 \cdot 19^2, \text{ com}$$

$$\sigma(173369889) = \frac{3^5-1}{3-1} \cdot \frac{7^3-1}{7-1} \cdot \frac{11^3-1}{11-1} \cdot \frac{19^3-1}{19-1} = 121 \cdot 57 \cdot 133 \cdot 381 = 349491681,$$

onde o divisor redundante é 2751903.

CONCLUSÃO

Podemos perceber que o tópico de Teoria dos Números sobre números perfeitos e quase perfeitos possui estudos bem atuais sendo desenvolvidos por pesquisadores do mundo inteiro. Isso é apenas uma pequena amostra de como a matemática é dinâmica e viva. Desta maneira, instigamos o leitor, seja ele professor ou aluno dos colégios ou universidades a enxergar a matemática sob um prisma diferente do que tradicionalmente é ensinado em boa parte dos estabelecimento de ensino de nosso país.

Esta maneira de se relacionar com a matemática, certamente traz maior interesse em seu estudo, proporcionando novas descobertas e melhorias no aprendizado da matemática.

A matemática tida como uma disciplina que basta apenas decorarmos as fórmulas, não pode mais ter espaço dentro do aprendizado de nosso país. É preciso desmitificar a matemática e torná-la mais acessível aos alunos.

Enquanto educadores de matemática, devemos despertar em nossos alunos a vontade de procurar saber cada vez mais, estimulando neles a capacidade investigativa que todo pesquisador possui.

A matemática precisa ser ensinada, sem medos, sem fronteiras, como uma ciência viva que é e não parou no tempo.

Desenvolver o potencial do aluno e fazê-lo se sentir capaz estimulando-o, é dever de todo educador.

A natureza está impregnada da matemática. Que sejamos sensíveis o suficiente para perceber na criação (natureza) as leis matemáticas que as regem.

Desejo ao leitor que esse trabalho possa ser um ponto de partida para um novo olhar sobre a matemática, estimulando e motivando a descobrir novas ideias.

REFERÊNCIAS

1 LIMA, E. L. O princípio da indução. *Eureka*, v. 3, p. 26–43, 1998.

2 DOMINGUES, H. H. *Fundamentos de aritmética*. [S.l.]: Ed. da UFSC, 2009.

3 HEFEZ, A. *Elementos de aritmética*. [S.l.]: Sociedade Brasileira de Matemática, 2006.

4 FILHO, E. de A. *Teoria elementar dos números*. [S.l.]: Nobel, 1981.

5 Marcelo Viana. *Primos gêmeos constituem um dos mistérios mais intrigantes*. 2022. Disponível em: ⟨https://impa.br/noticias/primos-gemeos-constituem-um-dos-misterios-mais-intrigantes-da-aritmetica⟩. Acesso em: 23 de abril de 2022.

6 HA Helfgott. *Major arcs for Goldbach's theorem*. 2022. Disponível em: ⟨https://arxiv.org/abs/1305.2897⟩. Acesso em: 23 de abril de 2022.

7 HA Helfgott. *Minor arcs for Goldbach's problem*. 2022. Disponível em: ⟨https://arxiv.org/abs/1205.5252?context=math⟩. Acesso em: 23 de abril de 2022.

8 TERRA. *Peruano resolve problema matemático indecifrável havia 271 anos*. 2022. Disponível em: ⟨https://www.terra.com.br/noticias/educacao/peruano-resolve-problema-matematico-indecifravel-havia-271-anos,f7ccbe63ec6de310VgnVCM4000009bcceb0aRCRD.html⟩. Acesso em: 23 de abril de 2022.

9 GIMPS. *Largest Known Prime Number:* $2^{82.589.933}$*-1*. 2022. Disponível em: ⟨https://www.mersenne.org/primes/?press=M82589933⟩. Acesso em: 25 de abril de 2022.

10 POLLACK, P.; SHEVELEV, V. On perfect and near-perfect numbers. *Journal of Number Theory*, Elsevier, v. 132, n. 12, p. 3037–3046, 2012.

11 REN, X.-Z.; CHEN, Y.-G. On near-perfect numbers with two distinct prime factors. *Bulletin of the Australian Mathematical Society*, Cambridge University Press, v. 88, n. 3, p. 520–524, 2013.

12 OEIS. *Números abundantes n para os quais a abundância* $d = \sigma(n) - 2 \cdot n$ *é um divisor próprio, ou seja,* $d \mid n$. 2022. Disponível em: ⟨https://oeis.org/A181595⟩. Acesso em: 28 de abril de 2022.

13 OEIS. *Abundância de A181595 (n)*. 2022. Disponível em: ⟨https://oeis.org/A181596⟩. Acesso em: 28 de abril de 2022.

14 LI, Y.; LIAO, Q. A class of new near-perfect numbers. *Journal of the Korean Mathematical Society*, Korean Mathematical Society, v. 52, n. 4, p. 751–763, 2015.