UNIVERSIDADE ESTADUAL DA PARAÍBA - UEPB,

CENTRO DE CIÊNCIAS HUMANAS E EXATAS - CCHE

CURSO DE LICENCIATURA PLENA EM MATEMÁTICA

Aran Jônatas Lucena Ferreira

Números Perfeitos

Monteiro - PB

2014

ARAN JÔNATAS LUCENA FERREIRA

Números Perfeitos

Trabalho de Conclusão do Curso apresentado ao Centro de Ciências Humanas e Exatas - CCHE da Universidade Estadual da Paraíba - UEPB, em cumprimento às exigências legais para a obtenção do título de Graduado no Curso de Licenciatura Plena em Matemática .

Orientação do Professor Me. Luiz Lima de Oliveira Junior.

Monteiro - PB
2014

F288n Ferreira, Aran Jônatas Lucena.
Números Perfeitos [manuscrito] : / Aran Jônatas Lucena Ferreira. - 2014.
43 p.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências Humanas e Exatas, 2014.
"Orientação: Prof. Me. Luiz Lima de Oliveira Junior, Departamento de Matemática".

1. Números Perfeitos. 2. Primos de Mersenne. 3. Perfeitos Ímpares. I. Título.

21. ed. CDD 510

ARAN JÔNATAS LUCENA FERREIRA

Números Perfeitos

Trabalho de Conclusão do Curso apresentado ao Centro de Ciências Humanas e Exatas - CCHE da Universidade Estadual da Paraíba - UEPB, em cumprimento às exigências legais para a obtenção do título de Graduado no Curso de Licenciatura Plena em Matemática .

Aprovado pela banca examinadora em 07 de julho de 2014.

Banca Examinadora

Profº. Me. Luiz Lima de Oliveira Junior
Departamento de Matemática - Campus VI/UEPB
Orientador

Profº. Me. José Marcos da Silva
Núcleo de Formação Docente - Campus do Agreste -UFPE

Profº. Me. Maciel Medeiros de Oliveira
Departamento de Matemática - Campus VI/UEPB

Dedico este trabalho a minha família que sempre está me dando apóio no curso de graduação em matemática, especificamente a meus pais, pelas angustias e preocupações que passaram por minha causa, por terem dedicado suas vidas a mim, pelo amor, carinho, e estimulo que me ofereceram. A minha esposa pela paciência comigo, e ao meu filho por existir, pois sem ele, não teria estimulo para nada.

Agradecimentos

Primeiramente, a Deus por este objetivo feito.
A todos os professores que participaram da minha formação, em especial ao professor Luiz Lima de Oliveira Junior, que me orientou no desenvolvimento deste trabalho, aos colegas que trilharam este caminho comigo e contribuirão de forma significativa para este momento, em especial a Stanley Borges de Oliveira, que nunca negou ajuda quando precisei, ao meu primo Luan Lucena que mim ajudou nas traduções, a meus pais pelo apoio e preocupação, a meus irmãos por estarem sempre preocupados e interessados no término deste trabalho, e a minha família, Tamiles Oliveira da Silva e Carlos Pyetro da Silva Ferreira, pelo incentivo que eles mim dão. Enfim, são muitos que gostaria de agradecer, mas tenho certeza que não faltarão oportunidade para agradecê-los.

"O número é perfeito em si mesmo e não porque Deus criou todas as coisas em seis dias. O inverso é mais verdadeiro, Deus criou todas as coisas em seis dias porque este número é perfeito. E continuaria perfeito mesmo que o trabalho de seis dias não existisse".

Santo Agostinho

Resumo

Este trabalho tem como objetivo apresentar resultados referente aos números perfeitos, no qual mostramos um estudo histórico desses números, e alguns tópicos da teoria dos números que são fundamentais para o desenvolvimento do tema em questão. Mencionamos a representação de um número perfeito par, e as condições para encontrá-los, assim como alguns resultados sobre a existência ou não de números perfeitos ímpares. Houve uma pesquisa exploratória, envolvendo busca em documentos eletrônicos disponíveis na internet, além das obras de referências. Como principal conclusão deste trabalho, pode-se ressaltar a não comprovação da existência ou não dos números perfeitos ímpares, onde tem-se alguns resultados mostrando como seria esses números, se existir, mas não se tem provas ainda de sua existência.
Palavras chave: Números Perfeitos, Primos de Mersenne, Perfeitos Ímpares.

Abstract

This study has the aim to present results related to the perfect numbers, which we show a historical view, and some topics of the numbers theory that are elementary to the development of the subject. It's mentioned the representation of a perfect even, and the conditions to find them, as well as a few results about the existence, or not, of a perfect odd number. Within the methodology, in addition to the reference works, there has been an exploratory research, involving some hunting in the internet for contents on electronic documents. As a primal conclusion for this study, there has been found many results showing how odd perfects could be, although not proven their existence.

Keywords: Perfect numbers, Mersenne primes, Odd Perfects.

SUMÁRIO

Introdução

O grande interesse e a curiosidade em estudar a teoria dos números foram primordiais para a escolha do tema de minha pesquisa, por este motivo resolvi desenvolver um trabalho monográfico para aprofundar meus estudos e tentar entender melhor os números perfeitos, que, durante a graduação, não tive a oportunidade, de estudar, haja vista a grade curricular do curso de matemática.

O principal objetivo deste trabalho é mostrar resultados sobre os números perfeitos. Para tanto, é imprescindível um bom entendimento total ou de parte dos principais conceitos da teoria dos números, que foram estudadas em nível de graduação.

A maioria dos resultados aqui apresentados foram coletados dos estudos realizados em sala de aula na disciplina de introdução à teoria dos números e, os demais, foram coletados por meio do sistema eletrônico na internet. Uma vez reunida todas as pesquisas, foi organizado um estudo bibliográfico para fins de análise que, posteriormente, foram arranjadas em três capítulos.

No capítulo I, veremos fatos históricos que são indispensáveis para uma melhor compreensão dos números perfeitos, bem como todos eles encontrados até hoje.

No capítulo II, estudaremos todos os resultados que são importantes para o desenvolvimento do capítulo III, onde neste último veremos o que é um número perfeito, e apresentaremos resultados referentes a esses números. Finalizando o trabalho, temos as considerações finais, e as referências utilizadas no desenvolvimento desta monografia.

1 Fatos Históricos

Neste capítulo temos uma considerável história sobre os números perfeitos, onde citaremos vários matemáticos envolvidos nesse estudo e suas descobertas. Também está incluso aqui todos os números perfeitos encontrados, juntamente com seu descobridor e o ano da descoberta.

1.1 A História dos Números Perfeitos

Não se sabe exatamente quando os números perfeitos foram primeiramente introduzidos, mas é possível que os egípcios tenham formado-os através de números comuns, de maneira que seus métodos de cálculo funcionassem("frações unitárias","frações egípcias"). As propriedades místicas desses números foram estudados por Pitágoras, e seus seguidores. Para a escola pitagórica, as partes de um número são seus divisores. Um número que pode ser formado por suas partes (somando seus divisores) deve ser realmente admirável, perfeitamente criado por Deus. Deus criou o mundo em seis dias, e o número de dias que a lua demora para dar uma volta na terra é exatamente 28. Esses são os dois primeiros números perfeitos. Os quatro primeiros $6, 28, 496$ e 8128 parecem que foram descobertos há muito tempo atrás, e não se tem registros destas descobertas. O primeiro resultado registrado relacionado aos números perfeitos que se tem conhecimento aparece no livro "Elementos de Euclides" (escrito por volta de 300 a.c.), mais precisamente, na proposição 36 do livro IX, que diz:

> "se tantos números quantos quisermos, começando com uma unidade, e sendo postos, continuadamente, na proporção duplicada, até que a soma de todos se torne primo, multiplicando esse resultado pelo último número, o produto será perfeito".

Na proporção duplicada significa que cada número da sequência é duas vezes o anterior. Uma vez que

$$1+2+4+...+2^{k-1}=2^k-1,$$

a afirmação acima mostra que:

se, para qualquer número inteiro $k>1, 2^k-1$ é primo, então

$$2^{k-1}(2^k-1) \text{ é perfeito.} \tag{1.1}$$

Aqui nós desejamos mencionar outra origem para os números perfeitos (geralmente ignorada pelos historiadores da matemática) há muito tempo atrás, mais precisamente, na república de Platão, onde os tão falados números perfeitos periódicos foram introduzidos. É notável que 2000 anos depois, quando Euler provou a recíproca de (1.1), ele não fez referência a Euclides. Contudo, Euler faz referência aos números perfeitos periódicos de Platão. Euler foi provavelmente inspirado em Platão. Uma outra referência mais primitiva mostra ser de Euphorion, um poeta do século III a.c.. O próximo estudo significante dos números perfeitos foi feito por Nichomachus de Gerasa, por volta de 100 d.c.. Ele escreveu seu famoso "Introdução à Aritmética", o qual classifica os números em três classes: números abundantes (os quais tem a propriedade de que o resultado da soma de seus divisores ou partes é maior do que o próprio número), números deficientes (os quais tem a propriedade de que o resultado da soma de suas partes é menor do que o próprio número), e os números perfeitos (os quais tem a propriedade de que o resultado da soma de suas partes é igual ao seu dobro). Nichomachus usou essa classificação também em termos morais, ou analogias biológicas:

"... no caso de muito, é produzido em excesso, em exagero, no caso de pouco, é produzido em falta, com privações e insuficiências ..."

"... números abundantes são como um animal com dez bocas, ou nove lábios, e munidos com três fileiras de dentes; ou com cem braços ..."

"... números deficientes são como animais com só um olho, com um braço ou com só uma de suas mãos, com menos de cinco dedos, ou como se ele não tivesse língua".

No livro de Nichomachus apareceram cinco resultados não provados com relação aos números perfeitos:

1. O enésimo número perfeito tem n algarismos;
2. Todos os números perfeitos são pares;
3. Todos os números perfeitos terminam em 6 ou 8, alternadamente;
4. Todo número perfeito é escrito da forma $2^{k-1}(2^k-1)$, para qualquer inteiro $k>1$, com 2^k-1 primo;
5. Existem infinitos números perfeitos.

Apesar do fato de Nichomachus não ter oferecido uma justificativa para essas afirmações, elas foram tomadas como fato por muitos anos. A descoberta de outros números perfeitos desmentiram imediatamente as afirmações (1) e (3). Por outro lado, as afirmações (2), (4) e (5) permanecem não provadas praticamente até hoje.

Os matemáticos árabes eram também fascinados pelos números perfeitos, e Thabit Ibn Quarra escreveu "Tratando dos Números Amigáveis" no qual ele examinou quando os números da forma $2^n p$ (p primo) podem ser perfeitos. Ele provou também a "Lei de Thabit". Ibn Al-haytham provou uma parte contrária na proposição de Euclides (1.1), na obra não publicada "Tratando com Análises e Sínteses". Dentre os matemáticos árabes que continuaram a investigação (estudo) dos gregos sobre os números perfeitos com grande entusiasmo foi Ismail Ibn Ibrahim Ibn Fallus (1194-1239), que escreveu uma tese baseado em Nichomachus sobre o texto mencionado. Ele também deu uma lista de dez números dizendo serem perfeitos. Os sete primeiros estavam corretos, e de fato esses são sem dúvida os primeiros sete números perfeitos. Para maiores detalhes sobre esse seu trabalho veja os escritos de S. Brentjes. O 5^{o} número perfeito foi redescoberto por Regiomontanus durante sua estadia na universidade de Viena, da qual ele saiu em 1461. Isto também foi encontrado no manuscrito escrito por um autor anônimo por volta de 1458, enquanto que o 5^{o} e o 6^{o} número perfeito foram encontrados em outro manuscrito pelo o mesmo autor, pouco depois de 1460. O 5^{o} número perfeito é 33550336, e o 6^{o} é 8589869056. Isso mostra que os primeiros números ditos por Nichomachus são falsos (1) e (3), desde que o 5^{o} número perfeito tem 8 dígitos, e o 5^{o} e o 6^{o} número perfeito ambos terminam em 6.

Em 1536, Hudalrichus Regius publicou "Utriusque Arithmetices," no qual ele encontrou o primeiro primo p ($p = 11$) tal que $2^{p-1}(2^p - 1)$ não é um número perfeito. Em 1603, Cataldi encontrou os fatores de todos os números até 800 e também uma lista de todos os primos até 750. Ele usou sua lista de primos para conferir se $2^{19} - 1 = 524287$ era primo. Então, ele encontrou o 7^{o} número perfeito: 137438691328. Dentre os muitos matemáticos interessados nos números perfeitos, deve ser mencionado Descartes, que em 1638 escreveu em uma carta para Mersenne:

"... Os números perfeitos são poucos... tão poucos quanto pessoas perfeitas...". Sobre isso veja também no manuscrito Perso. "... Eu acho que sou capaz de provar que não existem números pares perfeitos além daqueles de Euclides; e que não existem números ímpares perfeitos, a menos que eles sejam compostos de um único número primo, multiplicado pelo quadrado daqueles que a raiz é composta de vários outros números primos. Mas eu não posso ver nada que previna alguém de encontrar números desse tipo... mas, seja qual for o método que alguém use, isso iria requerer muito tempo na busca por estes números...".

A próxima grande contribuição foi feita por Fermat. Ele falou a Roberval em 1636 que estava trabalhando no assunto e, embora os problemas fossem muito dificílimos, ele tinha a intenção de publicar um tratado do assunto. O tratado nunca foi escrito, talvez pelo fato de não alcançar os resultados que esperava. Em junho de 1640, Fermat escreveu uma carta a Mersenne

contando a ele suas descobertas sobre os números perfeitos. Logo após escrever a Mersenne, Fermat escreveu a Frenicle de Bessy, generalizando os resultados da carta anterior. Em suas investigações Fermat usou três teoremas:

1. Se n é composto, então $2^n - 1$ é composto;
2. Se n é primo, então $a^n - a$ é múltiplo de n;
3. Se n é primo, e p é divisor de $2^n - 1$, então $p - 1$ é um múltiplo de n.

Usando este "pequeno teorema", Fermat mostrou que $2^{23} - 1$ é composto e que $2^{37} - 1$ também é composto. Mersenne ficou muito interessado nos resultados que Fermat o enviou sobre os números perfeitos. Em 1644, ele publicou "Cogitata Physica Mathematica", no qual ele afirmou que $2^{p-1}(2^p - 1)$ é perfeito para $p = 2,3,5,7,13,17,19,31,67,127,257$ e para nenhum valor de p acima de 257. É notável que, dentre os 47 primos, o valor de p entre 19 e 258 para o qual $2^p - 1$ é primo, para 42 casos Mersenne estava certo. Primos da forma $2^p - 1$ são chamados primos de Mersenne.

O próximo matemático que fez uma importante contribuição foi Euler. Em 1732, ele provou que o 8^o número perfeito era $2^{30} \cdot (2^{31} - 1)$. Este foi o primeiro número perfeito descoberto em 125 anos. Mas, a maior contribuição feita por Euler, foi obtida em dois manuscritos não publicados durante sua vida. Em um deles ele provou a recíproca do pensamento de Euclides:

Todos os números perfeitos pares são da forma $2^{p-1} \cdot (2^p - 1)$.

Citando R.C.Vaughan: "Nós temos um exemplo de um teorema que levou 2000 anos para ser provado..., mas verdadeiros matemáticos devem trabalhar durante um vasto tempo...". Os resultados de Euler com os números perfeitos ímpares e os números amigáveis serão considerados mais tarde. Depois da descoberta de Euler que $2^{31} - 1$ é um número primo, a busca por números perfeitos agora se tornou uma tentativa para checar se Mersenne estava correto em suas afirmativas. O primeiro erro na lista de Mersenne foi descoberto em 1876 por Lucas; e mostrou que $2^{67} - 1$ é composto. Mas como $2^{127} - 1$ é um primo de Mersenne, então ele obteve um novo número perfeito (não o nono, porém depois irão perceber que é o vigésimo). Lucas fez também uma descoberta teórica, a qual foi modificada por Lehmer e será a base de uma busca pelos primos de Mersenne. Em 1883, Pervusin demonstrava que $2^{61} - 1$ é primo, desta forma dando o nono número perfeito. Em 1911 a 1914, Powers provou que $2^{89} - 1$ e $2^{101} - 1$ são primos. $2^{88}(2^{89} - 1)$ era de fato o último número perfeito descoberto por meio de cálculos. Todos os outros foram encontrados através de máquinas ou um computador. De fato, computadores tiveram grande influência no ressurgimento do interesse de descoberta dos números primos de Mersenne, e mais adiante nos números perfeitos. Os primeiros resultados significativos com os números perfeitos ímpares foram obtidos por Sylvester. Na sua opinião: "... A existência de números perfeitos ímpares ainda não foi provado, pois há uma complexa teia de condições que os cerca, seria um pequeno milagre...". Em 1888, ele provou que alguns

números perfeitos ímpares tem no mínimo 4 fatores primos distintos. Alguns anos depois, ele aumentou este resultado para cinco fatores. Finalmente, vamos incluir aqui todos os números perfeitos conhecidos juntamente com o ano da descoberta e seu descobridor. Seja P_k o k-ésimo número perfeito. Então, $P_k = 2^{p-1}(2^p - 1) = A_p$, onde $2^p - 1$ é um primo de Mersenne.

Números perfeitos	Ano e Descobridor
$P_1 = A_2 = 6,$	
$P_2 = A_3 = 28,$	
$P_3 = A_5 = 496,$	
$P_4 = A_7 = 8128,$	
$P_5 = A_{13} = 33550336$	1456, Anonymous
$P_6 = A_{17} = 8589869056$	1588, Cataldi
$P_7 = A_{19} = 137438691328$	1588, Cataldi
$P_8 = A_{31} = 2305843008139952128$	1772, Euler
$P_9 = A_{61}$	1883, Pervushin
$P_{10} = A_{89}$	1911, Powers
$P_{11} = A_{107}$	1914, Powers
$P_{12} = A_{127}$	1876, Lucas
$P_{13} = A_{521}$	1952, Robinson
$P_{14} = A_{607}$	1952, Robinson
$P_{15} = A_{1279}$	1952, Robinson
$P_{16} = A_{2203}$	1952, Robinson
$P_{17} = A_{2281}$	1952, Robinson
$P_{18} = A_{3217}$	1952, Riesel
$P_{19} = A_{4253}$	1961, Hurwitz
$P_{20} = A_{4423}$	1961, Hurwitz
$P_{21} = A_{9689}$	1963, Gillies
$P_{22} = A_{9941}$	1963, Gillies
$P_{23} = A_{11213}$	1963, Gillies
$P_{24} = A_{19937}$	1971, Tuckerman
$P_{25} = A_{21701}$	1978, Noll e Nickel
$P_{26} = A_{23209}$	1979, Noll
$P_{27} = A_{44497}$	1979, Nelson e Slowinski
$P_{28} = A_{86243}$	1982, Slowinski
$P_{29} = A_{110503}$	1988, Colquitt e Welsh
$P_{30} = A_{132049}$	1983, Slowinski

Números perfeitos	Ano e Descobridor
$P_{31} = A_{216091}$	1985, Slowinski
$P_{32} = A_{756839}$	1992, Slowinski e Gage
$P_{33} = A_{859433}$	1994, Slowinski e Gage
$P_{34} = A_{1257787}$	1996, Slowinski e Gage
$P_{35} = A_{1398269}$	1996, Joel Armengaud
$P_{36} = A_{2976221}$	1997, Gordon Spence
$P_{37} = A_{3021377}$	1998, Roland Clarkson
$P_{38} = A_{6972593}$	1999, Nayan Hajratwala
$P_{39} = A_{13466917}$	2001,Michael Cameron
$P_{40} = A_{20996011}$	2003, Michael Shafer
$P_{41} = A_{24036583}$	2004, Josh Findley
$P_{42} = A_{25964951}$	2005, Martin Nowak
$P_{43} = A_{30402457}$	2005, Curtis Cooper e Steven Boone
$P_{44} = A_{32582657}$	2006, Curtis Cooper e Steven Boone
$P_{45} = A_{37156667}$	2008, Hans-Michael Elvenich
$P_{46} = A_{42643801}$	2009, Odd Magnar Strindmo
$P_{47} = A_{43112609}$	2008, Edson Smith
$P_{48} = A_{578885161}$	2013, Curtis Cooper

2 Resultados Fundamentais

Neste Capítulo, veremos alguns resultados preliminares utilizados no desenvolvimento desta monografia e que servirão de base para uma melhor compreensão dos números perfeitos, onde citaremos algumas definições e resultados importantes da Teoria dos Números[1].

2.1 Indução

Definição 2.1 (Princípio da Boa Ordem (PBO))**.** *Todo conjunto não-vazio de inteiros positivos contém um elemento mínimo.*

Teorema 2.1 (Princípio de Indução Finita)**.** *Seja B um subconjunto dos inteiros positivos. Se B possui as duas seguintes propriedades*

1. $1 \in B$
2. $k+1 \in B$ *sempre que* $k \in B$,

então B contém todos os inteiros positivos.

Demonstração: Vamos supor que, mesmo possuindo as propriedades (1) e (2) o conjunto B não contenha todos os inteiros positivos. Seja A o conjunto dos inteiros positivos não contidos em B. Pela definição 2.1, A possui um menor elemento e este é maior do que 1, pois $1 \in B$. Seja a_0 este elemento. É claro que $a_0 - 1$, pertence a B e como B satisfaz as propriedades (1) e (2) então o sucessor de $a_0 - 1$, que é a_0, também deve pertencer a B. Esta contradição nos leva a concluir que A tem que ser vazio, o que conclui a demonstração. ■

Teorema 2.2 (Princípio de Indução Matemática)**.** *Seja $P(n)$ uma proposição associada a cada inteiro positivo n e que satisfaz às duas seguintes condições:*

1. $P(1)$ *é verdadeira;*

[1] ver nas referências (ALENCAR,1981) ou qualquer livro introdutório à Teoria dos Números.

2. *Para todo inteiro positivo k, se $P(k)$ é verdadeira, então $P(k+1)$ também é verdadeira. Nestas condições, a proposição $P(n)$ é verdadeira para todo inteiro positivo n.*

Demonstração: Seja S o conjunto de todos os inteiros positivos n para os quais a proposição $P(n)$ é verdadeira, isto é:

$$S = \{n \in \mathbb{N} \mid P(n) \text{ é verdadeira}\}.$$

Pelas condições (1) e (2), $P(1)$ é verdadeira e, portanto, $1 \in S$, e para todo inteiro positivo k, se $k \in S$, então $k+1 \in S$. Logo, o conjunto S satisfaz às condições (1) e (2) do Teorema (2.1) e, portanto, a proposição $P(n)$ é verdadeira para todo inteiro positivo n. ■

Exemplo 2.1. *Demonstrar a proposição:*

$$P(m): \quad \textit{Todo número ímpar da sequência } 3,7,11,15,\ldots,a_m \textit{ é da forma } 4m-1; \forall m \in \mathbb{N} \quad (2.1)$$

Demonstração:

- *$P(1)$ é verdadeira, visto que $a_1 = 4 \cdot 1 - 1 = 3$.*
- *Por hipótese de indução $P(k)$ é verdadeira, com $k \in \mathbb{N}$. Isto é, $a_k = 4k-1$, com $4k-1$ sendo um número ímpar da sequência dada na equação 2.1, então*

$$a_{k+1} = 4(k+1) - 1 = (4k-1) + 4 = a_k + 4$$

também é um número ímpar da sequência dada na equação 2.1.

Portanto $P(k+1)$ é verdadeira, e pelo Teorema 2.2, a proposição $P(m)$ é verdadeira para todo inteiro positivo m. ■

Analogamente mostra-se que

$P(m)$: Todo número ímpar da sequência $1,5,9,13,\ldots b_m$ é da forma $4m-3; \forall m \in \mathbb{N}$.

Teorema 2.3 (Princípio de Indução Matemática, 2ª Forma)**.** *Seja $p(n)$ uma proposição associada a cada inteiro positivo n tal que*

i) $p(a)$ é verdade, e que

ii) Para todo $n, p(a)$ e $p(a+1)$ e $\cdots$ e $p(n) \Longrightarrow p(n+1)$ é verdade, então, $p(n)$ é verdade para todo $n \geq a$.

Demonstração: Considere o conjunto

$$V = \{n \in a + \mathbb{N}; p(n)\}.$$

Queremos provar que o conjunto $W = (a+\mathbb{N}) - V$ é vazio. Suponha, por absurdo, que vale o contrário. Logo, pela Definição 2.1, W teria um menor elemento k, e, como sabemos de i)

que $a \notin W$, segue-se que existe n tal que $k = a+n > a$. Portanto, $a, a+1, \ldots, k-1 \notin W$; logo $a, a+1, \ldots, k-1 \in V$. Por (ii) acima conclui-se que $k = k-1+1 \in V$, o que contradiz o fato de $k \in W$. ■

2.2 Divisibilidade

Definição 2.2. *Se a e b são inteiros, dizemos que a divide b, denotando por* $a \mid b$, *se existir um inteiro k tal que* $b = ak$. *Se a não divide b escrevemos* $a \nmid b$.

Teorema 2.4 (Transitividade da divisão)**.** *Se* a, b *e c são inteiros,* $a \mid b$ *e* $b \mid c$, *então* $a \mid c$.

Demonstração: Como $a \mid b$ e $b \mid c$, de acordo com Definição (2.2) existem inteiros k_1 e k_2 com $b = k_1 a$ e $c = k_2 b$. Substituindo o valor de b na equação $c = k_2 b$, teremos $c = k_2 k_1 a$ o que implica $a \mid c$. ■

Exemplo 2.2. *Como* $4 \mid 16$ *e* $16 \mid 32$, *então* $4 \mid 32$. *Como não existe um número inteiro c satisfazendo a equação* $25 = 4.c$, *então* $4 \nmid 25$.

Teorema 2.5. *Se* a, b, c, m *e n são inteiros,* $c \mid a$ *e* $c \mid b$, *então* $c \mid (ma+nb)$.

Demonstração: Se $c \mid a$ e $c \mid b$, então $a = k_1 c$ e $b = k_2 c$. Multiplicando-se estas duas equações respectivamente por m e n teremos $ma = mk_1 c$ e $nb = nk_2 c$. Somando-se membro a membro obtemos

$$ma + nb = (mk_1 + nk_2)c, \text{ o que nos diz que } c \mid (ma+nb).$$

■

Exemplo 2.3. *Como* $4 \mid 8$ *e* $4 \mid 12$, *então* $4 \mid (2.8+1.12)$.

Teorema 2.6 (Algoritmo da Divisão)**.** *Se a e b são dois inteiros, com* $b > 0$, *então existem e são únicos os inteiros q e r que satisfazem às condições:*

$$a = bq + r \quad e \quad 0 \leq r < b. \tag{2.2}$$

Demonstração: Seja S o conjunto de todos os inteiros não negativos (≥ 0) que são da forma $a - bx$, com $x \in \mathbb{Z}$, isto é:

$$S = \{a - bx;\ x \in \mathbb{Z},\ a - bx \geq 0\}$$

Este conjunto S não é vazio, porque, sendo $b > 0$, temos $b \geq 1$ e, portanto, para $x = -\mid a \mid$, resulta:

$$a - bx = a + b \mid a \mid \geq a + \mid a \mid \geq 0$$

Assim sendo, pela Definição (2.1), existe o elemento mínimo r de S tal que

$$r \geq 0 \quad \text{e} \quad r = a - bq \quad \text{ou} \quad a = bq + r, \quad \text{com} \quad q \in \mathbb{Z}.$$

Além disso, temos $r < b$, pois, se fosse $r \geq b$, teríamos:

$$0 \leq r - b = a - bq - b = a - b(q+1) < r$$

isto é, r não seria o elemento mínimo de S. Para demonstrar a unicidade de q e r, suponhamos que existem dois outros inteiros q_1 e r_1 tais que,

$$a = bq_1 + r_1 \quad \text{e} \quad 0 \leq r_1 < b. \tag{2.3}$$

Logo, as equações (2.2) e (2.3) são iguais, ou seja:

$$bq_1 + r_1 = bq + r \Longrightarrow r_1 - r = (q - q_1)b \Longrightarrow b \mid (r_1 - r).$$

Por outro lado, temos:

$$-b < -r \leq 0 \quad \text{e} \quad 0 \leq r_1 < b,$$

o que implica:

$$-b < r_1 - r < b, \quad \text{isto é} , \quad \mid r_1 - r \mid < b.$$

Assim, $b \mid (r_1 - r)$ e $\mid r_1 - r \mid < b$, portanto, $r_1 - r = 0$, e como $b \neq 0$, também temos $q - q_1 = 0$. Logo, $r_1 = r$ e $q_1 = q$. ■

2.3 Máximo Divisor Comum

Definição 2.3 (Máximo Divisor Comum de Dois Inteiros)**.** *Sejam a e b dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$). Chama-se máximo divisor comum de a e b o inteiro positivo d ($d > 0$) que satisfaz às condições:*

1. *$d \mid a$ e $d \mid b$*
2. *se $c \mid a$ e se $c \mid b$, então $c \leq d$.*

O máximo divisor comum de a e b indica-se pela notação $mdc(a,b)$.

Exemplo 2.4. *Sejam os inteiros $a = 12$ e $b = 30$. Os divisores comuns positivos de 12 e 30 são $1, 2, 3$ e 6, como o maior deles é 6, segue-se que o $mdc(12,30) = 6$.*

Teorema 2.7. *Se a e b são dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$), então existe e é único $d = mdc(a,b)$, além disso, existem inteiros x e y tais que*

$$mdc(a,b) = ax + by, \tag{2.4}$$

isto é, o $mdc(a,b)$ é uma combinação linear de a e b.

Demonstração:

Seja S o conjunto de todos os inteiros positivos da forma $au+bv$, com $u,v \in \mathbb{Z}$, isto é:

$$S = \{au+bv; au+bv > 0 \text{ e } u,v \in \mathbb{Z}\}.$$

Este conjunto S não é vazio, porque, se $a \neq 0$, então um dos dois inteiros:

$$a = a.1+b.0 \quad \text{e} \quad -a = a.(-1)+b.0$$

é positivo e pertence a S. Logo, pela Definição (2.1), existe e é único o elemento mínimo $d > 0$ de S. E, consoante a definição de S, existem inteiros x e y tais que $d = ax+by$. Posto isto, vamos mostrar que $d = mdc(a,b)$. Com efeito, pelo Teorema 2.6, temos:

$$a = dq+r, \quad \text{com} \quad 0 \leq r < d,$$

o que dá:

$$r = a-dq = a-(ax+by)q = a(1-qx)+b(-qy),$$

isto é, o resto r é uma combinação linear de a e b. Como $0 \leq r < d$ e $d > 0$ é o elemento mínimo de S, segue-se que $r = 0$ e $a = dq$, isto é, $d \mid a$. Com raciocínio inteiramente análogo se conclui que também $d \mid b$. Logo, d é um divisor comum positivo de a e b. Finalmente, se c é um divisor comum positivo qualquer de a e b ($c \mid a$ e $c \mid b, c > 0$), então, pelo Teorema (2.5) temos:

$$c \mid (ax+by) \Longrightarrow c \mid d \Longrightarrow c \leq d,$$

isto é, d é o maior divisor comum positivo de a e b, ou seja:

$$mdc(a,b) = d = ax+by, \quad \text{com} \quad x,y \in \mathbb{Z},$$

e o teorema fica demonstrado. ■

Exemplo 2.5. *Sejam os inteiros $a = 6$ e $b = 27$. Temos:*

$$mdc(6,27) = 3 = 6(-4)+27.1.$$

Teorema 2.8 (De Euclides)**.** *Se $a \mid bc$ e se o $mdc(a,b) = 1$, então $a \mid c$.*

Demonstração: Com efeito:

$$a \mid bc \Longrightarrow bc = aq, \text{ com } q \in \mathbb{Z} \text{ (Definição 2.2).}$$

Pelo Teorema (2.7), existem $x,y \in \mathbb{Z}$ tais que

$$mdc(a,b) = 1 \Longrightarrow ax+by = 1, \tag{2.5}$$

o que implica que

$$acx + bcy = c \text{ (multiplicando a equação (2.5) por } c).$$

Como $bc = aq$, então:

$$c = acx + bcy = acx + aqy = a(cx + qy) \Longrightarrow a \mid c.$$

■

Exemplo 2.6. *Sejam os inteiros* $a = 3, b = 5$ *e* $c = 9$*, temos:*

$$3 \mid 5.9 \text{ e o } mdc(3,5) = 1, \text{ então } 3 \mid 9.$$

Corolário 2.1. *Se* $a \mid c$*, se* $b \mid c$ *e se o* $mdc(a,b) = 1$*, então* $ab \mid c$*.*

Demonstração: Com efeito:

$$a \mid c \Longrightarrow c = aq_1, \text{ com } q_1 \in \mathbb{Z} \text{ (Definição 2.2)}$$

$$b \mid c \Longrightarrow c = bq_2, \text{ com } q_2 \in \mathbb{Z} \text{ (Definição 2.2)}$$

Pelo Teorema (2.7), existem $x, y \in \mathbb{Z}$ tais que

$$mdc(a,b) = 1 \Longrightarrow ax + by = 1, \tag{2.6}$$

O que implica que

$$acx + bcy = c \tag{2.7}$$

(multiplicando a equação (2.6) por c).

Portanto, substituindo c por aq_1 e por bq_2 na equação (2.7) temos:

$$c = a(bq_2)x + b(aq_1)y = ab(q_2x + q_1y) \Longrightarrow ab \mid c.$$

■

Exemplo 2.7. *Sejam os inteiros* $a = 2, b = 3$ *e* $c = 24$*. Temos:*

$$mdc(2,3) = 1 \text{ e } 2 \mid 24, 3 \mid 24, \text{ então } 2.3 = 6 \mid 24.$$

2.4 Números Primos

Definição 2.4. *Um inteiro não nulo* p*, com* $p \neq 1$ *e* $p \neq -1$ *é dito primo se tem exatamente dois divisores positivos 1 e* $\mid p \mid$ *. Caso contrário p é composto, ou seja,* $p = a.b$*, onde a e b são inteiros e* $1 < a, b < p$*.*

Definição 2.5. *Dois inteiros a e b dizem-se relativamente primos se* $mdc(a,b) = 1$.

Teorema 2.9. *Se um primo p não divide um inteiro a, então a e p são primos entre si.*

Demonstração: Seja $d = mdc(a,p)$. Então, pela Definição (2.3), $d \mid a$ e $d \mid p$. Da relação $d \mid p$, resulta que $d = 1$ ou $d = p$, porque p é primo, e como a segunda igualdade é impossível, já que p não divide a, segue-se que $d = 1$, isto é, o $mdc(a,p) = 1$. Logo, pela Definição (2.5) a e p são primos entre si. ■

Exemplo 2.8. *São primos entre si os inteiros 2 e 5, -9 e 16, -27 e -35, pois temos,*

$$mdc(2,5) = mdc(-9,16) = mdc(-27,-35) = 1.$$

Teorema 2.10. *Se p é um primo tal que* $p \mid ab$, *então* $p \mid a$ *ou* $p \mid b$.

Demonstração: Se $p \mid a$, nada há que demonstrar, e se, ao invés, p não divide a, então, pelo Teorema (2.9), o $mdc(p,a) = 1$. Logo, pelo Teorema (2.8), $p \mid b$. ■

Teorema 2.11. *Se p é um número primo tal que* $p \mid a_1 a_2 \ldots a_n$, *então existe um índice k, com* $1 \leq k \leq n$, *tal que* $p \mid a_k$.

Demonstração:

Considere a sentença: $P(n)$: Se $p \mid a_1 a_2 \ldots a_n$, então $\exists k \in \mathbb{Z}$, com $1 \leq k \leq n$, tal que $p \mid a_k$. Usando o Teorema (2.1), a sentença $P(n)$ é verdadeira para $n = 1$ (imediato), e também é verdadeira para $n = 2$ (pelo Teorema 2.10). Suponhamos, pois, $n > 2$ e que, se p divide um produto com menos de n fatores, então p divide pelo menos um dos fatores (hipótese de indução). Pelo Teorema (2.10), se $p \mid a_1 a_2 \ldots a_n$, então

$$p \mid a_n \text{ ou } p \mid a_1 a_2 \ldots a_{n-1}.$$

Se $p \mid a_n$, o Teorema está demonstrado, e se, ao invés, $p \mid a_1 a_2 \ldots a_{n-1}$, então a hipótese de indução assegura que $p \mid a_k$, com $1 \leq k \leq n-1$. Em qualquer dos dois casos, existe um índice k, com $1 \leq k \leq n$, tal que $p \mid a_k$.

■

Teorema 2.12. *Se* $p, p_1, \ldots, p_n$ *são números primos e, se* $p \mid p_1 \ldots p_n$, *então* $p = p_i$, *para algum* $i = 1, \ldots, n$.

Demonstração: Com efeito, pelo Teorema (2.11), existe um índice i, com $1 \leq i \leq n$, tal que $p \mid p_i$, e como os únicos divisores positivos de p_i são 1 e p_i, porque p_i é primo, segue-se que $p = 1$ ou $p = p_i$. Mas, $p > 1$, porque p é primo. Logo, $p = p_i$. ■

Teorema 2.13. *Todo inteiro composto possui um divisor primo.*

Demonstração: Seja a um inteiro composto. Consideremos o conjunto $A \neq \varnothing$ de todos os divisores positivos de a, exceto os divisores triviais 1 e a, isto é:

$$A = \{x \mid a; 1 < x < a\}.$$

Por 2.1 existe o elemento mínimo p de A, que vamos mostrar ser primo. Com efeito, se p fosse composto, admitiria pelo menos um divisor d tal que $1 < d < p$, e então $d \mid p$ e $p \mid a$, pelo Teorema 2.4 $d \mid a$, isto é, p não seria o elemento mínimo de A. Logo, p é primo. ■

Teorema 2.14 (Teorema Fundamental da Aritmética)**.** *Todo número natural maior do que* 1 *ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Demonstração: Usaremos o Teorema 2.3. Se $n = 2$, o resultado é obviamente verificado, pois 2 é primo. Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar. Suponhamos, então, que n seja composto. Logo, existem números naturais n_1 e n_2 tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, \ldots, p_r$ e $q_1, \ldots, q_s$ tais que $n_1 = p_1 \ldots p_r$ e $n_2 = q_1 \ldots q_s$. Portanto, $n = p_1 \ldots p_r q_1 \ldots q_s$.

Vamos, agora, provar a unicidade da escrita. Suponha, agora, que $n = p_1 \ldots p_r = q_1 \ldots q_s$, onde os p_i e os q_j são números primos. Como $p_1 \mid q_1 \ldots q_s$, pelo Teorema (2.12), temos que $p_1 = q_j$ para algum j, que, após reordenamento de $q_1, \ldots, q_s$, podemos supor que seja q_1. Portanto,

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

Como $p_2 \ldots p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares. ■

Teorema 2.15 (Euclides)**.** *Há um número infinito de primos.*

Demonstração: Suponha que exista apenas um número finito de números primos $p_1, \ldots, p_r$. Considere o número natural

$$n = p_1 p_2 \ldots p_r + 1.$$

Pelo Teorema 2.14, o número n possui um fator primo p que, portanto, deve ser um dos $p_1, \ldots, p_r$ e, consequentemente, divide o produto $p_1 p_2 \ldots p_r$. Mas isto implica que p divide 1, o que é absurdo, pois $p > 1$ e o único divisor positivo de 1 é o próprio 1, além de 1 não ser um número primo. 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. ■

Teorema 2.16. *Se um inteiro positivo $a > 1$ é composto, então a possui um divisor primo $p \leq \sqrt{a}$.*

Demonstração: Com efeito, se o inteiro positivo $a > 1$ é composto, então:

$$a = bc, \text{ com } 1 < b < a \text{ e } 1 < c < a.$$

Portanto, supondo $b \leq c$, teremos:

$$b^2 \leq bc = a \Longrightarrow b \leq \sqrt{a}.$$

Por ser $b > 1$, o Teorema 2.14 assegura que b tem pelo menos um divisor primo p, de modo que $p \leq b \leq \sqrt{a}$. E como $p \mid b$ e $b \mid a$, segue-se que $p \mid a$ (Teorema 2.4), isto é, o inteiro primo $p \leq \sqrt{a}$ é um divisor de a. ■

2.5 Congruência

Definição 2.6. *Sejam **a** e **b** dois inteiros quaisquer e seja **m** um inteiro positivo fixo. Diz-se que **a** é congruente a **b** módulo **m** se, e somente se, **m** divide a diferença **a - b.** Com a notação $a \equiv b \pmod{m}$, indica-se que **a** é congruente a **b** módulo **m.***

Exemplo 2.9. *Sejam os inteiros $16, 4$ e 6, temos que:*

$$16 \equiv 4 \pmod{6}, \text{ porque } 6 \mid (16-4).$$

Teorema 2.17. *Seja m um inteiro positivo fixo $(m > 0)$, e sejam a, b, c e d inteiros quaisquer. Subsistem as seguintes propriedades:*

1. *Se $a \equiv b \pmod{m}$ e se $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.*
2. *Se $a \equiv b \pmod{m}$ e se $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$ e $ac \equiv bd \pmod{m}$.*
3. *Se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m}$ para todo inteiro positivo n.*

Demonstração: 1) - Com efeito, se $a \equiv b \pmod{m}$ e se $b \equiv c \pmod{m}$, então pela Definição (2.6) $m \mid (a-b)$ e $m \mid (b-c)$, logo pela Definição (2.2) existem inteiros h e k tais que

$$a - b = hm \quad \text{e} \quad b - c = km.$$

Portanto:

$$a-c=(a-b)+(b-c)=hm+km=(h+k)m,$$

e isto significa que $a \equiv c \pmod{m}$.

2) - Com efeito, se $a \equiv b \pmod{m}$ e se $c \equiv d \pmod{m}$, análogo ao item anterior, existem inteiros h e k tais que $a-b=hm$ e $c-d=km$. Portanto:

$$(a+c)-(b+d)=(a-b)+(c-d)=hm+km=(h+k)m$$

e

$$ac-bd=(b+hm)(d+km)-bd=(bk+dh+hkm)m,$$

o que implica:

$$a+c \equiv b+d \pmod{m} \text{ e } ac \equiv bd \pmod{m}.$$

3) - Usando o Teorema 2.2, a proposição é verdadeira para $n=1$, supondo que seja verdadeira para um inteiro positivo k, temos:

$$a^k \equiv b^k \pmod{m} \quad \text{e} \quad a \equiv b \pmod{m}.$$

Portanto, pela Propriedade (2):

$$a^k \cdot a \equiv b^k \cdot b \pmod{m} \quad \text{ou} \quad a^{k+1} \equiv b^{k+1} \pmod{m},$$

isto é, a proposição é verdadeira para o inteiro positivo $k+1$. Logo, a proposição é verdadeira para todo inteiro positivo n. ■

Exemplo 2.10. *Vejamos alguns exemplos:*

1. $36 \equiv 12 \pmod{2}$ *e* $12 \equiv 6 \pmod{2}$ *logo* $36 \equiv 6 \pmod{2}$.
2. $8 \equiv 4 \pmod{2}$ *e* $9 \equiv 3 \pmod{2}$ *logo* $8+9 \equiv 4+3 \pmod{2}$ *e* $8 \cdot 9 \equiv 4 \cdot 3 \pmod{2}$.
3. $4 \equiv 2 \pmod{2}$ *logo* $4^2 \equiv 2^2 \pmod{2}$, *ou seja,* $16 \equiv 4 \pmod{2}$.

2.6 Divisores de um Inteiro

Teorema 2.18. *Se* $n = p_1^{r_1} \cdot p_2^{r_2} \ldots p_k^{r_k}$ *é a decomposição canônica do inteiro positivo* $n > 1$, *então os divisores positivos de n são precisamente os inteiros d da forma:*

$$d = p_1^{h_1} \cdot p_2^{h_2} \ldots p_k^{h_k} \tag{2.8}$$

onde $0 \leq h_i \leq r_i \quad com \quad i = 1, 2, \ldots k$.

Demonstração: Obviamente, os divisores triviais $d = 1$ e $d = n$ de n se obtém quando, respectivamente:

$$h_1 = h_2 = ... = h_k = 0$$

e

$$h_1 = r_1, h_2 = r_2, \ldots, h_k = r_k.$$

Suponhamos, pois, que d é um divisor não trivial de n, isto é:

$$n = dd_1, \text{ com } d > 1 \text{ e } d_1 > 1.$$

Exprimindo d e d_1 como produtos de primos:

$$d = q_1 q_2 \ldots q_s, \quad d_1 = t_1 t_2 \ldots t_u,$$

obtemos:

$$n = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k} = q_1 q_2 \ldots q_s t_1 t_2 \ldots t_u,$$

que são duas decomposições do inteiro positivo n num produto de primos, e pelo Teorema (2.14) sua decomposição é única, então cada primo q_i coincide com um p_j, de modo que, substituindo os produtos de primos iguais por potências de expoente inteiro, teremos:

$$d = q_1 q_2 \ldots q_s = p_1^{h_1} p_2^{h_2} \ldots p_k^{h_k},$$

onde é possível algum $h_i = 0$.

Reciprocamente, todo inteiro

$$d = p_1^{h_1} p_2^{h_2} \ldots p_k^{h_k} \ \ (0 \leq h_i \leq r_i),$$

é um divisor de n, pois, podemos escrever:

$$n = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k} = (p_1^{h_1} p_2^{h_2} \ldots p_k^{h_k})(p_1^{r_1 - h_1} p_2^{r_2 - h_2} \ldots p_k^{r_k - h_k}) = d(p_1^{r_1 - h_1} p_2^{r_2 - h_2} \ldots p_k^{r_k - h_k}),$$

onde $r_i - h_i \geq 0$ para cada i. Logo, d é um divisor de $n (d \mid n)$. ■

Exemplo 2.11. *Os divisores positivos do inteiro* $n = 630 = 2 \cdot 3^2 \cdot 5 \cdot 7$, *são precisamente, os inteiros da forma:*

$$d = 2^{h_1} \cdot 3^{h_2} \cdot 5^{h_3} \cdot 7^{h_4}, \tag{2.9}$$

onde $0 \leq h_1 \leq 1, \quad 0 \leq h_2 \leq 2, \quad 0 \leq h_3 \leq 1 \quad e \quad 0 \leq h_4 \leq 1.$
Logo $h_1 = 0, 1, \ \ h_2 = 0, 1, 2, \ \ h_3 = 0, 1$ *e* $h_4 = 0, 1.$
Assim, com $h_1 = 1, \ \ h_2 = 2, \ \ h_3 = 0$ *e* $h_4 = 1$, *obtemos*

$$d = 2 \cdot 3^2 \cdot 5^0 \cdot 7^1 = 2 \cdot 9 \cdot 1 \cdot 7 = 126,$$

um divisor de 630. *De fato,* $630 = 126 \cdot 5$.

2.7 Soma de Divisores

Seja n um número inteiro positivo. A soma dos seus divisores positivos é indicada por $\sigma(n)$.

Assim, por exemplo, os divisores positivos de 6 são $1, 2, 3$ e 6, de maneira que

$$\sigma(6) = 1 + 2 + 3 + 6 = 12.$$

Os divisores positivos de 11 são 1 e 11, de modo que

$$\sigma(11) = 1 + 11 = 12.$$

Os divisores positivos de 11^2 são 1,11 e 11^2, de modo que

$$\sigma(11^2) = 1 + 11 + 11^2 = 133.$$

Se p é um número primo, então $\sigma(p) = 1 + p$, porque os únicos divisores positivos de p (Ver definição 2.4) são 1 e p.

Teorema 2.19. *Se* $n = p_1^{r_1} \cdot p_2^{r_2} \ldots p_k^{r_k}$ *é decomposição canônica do inteiro positivo* $n > 1$, *então*

$$\sigma(n) = \frac{p_1^{r_1+1} - 1}{(p_1 - 1)} \cdot \frac{p_2^{r_2+1} - 1}{(p_2 - 1)} \cdots \frac{p_k^{r_k+1} - 1}{(p_k - 1)} = \prod_1^k \frac{p_i^{r_i+1} - 1}{(p_i - 1)} \tag{2.10}$$

Demonstração: Consideremos o produto:

$$(1 + p_1 + p_1^2 + \ldots + p_1^{k_1})(1 + p_2 + p_2^2 + \ldots + p_2^{k_2}) \ldots (1 + p_r + p_r^2 + \ldots + p_r^{k_r}).$$

Pelo Teorema 2.18, cada divisor positivo de n é um termo do desenvolvimento deste produto e vice-versa, de modo que

$$\sigma(n) = (1 + p_1 + p_1^2 + \ldots + p_1^{k_1})(1 + p_2 + p_2^2 + \ldots + p_2^{k_2}) \ldots (1 + p_r + p_r^2 + \ldots + p_r^{k_r}).$$

Aplicando a cada parêntese do segundo membro desta igualdade a fórmula que dá a soma dos termos de uma progressão geométrica finita, temos:

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1},$$

ou seja:

$$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{k_i+1} - 1}{p_i - 1}.$$

Nota-se que

$$\sigma(n) = \sigma(p_1^{k_1})\sigma(p_2^{k_2}) \ldots \sigma(p_r^{k_r}).$$

■

Exemplo 2.12. *O número* $4200 = 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^1$, *de modo que a soma de seus divisores positivos é:*

$$\sigma(n) = \frac{2^4 - 1}{(2-1)} \cdot \frac{3^2 - 1}{(3-1)} \cdot \frac{5^3 - 1}{(5-1)} \cdot \frac{7^2 - 1}{(7-1)} = 15 \cdot 4 \cdot 31 \cdot 8 = 14880.$$

2.8 Funções Aritméticas

Definição 2.7. *Chama-se função aritmética toda função* f *definida no conjunto* $\mathbb{N}$ *dos inteiros positivos e com valores no conjunto* $\mathbb{Z}$ *dos inteiros, isto é, toda função* f *de* $\mathbb{N}$ *em* $\mathbb{Z}$ ($f : \mathbb{N} \longrightarrow \mathbb{Z}$).

Portanto, o domínio e o contradomínio de uma função aritmética f são os conjuntos $\mathbb{N}$ e $\mathbb{Z}$, respectivamente, e a imagem é o conjunto:

$$Im(f) = \{f(n) \in \mathbb{Z}; n \in \mathbb{N}\}$$

que, obviamente, é uma parte de $\mathbb{Z} : Im(f) \subset \mathbb{Z}$.

Duas funções aritméticas importantes são as funções d e σ de $\mathbb{N}$ em $\mathbb{N}$ ($d, \sigma : \mathbb{N} \longrightarrow \mathbb{N}$) assim definidas para todo inteiro positivo n :

$$d(n) = \text{ número de divisores positivos de } n$$

e

$$\sigma(n) = \text{ soma dos divisores positivos de } n.$$

Definição 2.8 (Funções Aritméticas Multiplicativas)**.** *Uma função aritmética* f *diz-se uma função aritmética multiplicativa se*

$$f(rs) = f(r)f(s),$$

para todo par de inteiros positivos r *e* s *tais que o* $mdc(r,s) = 1$.

Teorema 2.20. *A função* $\sigma(n)$ *é uma função aritmética multiplicativa.*

Demonstração:

Sejam u e v dois inteiros positivos tais que o $mdc(u,v) = 1$. Se $u = 1$ ou $v = 1$, então, obviamente:

$$\sigma(uv) = \sigma(u)\sigma(v).$$

Suponhamos, pois, $u > 1$ e $v > 1$, e sejam

$$u = p_1^{k_1} p_2^{k_2} \dots p_i^{k_i}, \;\; v = q_1^{h_1} q_2^{h_2} \dots q_j^{h_j}$$

as decomposições canônicas de u e v.
Como $p_x \neq q_y$ para $x = 1,2,\dots,i$ e $y = 1,2,\dots,j$, visto que o $mdc(u,v) = 1$, segue-se que a decomposição canônica do produto uv é dada pela igualdade:

$$uv = p_1^{k_1} p_2^{k_2} \dots p_i^{k_i} q_1^{h_1} q_2^{h_2} \dots q_j^{h_j}$$

c, portanto:

$$\sigma(uv) = \left[\frac{p_1^{k_1+1}-1}{p_1-1} \dots \frac{p_i^{k_i+1}-1}{p_i-1}\right] \cdot \left[\frac{q_1^{h_1+1}-1}{q_1-1} \dots \frac{q_j^{h_j+1}-1}{q_j-1}\right] = \sigma(u)\sigma(v),$$

de modo que $\sigma(n)$ é uma função aritmética multiplicativa. ■

Exemplo 2.13. *Verificar que a função $\sigma(n)$ é uma função aritmética multiplicativa para $n = 28$. Temos $28 = 2^2 \cdot 7$ e o $mdc(4,7) = 1$. Portanto:*

$$\sigma(28) = \frac{2^3-1}{2-1} \cdot \frac{7^2-1}{7-1} = 7 \cdot 8 = 56,$$

$$\sigma(4) = \frac{2^3-1}{2-1} = 7,$$

$$\sigma(7) = \frac{7^2-1}{7-1} = 8.$$

Podemos notar que

$$\sigma(28) = \sigma(4)\sigma(7).$$

3 Resultados Principais

Atualmente, um dos problemas mais famosos da teoria dos números é se existe algum número perfeito ímpar. Isso motiva os estudiosos e amantes da matemática, o que a torna uma ciência atual e em constante desenvolvimento. Assumindo a existência dos números perfeitos ímpares, são consideradas condições necessárias para estes números serem encontrados. Temos alguns resultados a respeito nesse capítulo.

3.1 Números Perfeitos

Definição 3.1. *Um número inteiro positivo n diz-se um número perfeito se a soma de todos os seus divisores positivos é igual ao seu dobro. Ou seja,*

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

Assim, por exemplo, para $n = 6$ e $n = 28$, temos:

$$\sigma(6) = 1+2+3+6 = 12 = 2\cdot 6$$

e

$$\sigma(28) = 1+2+4+7+14+28 = 56 = 2\cdot 28$$

de modo que os inteiros positivos 6 e 28 são ambos números perfeitos. Os números perfeitos são muito raros e até hoje (2014) são conhecidos apenas 48, todos pares, e os oito primeiros são:

$$\begin{aligned} P_1 &= 6, \\ P_2 &= 28, \\ P_3 &= 496, \\ P_4 &= 8128, \\ P_5 &= 33550336, \\ P_6 &= 8589869056, \\ P_7 &= 137438691328, \\ P_8 &= 2305843008139952128, \end{aligned}$$

os quais (pelo Teorema 3.4) terminam em 6 ou em 8 e, com exceção de 6, são da forma $9k+1$, no qual o único número perfeito par da forma x^3+1 (x inteiro positivo) é o 28. Os números 6 e 28 são números perfeitos da forma $n-1$ e $\frac{n(n+1)}{2}$, onde $n>1$ e este é obtido por $n=7$.

Não se conhece nenhum número perfeito ímpar, e nem mesmo se sabe se existem, mas, se existem, são muito grandes - maiores que 10^{1000}. Para ter uma noção da grandeza dos números perfeitos, o

$$P_{12} = 2^{126}(170141183460469231731731687303715884105727),$$

onde o número 170141183460469231731687303715884105727 é um primo de Mersenne[1].

Teorema 3.1 (de Euclides)**.** *Se 2^k-1 é primo $(k>1)$, então o número natural $n=2^{k-1}(2^k-1)$ é um número perfeito.*

Demonstração:

Seja $2^k-1=p$ $(k>1)$ um primo. Consideremos o número natural $n=2^{k-1}p$. Como o $mdc(2^{k-1},p)=1$ e $\sigma(n)$ é uma função aritmética multiplicativa (Teorema (2.20)), temos:

[1] Chama-se número de Mersenne todo inteiro positivo da forma:

$$M_n = 2^n - 1 (n \geq 2).$$

Se M_n é primo diz-se que é um primo de Mersenne.

$$\begin{aligned}
\sigma(n) &= \sigma(2^{k-1}p) \\
&= \sigma(2^{k-1})\sigma(p) \\
&= \frac{2^{k-1+1}-1}{2-1}(p+1) \\
&= (2^k-1)(2^k-1+1) \\
&= (2^k-1)2^k = (2^k-1)2\frac{2^k}{2} \\
&= 2.2^{k-1}(2^k-1) = 2n.
\end{aligned}$$

Logo, por definição, n é um número perfeito.

■

Assim, todas as vezes que se conhece um natural $k > 1$ tal que $2^k - 1$ é primo, pode-se construir um número perfeito.

Para $k = 13$, por exemplo, temos $2^{13} - 1 = 8191$, um primo, o que dá o 5^o número perfeito:

$$2^{13-1}(2^{13}-1) = 2^{12}(2^{13}-1) = 33550336 = P_5.$$

Nota: Os quatro primeiros números perfeitos se obtém pela fórmula de Euclides atribuindo a k os valores 2, 3, 5 e 7, isto é:

$$\begin{aligned}
P_1 &= 2^{2-1}(2^2-1) = 6, \\
P_2 &= 2^{3-1}(2^3-1) = 28, \\
P_3 &= 2^{5-1}(2^5-1) = 496, \\
P_4 &= 2^{7-1}(2^7-1) = 8128.
\end{aligned}$$

Para $k = 17$ e $k = 19$, temos o sexto e o sétimo números perfeitos, respectivamente:

$$\begin{aligned}
P_6 &= 2^{17-1}(2^{17}-1) = 2^{16}(2^{17}-1) = 8.589.869.056 \\
&\quad e \\
P_7 &= 2^{19-1}(2^{19}-1) = 2^{18}(2^{19}-1) = 137.438.691.328,
\end{aligned}$$

os quais foram determinados, pela primeira vez, pelo matemático italiano Pietro Cataldi em 1603.

Os outros 41 números perfeitos conhecidos se obtém pela fórmula de Euclides atribuindo a k os seguintes valores:

31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, 20996011, 24036583, 25964951, 30402457, 32582657, 37156667, 43112609, 42643801 e 57885161.

3.2 Números Perfeitos Pares

O próximo resultado é a reciproca do Teorema 3.1(de Euclides) e foi demonstrado por Euler cerca de 2000 anos depois de Euclides.

Teorema 3.2 (de Euler)**.** *Se n é um número perfeito par, então,* $n = 2^{k-1}(2^k - 1)$*, onde* $2^k - 1$ *é primo.*

Demonstração: Suponhamos que n é um número perfeito par. Então, n pode ser escrito como produto de um número par e um número ímpar, ou seja, sob a forma: $n = 2^{k-1}m$, onde m é um número natural ímpar e $k \geq 2$.

Como o $mdc(2^{k-1}, m) = 1$ e $\sigma(n)$ é uma função aritmética multiplicativa (Teorema (2.20)), temos:

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

Por outro lado, como n é um número perfeito, temos: $\sigma(n) = 2n = 2 \cdot 2^{k-1} \cdot m = 2^k \cdot m$, portanto:

$$2^k m = (2^k - 1)\sigma(m) \tag{3.1}$$

de modo que $(2^k - 1) \mid 2^k m$. Mas, o $mdc(2^k - 1, 2^k) = 1$, o que implica, $(2^k - 1) \mid m$, isto é, $m = (2^k - 1) \cdot M$, para algum inteiro M.

Substituindo este valor de m na equação (3.1) e cancelando o fator comum $2^k - 1$, obtemos: $\sigma(m) = 2^k M$. Como m e M são ambos divisores positivos de m (com $M < m$), temos:

$$2^k M = \sigma(m) \geq m + M = 2^k M,$$

o que implica:

$$\sigma(m) = m + M.$$

Assim, m e M são os únicos divisores positivos de m, e isto significa que m é primo e $M = 1$. Então:

$$m = (2^k - 1)M = 2^k - 1$$

é um primo, e por ser escrito como:

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

o Teorema de Euler fica demonstrado.

■

O teorema que se segue estabelece uma condição necessária, mas não suficiente, para que um inteiro da forma

$$2^k - 1 \ \ (k \geq 2),$$

seja primo.

Teorema 3.3. *Se* $2^k - 1 \ \ (k \geq 2)$ *é primo, então k também é primo.*

Demonstração:

Suponhamos o inteiro $2^k - 1 (k \geq 2)$ primo. Se o inteiro k fosse composto, então teríamos $k = rs$, com $r > 1$ e $s > 1$, o que implica:

$$2^k - 1 = 2^{rs} - 1 = (2^r)^s - 1,$$

ou seja:

$$2^k - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + ... + 2^r + 1).$$

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

■

Nota: A recíproca do Teorema 3.3 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:

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

Esses últimos resultados mostram que os números da forma $2^k - 1, (k > 2)$ são de fundamental importância para o estudo dos números perfeito e são chamados números de Mersenne e denotados por $M_k = 2^k - 1$, quando primos, são chamados primos de Mersenne. Note também que a fórmula $P_n = 2^{k-1}(2^k - 1)$ não relaciona o índice com o expoente, o que aumenta a dificuldade para achar mais números perfeitos. A tarefa diretora é achar um inteiro k de forma que $2^k - 1$ seja um número primo, onde só pode ser feito por inspeção.

Teorema 3.4. *Todo número perfeito par termina em* 6 *ou* 8.

Demonstração:

Seja n um número perfeito par. Pelo Teorema 3.2 (de Euler), temos:

$$n = 2^{k-1}(2^k - 1), \text{ onde } 2^k - 1 \quad \text{é primo.}$$

E, pelo Teorema 3.3, 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 ímpar, logo pelo exemplo 2.1, página 16, ele é da forma $4m-1$ ou $4m-3$, que adicionando 4 as duas expressões obtemos, $4m+3$ e $4m+1$, para todo inteiro m, respectivamente (ambos expressões números ímpares). Se k é da forma $4m+1$, então:

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

Por ser $16^t \equiv 6 \pmod{10}$, qualquer que seja o inteiro positivo t, segue-se que

$$n \equiv (2 \cdot 6 - 6) \equiv 6 \pmod{10},$$

isto é: $n = 10h + 6$ e, portanto, n termina em 6.

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

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

Por ser $16^t \equiv 6 \pmod{10}$, qualquer que seja o inteiro positivo t, segue-se que

$$n \equiv (2.6 - 4.6) \equiv (-12) \equiv 8 \pmod{10},$$

isto é: $n = 10h' + 8$ e, portanto, n termina em 8.

■

Teorema 3.5. *Um primo não pode ser um número perfeito.*

Demonstração:

Seja p um primo qualquer. Então, $\sigma(p) = p + 1$. Se p é um número perfeito, então $\sigma(p) = 2p$. Portanto:

$$p + 1 = 2p \Longrightarrow p = 1.$$

Como $p \geq 2$, segue-se que p não é um número perfeito. Logo, um primo não pode ser um número perfeito.

■

Observação 3.1. *A raiz digital de um número inteiro não negativo é o resto da sua divisão por* 9. *Um modo prático de calcular a raiz digital de um número é fazendo a soma de seus algarismos, se esssa soma resultar em um número maior que* 9, *fazemos novamente a soma de seus algarismos e, assim, sucessivamente, até resultar em um único algarismo, se for* 9, *a raiz é zero, se for entre* 0 *e* 9, *essa será a raiz digital do número (por exemplo, 556; 5 + 5 + 6 = 16; 1 + 6 = 7). Uma das propriedades mais interessantes dos números perfeitos pares é que a raiz digital de qualquer número perfeito par sempre será* 1.

Teorema 3.6. *Somando os dígitos de qualquer número perfeito par (exceto* 6*), em seguida, somar os algarismos do número resultante, repetindo este processo até chegar um único dígito, então este dígito será sempre* 1.

Demonstração:

Suponhamos p primo ímpar. Sabemos que $2 \equiv -1 \pmod 3$. Pelo Teorema 2.17, item 3, temos que, $2^{p-1} \equiv (-1)^{p-1} \pmod 3$. Mas $p-1$ é par se $p \neq 2$, e, assim, $2^{p-1} \equiv 1 \pmod 3$, isto é,

$$2^{p-1} = 3k+1, \tag{3.2}$$

para algum k inteiro. Multiplicando a equação (3.2) por 2, teremos $2^p = 6k+2$, ou seja, $2^p - 1 = 6k+1$. Logo,

$$2^{p-1}(2^p-1) = (3k+1)(6k+1) = 18k^2+9k+1 = 9(2k^2+k)+1 = 9K+1 \equiv 1 \pmod 9,$$

com $K = 2k^2+k$. Portanto, a raiz digital (observação 3.1) de um número perfeito par (diferente de 6) é 1. ■

Nota: 6 falha pois, ao usarmos a fórmula $2^{p-1}(2^p-1)$, teremos $p = 2$. Também chegamos a conclusão que os números perfeitos são da forma $9K+1$(mencionado no começo do capítulo), ou seja, deixam resto 1 quando divididos por 9.

Exemplo 3.1.

$28; 2+8 = 10; 1+0 = 1,$

$496; 4+9+6 = 19; 1+9 = 10; 1+0 = 1,$

$8128; 8+1+2+8 = 19; 1+9 = 10; 1+0 = 1,$

$33550336; 3+3+5+5+0+3+3+6 = 28; 2+8 = 10; 1+0 = 1,$

$8589869056; 8+5+8+9+8+6+9+0+5+6 = 64; 6+4 = 10; 1+0 = 1,$

$137438691328; 1+3+7+4+3+8+6+9+1+3+2+8 = 55; 5+5 = 10; 1+0 = 1,$

$2305843008139952128; 2+3+0+5+8+4+3+0+0+8+1+3+9+9+5+2+1+2+8 = 73; 7+3 = 10; 1+0 = 1.$

Teorema 3.7. *Todo número perfeito par maior que* 6 *é múltiplo de* 4.

Demonstração: Seja

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

um número perfeito par. Então, k é um número primo ímpar (pois $n > 6$). Logo, sendo k um número primo ímpar, temos que:

$$k = 4t + 1 \text{ ou } k = 4t + 3.$$

Caso 1: Sendo $k = 4t + 1$, onde $t \in \mathbb{N}$, temos:

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

Caso 2: Agora para $k = 4t + 3$, onde $t \in \mathbb{N}$, temos:

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

■

Teorema 3.8. *Todo número perfeito par maior que* 6 *pode ser escrito como uma diferença de dois quadrados perfeitos.*

Demonstração: Seja n um número perfeito par maior que 6. Então, pelo Teorema (3.7), $n = 4k$, para algum $k \in \mathbb{N}$. Logo,

$$n = (k+1)^2 - (k-1)^2.$$

■

Teorema 3.9. *Qualquer número mesmo perfeito maior que* 28 *pode ser representado como a soma de pelo menos dois números perfeitos.*

Demonstração:

Para provar este teorema, temos que usar a proposição dos números naturais que diz assim:

Se p e q são números naturais tal que o $mdc(p,q) = 1$, então todo número natural maior que ou igual a $pq - p - q + 1$ é obtido através de uma combinação linear $mp + nq$, com m e n inteiros não-negativos.

Agora temos que o $mdc(3,14) = 1$, todo número natural maior que $3 \cdot 14 - 3 - 14 + 1 = 26$ pode ser representado através de uma combinação linear da forma $3x + 14y$ com $x, y \geq 0$. Multiplicando por 2, nós temos que todo número par maior que 52, em particular, todo número perfeito par $n > 28$, pode ser representado como uma combinação linear de $6x + 28y$.

■

Teorema 3.10. *A soma dos inversos de todos os divisores de um número perfeito par (incluindo ele próprio) é igual a 2.*

Demonstração:

Se n é um número perfeito par e $d_1, d_2, ..., d_r$ são seus divisores não triviais, teremos a expressão

$$\frac{1}{1}+\frac{1}{d_1}+\frac{1}{d_2}+\frac{1}{d_3}+...+\frac{1}{n}=\frac{n+...+d_3+d_2+d_1+1}{n}.$$

Mas $1+d_1+d_2+d_3+...=n$, então a soma será

$$\frac{n+n}{n}=\frac{2n}{n}=2$$

■

Nota: Um número triangular é a soma de números consecutivos, ou seja,

$$1+2+3+...+n=\frac{n(n+1)}{2}=T_n,$$

com $n \in \mathbb{N}$.

Teorema 3.11. *Números perfeitos pares são triangulares.*

Demonstração:

Suponha P um número perfeito par. Logo, pela fórmula de Euclides,

$$P=2^{m-1}(2^m-1)=\frac{(2^m-1)2^m}{2}.$$

Assim, fazendo $2^m-1=n$, teremos $2^m=n+1$. Substituindo, teremos

$$P=\frac{n(n+1)}{2}.$$

■

Teorema 3.12. *Se n é um número perfeito par, então* $8n+1$ *é um quadrado perfeito.*

Demonstração: Seja n um número perfeito par, isto é, $n=2^{k-1}(2^k-1)$.Então,

$$\begin{aligned} 8n+1 &= 8[2^{k-1}(2^k-1)]+1=2^3[2^{k-1+k}-2^{k-1}]+1 \\ &= 2^{3+k-1+k}-2^{3+k-1}+1=2^{2k+2}-2^{k+2}+1 \\ &= 2^{2(k+1)}-2^{k+1+1}+1=(2^{k+1})^2-2.2^{k+1}+1 \\ &= (2^{k+1}-1)^2. \end{aligned}$$

Portanto $8n+1$ é um quadrado perfeito.

■

Teorema 3.13. *Seja $A(n)$ o conjunto de divisores primos de $n > 1$. Se n é um número perfeito par, então é imediato que*

$$A(n) = A(\sigma(n)). \tag{3.3}$$

Demonstração: Seja $p \in A(n)$ pelo Teorema 2.16, temos:

$$p \leq \sqrt{n} \leq \sqrt{2}\sqrt{n} = \sqrt{2n} \Longrightarrow p \in A(2n).$$

Portanto,

$$A(n) \subseteq A(\sigma(n)),$$

pois n é um número perfeito par.

Reciprocamente, se

$$p \in A(\sigma(n)) = A(2n) \Longrightarrow p \mid 2n \Longrightarrow p \mid 2 \text{ ou } p \mid n.$$

Se $p \mid 2$, então $p \mid n$, pois n é perfeito. Logo $p \in A(n)$.

■

Teorema 3.14 (C.Pomerance)**.** *Se a equação 3.3 é válido para um número n, então n deve ser mesmo perfeito.*

Para ver a sua demonstração consulte: C. Pomerance, Problema 6036, 82(1975), p. 671; e 84(1977), p. 225; solução por a University of British Columbia Problems Group, same journal, 85(1978), 830.

Já sabemos que para um número n ser perfeito a soma de seus divisores tem que ser igual a $2n$. E vimos também que a soma dos divisores de um número natural é igual a

$$\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1}.\frac{p_2^{k_2+1}-1}{p_2-1}...\frac{p_r^{k_r+1}-1}{p_r-1}.$$

Teorema 3.15. *Seja $n = p_1^{k_1}p_2^{k_2}p_3^{k_3}...p_r^{k_r}$ um número natural em sua decomposição em fatores primos. Se k_i é um expoente par, onde $1 \leq i \leq r$, então $\sigma(p_i^{k_i})$ é ímpar.*

Demonstração: Vamos analisar o que acontece com cada um dos fatores acima quando o expoente é par. Primeiramente, vamos supor que o expoente é um número par. Então: para $k = 2\alpha$, com $\alpha \in \mathbb{Z}$, temos:

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

Como $\dfrac{p^{\alpha}-1}{p-1} = p^{\alpha-1}+p^{\alpha-2}+...+p+1$ temos:

$$a = p(p^{\alpha}+1).(p^{\alpha-1}+p^{\alpha-2}+...+p+1)+1.$$

Para $p=2 \Longrightarrow a = 2K+1$, ou seja, a é ímpar. Para $p>2$, o fator $p^{\alpha}+1$ é par. Portanto, $a = 2K_1+1$, que é ímpar. Logo para k par, então o fator $\dfrac{p^{k+1}-1}{p-1}$ sempre resulta em um número ímpar. ■

Teorema 3.16. *Um número quadrado perfeito não pode ser um número perfeito.*

Demonstração: De fato, se $n = p_1^{k_1}.p_2^{k_2}.p_3^{k_3}...p_r^{k_r}$ é um quadrado perfeito em sua decomposição em fatores primos, os expoentes k_i são todos números pares. Logo, pelo Teorema 3.15, todos os fatores de $\sigma(n)$ são ímpares. Pela proposição 29 do livro IX de Euclides que diz:

"Caso um número ímpar, tendo multiplicado um número ímpar, faça algum, o produzido será ímpar."

Portanto, a soma dos divisores de um número quadrado perfeito sempre será um número ímpar, ou seja, não pode ser da forma $2n$. Logo, não pode ser um número perfeito. ■

3.3 Números Perfeitos Ímpares

Vamos analisar agora o que acontece quando temos um número natural ímpar.

Quando

$$n = p_1^{k_1}.p_2^{k_2}.p_3^{k_3}...p_r^{k_r}$$

é ímpar, cada p_i também será ímpar.

Teorema 3.17. *Seja $n = p_1^{k_1}p_2^{k_2}p_3^{k_3}...p_r^{k_r}$ um número natural ímpar, em sua decomposição em fatores primos. Se k_i é um expoente ímpar, onde, $1 \leq i \leq r$, então $\sigma(p_i^{k_i})$ é par.*

Demonstração: Agora vamos analisar quando o expoente é um número ímpar, ou seja: $k = 2\alpha+1$. Temos:

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

Chamando a expressão acima de b, temos para $p>2$, o fator $p^{\alpha}+1$ é par, o que implica que

$$\frac{p^2(p^{\alpha}-1).(p^{\alpha}+1)}{p-1}$$

também é par. Sejam $\frac{p^2(p^\alpha-1).(p^\alpha+1)}{p-1} = 2q_1$ e $p+1 = 2r$, temos que,

$$b = 2q_1 + 2r = 2(q_1 + r) = 2K_3,$$

com $K_3 = q_1 + r$. Portanto, $\frac{p^{k+1}-1}{p-1}$ é par, quando k é ímpar, com $p > 2$.

■

Exemplo 3.2. *Seja $n = 4725 = 3^3.5^2.7$, então vamos calcular a soma dos divisores de n.*

Temos:

$$\sigma(4725) = \frac{3^{3+1}-1}{3-1}.\frac{5^{2+1}-1}{5-1}.\frac{7^{1+1}-1}{7-1} = 40 \cdot 31 \cdot 8.$$

Note que as potências de $3, 5$ e 7 do natural 4725 (de expoentes respectivamente ímpar, par e ímpar) correspondem respectivamente aos fatores $40, 31$ e 8 (e estes são números respectivamente par, ímpar e par).

O próximo resultado mostra quando um número inteiro ímpar não pode ser perfeito.

Teorema 3.18. *Um número natural ímpar que tem pelo menos dois fatores com expoentes ímpares, não pode ser perfeito.*

Demonstração: Tomemos $n = p_1^{k_1}.p_2^{k_2}.p_3^{k_3}...p_r^{k_r}$, um número natural ímpar, suponhamos que k_1 e k_2 sejam ímpares e os demais expoentes com qualquer paridade. Então, pelo Teorema 3.17 os dois primeiros fatores de $\sigma(n)$ serão pares, portanto $\sigma(n)$ será múltiplo de 4. Logo, não pode ser igual a $2n$, o que mostra que n não pode ser perfeito.

■

Infelizmente, a argumentação que usamos com sucesso nos casos anteriores falha no caso em que é ímpar apenas um dos expoentes em

$$n = p_1^{k_1}.p_2^{k_2}.p_3^{k_3}...p_r^{k_r}.$$

Nesse caso, apenas um dos fatores de $\sigma(n)$ será par. Assim sendo, $\sigma(n)$ será múltiplo de 2, mas não de 4. Como n é ímpar, não há contradição em admitir a igualdade $\sigma(n) = 2n$ verdadeira. Então não podemos concluir que um número ímpar não pode ser perfeito no caso em que apenas um dos expoentes da fatoração seja ímpar.

Segundo (ALBURQUERQUE,2000) uma das conjecturas mais antigas da Matemática que ainda está em aberto, diz que não existe números perfeitos ímpares. Para demonstrar o próximo teorema temos primeiramente que utilizar a seguinte afirmação:

Teorema 3.19. *Seja $n \in \mathbb{N}$. Se n é ímpar, então n é uma diferença de dois quadrados.*

Demonstração: Se n é ímpar, como $n \geq 1$, então $n-1$ e $n+1$ são pares e, portanto, $\frac{n-1}{2}$ e $\frac{n+1}{2}$ são números naturais. Logo,

$$\left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2 = \frac{n^2+2n+1-n^2+2n-1}{4} = \frac{4n}{4} = n.$$

■

Teorema 3.20. *Se existir um número perfeito ímpar, ele será a diferença de dois quadrados perfeitos.*

Demonstração:

Suponhamos que n seja um número perfeito ímpar, logo $\sigma(n) = 2n$ pela definição (3.1). Como n é ímpar, sua decomposição em fatores primos(ímpares) é

$$n = p_1^{k_1} p_2^{k_2} p_3^{k_3} ... p_r^{k_r},$$

então

$$\sigma(n) = 2[p_1^{k_1} p_2^{k_2} p_3^{k_3} ... p_r^{k_r}].$$

Como

$$\sigma(p_1^{k_1} p_2^{k_2} p_3^{k_3} ... p_r^{k_r}) = \sigma(p_1^{k_1})\sigma(p_2^{k_2})\sigma(p_3^{k_3})...\sigma(p_r^{k_r}),$$

pois $\sigma(n)$ é uma função aritmética multiplicativa. Assim,

$$\sigma(p_1^{k_1})\sigma(p_2^{k_2})\sigma(p_3^{k_3})...\sigma(p_r^{k_r}) = 2[p_1^{k_1} p_2^{k_2} p_3^{k_3} ... p_r^{k_r}],$$

o que implica que existe somente um único número i, $1 \leq i \leq r$ com $\sigma(p_i^{k_i})$ par, sendo os fatores restantes todos ímpares. Então pelo Teorema (3.17) k_i é ímpar e pelo Teorema (3.15) k_j é par para $1 \leq j \leq r$ e $j \neq i$. Logo, $\frac{n}{p_i^{k_i}}$ é um quadrado perfeito, já que as potências inteiras dos primos que restaram são pares. Sendo p_i um primo ímpar, então $p_i^{k_i}$ é um número ímpar, logo pelo Teorema (3.19) afirma que $p_i^{k_i}$ pode ser decomposto numa diferença de dois quadrados perfeitos $a^2 - b^2$.

Então, $\frac{n}{p_i^{k_i}} = c^2$ e $p_i^{k_i} = a^2 - b^2$, logo

$$n = c^2(a^2 - b^2) = (ca)^2 - (cb)^2.$$

■

Observamos que o matemático e filósofo francês René Descartes, um dos fundadores da Geometria Analítica, acreditava na possibilidade de existirem números perfeitos ímpares.

Conclusão

Os números perfeitos tem uma história interessante, onde estão envolvidos grandes matemáticos, como foi mostrado no primeiro capítulo deste trabalho, assim como uma tabela contendo todos os números perfeitos(48) encontrados,ano de descoberta e seus descobridores. No segundo capítulo apresentamos os resultados fundamentais, que foi a base para o desenvolvimento do tema principal.

Dessa forma, preocupamo-nos em desenvolver uma pesquisa sobre os números perfeitos, no qual, observa-se conceitos simples que dão origem a problemas complicados, com alguns ainda sem solução. O conceito de número perfeito não foge a essa regra e até hoje não se sabe se existem números ímpares que sejam também perfeitos.

Contudo, concluímos a respeito dos números perfeitos ímpares, que se tem condições para sua existência, mas não tem nenhuma prova ainda dela, assim como, ninguém até hoje conseguiu demonstrar a não existência.

Em suma, diante do que abordamos neste trabalho, esperamos contribuir para uma compreensão, por parte do leitor, do que se trata realmente um número perfeito. E assim, instigar nos leitores a curiosidade de encontrar novos resultados para os números perfeitos ímpares.

Referências

A. BRAUER. **On the non-existence of odd perfect numbers of form** $p^{\alpha}q_1^2 \dots q_{t.1}^2 \cdot q_t^4$, Bull. A.M.S. 49 (1943). p.712-718.

A. MAKOWSKI. **Remark on perfect numbers**. Elem. Math. 17 1962 n^{o}.5, 109.

C. POMERANCE.**Multiply perfect numbers, Mersenne primes and effective computability**.

DE ALBUQUERQUE, Roberto Stenio AC. **EM BUSCA DA PERFEIÇÃO**.REVISTA DO PROFESSOR DE MATEMÁTICA, v. 44, p. 33, 2000.

LOPES, Jaqueline Vieira; AVILA, Jorge Andrés Julca.**Limitação de qualquer fator primo de um número perfeito impar**. 2013.

DO NASCIMENTO, Mauri Cunha; DE ARAUJO FEITOSA, Hércules. **Elementos da Teoria dos Números**.

SÁNDOR, József; CRSTICI, Borislav. **Handbook of number theory II**. springer, 2004.

ZATARIAN, Daniella et al. **Números curiosos**. 2012.

DE ALENCAR FILHO, Edgard. **Teoria elementar dos números**. Nobel, 1981.

PRIMES, Mersenne. História, Teoremas e Listas.Disponível em: http://primes. UTM. edu/mersenne/index.html,2007.

MAGRINI, Luciano Aparecido.**SOBRE NÚMEROS PERFEITOS**.REVISTA DO PROFESSOR DE MATEMÁTICA, v. 78, p. 16, 2012.

HEFEZ, Abramo. **Elementos de aritmética**. Sociedade Brasileira de Matemática, 2006.

DE OLIVEIRA SANTOS, José Plínio. **Introdução à teoria dos números**. Instituto de Matemática Pura e Aplicada, 1998.