UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS EXATAS E DA NATUREZA
DEPARTAMENTO DE MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

Números Perfeitos [1]

por

Sívio Orleans Cruz

sob orientação do

Prof. Dr. Napoleón Caro Tuesta

JOÃO PESSOA - PB

2013

[1] O presente trabalho foi realizado com apoio da CAPES.

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS EXATAS E DA NATUREZA
DEPARTAMENTO DE MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

Números Perfeitos

por
Sívio Orleans Cruz

Trabalho de Conclusão do Mestrado Profissional em Matemática em Rede Nacional pela Universidade Federal da Paraíba como parte dos requisitos para obtenção do título de Mestre em Matemática, sob orientação do Prof. Dr. Napoleón Caro Tuesta.

JOÃO PESSOA - PB
2013

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS EXATAS E DA NATUREZA
DEPARTAMENTO DE MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

Números Perfeitos

por

Sívio Orleans Cruz

A banca examinadora abaixo-assinada aprova o Trabalho de Conclusão do Mestrado apresentado como parte dos requisitos para a obtenção do Certificado de Conclusão do Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) pela Universidade Federal da Paraíba.

Aprovado em: _____ de_____ 2013

Prof. Dr. Napoleón Caro Tuesta-UFPB (Orientador)

Prof. Dr. Lizandro Sanchez Challapa-UFPB

Prof. Dr. Gilberto Fernandes Vieira-UFCG

"A matemática goza de um prestígio especial, e isto, por uma razão única: é que suas teses são absolutamente certas e irrefutáveis, ao passo que as outras ciências são controvertidas até certo ponto e sempre estão em perigo de serem derrubadas por fatos recém-descobertos. A matemática goza deste prestígio porque é ela que dá às outras ciências certa medida de segurança que elas não poderiam alcançar sem a matemática".

(Albert Einstein)

Sumário

Agradecimentos

A Deus, que em sua infinita sabedoria, tem nos mostrado que os caminhos mais difíceis são os mais férteis para o nosso aprimoramento espiritual.

Aos meus pais Orleans e Olívia, que sempre depositaram em mim, toda sua confiança, acreditando no meu sucesso.

A minha esposa Simone e minhas filhas Tawenne e Tawara, pelo apoio e incentivo em todas as horas, principalmente pela minha ausência no dia a dia e pelos meus momentos de stress.

Ao Professor Dr. Napoleón Caro Tuesta, que me aceitou como seu orientando, sugerindo o tema do meu trabalho e acreditando que seria possível realizá-lo.

A todos os alunos do curso do Mestrado Profissional em Matemática (PROFMAT), turma 2011, UFPB e em especial a meu grande amigo e irmão Ambrósio Elias que não mediu esforços em me ajudar, contribuindo para o meu aprendizado e sanando todas as minhas dificuldades.

Aos Professores da UFPB, pelas aulas, paciência, atenção, e troca de experiências.

Resumo

Nesta dissertação fazemos um estudo de alguns tópicos da Teoria dos Números como motivação para o estudo dos Números Perfeitos e Primos de Mersenne. Apresentamos alguns resultados importantes para o nosso estudo e analisamos algumas demonstrações do Pequeno Teorema de Fermat, evidenciando a demonstração de vários matemáticos que os provaram sob vários aspectos lógicos.

Evidenciamos alguns aspectos históricos e conjecturas para os números perfeitos, através de uma narrativa simples dos fatos e que certamente nos dão a ênfase que motivou e motiva vários matemáticos para o estudo dos números perfeitos.

Abstract

In this thesis we study some topics of the Theory of Numbers as an inspiration for future studies of Perfect Numbers and Mersenne Primes. We present some important results for our study and analyze some statements of Fermat's Little Theorem, showing the various mathematical demonstrations that proved under various logical aspects.

We have clarified some historical aspects and conjectures for perfect numbers, through a simple narrative of facts and this will certainly give us the emphasis that have motivated and still motivates many mathematicians for the study of Perfect Numbers.

Introdução

Esta dissertação tem como objetivo refletir sobre um tema da Teoria dos Números a saber: *Números Perfeitos*, grande preocupação com uma expressão matemática que nos desse todos os Números Perfeitos. Foi o objetivo dos matemáticos da antiguidade como Fermat, Euler e tantos outros.

Ainda hoje os matemáticos e estudiosos estão à procura de números perfeitos e através de métodos computacionais determinaram o 47º *Número Perfeito*.

Acreditamos que, orientados por uma perspectiva crítico-reflexiva sobre os Números Perfeitos e suas propriedades, seja possível repensar as estruturas matemáticas estudadas nos cursos de Licenciatura complementando a formação do docente através das noções específicas sobre a Teoria dos Números, despertando o alunado para investigações dos resultados obtidos por aqueles matemáticos no aspectos histórico e atual.

Trata-se de um trabalho de natureza qualitativa de cunho explicativo, resultante da análise de artigos sobre temas da Teoria dos Números, particularmente dos *Números perfeitos*. Nosso trabalho foi dividido didaticamente em três capítulos, para melhor distribuir a evolução do tema em estudo.

No capítulo 1, revemos a divisão de números naturais e suas propriedades básicas, Teorema de Euclides, Teorema Fundamental da Aritmética, Divisores de um Número, Soma dos Divisores de um Número, Maior Divisor Comum, Números Primos, Algoritmo de Euclides e Congruências.

No capítulo 2 estudamos os *Números Primos de Mersenne* e suas conjecturas, os *Números Perfeitos* e seus principais resultados e suas conjecturas, Números Pares Perfeitos, conjectura sobre os Números Perfeitos Ímpares e Pequeno Teorema de Fermat.

No capítulo 3, dissertamos sobre a evolução da Teoria dos Números, particularmente conduzindo o estudo para os *Números Primos de Mersenne* e suas conjecturas.

Capítulo 1

Divisão em $\mathbb{N}$

Neste capítulo estudaremos as definições e propriedades básicas da divisão no conjunto dos números naturais $\mathbb{N} = \{0, 1, 2, \ldots\}$

1.1 Divisão em $\mathbb{N}$

Definição 1.1. Dados dois números naturais a e b com $a \neq 0$, dizemos que a divide b, escrevendo $a \mid b$, quando existir um $c \in \mathbb{N}$ tal que $b = a \cdot c$. Neste caso, dizemos também que a é um divisor ou um fator de b ou, ainda, que b é múltiplo de a. O número natural c é chamado de *quociente de b por a* e denotado por $c = \dfrac{b}{a}$.

1.1.1 Propriedades

Denotaremos por $\mathbb{N}^* = \{1, 2, 3, \ldots\}$

Proposição 1.1. *Sejam $a, b \in \mathbb{N}^*$ e $c \in \mathbb{N}$. Então, tem-se que:*

i) $1 \mid c,\ a \mid a,\ a \mid 0$.

ii) Se $a \mid b$ e $b \mid c$, então $a \mid c$.

Demonstração:

i) Decorre das igualdades: $c = 1 \cdot c,\ a = a \cdot 1$ e $a \cdot 0 = 0$

ii) Se $a \mid b$ e $b \mid c$, então existem $f, g \in \mathbb{N}$, tais que se, $b = a \cdot f$ e $c = b \cdot g$, então $c = (a \cdot f) \cdot g = a \cdot (f \cdot g) = a \cdot h$, $h \in \mathbb{N}$, o que nos mostra que $a \mid c$.

■

Proposição 1.2. *Sejam $a, b, c, d \in \mathbb{N}$, com $a \neq 0$ e $c \neq 0$, se $a \mid b$ e $c \mid d$, então $a \cdot c \mid b \cdot d$.*

Demonstração: Se $a \mid b$ e $c \mid d$, então existem $f, g \in \mathbb{N}$ tais que $b = a \cdot f$ e $d = c \cdot g$. Portanto, se $b \cdot d = (a \cdot c)(f \cdot g)$, então $a \cdot c \mid b \cdot d$. Em particular, se $a \mid b$, então $a \cdot c \mid b \cdot c$ para todo $c \in \mathbb{N}^*$. ■

Proposição 1.3. *Sejam $a, b, c \in \mathbb{N}$, com $a \neq 0$, tais que $a \mid (b + c)$, então $a \mid b$ se, e somente se $a \mid c$.*

Demonstração: Como $a \mid (b + c)$, existe $f \in \mathbb{N}$ tal que $b + c = f \cdot a$. Se $a \mid b$, existe $g \in \mathbb{N}$ tal que $b = a \cdot g$ logo $a \cdot g + c = f \cdot a = a \cdot f$ donde $a \cdot f > a \cdot g$ logo $f > g$. Portanto, se $c = a \cdot f - a \cdot g = a \cdot (f - g)$ então $a \mid c$, pois $f - g \in \mathbb{N}$. Reciprocamente, se $a \mid c$, existe $h \in \mathbb{N}$ tal que $c = a \cdot h$ se então $b + a \cdot h = f \cdot a = a \cdot f$ se $a \cdot f > a \cdot h$ então $f > h$.
Portanto, se $b = a \cdot f - a \cdot h = a \cdot (f - h)$ então $a \mid b$, pois $f - h \in \mathbb{N}$. ■

Proposição 1.4. *Sejam $a, b, c \in \mathbb{N}$, com $a \neq 0$ e $b \geq c$, tais que $a \mid (b - c)$. Então $a \mid b$ se, e somente se $a \mid c$.*

Demonstração: Como $a \mid (b - c)$, existe $f \in \mathbb{N}$ tal que $b - c = f \cdot a$. Se $a \mid b$, existe $g \in \mathbb{N}$ tal que $b = a \cdot g$, então $a \cdot g - c = f \cdot a = a.f$ logo, $a \cdot g = a \cdot f + c$ donde, $a \cdot g > a.f$ logo $g > f$. Portanto, se $c = a \cdot g - a \cdot f = a \cdot (g - f)$ então $a \mid c$, pois $g - f \in \mathbb{N}$. Reciprocamente, se $a \mid c$, existe $h \in \mathbb{N}$ tal que $c = a \cdot h$ logo, $b - a \cdot h = f \cdot a = a \cdot f$ donde, $b = a \cdot h + a \cdot f = a \cdot (h + f)$, então $a \mid b$, pois $h + f \in \mathbb{N}$. ■

Proposição 1.5. *Sejam $a, b, c \in \mathbb{N}$, com $a \neq 0$ e $x, y \in \mathbb{N}$ são tais que $a \mid b$ e $a \mid c$, então $a \mid (x \cdot b + y \cdot c)$, e se $x \cdot b \geq y \cdot c$, então $a \mid (x \cdot b - y \cdot c)$.*

Demonstração: Como $a \mid b$ e $a \mid c$, então existem $f, g \in \mathbb{N}$ tais que $b = a \cdot f$ e $c = a \cdot g$. Logo $x \cdot b = x \cdot (a \cdot f)$ e $y \cdot c = y \cdot (a \cdot g)$ se então $x \cdot b \pm y \cdot c = x \cdot (a \cdot f) \pm y \cdot (a \cdot g) = a \cdot (x \cdot f) \pm a \cdot (y \cdot g) = a \cdot (x \cdot f \pm y \cdot g)$ logo, $a \mid (x \cdot f \pm y \cdot g)$, pois $x \cdot f \pm y \cdot g \in \mathbb{N}$. ■

Proposição 1.6. *Sejam $a, b \in \mathbb{N}^*$, temos que se $a \mid b$, então $a \leq b$.*

Demonstração: De fato, se $a \mid b$, existe $c \in \mathbb{N}^*$ tal que, se $b = a \cdot c$ então $a \leq b$, pois $c \geq 1$. Em particular, se $a \mid 1$, então $a \leq 1$ e, segue-se que $a = 1$. ■

Observação 1.1. A relação de divisibilidade em $\mathbb{N}^*$ é uma relação de ordem, pois:

i) É reflexiva: Para todo $a \in \mathbb{N}^*$, $a \mid a$. Proposição 1.1.

ii) É transitiva: Se $a \mid b$ e $b \mid c$, então $a \mid c$. Proposição 1.1.

iii) É antissimétrica: Se $a \mid b$ e $b \mid a$, então $a = b$. Proposição 1.6.
De fato, se $a \mid b$, então $a \leq b$ e se $b \mid a$, então $b \leq a$. Logo, $a = b$.

Definição 1.2. Seja S um subconjunto de $\mathbb{N}$, dizemos que um número natural a é um menor elemento de S se possuir as seguintes propriedades:

i) $a \in S$,

ii) Para todo $n \in S$, $a \leq n$.

Observação 1.2. Este menor elemento se existe, é único e será denotado por $\min S$. De fato, se a e a' são os menores elementos de S, então $a \leq a'$ e $a' \leq a$ nos leva a que $a = a'$. (Propriedade antissimétrica da relação de ordem).

Proposição 1.7 (Propriedade da Boa Ordem)**.** *Todo subconjunto não vazio de* $\mathbb{N}$ *possui um menor elemento.*

Demonstração: A demostração será feita por redução ao absurdo.
Seja S um subconjunto não vazio de $\mathbb{N}$ e suponha, por absurdo, que S não possui um menor elemento. Queremos mostrar que S é vázio, conduzindo a uma contradição.
Considere o conjunto T, complementar de S em $\mathbb{N}$. Queremos, portanto, mostrar que $T = \mathbb{N}$.
Defina o conjunto

$$I_n = \{k \in \mathbb{N}; k \leq n\},$$

e considere a sentença aberta

$$p(n) : I_n \subset T.$$

Como $0 \leq n$ para todo n, segue-se que $0 \in T$, pois, caso contrário, 0 seria um menor elemento de S. Logo, $p(0)$ é verdade.
Suponha agora que $p(n)$ seja verdade. se $n+1 \in S$, como nenhum elemento de I_n está em S, teríamos que $n+1$ é um menor elemento de S, o que não é permitido. Logo, $n+1 \in T$, seguindo daí que

$$I_{n+1} = I_n \cup \{n+1\} \subset T,$$

o que prova que $\forall\, n, I_n \subset T$; protanto, $\mathbb{N} \subset T \subset \mathbb{N}$ e, consequentemente, $T = \mathbb{N}$. ■

Teorema 1.1. *Sejam* a *e* b *dois números naturais com* $0 < a < b$*. Existem dois únicos números naturais* q *e* r *tais que* $b = a \cdot q + r$*, com* $r < a$*.*

Demonstração: Suponha que $b > a$ e considere enquanto fizer sentido, os números $b, b-a, b-2a, \ldots, b-n\cdot a, \ldots$. Pela propriedade da boa ordem, o conjunto S formado pelos elementos acima tem um menor elemento $r = b - q \cdot a$. Vamos provar que $r < a$. Se $a \mid b$, então $r = 0$ e nada mais temos a provar.

Se $a \nmid b$, então $r \neq 0$, e portanto, basta mostrar que não pode ocorrer $r > a$. De fato, se isso ocorresse, existiria um número natural $c < r$ tal que $r = c + a$. Como $r = b - q \cdot a$, temos, $c + a = b - q \cdot a$ logo $c = b - q \cdot a - a = b - (q+1) \cdot a \in S$ com $c < r$, contradizendo o fato de ser r é o menor elemento de S. Portanto $b = a \cdot q + r$ com $r < a$, provando a existência de q e r.
Provemos a unicidade de q e r.
Dados dois elementos distintos de S, a diferença entre o maior e o menor desses elementos, sendo um múltiplo de a, é pelo menos a. Logo, se $r = b - a \cdot q$ e $r' = b - a \cdot q'$ com $r < r' < a$, teríamos $r' - r = b - a \cdot q' - (b - a \cdot q) = b - a \cdot q' - b + a \cdot q = a(q - q')$. Portanto $a \mid r' - r$ logo $a \leq r' - r$ implicando que $r' \geq a + r \geq a$ (absurdo). Logo $r' = r$. Como $r' = r$ segue que $b - a \cdot q = b - a \cdot q' \Rightarrow -a \cdot q = -a \cdot q' \Rightarrow a \cdot q = a \cdot q' \Rightarrow q = q'$. ■

Nas condições do teorema acima, os números q e r são chamados, respectivamente, de *quociente e de resto da divisão de b por a.*

Corolário 1.1. *Dados dois números naturais a e b com* $1 < a \leq b$*, existe um número natural n tal que*

$$na \leq b < (n+1)a.$$

Demonstração: Pela divisão euclidiana, temos que existem $q, r \in \mathbb{N}$ com $r < a$, univocamente determinados, tais que $b = a \cdot q + r$. Basta agora tomar $n = q$ ■

Exemplo 1.1. Vamos mostrar aqui que o resto da divisão de 10^n por 9 é sempre 1, qualquer que seja o número natural n.
Isto será feito por indução. Para $n = 0$, temos $10^0 = 9 \cdot 0 + 1$; portanto, o resultado vale.
Suponha, agora, o resultado válido para um dado n, isto é $10^n = 9 \cdot q + 1$. Considere a igualdade

$$10^{n+1} = 10 \cdot 10^n = (9+1)10^n = 9 \cdot 10^n + 10^n = 9 \cdot 10^n + 9 \cdot q + 1 = 9(10^n + q) + 1,$$

provando que o resultado vale para $n + 1$ e, consequentemente, vale para todo $n \in \mathbb{N}$.

Exemplo 1.2. Dado um número natural $n \in \mathbb{N}^*$ qualquer, temos duas possibilidades:

i) O resto da divisão de n por 2 é 0, isto é, existe $q \in \mathbb{N}$ tal que $n = 2 \cdot q$; ou

ii) O resto da divisão de n por 2 é 1, isto é, existe $q \in \mathbb{N}$ tal que $n = 2 \cdot q + 1$.

Portanto, os números naturais se dividem em duas classes, a dos números da forma $2q$ para algum $q \in \mathbb{N}$, chamamos de *números pares*, e a dos números da forma $2q + 1$,

chamados de *números ímpares*. Os naturais são classificados em pares e ímpares, pelo menos, desde Pitágoras, 500 anos antes de Cristo.

Exemplo 1.3. Mais geralmente, fixado um número natural $m \geq 2$, pode-se sempre escrever um número qualquer n, de modo único, na forma $n = mk + r$, onde $k, r \in \mathbb{N}$ e $r < m$.

Exemplo 1.4. Dados $a, n \in \mathbb{N}^*$, com $a > 2$ e ímpar, determinar a paridade de $\dfrac{a^n - 1}{2}$.
Como a é ímpar, a^n é impar e $a^n - 1$ é par, e, portanto $\dfrac{a^n - 1}{2}$ é um número natural, portanto é legítimo determinar sua paridade.
Observe que

$$\frac{a^n - 1}{2} = \frac{a - 1}{2} \cdot (a^n - 1 + \ldots + a + 1)$$

Sendo a ímpar, temos que $a^n - 1 + \ldots + a + 1$ é par ou ímpar, segundo n seja par ou ímpar. Portanto, basta verificar a paridade de $\dfrac{a - 1}{2}$.
Sendo a ímpar, ele é da forma $4k + 1$ ou $4k + 3$. Se $a = 4k + 1$, então

$$\frac{a - 1}{2} = \frac{4k + 1 - 1}{2} = \frac{4k}{2} = 2k$$

é par. Enquanto que

$$\frac{a - 1}{2} = \frac{4k + 3 - 1}{2} = \frac{4k + 2}{2} = 2k + 1$$

é ímpar. Portanto, $\dfrac{a^n - 1}{2}$ é par se, e somente se, n é par ou a é da forma $4k + 1$.

1.2 Números primos

Definição 1.3. Um número natural maior do que 1 e que só é divisível por 1 e por si próprio é chamado de *número primo*.

Observação 1.3. Dados dois números primos p e q e um número natural a qualquer, observam-se os seguintes casos:

i) Se $p \mid q$, então $p = q$. De fato, como $p \mid q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Sendo p primo, tem-se que, se $p > 1$ então $p = q$.

ii) Se $p \mid a$, então M.D.C$(p, a) = (p, a) = 1$. De fato, se $(p, a) = d$, temos que $d \mid p$ e $d \mid a$, portanto $d = p$ ou $d = 1$. Mas $d \neq p$, pois $p \nmid a$ e, consequentemente, $d = 1$.

Definição 1.4. Chama-se *número composto* a todo número maior do que 1 e que não é primo. Portanto, se um número n é *composto*, existirá um divisor n_1 de n tal que

$n_1 \neq 1$ e $n_1 \neq n$. Assim, existirá um número natural n_2 tal que $n = n_1 \cdot n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$.

Observação 1.4. Sob o ponto de vista da estrutura multiplicativa dos números naturais, os números primos são os mais simples e ao mesmo tempo são suficientes para gerar todos os números naturais, conforme veremos no Teorema Fundamental da Aritmética.

Proposição 1.8. *Sejam* $a, b, p \in \mathrm{N}^*$*, com* p *primo. Se* $p \mid a \cdot b$*, então* $p \mid a$ *ou* $p \mid b$*.*

Demonstração: Basta provar que, se $p \mid a \cdot b$ e $p \nmid a$, então $p \mid b$. Mas se $p \nmid a$, temos que $(p, a) = 1$ e, temos $p \mid a \cdot b$ e $(p, a) = 1$ nos leva a $p \mid b$. (Propriedade do M.D.C.) ■

Axioma de Indução

Seja S um subconjunto de $\mathbb{N}$ tal que

i) $0 \in S$

ii) S é fechado com relação à operação de somar 1 a seus elementos, ou seja, para todo $n \in S$ implica $n + 1 \in S$. Então, $S = \mathbb{N}$.
Se $A \subset \mathbb{N}$ e $a \in \mathbb{N}$, $a + A = \{a + x\,;\, x \in A\}$ e $a + \mathbb{N} = \{m \in \mathbb{N}\,;\, m \geq a\}$.

Proposição 1.9 (Princípio de indução matemática 1ª forma)**.** *Seja* $a \in \mathbb{N}$ *e seja* $p(n)$ *uma sentença aberta em* n*. Suponha que*

i) $p(a)$ *é verdadeira, e que*

ii) Para todo $n \geq a$*,* $p(n)$ *implica* $p(n+1)$ *é verdade, então* $p(n)$ *é verdade para todo* $n \geq a$*.*

Demonstração: Seja $V = \{n \in \mathbb{N}\,;\, p(u)\}$, isto é, V é um subconjunto dos naturais para os quais $p(n)$ é verdade.
Considere o conjunto $S = \{m \in \mathbb{N}\,;\, a + m \in V\}$, que trivialmente nos leva $a + S \subset V$.
Como pela condição (i), temos que $a + 0 = a \in V$, segue-se que $0 \in S$.
Por outro lado, se $m \in S$, então $a + m \in V$ e por (ii), temos que $a + m + 1 \in V$, logo $m + 1 \in S$. Assim, pelo axioma de indução, temos $S = \mathbb{N}$. Portanto, $\{m \in \mathbb{N}\,;\, m \geq a\} = a + \mathbb{N} \subset V$ o que prova o resultado. ■

Proposição 1.10 (Princípio de indução matemática 2ª forma)**.** *Seja* $p(n)$ *uma setença aberta tal que*

i) $p(a)$ *é verdade, e que*

ii) Para todo n, $p(a)$ *e* $p(a+1)$ *e* ... $p(n)$ *implica* $p(n+1)$ *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 vázio.
Suponha, por absurdo, que vale o contrário. Logo, pela propriedade da boa ordem, W teria um menor elemento k, e, como sabemos de (i) que $a \notin W$, segue-se que existem tal que $k = a + n > a$. Portanto, $a, a+1, \ldots, k-1 \notin W$; Logo $a, a+1, \ldots, k-1 \notin V$. Por (ii) conclui-se que $k = k - 1 + 1 \in V$, o que contradiz o fato de $k \in W$. ■

Corolário 1.2. *Se* $p, p_1, p_2, \ldots, p_n$ *são números primos e, se* $p \mid p_1 \cdot p_2 \cdot \ldots \cdot p_n$, *então* $p = p_i$, *para algum* $i = 1, 2, \ldots, n$.

Demonstração: Usando a indução sobre n.
Para $n = 1$, $p = p_1$ ok!
Para $n = 2$, sejam p, p_1 e p_2 tais que $(p_1, p) = 1$, $(p_2, p) = 1$.
Se $p \mid p_1 p_2$, pela Proposição 1.8, $p \mid p_1$ ou $p \mid p_2$, mas p é primo. Logo $p = p_1$ ou $p = p_2$ para $i = 1, 2$.
Agora $n = k$, pela hipótese de indução, temos, se $p \mid p_1 p_2 \ldots p_k$, então $p = p_i$ para $i = 1, 2, \ldots, k$, pois eles são primos.
Para $n = k + 1$, considere os números primos $p, p_1, p_2, \ldots, p_k, p_{k+1}$. Se $p \mid p_1, p_2, \ldots, p_k, p_{k+1}$, então $p \mid p_1, p_2, \ldots, p_k$ ou $p \mid p_{k+1}$, pela Proposição 1.8, $p = p_i$, $i = 1, 2, \ldots, k$ ou $p = p_k + 1$. ■

Teorema 1.2 (Teorema Fundamental da Aritmética)**.** *Todo número natural maior do que* 1 *ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como produto de números primos.*

Demonstração: Usaremos a segunda forma do Princípio de Indução. Se $n = 2$, o resultado é obviamente verificado.
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 $p_1 p_2 \cdots p_r$ e $q_1 q_2 \cdots q_s$ tais que $n_1 = p_1 p_2 \cdots p_r$ e $n_2 = q_1 q_2 \cdots q_s$. Portanto, $n = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$.
Vamos, agora, provar a unicidade da escrita. Suponha, agora, que $n = p_1 \cdot p_r = q_1 \cdots q_s$, onde os p_i e os p_j são números primos . Como $p_1 \mid q_1 q_2 \cdots q_s$ Pelo Corolário 1.2, temos que $p_1 = p_j$ para algum j, que após reordenamento de $q_1 q_2 \cdots q_s$, podemos supor que seja q_1. Portanto,

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

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

Proposição 1.11. *Seja* $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ *um número natural. Se* n' *é um divisor de* n*, então*

$$n' = p_1^{\beta_1} \cdots p_r^{\beta_r},$$

onde $0 \leq \beta_i \leq \alpha_i$*, para* $i = 1, \ldots, r$*.*

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

Denotando por $d(n)$ o número de divisores do número natural n, segue, por uma contagem fácil, que se $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, onde $p_1, \ldots, p_r$ são números primos e $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$, então

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1).$$

Exemplo 1.5. A fórmula acima nos mostra que um número $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ possui uma quantidade ímpar de divisores se, e somente se, cada α_i é par, ou seja, se, e somente se, n é um quadrado perfeito.

Exemplo 1.6. Seja $n > 4$ um número natural composto; vamos provar que $n \mid (n-2)!$. Provaremos inicialmente que $n \mid (n-1)!$. De fato, seja $n = n_1 n_2$ com $n_1 < n$ e $n_2 < n$. Se $n_1 \neq n_2$, podemos supor que $n_1 < n_2$, e portanto,

$$(n-1)! = 1 \cdots n_1 \cdots n_2 \cdots (n-1),$$

o que mostra que $n \mid (n-1)!$, neste caso.
Suponhamos que $n_1 = n_2 > 2$. Logo, $n = n_1^2 > 2n_1$; então

$$(n-1)! = 1 \cdots n_1 \cdots 2n_1 \cdots (n-1),$$

o que implica que $n = n_1^2$ divide $(n-1)!$.
Agora, note que $(n, n-1) = 1$ e que $n \mid (n-2)!(n-1)$; portanto, $n \mid (n-p)!$
De fato, temos que $(n-1, n) = 1$ e que $n \mid (n-2)!(n-1)$; Portanto, $n \mid (n-2)!$

Observação 1.5. A propriedade acima pode ser generalizada como segue:

Sejam $n > 4$ composto e o p o menor número primo que divide n então $n \mid (n-p)!$. De fato, temos que $(n-1, n) = 1, \ldots, (n-2, n) = 1, \ldots, (n-(p-1), n) = 1$. Logo, segue que $((n-1)(n-2)\cdots(n-p+1), n) = 1$, o que, em vista de $n \mid (n-1)!$, o que acarreta $n \mid (n-p)!$.

1.2.1 Sobre a distribuição dos números primos

Quantos serão os números primos? Essa pergunta foi respondida por Euclides no Livro IX dos Elementos. Utilizaremos a mesma prova dada por Euclides, onde pela primeira vez se registra o uso de uma demonstração por redução ao absurdo em matemática. Essa prova é considerada uma das pérolas da matemática.

Teorema 1.3. *Existem infinitos números primos.*

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

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

Pelo Teorema 1.2, o número n possui um fator primo p que, portanto, deve ser um dos $p_1, \ldots, p_r$ e, consequentemente, divide o produto $p_1 p_2 \cdots p_r$. Mas isto implica que p divide $n = p_1 p_2 \cdots p_r + 1$ e consequentemente p divide 1, o que é absurdo. Logo, existem infinitos números primos. ■

Agora que sabemos que existem infinitos números primos, nos perguntamos, inicialmente, como podemos obter uma lista contendo os números primos até uma dada ordem. A seguir, apresentaremos um dos mais antigos métodos para elaborar tabelas de números primos o chamado *Crivo de Eratósteles*, devido ao matemático grego Eratóstenes, que viveu por volta de 230 anos antes de Cristo; permite determinar todos os números primos até a ordem que se desejar, mas não é muito eficiente para ordens muito elevadas.

Por exemplo, vamos elaborar a tabela de todos os números primos inferiores a 120.

Escrevem-se todos os números naturais de 2 a 120. Riscam-se, de modo sistemático, todos os números compostos da tabela, seguindo o roteiro abaixo.

Risque todos os múltiplos de 2 acima de 2, já que nenhum deles é primo.

O segundo número não riscado é 3, que é primo. Risque todos os múltiplos de 3 maiores do que 3 pois esses não são primos.

O terceiro número não riscado que aparece é 5, que é primo. Risque todos os múltiplos de 5 maiores do que 5 pois esses não são primos.

O quarto número não riscado que ora aparece é 7, que é primo. Risque todos os múltiplos de 7 maiores do que 7 pois esses não são primos.

Será necessário prosseguir com este procedimento até chegar a 120? A resposta é não e se baseia no seguinte resultado devido ao próprio Eratóstenes.

Lema 1.1. *Se um número natural $n > 1$ não é divisível por nenhum número primo p tal que $p^2 \leq n$, então ele é primo.*

Demonstração: Suponhamos, por absurdo, que n não seja divisível por nenhum número primo p tal que $p^2 \leq n$ e que não seja primo. Seja q o menor número primo que divide n; então, $n = qn_1$, com $q \leq n_1$. Segue daí que $q^2 \leq qn_1 = n$. Logo, n é divisível por um número primo q tal que $q^2 \leq n$, absurdo. ■

Portanto, na tabela de números de 2 a 120, devemos ir até alcançarmos o primo 7, pois o próximo primo é 11, cujo quadrado supera 120.

	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~~	101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~
109	~~110~~	~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~

Note que o Lema 1.1 também nos fornece um teste de primalidade, pois, para verificar se um dado número n é primo, basta verificar que não é divisível por nenhum primo p que não supere $\sqrt{n}$.

Tanto o Crivo de Eratóstenes para gerar números primos, quanto o teste de primalidade acima descrito, são extremamente lentos e trabalhosos. Muitos progressos têm sido feitos nessa direção.

Uma questão importante que se coloca é de como os números primos se distribuem dentro dos números naturais. Em particular, qual pode ser a distância entre dois primos consecutivos? Qual é a sua frequência?

Olhando para tabela acima , nota-se que há vários pares de números primos que diferem de duas unidades. Esses são: (3,5), (5,7), (11,13), (17,19), (41,43), (59,61), (71,73), (101, 103), (107, 109).

Pares de números primos com esta propriedade são chamados de *primos gêmeos*. Até o presente momento, ainda não se sabe se existem infinitos pares de números primos gêmeos.

Por outro lado, em contraste com esses pares de primos consecutivos muito próximos, existem primos consecutivos arbitrariamente afastados.

De fato, dado n, a sequência

$$(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + n + 1$$

de números naturais é formada por n números consecutivos compostos.

Portanto, a resposta à primeira pergunta é que não há nenhum padrão que descreva o quanto dois primos consecutivos estão longe um do outro.

Quanto à segunda pergunta, é necessário formalizar o conceito de frequência de primos, que é a mesma coisa que probabilidade. Denotaremos, por $\pi(x)$, a quantidade de números primos menores ou iguais a x. Portanto, a probabilidade de que um elemento do conjunto $\{1, \ldots, x\}$ seja primo é dada por

$$\frac{\pi(x)}{x}.$$

Como este quociente é uma função bastante complexa, o que se gostaria de fazer é achar uma função de comportamento bem conhecido que se aproxima do quociente acima para n suficientemente grande.

Legendre e Gauss, analisando tabelas, chegaram à conclusão de que este quociente tem a ver com $\frac{1}{\ln x}$. Por volta de 1900, J. Hadamard e Ch. de la Valleè- Poussin, independentemente, provaram o profundo resultado chamado de *Teorema dos Números Primos* e cujo enunciado simplesmente é

$$\lim_{x\to\infty} \frac{\pi(x)}{x} \left(\frac{1}{\ln x}\right)^{-1} = 1.$$

Em 1949, A. Selberg simplificou substancialmente a prova do Teorema dos Números Primos, merecendo por esse seu trabalho a Medalha Fields.

A distribuição dos números primos é algo ainda bastante misterioso e a ela estão associados muitos problemas em aberto. Por exemplo, o já citado problema de saber se existem infinitos números primos gêmeos.

1.3 Maior divisor comum

Dados dois números naturais a e b, não simultaneamente nulos, diremos que o número natural $d \in \mathbb{N}^*$ é um *divisor comum* de a e b se $d \mid a$ e $d \mid b$.

Por exemplo, os números $1, 2, 3$ e 6 são os divisores comuns de 12 e 18.

A definição que se segue é exatamente a definição dada por Euclides nos *Elementos* e se constitui em um dos pilares da sua aritmética.

Diremos que d é um *máximo divisor comum* (mdc) de a e b se possuir as seguintes propriedades:

i) d é um divisor comum de a e de b, e

ii) d é divisível por todo divisor comum de a e b.

A condição (ii) acima pode ser reenunciada como se segue:

ii') Se c é um divisor comum de a e b, então $c \mid d$.

Portanto, se d é um mdc de a e b e c é um divisor comum desses números, então $c \leq d$. Isto nos mostra que o máximo divisor comum de dois números é efetivamente o maior dentre todos os divisores comuns desses números.

Em particular, isto nos mostra que, se d e d' são dois mdc de um mesmo par de números, então $d \leq d'$ e $d' \leq d$, e, consequentemente, $d = d'$. Ou seja, o mdc de dois números, quando existe, é único.

O mdc de a e b, quando existe (veremos mais adiante que sempre existe o mdc de dois números naturais não simultaneamente nulos), está sendo denotado por (a, b). Como o mdc de a e b não depende da ordem em que a e b são tomados, temos que

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

Em alguns casos particulares, é facil verificar a existência do mdc. Por exemplo, se a e b são números naturais, tem-se claramente que $(0, a) = a$. $(1, a) = 1$ e que $(a, a) = a$. Mais ainda, temos que

$$a \mid b \Longleftrightarrow (a, b) = a. \tag{1.1}$$

De fato, se $a \mid b$, temos que a é um divisor comum de a e b, e, se c é um divisor comum de a e b, então c divide a, o que mostra que $a = (a, b)$.

Reciprocamente, se $(a, b) = a$, segue-se que $a \mid b$.

A demonstração da existência do mdc de qualquer par de números naturais, não ambos nulos, é bem mais sutil. Poder-se-ia, como se faz usualmente no Ensino Fundamental, definir o máximo divisor comum de dois números a e b como sendo o maior elemento do conjunto de todos divisores comuns desses números, o que de imediato garantia a sua existência. De qualquer modo, seria necessário provar a propriedade (ii) da definição de mdc; pois é ela que possibilita provar os resultados subsequentes, e não o fato do mdc ser o resultado abaixo.

Lema 1.2 (Lema de Euclides)**.** *Sejam* $a, b, n \in \mathbb{N}$ *com* $a < na < b$. *Se existe* $(a, b-na)$, *então* (a, b) *existe, e*

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

Demonstração: Seja $d = (a, b - na)$. Como $d \mid a$ e $d \mid (b - na)$, segue que d divide $b = b - na + na$. Logo, d é um divisor comum de a e b. Suponha agora que c seja um

divisor comum de a e b; logo, c é um divisor comum de a e $b - na$ e, portanto, $c \mid d$. Isso prova que $d = (a, b)$. ■

Observação 1.6. Com a mesma técnica usada na prova do Lema de Euclides, poder-se-ia provar que, para todos a, b, $n \in \mathbb{N}$,

$$(a, b) = (a, b + na),$$

ou que, se $na > b$, então

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

O Lema de Euclides é efetivo para calcular mdc, conforme veremos nos exemplos a seguir, e será fundamental para estabelecermos o algoritmo de Euclides, que permitirá, com muita eficiência, calcular o mdc de dois números naturais quaisquer.

Exemplo 1.7. Dados $a, m \in \mathbb{N}$ com $a > 1$, temos que

$$\left(\frac{a^m - 1}{a - 1}, a - 1\right) = (a - 1, m).$$

De fato, chamado de d o primeiro membro da igualdade, temos que

$$d = (a^{m-1} + a^{m-2} + \ldots + a + 1, a - 1) = ((a^{m-1} - 1) + (a^{m-2} - 1) + \ldots + (a - 1) + m, a - 1).$$

Como,

$$a - 1 \mid (a^{m-1} - 1) + (a^{m-2} - 1) + \ldots + (a - 1)$$

segue-se que $(a^{m-1} - 1) + (a^{m-2} - 1) + \ldots + (a - 1) = n(a - 1)$ para algum $n \in \mathbb{N}$, e, portanto, pela Observação 1.6, tem-se que

$$d = (n(a - 1) + m, a - 1) = (a - 1, n(a - 1) + m) = (a - 1, m).$$

Exemplo 1.8. Vamos, neste exemplo, determinar os valores de a e n para os quais $a + 1$ divide $a^{2n} + 1$.

Note inicialmente que

$$a + 1 \mid a^{2n} + 1 \iff (a + 1, a^{2n} + 1) = a + 1.$$

Como $a^{2n} + 1 = (a^{2n} - 1) + 2$, e, segue-se, pela Observação 1.6, que para todo n,

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

Portanto, $a+1 \mid a^{2n}+1$, para algum $n \in \mathbb{N}$, se, e somente se, $a+1 = (a+1, 2)$, o que ocorre se, e somente se, $a = 0$ ou $a = 1$.

Exemplo 1.9. Vamos, neste exemplo, determinar os valores de a e n para os quais $a+1$ divide $a^{2n+1}-1$.
Note que

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

Portanto, $a+1 \mid a^{2n+1}-1$, para algum $n \in \mathbb{N}$, se, e somente se,

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

o que ocorre se, e somente se, $a = 1$.

Algoritmo de Euclides

A seguir, apresentaremos a prova construtiva da existência do mdc dada por Euclides (Os Elementos, Livro VII, Proposição 2). O método, chamado de *Algoritmo de Euclides*, é um primor do ponto de vista computacional e pouco conseguiu-se aperfeiçoá-lo em mais de dois milênios.

Dados $a, b \in \mathbb{N}$, podemos supor $a \leq b$. Se $a = 1$ ou $a = b$, ou ainda $a \mid b$, já vimos que $(a, b) = a$. Suponhamos, então, que $1 < a < b$ e que a $a \nmid b$. Logo, pela divisão euclidiana, podemos escrever

$$b = aq_1 + r_1, \quad \text{com } r_1 < a.$$

Temos duas possibilidades:

a) $r_1 \mid a$, e, em tal caso, por (1.1) e pelo Lema 1.2,

$$r_1 = (a, r_1) = (a, b - q_1 a) = (a, b),$$

e termina o algoritmo, ou

b) $r_1 \nmid a$, e, em tal caso, podemos efetuar a divisão de a por r_1, obtendo

$$a = r_1 q_2 + r_2, \quad \text{com } r_2 < r_1.$$

Novamente, temos duas possibilidades:

a') $r_2 \mid r_1$, e, em tal caso, novamente, por (1.1) e pelo Lema 1.2,

$$r_2 = (r_1, r_2) = (r_1, a - q_2 r_1) = (r_1, a) = (b - q_1 a, a) = (b, a) = (a, b),$$

e paramos, pois termina o algoritmo, ou

b') $r_2 \nmid r_1$, e, em tal caso, podemos efetuar a divisão de r_1 por r_2, obtendo

$$r_1 = r_2 q_3 + r_3, \quad \text{com } r_3 < r_2.$$

Este procedimento não pode continuar indefinidamente, pois teríamos uma sequência de números naturais $a > r_1 > r_2 > \ldots$ que não possui menor elemento, o que não é possível pela Propriedade da Boa Ordem. Logo, para algum n, temos que $r_n \mid r_{n-1}$, o que implica que $(a, b) = r_n$.

O algoritmo acima pode ser sistematizado e realizado na prática, como mostramos a seguir.

Inicialmente, efetuamos a divisão $b = aq_1 + r_1$ e colocamos os números envolvidos no seguinte diagrama:

	q_1	
b	a	
r_1		

A seguir, continuamos efetuando a divisão $a = r_1 q_2 + r_2$ e colocamos os números envolvidos no diagrama

	q_1	q_2	
b	a	r_1	
r_1	r_2		

Prosseguindo, enquanto for possível, teremos

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

Exemplo 1.10. Calculemos o mdc de 372 e 162:

	2	3	2	1	2
372	162	48	18	12	6
48	18	12	6		

Observe que, no exemplo acima, o Algoritmo de Euclides nos fornece:
$6 = 18 - 1 \cdot 12$
$12 = 48 - 2 \cdot 18$
$18 = 162 - 3 \cdot 48$
$48 = 372 - 4 \cdot 162$
Donde se segue que $6 = 18 - 1 \cdot 12 = 18 - 1 \cdot (48 - 2 \cdot 18) = 3 \cdot 18 - 48 = 3 \cdot (162 - 3 \cdot 48) - 48 = 3 \cdot 162 - 10 \cdot 48 = 3 \cdot 162 - 10 \cdot (372 - 2 \cdot 162) = 23 \cdot 162 - 10 \cdot 372$.
Temos, então, que

$$(372, 162) = 6 = 23 \cdot 162 - 10 \cdot 372.$$

Note que conseguimos, através do uso do Algoritmo de Euclides, de trás para frente, escrever $6 = (372, 162)$ como múltiplo de 162 menos um múltiplo de 372.

O Algoritmo de Euclides nos fornece, portanto, um meio prático de escrever o mdc de dois números como diferença entre os dois números em questão. Esta é uma propriedade geral do mdc que redemonstraremos com todo rigor na próxima subseção.

1.3.1 Propriedades do mdc

Sejam $a, b \in \mathbb{N}^*$, definimos o conjunto $J(a, b)$ como sendo:

$$J(a, b) = \{x \in \mathbb{N}^* \,;\, \exists\, m, n \in \mathbb{N} \,;\, x = m \cdot a - n \cdot b\}.$$

Teorema 1.4. *Sejam $a, b \in \mathbb{N}^*$ e seja $d = \min J(a, b)$. Tem-se que*

i) d é o mdc de a e b

ii) $J(a, b) = \{nd \,;\, n \in \mathbb{N}\}$.

Demonstração:

i) Suponha que c divida a e b. Logo, c divide todos os números naturais da forma $m \cdot a - n \cdot b$; portanto, divide todos os elementos de $J(a, b)$, e, consequentemente $c \mid d$.
Vamos mostrar agora que que d divide todos os elementos de $J(a, b)$. Seja $x \in J(a, b)$ e suponha, por absurdo, que $d \nmid x$. Logo, pela Divisão Euclidiana

$$x = d \cdot q + r, \quad \text{com } 0 < r < d.$$

Como $x = M \cdot a - N \cdot b$ e $d = m \cdot b - n \cdot a$, para alguns $M, N, m, n \in \mathbb{N}$, segue-se

que

$$\begin{aligned} r &= M \cdot a - N \cdot b - (m \cdot a - n \cdot b) \cdot q \\ &= M \cdot a + m \cdot a \cdot q - N \cdot b - n \cdot b \cdot q \\ &= (M + m \cdot q) \cdot a - (N + q \cdot n) \cdot b \in J(a,b) \end{aligned}$$

que é um absurdo, pois $d = \min J(a,b)$ e $r < d$. Em particular, $d \mid a$ e $d \mid b$.

ii) Dado que $ld = l(ma - nb) = (lm)a - (ln)b \in J(a,b)$, é claro que

$$\{ld;\, l \in \mathbb{N}\} \subset J(a,b).$$

Por outro lado, já provamos que todo $x \in J(a,b)$ é tal que $d \mid x$, e, portanto,

$$J(a,b) \subset \{ld;\, l \in \mathbb{N}\}.$$

■

O teorema acima nos dá uma outra demonstração da existência do mdc de dois números. Note que esssa demonstração, ao contrário da prova de Euclides, não é construtiva, no sentido de que não nos fornece nenhum meio prático para achar o mdc dos dois números.

Corolário 1.3. *Quaisquer que sejam* $a, b \in \mathbb{N}^*$, $(na, nb) = n(a,b)$.

Demonstração: Note inicialmente que

$$J(na, nb) = nJ(a,b) = \{nx; x \in J(a,b)\}.$$

Agora, o resultado segue do Teorema 1.4 e do fato de que

$$\min nJ(a,b) = n \min J(a,b).$$

■

Corolário 1.4. *Dados* $a, b \in \mathbb{N}$, *tem-se que*

$$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1.$$

Demonstração: Pelo Corolário 1.3, temos que

$$(a,b)\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=\left((a,b)\frac{a}{(a,b)},(a,b)\frac{b}{(a,b)}\right)=(a,b),$$

o que prova o resultado. ■

Dois números naturais a e b serão ditos *primos entre si*, ou *coprimos*, se $(a,b)=1$; ou seja, se o único divisor comum de ambos é 1.

Proposição 1.12. *Dois números naturais a e b serão primos entre si se, e somente se, existirem números naturais n e m tais que $na-mb=1$.*

Demonstração: Suponha que a e b sejam primos entre si. Logo, $(a,b)=1$. Como, pelo Teorema 1.4, existem números naturais n e m tais que $na-mb=(a,b)=1$, segue-se a primeira parte da proposição.
Reciprocamente, suponha que existam números naturais n e m tais que $ma-mb=1$. Se $d=(a,b)$, temos que $d\mid(na-mb)$, o que mostra que $d\mid 1$. e, protanto, $d=1$ ■

A Proposição 1.12 estabelece uma crucial relação entre as estruturas aditiva e multiplicativa dos números naturais, o que permititá provar, entre vários outros resultados, o importante teorema a seguir.

Teorema 1.5. *Sejam a,b e c números naturais. Se $a\mid b\cdot c$ e $(a,b)=1$, então $a\mid c$.*

Demonstração: Se $a\mid b\cdot c$, então existe $c\in\mathbb{N}$ tal que $bc=ac$.
Se $(a,b)=1$, então, pela Proposição 1.12, temos que existem $m,n\in\mathbb{N}$ tais que

$$na-mb=1.$$

Multiplicando por c ambos os lados da igualdade acima, temos que

$$c=nac-mbc.$$

Substituindo bc por ac nesta última igualdade, temos que

$$c=nac-mac=a(nc-mc)$$

e, portanto, $a\mid c$. ■

Corolário 1.5. *Dados $a\in\mathbb{N}$ e $b,c\in\mathbb{N}^*$, temos que*

$$b\mid a \text{ e } c\mid a\iff\frac{bc}{(b,c)}\mid a.$$

Demonstração: De fato, temos que $a = nb = mc$ para alguns $n, m \in \mathbb{N}$. Logo,

$$n\frac{b}{(b,c)} = m\frac{c}{(b,c)}.$$

Como $\left(\frac{b}{(b,c)}, \frac{c}{(b,c)}\right) = 1$, segue-se $\frac{b}{(b,c)} \mid m$, o que implica que $c\frac{b}{(b,c)} \mid cm$. Como $cm = a$, o resultado se segue. ■

A noção de mdc pode ser generalizada como se segue.

Um número natural d será dito mdc de dados números naturais $a_1, \ldots, a_n$ se possuir as seguintes propriedades:

i) d é um divisor comum de $a_1, \ldots, a_n$.

ii) Se c é um divisor comum de $a_1, \ldots, a_n$, então $c \mid d$.

O mdc, quando existe, é certamente único e será representado por

$$(a_1, \ldots, a_n).$$

Proposição 1.13. *Dados os números naturais* $a_1, \ldots, a_n$, *existe o seu mdc e* $(a_1, \ldots, a_n) = (a_1, \ldots, (a_{n-1}, a_n))$.

Demonstração: Vamos provar a proposição por indução sobre $n(\geq 2)$. Para $n = 2$, sabemos que o resultado é válido. Suponha que o resultado vale para n. Para provar que o resultado é válido para $n + 1$, basta mostrar que

$$(a_1, \ldots, a_n, a_{n+1}) = (a_1, \ldots, (a_n, a_{n+1})),$$

pois isso provará também a existência.
Seja $d = (a_1, \ldots, (a_n, a_{n+1}))$. Logo, $d \mid a_1, \ldots, d \mid a_{n-1}$ e $d \mid (a_n, a_{n+1})$. Portanto, $d \mid a_1, \ldots, d \mid a_{n-1}, d \mid a_n$ e $d \mid a_{n+1}$.
Por outro lado, seja c um divisor comum de $a_1, \ldots, a_n, a_{n+1}$; logo, c é um divisor comum de $a_1, \ldots, a_{n-1}$ e (a_n, a_{n+1}); e, portanto, $c \mid d$. ■

Para calcular o número $(a_1, \ldots, a_n)$, pode-se usar recursivamente o Algoritimo de Euclides.

1.4 Congruências

1.4.1 Aritmética dos restos

Definição 1.5. Seja m um número natural diferente de zero. Dizemos que dois números naturais a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Neste caso, usamos a notação $a \equiv b \bmod m$.

Observação 1.7. Quando a e b não são congruentes, escrevemos $a \not\equiv b \bmod m$. Como o resto da divisão de um número natural qualquer por 1 é sempre nulo, temos que $a \equiv b \bmod 1$, quaisquer que sejam a e $b \in \mathbb{N}$. Portanto consideremos sempre $m > 1$.

Proposição 1.14. *Suponha que $a, b \in \mathbb{N}$ são tais que $b \geq a$, então $a \equiv b \bmod m$ se, e somente se, $m \mid (b - a)$.*

Demonstração: Sejam $a = m \cdot q + r$, com $r < m$ e $b = m \cdot q + r'$, com $r' < m$, as divisões euclidianas de a e b por m, respectivamente. Logo

$$b - a = \begin{cases} m(q' - q) + r' - r, & \text{se } r' \geq r \\ m(q' - q) - (r - r'), & \text{se } r \geq r' \end{cases}$$

onde $r' - r < m$ ou $r - r' < m$.
Portanto, $a \equiv b \bmod m$ se, e somente se, $r = r'$. O que é equivalente a dizer que $m \mid (b - a)$. ∎

Proposição 1.15. *A congruência é uma relação de equivalência.*
Seja $m \in \mathbb{N}$, $m > 1$. Para todos $a, b, c \in \mathbb{N}$, temos que:

i) $a \equiv a \bmod m$ (reflexidade);

ii) Se $a \equiv b \bmod m$, então $b \equiv a \bmod m$ (simetria);

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

Demonstração:

i) De fato, basta tomar $b = a$ em $a \equiv b \bmod m$.

ii) Se $a \equiv b \bmod m$, então existem q_1, q_2, r tais que $a = m \cdot q_1 + r$ e $b = m \cdot q_2 + r$. Logo $a - b = m \cdot q_1 + r - (m \cdot q_2 + r) = m \cdot q_1 - m \cdot q_2$. Multiplicando por -1, temos $b - a = m \cdot (q_2 - q_1)$, que é equivalente $b \equiv a \bmod m$.

iii) Se $a \equiv b \bmod m$, então existem q_1, q_2, r tais que $a = m \cdot q_1 + r$ e $b = m \cdot q_2 + r$. Se $b \equiv c \bmod m$, então existem q_2, q_3, r tais que $b = m \cdot q_2 + r$ e $c = m \cdot q_3 + r$. Daí,

$$\begin{cases} a - b = m \cdot q_1 - m \cdot q_2 \\ b - c = m \cdot q_2 - m \cdot m \cdot q_3 \end{cases}$$

Consequentemente,
$a - c = m \cdot q_1 - m \cdot q_3 = m(q_1 - q_3)$ e então $a = c \bmod m$.

■

Proposição 1.16. *Sejam* $a, b, c, d, m \in \mathbb{N}$, *com* $m > 1$.

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

ii) Se $a \equiv b \bmod m$ *e* $c \equiv d \bmod m$, *então* $(a \cdot c) \equiv (b \cdot d) \bmod m$.

Demonstração:

i) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, podemos supor sem perda de generalidade, que $b \geq a$ e $d \geq c$. Logo, se $m \mid (b - a)$ e $m \mid (d - c)$ então $m \mid (b - a) + (d - c)$ e, portanto, se $m \mid (b + d) - (a + c)$ então $a + c \equiv (b + d) \bmod m$.

ii) Basta observar que $bd - ac = bd - ad - ac + ad = d \cdot (b - a) + a \cdot (d - c)$. Se $m \mid (b - a)$ e $m \mid (d - c)$ então $m \mid (bd - ac)$. Logo $a \cdot c \equiv b \cdot d \bmod m$.

■

Proposição 1.17. *Sejam* $a, b, c, m \in \mathbb{N}$, *com* $m > 1$. *Tem-se:* $(a + c) \equiv (b + c) \bmod m$ *se, e somente se* $a \equiv b \bmod m$.

Demonstração: Basta observar que

$$\begin{cases} a \equiv b \bmod m \\ c \equiv c \bmod m \end{cases},$$

logo $(a + c) \equiv (b + c) \bmod m$.
Reciprocamente, suponhamos que $(a+c) \equiv (b+c) \bmod m$. Sem perda de generalidade, podemos supor que $b + c \geq a + c$. Então, $m \mid (b + c) - (a + c) \Rightarrow m \mid (b - a)$. Portanto $a \equiv b \bmod m$. ■

Proposição 1.18. *Sejam* $a, b, c, m \in \mathbb{N}$, *com* $c \neq 0$ *e* $m > 1$. *Temos que* $a \cdot c \equiv b \cdot c \bmod m$ *se, e somente se,* $a \equiv b \bmod \dfrac{m}{(c, m)}$.

Demonstração: Podemos supor, sem perda de generalidade, que $bc > ac$. Como $\frac{m}{(c,m)}$ e $\frac{c}{c,m}$ são coprimos, temos que $ac \equiv bc \bmod m$ se, e somente se, $m \mid (b-a)c$ se, e somente, se $\frac{m}{(c,m)} \mid (b-c)\frac{c}{c,m}$ se, e somente se, $\frac{m}{c,m} \mid (b-a)$ se, e somente se, $a \equiv b \bmod \frac{m}{(c,m)}$.
Se $(c,m) = 1$ temos $ac \equiv bc \bmod m$ se, e somente se, $a \equiv b \bmod d$. Pela Proposição anterior. ■

1.5 Pequeno Teorema de Fermat

Desde, pelo menos, 500 anos antes de Cristo, os chineses sabiam que, se p é um número primo, então $p \mid 2^p - 2$. Coube a Pierre de Fermat, no século XVII, generalizar este resultado, enunciando um pequeno mas notável teorema que se constitui no resultado central desta seção.

Para demonstrar o Teorema de Fermat, necessitaremos do lema a seguir.

Lema 1.3. *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, $i! \mid p(p-1)\cdots(p-i+1)$. Como $(i!, p) = 1$, decorre que $i! \mid (p-1)\cdots(p-1+1)$, e o resultado se segue, pois

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

■

Teorema 1.6 (Pequeno Teorema de Fermat)**.** *Dado um número primo p, tem-se que p divide o número $a^p - a$, para todo $a \in \mathbb{N}$.*

Demonstração: Vamos provar o resultado por indução sobre a. O resultado vale claramente para $a = 1$, pois $p \mid 0$.
Supondo o resultado válido para a, iremos prová-lo para $a+1$. Pela fórmula do binômio de Newton,

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

Como, pelo Lema 1.3 e pela hipótese de indução, o segundo membro da igualdade acima é divisível por p, o resultado se segue. ■

Exemplo 1.11. 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.

A afirmação acima é equivalente a $10 \mid n^9 - n$. Como n^9 e n têm a mesma paridade, segue-se $n^9 - n$ é par; isto é, $2 \mid n^9 - n$.
Por outro lado,

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

Logo, pelo Teorema de Fermat, temos que $5 \mid n^5 - n$ e, portanto, $5 \mid n^9 - n$. Tem-se, então, que $10 \mid n^9 - n$.

Corolário 1.6. *Se p é um número primo e se a é um número natural não divisível por p, então p divide $a^{p-1} - 1$.*

Demonstração: Como, pelo Pequeno Teorema de Fermat, $p \mid a(a^{p-1} - 1)$ e como $(a, p) = 1$, segue-se, imediatamente, que p divide $a^{p-1} - 1$. ∎

O Corolário acima também será chamado de Pequeno Teorema de Fermat.

Observação 1.8. No que o Pequeno Teorema de Fermat nos fornece um teste de não primalidade. De fato, dado $m \in \mathbb{N}$, com $m > 1$, se existir algum $a \in \mathbb{N}$, com $(a, m) = 1$, tal que $m \nmid a^{m-1} - 1$, então m não é primo.

Os chineses achavam também que se m era composto, então $m \nmid 2^m - 2$, uma recíproca do Teorema de Fermat, no caso $a = 2$. Muitos matemáticos acreditavam neste resultado, até que, em 1819, Sarrus mostrou que o número $341 (= 31 \times 11)$ divide $2^{341} - 2$.

Poder-se-ia perguntar se vale a recíproca mais restritiva do Pequeno Teorema de Fermat:
Dado um inteiro $m > 1$, a condição $m \mid a^m - 1$ para todo $a \in \mathbb{N}$ tal que $(a, m) = 1$. acarreta, necessariamente, que m é primo?

Veremos, no próximo exemplo, que isto também é falso.

Exemplo 1.12. Seja $a \in \mathbb{N}$ tal que $(a, 3) = (a, 11) = (a, 17) = 1$. Note que essa condição é equivalente a $(a, 561) = 1$, pois $3 \cdot 11 \cdot 17 = 561$.
Por outro lado,

$$(a^{280}, 3) = (a^{56}, 11) = (a^{35}, 17) = 1,$$

e, portanto, pelo Pequeno Teorema de Fermat, 3 divide $(a^{280})^2 - 1 = a^{560} - 1$, 11 divide $(a^{56})^{10} - 1 = a^{560} - 1$ e 17 divide $(a^{35})^{16} - 1 = a^{560} - 1$.
Segue-se daí que 561 divide $a^{560} - 1$, para todo a tal que $(a, 561) = 1$, sem que 561 seja primo.

Exemplo 1.13. O Pequeno Teorema de Fermat nos diz que

$$47 \mid 2^{46} - 1.$$

Logo, temos que

$$47 \mid (2^{23} - 1)(2^{23} + 1),$$

e como

$$(2^{23} - 1, 2^{23} + 1) = (2^{23} - 1, 2) = 1,$$

segue-se que 47 divide um, e apenas um, dos números $2^{23} - 1$ ou $2^{23} + 1$.

Como decidir qual dessas duas opções, acima, é verificada?

Em geral, o Pequeno Teorema de Fermat nos diz que se $p > 2$ é um número primo e a um número natural tal que $p \nmid a$, então tem-se que

$$p \mid \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right).$$

Como p é primo, tem-se que $p \mid \left(a^{\frac{p-1}{2}} - 1\right)$ ou $p \mid \left(a^{\frac{p-1}{2}} + 1\right)$.

Decidir qual das duas condições de divisibilidade acima ocorre, é, em geral, um problema difícil.

Capítulo 2

Números Perfeitos

2.1 Primos de Fermat e de Mersenne

Nesta seção, estudaremos alguns tipos de números primos especiais e famosos. O primeiro resultado relaciona-se com os números conhecidos como números de Fermat em homenagem a Pierre de Fermat (1601-1665), jurista francês e matemático amador. Após Euclides e Eratóstenes, Fermat é considerado o primeiro matemático a contribuir para o desenvolvimento da Teoria dos Números do ponto vista teórico. Muitos dos resultados e problemas deixados por Fermat motivaram o extraordinário avanço da Matemática.

Proposição 2.1. *Sejam $a, b, n \in \mathbb{N}$, com $a+b \neq 0$. temos que $a+b$ divide $a^{2n+1}+b^{2n+1}$.*

Demonstração: Usando indução sobre n.
A afirmação é, obviamente verdade para $n = 0$, pois $a + b$ divide $a^1 + b^1$. Suponhamos agora, que $a + b \mid a^{2n+1} + b^{2n+1}$. Escrevemos

$$a^{2(n+1)+1} + b^{2(n+1)+1} = a^2a^{2n+1} + b^2b^{2n+1} = (a^2 - b^2)a^{2n+1} + b^2(a^{2n+1} + b^{2n+1})$$

Como $a + b \mid a^2 - b^2$ e, por hipótese, $a + b \mid a^{2n+1} + b^{2n+1}$, decorre das igualdades acima e pela Proposição 1.5 que $a + b \mid a^{2(n+1)+1} + b^{2(n+1)+1}$. Estabelecendo, assim, o resultado para todo $n \in \mathbb{N}$. ■

Proposição 2.2. *Sejam a e n números naturais maiores do que 1. Se $a^n + 1$ é primo, então a é par e $n = 2^m$, com $m \in \mathbb{N}$.*

Demonstração: Suponhamos que $a^n + 1$ seja primo, onde $a > 1$ e $n > 1$. Logo, a tem que ser par, pois, caso contrário, $a^n + 1$ seria par e maior do que dois, o que contraria o fato de ser primo.
Se n tivesse um divisor primo p diferente de 2, teríamos $n = n'p$ com $n' \in \mathbb{N}^*$. Portanto,

pela Proposição 2.1, $a^{n'}+1$ dividiria $(a^{n'})^p+1 = a^n+1$, contradizendo o fato desse último número ser primo. Isto implica que n é da forma 2^m. ■

Os *números de Fermat* são os números da forma

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

Em 1640, Fermat escreveu em uma de suas cartas que achava que esses números eram todos primos, baseado na observação de que $F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ são primos.

Em 1732, Leonhard Euler mostrou que

$$F_5 = 2^{2^5}+1 = 4.294.967.297 = 641 \times 6700417,$$

e, portanto, composto, desmentindo assim a afirmação de Fermat.

Os números de Fermat primos são chamados de *primos de Fermat*. Até hoje, não se sabe se existem outros primos de Fermat além dos quatro primeiros. Conjecturou-se (Hardy e Wright) que os primos de Fermat são em número finito.

Um resultado acerca desses números, é o seguinte

$$(F_n, F_m) = 1, \quad \text{se } n \neq m.$$

Note que esse resultado nos fornece uma outra prova de que existem infinitos números primos, pois cada número de Fermat tem pelo menos um divisor primo e esses divisores primos são todos distintos.

O resultado que se segue relaciona-se com outros números primos também famosos.

Proposição 2.3. *Sejam a e n números naturais maiores do que 1. Se a^n-1 é primo, então $a = 2$ e n é primo.*

Demonstração: Por hipótese a^n-1 é primo, com $a > 1$ e $n > 1$. Suponhamos, por absurdo, que $a > 2$. Logo $a-1 > 1$ e $(a-1) \mid (a^n-1)$. Logo a^n-1 não é primo, absurdo. Portanto, $a = 2$.
Por outro lado, suponha, por absurdo, que n não é primo. Logo n é composto, isto é, $n = r \cdot s$ com $r > 1$ e $s > 1$. Como 2^r-1 divide $(2^r)^s - 1 = 2^{r\cdot s} - 1 = 2^n - 1$. Logo $2^r - 1 \mid 2^s - 1$. Portanto $2^n - 1$ não seja primo, contradição. Logo n é primo. ■

Definição 2.1. Os números primos da forma 2^p-1, onde p é um número primo, são chamados *Primos de Mersenne*.

Notação: $M_p = 2^p - 1$.

Observação 2.1. No intervalo $2 \leq p \leq 5000$, os números de Mersenne que são primos, chamados primos de Mersenne, correspodem aos seguintes valores de p: $2, 3, 5, 7, 13, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253$ e 4423. Até dezembro de 2001, o maior primo de Mersenne era $M_{13466917}$, que possui no sistema decimal 4053946 dígitos, e é o trigésimo nono primo de Mersenne conhecido.

Enuciaremos a seguir, sem demostração, um resultado profundo devido ao matemático alemão do século XIX Lejeune Dirichlet

Teorema 2.1 (de Dirichlet)**.** *Em uma PA de números naturais, com primeiro termo e razão primos entre si, existem infinitos números primos.*

Observação 2.2. A demonstração deste resultado é muito difícil e pertence à teoria analítica dos números. No entanto, demonstraremos alguns casos particulares do teorema.

Como foi dito acima, temos muitas progressões artméticas do tipo acima que contém como termos infinitos números primos. Como por exemplo:

a) $1, 5, 9, 13, 17, \ldots, 4n+1, \ldots$

b) $3, 7, 11, 15, \ldots, 4n+3, \ldots$

c) $5, 17, 23, 29, \ldots, 6n+5, \ldots$

d) $2, 5, 8, 11, 14, \ldots, 3n+2, \ldots$

Demonstraremos alguns casos particulares do Teorema, usando as duas primeiras progressões aritméticas.

Proposição 2.4. *Na progressão aritmética* $3, 7, 11, 15, \ldots, 3+4n, \ldots$ *existem infinitos números primos.*

Demonstração: Trata-se de mostrar que existem infinitos números primos da forma $4n+3$.
Inicialmente, note que todo primo ímpar é da forma $4n+1$ ou $4n+3$.
Em seguida, observamos que o conjunto, $\Lambda = \{4n+1; n \in \mathbb{N}\}$ é fechado multiplicativamente. De fato,

$$(4n+1)(4n'+1) = 4(4nn' + n + n') + 1.$$

Suponhamos agora, por absurdo, que haja apenas um número finito de números primos $p_1 < \ldots < p_k$ da forma $4n+3$, com $n \geq 1$. Então, o número $a = 4(p_1 \cdot p_2 \cdots p_k) + 3$ não

é divisível por nenhum dos números primos 3, $p_1, \ldots, p_k$ e, portanto, sua decomposição em fatores primo só pode conter primos da forma $4n+1$. Consequentemente, a é da forma $4n+1$, o que é uma contradição, pois é da forma $4n+3$. ■

Proposição 2.5. *Sejam* $n, a \in \mathbb{N}$

a) Então existe $m \in \mathbb{N}$ *tal que* $(a+1)^m = ma+1$.

b) Se $a > 0$, *então existe* $m \in \mathbb{N}$ *tal que* $(a-1)^{2n+1} = ma-1$.

c) Se $a > 1$, *então existe* $m \in \mathbb{N}$ *tal que* $(a-1)^{2n} = ma+1$.

Demonstração:

a) Basta observar que

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} \cdot b^i.$$

Então

$$\begin{aligned}
(a+1)^n &= \sum_{i=0}^{n} \binom{n}{i} a^n \\
&= \binom{n}{0} a^{n-i} + \binom{n}{1} a^{n-1} + \ldots + \binom{n}{n-1} a^1 + \binom{n}{n} a^0 \\
&= a^n + n \cdot a^{n-1} + \ldots + \frac{n!}{(n-1)!(n-n+1)!} a^1 + 1 \\
&- a^n + na^{n-1} + \ldots + na + 1 \\
&= a(a^{n-1} + na^{n-2} + \ldots + n) + 1 = am + 1
\end{aligned}$$

b)

$$\begin{aligned}
(a-1)^{2n+1} &= \sum_{i=0}^{2n+1} \binom{2n+1}{i} a^{2n+1-i} \cdot (-1)^i \\
&= \binom{2n+1}{0} a^{2n+1} - \binom{2n+1}{1} a^{2n} + \binom{2n+1}{2} a^{2n-1} \\
&\quad - \ldots + \binom{2n+1}{2n+1-1} a^1 - \binom{2n+1}{2n+1} a^0 \\
&= a^{2n+1} - (2n+1)a^{2n} + \ldots + \binom{2n+1}{2n} a - 1 \\
&= a\left[a^{2n} - (2n+1)a^{2n-1} + \ldots + \binom{2n+1}{2n}\right] - 1 \\
&= ma - 1
\end{aligned}$$

c)

$$\begin{aligned}
(a-1)^{2n} &= \sum_{i=0}^{2n} \binom{2n}{i} a^{2n-i} \cdot (-1)^i \\
&= \binom{2n}{0} a^{2n} - \binom{2n}{i} a^{2n-1} + \ldots - \binom{2n}{2n-1} a^1 + \binom{2n}{2n} a^0 \\
&= a^{2n} - 2na^{2n-1} + \ldots - \binom{2n}{2n-1} a^1 + 1 \\
&= a\left[a^{2n-1} - 2na^{2n-2} + \ldots - \binom{2n}{2n-1}\right] + 1 \\
&= ma + 1.
\end{aligned}$$

■

Mostrar que existem infinitos primos da forma $4n+1$ é um pouco mais sutil e será provado a seguir. Antes, porém, provaremos um lema que será necessário para a prova do resultado.

Lema 2.1. *Seja $x \in \mathbb{N}^*$, com $x \geq 2$. Todo divisor ímpar de x^2+1 é da forma $4n+1$.*

Demonstração: Inicialmente, provaremos que todo divisor primo $p \neq 2$ de x^2+1 é da forma $4n+1$. O resultado em geral seguirá disso, pois o conjunto $\Lambda = \{4n+1; n \in \mathbb{N}\}$ é fechado multiplicativamente.
Suponhamos, então, que $p \mid x^2+1$, com p primo maior do que 2. temos que $(p-1)/2 \in \mathbb{N}$ e, para algum $\lambda \in \mathbb{N}$, que $x^2+1 = \lambda p$. Consequentemente,

$$x^2 = \lambda p - 1.$$

Elevando à potência $(p-1)/2$ ambos os lados da igualdade acima, temos, para alguns $\mu, \mu' \in \mathbb{N}$, que

$$x^{p-1} = (x^2)^{\frac{p-1}{2}} = (\lambda p - 1)^{\frac{p-1}{2}} = \begin{cases} \mu p + 1, & \text{se } \dfrac{p-1}{2} \text{ é par} \\ \mu' p - 1, & \text{se } \dfrac{p-1}{2} \text{ é ímpar} \end{cases}$$

Ver Proposição 2.5.
Se

$$x^{p-1} = \mu' p - 1$$

Subtraindo 1 de ambos os lados, teríamos que

$$x^{p-1} - 1 = \mu' p - 2. \tag{2.1}$$

Como $p \mid x^2 + 1$, segue que $p \nmid x$. Logo, pelo Pequeno Teorema de Fermat, temos que $p \mid x^{p-1} - 1$ e, consequentemente, por (2.1), $p \mid 2$, o que é uma contradição.
Portanto, a única alternativa possível é que $\dfrac{p-1}{2}$ seja par, o que implica que p é da forma $4n + 1$. ■

Proposição 2.6. *Na progressão aritmética* $1, 5, 9, 13, 17, \ldots, 4n + 1, \ldots$ *existem infinitos números primos.*

Demonstração: Suponha, por absurdo, que haja um número finito $p_1, \ldots, p_k$ de primos da forma $4n + 1$. Considere o número

$$a = 4p_1^2 \cdots p_k^2 + 1.$$

Como $p_i \nmid a$, para todo $i = 1, \ldots, k$; logo, todo divisor primo de a é da forma $4n + 3$, o que é um absurdo, em vista do Lema 2.1. ■

2.2 Soma dos divisores de um número natural

Definição 2.2. Um par de números $\{a, b\}$ é amigável quando cada um deles for igual à soma dos divisores próprios do outro.

Exemplo 2.1. 220 e 284

Soma dos divisores próprios de

$$220 : 1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284$$

Soma dos divisores próprios de

$$284 : 1 + 2 + 4 + 71 + 142 = 220.$$

Seja n um número natural maior do que 1. Denotamos por $S(n)$ a soma de todos os divisores de n. Observe que $S(0)$ não está definido e $S(1) = 1$. Consideremos, então $n \geq 2$ e encontremos $S(n)$. Convém antes tecer algumas considerações sobre $S(n)$.

1. m e n formam um par amigável se $S(m) = m + n = S(n)$.

2. p é primo se e apenas $S(p) = p + 1$.

3. n é um número perfeito se $S(n) = n + n = 2n$.

4. Se p é primo, então $S(p^r) = 1+p+p^2+\ldots+p^r = \dfrac{p^{n+1}-1}{p-1}$, pois $1+p+p^2+\ldots+p^r$ é a soma dos termo de uma P.G. finita de primeiro termo $a_1 = 1$ e razão $q = p$ e $r+1$ termos. Em particular, para $n = 2^r$, obtemos

$$S(n) = S(2^r) = \frac{2^{r+1}-1}{2-1} = 2^{r+1} - 1 = 2 \cdot 2^r - 1 = 2n - 1.$$

   Concluímos daí que uma potência de base 2 nunca é um número perfeito.

5. Se p e q são números primos diferentes, então $S(p \cdot q) = S(p) \cdot S(q)$ para provar esta relação, basta observar que os divisores de $p \cdot q$ são apenas $1, p, q$ e $p \cdot q$. Logo

$$S(p \cdot q) = 1 + p + q + p \cdot q = 1 + p + q \cdot (1 + p) = (1 + p) \cdot (1 + q) = S(p) \cdot S(q).$$

6. Se a e b são relativamente primos entre si, isto é, $(a, b) = 1$, então

$$S(a \cdot b) = S(a) \cdot S(b).$$

   Suponha que $a = p^2$ e $b = q \cdot r$, com p, q e r primos.

$$\begin{aligned}
S(a \cdot b) &= S(p^2 \cdot q \cdot r) \\
&= 1 + p + p^2 + q + p \cdot q + p^2 \cdot q \\
&\quad + r + p \cdot r + p^2 \cdot r + q \cdot r + p \cdot q \cdot r + + p^2 \cdot q \cdot r \\
&= (1 + p + p^2) + q \cdot (1 + p + p^2) + r \cdot (1 + p + p^2) + q \cdot r \cdot (1 + p + p^2) \\
&= (1 + p + p^2) \cdot (1 + q + r + q \cdot r) \\
&= (1 + p + p^2) \cdot (1 + r) \cdot (1 + q) \\
&= S(p^2) \cdot S(q) \cdot S(r) \\
&= S(p^2) \cdot S(q \cdot r) \\
&= S(a) \cdot S(b).
\end{aligned}$$

Lema 2.2. *A soma dos termos de uma Progressão Geométrica finita de primeiro termo a_1, enésimo termo a_n e razão q, é dada por* $S_n = \dfrac{a_n \cdot q - a_1}{q - 1}$.

Demonstração: Seja $(a_1, a_2, a_3, \ldots, a_{n-1}, a_n)$ uma Progressão Geométrica finita de primeiro termo a_1, enésimo termo a_n e razão q, então a soma S_n dos termos dessa

Progressão Geométrica finita é:

$$S_n = a_1 + a_2 + a_3 + \ldots + a_{n-1} + a_n,$$

e multiplicando ambos os temos dessa igualdade por q, temos:

$$S_n \cdot q = a_1 \cdot q + a_2 \cdot q + a_3 \cdot q + \ldots + a_{n-1} \cdot q + a_n \cdot q,$$

então

$$S_n \cdot q = a_2 + a_3 + a_4 + \ldots + a_n + a_n \cdot q.$$

Subtraindo-se as expressões $S_n \cdot q$ e S_n membro a membro, temos que

$$S_n \cdot q - S_n = a_2 + a_3 + a_4 + \ldots + a_n + a_n \cdot q - (a_1 + a_2 + a_3 + \ldots + a_{n-1} + a_n \cdot q).$$

Então $S_n \cdot q - S_n = a_n \cdot q - a_1$, logo

$$S_n = \frac{a_n \cdot q - a_1}{q - 1}.$$

■

Exemplo 2.2.

$$S(3) = \frac{3^2 - 1}{3 - 1} = \frac{9 - 1}{2} = \frac{8}{2} = 4,\ D(3) = \{1, 3\}$$

$$S(6) = S(2 \cdot 3) = \frac{2^2 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} = \frac{4 - 1}{1} \cdot \frac{9 - 1}{2} = 3 \cdot 4 = 12,$$

$D(6) = \{1, 2, 3, 6\}$.

$$S(18) = S(2 \cdot 3^2) = \frac{2^2 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} = \frac{4 - 1}{1} \cdot \frac{27 - 1}{2} = 3 \cdot 13 = 39,$$

$D(18) = \{1, 2, 3, 6, 9, 18\}$.

$$S(28) = S(2^2 \cdot 7) = \frac{2^3 - 1}{2 - 1} \cdot \frac{7^2 - 1}{7 - 1} = \frac{8 - 1}{1} \cdot \frac{49 - 1}{6} = 7 \cdot 8 = 56,$$

$D(28) = \{1, 2, 4, 7, 14, 28\}$.

$$S(45) = S(3^2 \cdot 5) = \frac{3^3 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = \frac{27 - 1}{2} \cdot \frac{25 - 1}{4} = 13 \cdot 6 = 78,$$

$D(45) = \{1, 3, 5, 9, 15, 45\}$

Note que $S(18) = 39$ e que $S(18) = S(3 \cdot 6) = S(3) \cdot S(6) = 4 \cdot 12 = 48$. Note que $(3, 6) = 3 \neq 1$. Observe que 6 e 28 são números iguais a metade da soma dos seus divisores.

2.3 Números Perfeitos

Definição 2.3. Um número n é chamado de *número perfeito* se $s(N) = 2n$. Ou ainda, se o número é igual à soma de seus divisores distintos dele mesmo. Na idade média, conhecia-se apenas os números perfeitos: 6, 28, 496, 8128. Atualmente, conhece-se mais alguns números perfeitos. Um fato curioso é que todos os números perfeitos são pares. Não se sabe nada sobre a existência ou não de números perfeitos ímpares.

Observação 2.3. Os resultados a seguir, principalmente o Teorema de Euclides-Euler, caracterizarão os números perfeitos pares, relacionando-os com os números primos de Mersenne.

Lema 2.3. *Seja $n \in \mathbb{N}^*$, tem-se que $S(n) = n + 1$ se, e somente se, n é um número primo.*

Demonstração: Se $S(n) = n + 1$, segue-se que $n > 1$ e que os únicos divisores de n são 1 e n: Logo n é primo. Reciprocamente, Se n é primo

$$S_n = \frac{n^2 - 1}{n - 1} = \frac{(n + 1)(n - 1)}{n - 1} = n + 1.$$

■

Teorema 2.2 (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 número primo de Mersenne.*

Demonstração: Suponha que $n = 2^{p-1} \cdot (2^p - 1)$, onde $2^p - 1$ é um número primo de Mersenne. Logo, $p > 1$, e, consequentemente, n par. Como $2^p - 1$ é ímpar, temos que $(2^{p-1}, 2^p - 1) = 1$. Logo, temos que

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

$$S(n) = \frac{2^p - 1}{2 - 1} \cdot 2^p = 2^p \cdot (2^p - 1) = 2 \cdot 2^{p-1} \cdot (2^p - 1) = 2 \cdot n.$$

Portanto n é perfeito. Reciprocamente, suponha que n é perfeito e par. Seja 2^{p-1} a maior potência de 2 que divide n. Logo, $p > 1$ e $n = 2^{p-1} \cdot b$, com b ímpar. Temos, então, que $(2^{p-1}, b) = 1$ e pela Proposição 2.5 e a consideração 6, segue-se que

$$S(n) = (2^p - 1) \cdot S(b).$$

Como $S(n) = 2n$, temos $(2^p - 1) \cdot S(b) = 2 \cdot 2^{p-1} \cdot b = 2^p \cdot b$, portanto $2^p - 1 \mid b$, pois $(2^p, 2^p - 1) = 1$. Logo, existe $c \in \mathbb{N}$ com $c < b$ tal que $b = c(2^p - 1)$. Substituindo em $(2^p - 1) \cdot S(b) = 2^p \cdot c \cdot (2^p - 1)$, resulta $S(b) = 2^p \cdot c$. Assim b e c são dois divisores distintos de b tais que $c + b = 2^p \cdot c$. Nessa situação, $c = 1$. De fato, suponha que $c \neq 1$. Temos, então, que $2^p \cdot c = S(b) \geq 1 + c + b > c + b = 2^p \cdot c$, o que é uma contradição. Logo $S(b) = b + 1$, o que implica b ser primo. Consequentemente, $N = 2^{p-1} \cdot (2^p - 1)$ com $2^p - 1$ um primo de Mersenne. ■

Observação 2.4. A primeira parte da demonstração do teorema acima, sem dúvida a mais fácil, já se encontra nos Elementos de Euclides. A recíproca data do século XVIII é devida a Euler. O fato do número $2^p - 1$, no enunciado do teorema, ser um número primo de Mersenne, implica que p é primo. Observe, ainda, que o teorema reduz a existência ou não de um número infinito de números perfeitos pares ao problema análogo para primos de Mersenne.

Observação 2.5. Todo número da forma $a_n = 2^{2n} \cdot (2^{2n+1} - 1)$, onde $n > 1$, na sua representação decimal, ou termina em 28 ou termina em $a6$, onde a é um algarismo ímpar. Em particular, todo número perfeito par termina em um desses modos.
De fato,

$$a_{2n+1} = 2^{4n+2} \cdot (2^{4n+2+1} - 1) = 2^{8n+5} - 2^{4n+2} = 2^{8n} \cdot 2^5 - 2^{4n} \cdot 2^2 = 256^n \cdot 32 - 16^n \cdot 4$$

$$a_{2n-1} = 2^{4n-2} \cdot (2^{4n-2+1} - 1) = 2^{8n-3} - 2^{4n-2} = 2^{8n} \cdot 2^{-3} - 2^{4n} \cdot 2^{-2} = \frac{256^n}{8} - \frac{16^n}{4}$$

$$\begin{aligned} 256 \cdot a_{2n-1} &= 256^n \cdot 32 - 16^n \cdot 64 \\ &= 256^n \cdot 32 - 16^n \cdot 4 - 16^n \cdot 60 \\ &= 256 \cdot a_{2n-1} + 16^n \cdot 60 \\ &= 256^n \cdot 32 - 16^n \cdot 4 \\ &= a_{2n+1} \end{aligned}$$

$$a_{2n+1} = 256 \cdot a_{2n-1} + 60 \cdot 16^n$$

$$a_{2n+2} = 2^{4n+4} \cdot (2^{4n+4+1} - 1) = 2^{8n+9} - 2^{4n+4} = 256^n \cdot 512 - 16^n \cdot 16$$

$$a_{2n} = 2^{4n} \cdot (2^{4n+1} - 1) = 2^{8n+1} - 2^{4n} = 256^n \cdot 2 - 16^n$$

$$256 \cdot a_{2n} = 256 \cdot (256^n \cdot 2 - 16^n) = 256^n \cdot 512 - 16^n \cdot 256 = 256^n \cdot 512 - 16^n \cdot 16 - 16^n \cdot 240$$

$$256 \cdot a_{2n} + 16^n \cdot 240 = 256^n \cdot 512 - 16^n \cdot 16 = a_{2n+2}.$$

Façamos agora a análise dos dois últimos algarismos de 16^n ao variar n em $\mathbb{N}$. Temos

que:

$$16 \equiv 16 \bmod 100$$

$$16^2 \equiv 56 \bmod 100$$

$$16^3 \equiv 96 \bmod 100$$

$$16^4 \equiv 36 \bmod 100$$

$$16^5 \equiv 76 \bmod 100$$

$$16^6 \equiv 16 \bmod 100$$

E daí para frente esses números se repetem ciclicamente. Portanto, para todo $n \in \mathbb{N}$, os dois últimos algarismos de 16^n são da forma $a6$, onde a é ímpar.
Observe agora que $a_2 = 96$, logo da forma $a6$, onde a é ímpar. Vamos provar, por indução sobre n, que o mesmo ocorre para todos os números da forma a_{2n}. Suponha que a_{2n} termina em $a6$, onde a é um algarismo ímpar; Logo

$$\begin{aligned} a_{2(n+1)} &= 256a_{2n} + 240 \cdot 16^n \equiv 56 \cdot a6 + 40 \cdot 16^n \\ &= (50+6)(10a+6) + 40(10b+6) \equiv 10(6a+3+4) + 6 \\ &\equiv 10c + 6 \bmod 100, \end{aligned}$$

onde c é um algarismo e o resultado segue-se, pois $6a+3+4 = 6a+6+1 = 6(a+1)+1 = 2[3(a+1)]+1 = 2n+1$ que é ímpar.
Observe agora que $a_1 = 28$; Logo, termina em 28. Vamos provar por indução sobre n que o número ocorre para todos os números da forma a_{2n+1}. Suponha que a_{2n-1} termina em 28. Logo,

$$\begin{aligned} a_{2n+1} &= 256a_{2n-1} + 60 \cdot 16^n \equiv 56 \cdot 28 + 60 \cdot 16^n \\ &\equiv 56 \cdot 28 + 60(10b+6) \equiv 68 + 60 \equiv 28 \ 28 \ 100. \end{aligned}$$

Teorema 2.3. *Um número perfeito ímpar tem pelo menos três fatores primos diferentes.*

Demonstração: Vamos supor, primeiramente, que n é um número ímpar perfeito com um simples fator primo, isto é, suponha que $n = p^r$, onde p é um número ímpar e $r \geq 1$. Então $S(n) = 2n$. Por outro lado

$$S(n) = 1 + p + p^2 + \ldots + p^r = \frac{p^{r+1} - 1}{p - 1}.$$

Mas $S(n) = 2n = 2p^r$. Assim $2p^r = \dfrac{p^{r+1}-1}{p-1}$ e daí, temos $2p^{r+1} - 2p^r = p^{r+1} - 1$. Então $p^{r+1} - 2p^r = -1$, e portanto, $2p^r - p^{r+1} = 1$. Absurdo, pois p é primo e divide o lado esquerdo da equação mas não divide o lado direito. Portanto um número ímpar perfeito não pode ter um simples fator primo.

Vamos supor agora que n seja composto de dois fatores primos diferentes, isto é, $n = p^r \cdot q^s$ é um número ímpar perfeito. Sem perda de generalidade, suponha $p < q$. Já vimos que $S(n) = 2n$ e $S(p^r \cdot q^s) = S(p^r) \cdot S(q^s)$. Daí temos

$$2 \cdot p^r \cdot q^s = \left(1 + p + p^2 + \ldots + p^r\right) \cdot \left(1 + q + q^2 + \ldots + q^r\right)$$

$$2 = \left(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^r}\right) \cdot \left(1 + \frac{1}{q} + \frac{1}{q^2} + \ldots + \frac{1}{q^s}\right).$$

Tomando $p = 3$ e $q = 5$, obtemos

$$2 \leq \left(1 + \frac{1}{3} + \frac{1}{3^2} + \ldots + \frac{1}{3^r}\right) \cdot \left(1 + \frac{1}{5} + \frac{1}{5^2} + \ldots + \frac{1}{5^s}\right)$$

$$\begin{aligned} 2 \leq \sum_{i=0}^{\infty} \frac{1}{3^i} \cdot \sum_{j=0}^{\infty} \frac{1}{5^j} &= \frac{1}{\frac{3-1}{3}} \cdot \frac{1}{\frac{5-1}{5}} \\ &= \frac{1}{\frac{2}{3}} \cdot \frac{1}{\frac{4}{5}} \\ &= \frac{3}{2} \cdot \frac{5}{4} \\ &= \frac{15}{8} = 1,875. \end{aligned}$$

Absurdo! Desta forma, se existe um número ímpar perfeito, ele terá pelo menos três fatores primos distintos. ∎

A existência ou não de números perfeitos ímpares é um desafio para a Teoria dos Números. De fato, não se conhecem atualmente números perfeitos ímpares e conjetura-se, com fortes indícios experimentais, que não existe nenhum. Em 2004 foi submetido ao arXiv um artigo pelo matemático australiano Simon Davis contendo a demonstração desta conjectura, que não foi no entanto ainda publicado.

2.4 Alguns resultados elementares sobre números perfeitos

Definição 2.4. A soma dos divisores de um número natural n é a função $S(n) = \sum_{d|n} d$ onde d é obtido ao longo dos divisores de n incluindo o próprio n.

Exemplo 2.3. $S(11) = 1 + 11 = 12$
$S(15) = 1 + 3 + 5 + 15 = 24$

Observação 2.6. A definição de um número perfeito equivale a dizer que a soma dos divisores próprios de n é igual a n. A razão para que utilizaremos a função $S(n)$ é que ela possui algumas propriedades muito especiais.

Proposição 2.7. *Se*

$$N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}$$

é a fatoração de N em fatores primos, então

$$S(N) = \prod_{i=1}^{r}(1 + p_i + p_i^2 + p_i^3 + \ldots + p_i^{\alpha_i}) = \prod_{i=1}^{r}\left(\frac{p_i^{\alpha_1+1} - 1}{p_i - 1}\right).$$

Demonstração: Observe que os únicos divisores de $p_i^{\alpha_1}$ são $1, p_i, p_i^2, p_i^3, \ldots, p_i^{\alpha_i}$, de sorte que

$$S(p_i^{\alpha_i}) = 1 + p_i + p_i^2 + p_i^3 + \ldots + p_i^{\alpha_i}$$

é a soma dos termos de uma P.G. finita de razão p_i e primeiro termo igual a 1

$$1 + x + x^2 + x^3 + \ldots + x^k = \sum_{i=0}^{k} x^i = \frac{x^{k+1} - 1}{x - 1}$$

Logo pelo Lema 2.2

$$S(p_i^{\alpha_i}) = \frac{p_i^{\alpha_1+1} - 1}{p_i - 1}.$$

Usando a multiplicidade de $S(N)$, temos:

$$S(N) = S\left(\prod_{i=1}^{r} p_i^{\alpha_1}\right) = \prod_{i=1}^{r} S(p_i^{\alpha_i}) = \prod_{i=1}^{r} \frac{p_i^{\alpha_1+1} - 1}{p_i - 1}.$$

■

Como aplicação dessa fórmula, provaremos dois lemas.

Lema 2.4. *Se $n \mid N$, é evidente que $S(n) < S(N)$ e $\dfrac{S(n)}{n} < \dfrac{S(N)}{N}$ com igualdade ocorrendo se $n = N$.*

Demonstração: Se $d \mid n = N$, existe $k \in \mathbb{N}$ tal que $n = k \cdot d$, logo $k = \dfrac{n}{d} \mid N$. Portanto $d \mid N$ se, e somente se $\dfrac{n}{d} \mid N$, isto é,

$$S(N) = \sum_{d|n} d = \sum_{d|n} \frac{N}{d} = N \sum_{d|n} \frac{1}{d}$$

Se n é um divisor próprio de N, temos

$$\frac{S(N)}{N} = \sum_{d|N} \frac{1}{d} > \sum_{d|n} \frac{1}{d} = \frac{S(n)}{n}.$$

■

Corolário 2.1. *Se N é um número perfeito, $\displaystyle\sum_{d|n} \frac{1}{d} = 2$.*

Demonstração: Acima, mostraremos que $d \mid N$ é equivalente a $(N \mid d) \mid N$, consequentemente $\displaystyle\sum_{d|n} d = \sum_{d|n} \frac{N}{d} = N \sum_{d|n} \frac{1}{d} = 2N$, então $\displaystyle\sum_{d|n} \frac{1}{d} = 2$. ■

2.5 Números pares perfeitos

Historicamente, o primeiro matemático que categorizou os números pares perfeitos foi Euclides. Ele observou que os quatro primeiros números perfeitos apresentam uma forma muito específica.

$$6 = 2^1 \cdot (1 + 2) = 2 \cdot 3$$

$$28 = 2^2 \cdot (1 + 2 + 2^2) = 4 \cdot 7$$

$$496 = 2^4 \cdot (1 + 2 + 2^2 + 2^3 + 2^4) = 16 \cdot 31$$

$$8128 = 2^6 \cdot (1 + 2 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6) = 64 \cdot 127$$

Observe, porém, que os números

$$90 = 2^3 \cdot (1 + 2 + 2^2 + 2^3) = 8 \cdot 15$$

$$2016 = 2^5 \cdot (1 + 2 + 2^2 + 2^3 + 2^4 + 2^5) = 32 \cdot 63$$

estão faltando nessa sequência porque $15 = 3 \cdot 5$ e $63 = 3^2 \cdot 7$ são números compostos, ao passo que 3, 7, 31 e 127 são todos números primos.

Teorema 2.4 (Teorema de Euclides)**.** *Se $2^n - 1$ é primo, então $N = 2^{n-1} \cdot (2^n - 1)$ é perfeito.*

Demonstração: Como $2^n - 1$ é primo, seus únicos divisores são $2^n - 1$ e 1. Logo $S(2^n - 1) = 2^n - 1 + 1 = 2^n$. Então $S(N) = S(2^{n-1}) \cdot S(2^n - 1) = \dfrac{2^n - 1}{2 - 1} \cdot 2^n = 2^n \cdot (2^n - 1) = 2 \cdot 2^{n-1} \cdot (2^n - 1) = 2N$ e N é perfeito. ■

Proposição 2.8 (Cataldi-Fermat)**.** *Se $2^n - 1$ é primo, então o próprio n é primo.*

Demonstração: Observe que $x^n - 1 = (x - 1) \cdot (x^{n-1} + x^{n-2} + \ldots + x + 1)$. Suponha, por absurdo, que $n = r \cdot s$ onde $r > 1$, $s > 1$. Assim, $2^n - 1 = 2^{r \cdot s} - 1 = (2^r)^s - 1 = (2^r - 1)[(2^r)^{s-1} + (2^r)^{s-2} + \ldots + 2^r + 1]$. De modo que $(2^r - 1) \mid (2^n - 1)$, Absurdo! Pois $2^n - 1$ é primo. ■

Observação 2.7. O inverso não é verdade, isto é, se n é primo, então $2^n - 1$ não é, necessariamente, primo. De fato, se $n = 11$, então $2^{11} - 1 = 2048 - 1 = 2047 = 23 \cdot 89$.

Observação 2.8. Todos os números perfeitos têm que ser do tipo de Euclides? Leonhard Euler, numa póstuma escritura, provou que todo número par perfeito é deste tipo. Existem muitas provas deste fato, vejamos algumas.

Leonhard Euler

⋆ 15 de abril de 1707, em Basel, Suíça.
† 18 de setembro de 1783, em São Petersburgo, Rússia.

Leonhard Euler, filho do pastor calvinista Paul Euler, e Margaret Brucker, teve duas irmãs mais novas, Anna Maria e Maria Magdalena.

Mudou-se para Riehen com um ano de idade, e lá foi criado. Seu pai o introduziu nos primeiros estudos de matemática.

Quando chegou à adolescência, Euler retornou a Basel para estudar, preparando-se para o curso de teologia na Universidade.

Euler não aprendeu matemática alguma na escola, mas seu interesse, despertado nas lições de seu pai, o levou a estudar sozinho textos diversos e a tomar lições particulares. Embora muito religioso, Euler não se entusiasmou com o estudo da teologia, e seu pai consentiu que ele mudasse para a matemática.

Terminado o curso, foi convidado a assumir a cadeira de um professor falecido na Universidade de São Petersburgo. Como não fora selecionado para a cadeira de física da Universidade de Basel, aceitou o primeiro convite e, em 1727, mudou-se para a Rússia. Chegando lá, afiliou-se à Academia de Ciências, onde teve contato com grandes cientistas como Jakob Hermann, Daniel Bernoulli e Christian Goldbach.

Em 1730, Euler tornou-se professor de Física da Academia, fato que o permitiu abandonar o posto de lugar-tenente da marinha Russa, que ele ocupava desde 1727. Três anos mais tarde, com o retorno de Daniel Bernoulli a Basel, Euler assumiu a cátedra de matemática da Academia, e os proventos advindos dessa nomeação permitiram que ele se casasse, em 1734, com Katharina Gsell, uma moça de ascendência suíça.

Os dois tiveram treze filhos, mas apenas cinco sobreviveram à infância. Euler atribui a essa fase algumas de suas maiores proezas científicas.

Em 1736-37, Euler publicou seu livro Mechanica, que tratou extensivamente da análise matemática da dinâmica newtoniana pela primeira vez. Foi também nesta época que seus problemas de saúde começaram. Euler era constantemente atormentado por fortes crises febris, e desenvolveu catarata, que acabou por lhe tirar a vista. Mas se sua saúde estava abalada, sua reputação, ao contrário, se firmava cada vez mais, e dois prêmios da Academia de Paris, em 1738 e 1740, acabaram por lhe valer uma oferta de trabalho em Berlim.

De início, Leonhard recusou, preferindo permanecer em São Petersburgo, mas a turbulência política na Rússia tornou difícil a vida de estrangeiros lá, e ele reconsiderou.

Chegou a Alemanha como diretor de matemática da recém-fundada Academia de Berlim, que tinha então como presidente Maupertius. As contribuçoes de Euler para a Academia foram notáveis. Ele supervisionava o observatório e o jardim botânico, selecionava pessoal, gerenciava várias questões financeiras. Além disso, coordenou a publicação de mapas geográficos, uma fonte de dividendos para a Academia. Também trabalhou no comitê da Academia, lidando com a publicação de trabalhos científicos. E como se não bastasse, sua própria produção científica neste período foi excepcional. Durante os 25 anos que morou em Berlim, Euler escreveu cerca de 380 artigos, livros sobre Cálculo de variações e órbitas dos planetas, sobre artilharia e balística, construção naval e navegação, sobre o movimento da Lua, cálculo diferencial e uma obra científica para leigos: Letters to a Princess of Germany (Cartas a uma Princesa da Alemanha, 3 vols. 1768-72).

Em 1759, com a morte de Maupertius, Euler assumiu a direção da Academia, embora não fosse nomeado presidente. Desavenças com Frederico, o Grande, em torno dessa questão fizeram-no deixar a Alemanha e retornar a São Petersburgo, em

1766. Em, 1771, velho e doente, Euler teve sua casa destruída num incêndio. Tudo o que ele salvou foram seus manuscritos. Foi nesta época que ele ficou totalmente cego. O impressionante é que mesmo depois disso, ele continuou com seus projetos, e quase a metade de toda a sua produção científica foi concluída após esses incidentes. Evidentemente, Euler não logrou todas essas conquistas sozinho. Ele contou com a ajuda valorosa de dois de seus filhos, Johann Albrecht Euler, que seguia os passos do pai, e Christoph Euler, que estava na carreira militar, e também dois membros da Academia, A. J. Lexell e o jovem matemático N. Fuss, esposo de sua neta. Euler morreu em 18 de setembro de 1783.

Teoria dos Números

O interesse de Euler na teoria dos números pode ser atribuída à influência de Christian Goldbach, seu amigo na Academia St. Petersburg. Muitos dos primeiros trabalhos de Euler na teoria dos números foram baseados nas obras de Pierre de Fermat. Euler desenvolveu algumas das idéias de Fermat, e refutou algumas das suas conjecturas. Euler ligou a natureza da distribuição privilegiada, com idéias de análise. Conseguiu provar que a soma dos recíprocos dos primos diverge. Ao fazer isso, ele descobriu a conexão entre a função zeta de Riemann e os números primos, o que é conhecido como a fórmula do produto de Euler para a função zeta de Riemann.

Euler provou identidades de Newton, Pequeno Teorema de Fermat, teorema de Fermat em somas de dois quadrados, e ele fez contribuições distintas ao Teorema de Fermat-Lagrange. Inventou também a função φ totiente (n). Usando as propriedades desta função, ele generalizou o teorema de Fermat ao que é hoje conhecido como o teorema de Euler. Ele contribuiu de forma significativa para a teoria dos números perfeitos, que havia fascinado os matemáticos desde Euclides. Euler também conjecturou a lei da reciprocidade quadrática. O conceito é considerado como um teorema fundamental da teoria dos números, e suas ideias pavimentaram o caminho para o trabalho de Carl Friedrich Gauss.

Euler e Fermat

Tanto Fermat como Euler sentiram-se bastante interessados pela teoria dos números. Embora não haja qualquer livro sobre este assunto, Euler escreveu cartas e artigos sobre vários aspectos desta teoria. Entre elas encontram-se as conjecturas apresentadas por Fermat, que foram derrubadas por Euler. Duas dessas conjecturas foram:

- Os números da forma $2^{2n} + 1$ são sempre primos;
- Se p é primo e a um inteiro, então $a^p - a$ é divisível por p.

A primeira, foi derrubada em 1732 com o auxílio do seu domínio em computação, evidenciando que $(2^2)^5 + 1 = 4294967297$ é factorizável em $6700417 \cdot 641$. No entanto, no recurso a um contraexemplo para deitar por terra a segunda conjectura, Euler também errou, apesar do erro só ter sido descoberto em 1966, dois séculos depois e com o auxílio de um computador.

Euler também realizou a demonstração de uma conjectura bastante conhecida, denominada como Pequeno Teorema de Fermat. Tal demonstração foi apresentada numa publicação em 1736, denominada Commentarii. Posteriormente, demonstrou uma afirmação mais geral do Pequeno Teorema de Fermat, que veio a chamar-se Função de Euler. Mas, contrariando o que seria esperado, Euler não foi capaz de demonstrar o Último Teorema de Fermat, embora provasse a impossibilidade de soluções inteiras de $x^n + y^n = z^n$ para $n = 3$.

Em 1747, definiu mais 27 números amigáveis, que se juntaram aos três já conhecidos por Fermat. Mais tarde aumentou o número para 60. Euler também provou que todos os números perfeitos pares são da forma dada por Euclides, $2^{n-1}(2^n - 1)$, onde $2^n - 1$ é primo. Se existe ou não um número ímpar perfeito foi uma questão levantada por Euler e Goldbach, através de correspondência, ainda hoje sem resposta.

Curiosidades:

- Por ter sido um dos melhores e mais produtivos matemáticos da história, foi representado na sexta série das notas do banco Suíço e em numerosos selos da Suíça, da Alemanha e da Rússia.
- O asteróide 2002 foi chamado Euler em sua homenagem.
- É também relembrado pela Igreja Luterana no dia 24 de Maio, no Calendário dos Santos.
- Euler foi também uma das inspirações na criação do jogo Sudoku. Um puzzle inspirado (provavelmente) no quadrado latino, invenção do século XVIII de Euler.
- Foi o criador da teoria dos Grafos, a partir da resolução do problema das Sete pontes de Königsberg.
- Leonard Euler morreu bebendo chá, em São Petersburgo.
- Existe uma anedota falsa sobre Euler e Diderot, quando este estava em São Petersburgo, Rússia, influenciando a corte russa com seu ateísmo, e Euler foi chamado a intervir. Euler teria uma prova matemática da existência de Deus, e teria dito "Monsieur, $\frac{a+b^n}{n} = x$, donc Dieu existe. Respondez!". Diderot não

teria conseguido responder, e retirou-se humilhado sob os risos da corte. Esta anedota é falsa.

"Leiam Euler, leiam Euler, ele é o mestre de todos nós".

Teorema 2.5 (Euler)**.** *Se N é um número par perfeito, N pode ser escrito na forma $N = 2^{n-1} \cdot (2^n - 1)$, onde $2^n - 1$ é primo.*

Demonstração 1: Esta primeira demonstração é devida a Euler.
Seja $N = 2^{n-1} \cdot m$ um número perfeito em que m é ímpar. Desde que $2 \nmid m$, ele é relativamente primo para 2^{n-1}, e $S(N) = S(2^{n-1} \cdot m) = S(2^{n-1}) \cdot S(m) = \dfrac{2^n - 1}{2 - 1} \cdot S(m) = 2^n - 1 \cdot S(m)$. Como N é perfeito, temos $S(N) = 2N = 2 \cdot 2^{n-1} \cdot m = 2^n \cdot m$. Logo $(2^n - 1) \cdot S(m) = 2^n \cdot m$.
Seja $S = S(m)$, então $2^n \cdot m = (2^n - 1) \cdot S$ e $m = (2^n - 1) \cdot \dfrac{S}{2^n}$. Como $2^n - 1$ é primo, $2^n \mid S$. Logo existe q tal que $m = (2^n - 1) \cdot q$.
Se $q = 1$, então $m = 2^n - 1$ e $S = S(m) = 2^n = 2^n - 1 + 1 = m + 1$.
Como $S(m)$ é a soma dos divisores de $m = 2^n - 1$, logo $m = 2^n - 1$ tem que ser um número primo, e

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

Se $q > 1$, a soma total dos divisores de $m = (2^n - 1) \cdot q$.
Os fatores de m incluem $1, q, 2^n - 1$ e m, de modo que

$$S = S(m) \geq 1 + q + 2^n - 1 + (2^n - 1) \cdot q = (2^n - 1) \cdot (1 + q) + (1 + q) = (1 + q) \cdot 2^n.$$

Logo

$$\frac{m}{s} \leq \frac{(2^n - 1) \cdot q}{2^n \cdot (q + 1)} = \left(\frac{2^n - 1}{2^n}\right) \cdot \left(\frac{q}{q + 1}\right) \leq \frac{2^n - 1}{2^n},$$

pois

$$S(N) = 2^n \cdot m = (2^n - 1) \cdot S,$$

implica que $m \mid s = (2^n - 1) \mid 2^n$. ∎

Demonstração 2: Dickson nos dá uma prova mais simples.
A partir de $2^n \cdot m = (2^n - 1) \cdot S(m)$ observe que:

$$S(m) = \frac{2^n \cdot m}{2^n - 1} = \frac{[(2^n - 1) + 1] \cdot m}{2^n - 1} = \frac{(2^n - 1) \cdot m}{2^n - 1} + \frac{m}{2^n - 1} = m + \frac{m}{2^n - 1},$$

como m e $S(m)$ são números inteiros, $d = \dfrac{m}{2^n - 1}$ também deve ser inteiro. Assim $(2^n - 1) \mid m$ e consequentemente $d \mid m$.

Mas

$$S(m) = m + \frac{m}{2^n - 1} = m + d$$

é a soma de todos os divisores de m, como pode ser isso?
Certamente 1 divide m, por isso somos forçados a concluir que $d = 1$, pois se isso não for verdade, então teríamos $S(m) = m + d + 1$, absurdo, portanto, $m = 2^n - 1$ e, consequentemente, $2^n - 1$ é primo. ■

Demonstração 3: Esta é a prova dada por Mc Daniel.
Desde que $2^n \cdot m = (2^n - 1) \cdot S(m)$, cada divisor primo de $2^n - 1$ deve também dividir m (por ser ímpar, não divide 2^n). Então suponha que p^n divide $2^n - 1$, com p primo. Pelo Lema 2.4, temos:

$$\frac{S(m)}{m} \geq \frac{S(p^\alpha)}{p^\alpha} = \frac{1 + p + p^2 + \ldots + p^\alpha}{p^\alpha} \geq \frac{p^{\alpha-1} + p^\alpha}{p^\alpha} = 1 + \frac{1}{p} = \frac{p+1}{p}.$$

Consequentemente,

$$\begin{aligned} 1 &= \frac{S(N)}{2N} \\ &= \frac{S(2^{n-1}) \cdot S(m)}{2^n \cdot m} \\ &\geq \frac{(2^n - 1) \cdot (1 + p)}{2^n \cdot m} \\ &= \frac{2^n + 2^n \cdot p - 1 - p}{2^n \cdot m} \\ &= 1 + \frac{(2^n - 1) - p}{2^n \cdot m} \end{aligned}$$

Logo $\frac{(2^n - 1) - p}{2^n \cdot m} = 0$, então $2^n - 1 = p$, $\alpha = 1$ e $m = p$. Portanto, N é um número perfeito. ■

Demonstração 4: Prova semelhante à anterior, dada por Cohen.
Começamos, novamente, com $2^n \cdot m = (2^n - 1) \cdot S(m)$ em que $2^n - 1 \mid m$. Escrevendo $\frac{S(m)}{m} = \frac{2^n}{2^n - 1}$, temos:

$$\frac{2^n}{2^n - 1} = \frac{S(m)}{m} > \frac{S(2^n - 1)}{2^n - 1} \geq \frac{1 + 2^n - 1}{2^n - 1} = \frac{2^n}{2^n - 1}.$$

Portanto, para termos a igualdade, devemos ter: $2^n - 1 = m$ e $S(m) = 1 + (2^n - 1) = 1 + m$ e, $m = (2^n - 1)$ é primo. ■

Demonstração 5: Esta prova foi dada por Carmichael.

Tome $N = 2^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_k^{\alpha_k} = 2^{\alpha_1} \cdot \prod_{i=2}^{k} p_i^{\alpha_i}$

$$\begin{aligned}
\frac{S(N)}{2N} &= \frac{1}{2}\frac{S(2^{\alpha_1}) \cdot S(\prod_{i=2}^{k} p_i^{\alpha_i})}{(2^{\alpha_1}) \cdot \prod_i^k p_i^{\alpha_i}} \\
&= \frac{1}{2}\left(\frac{S(2^{\alpha_1})}{2^{\alpha_1}}\right) \cdot \frac{S(\prod_{i=2}^{k} p_i^{\alpha_i})}{\prod_{i=2}^{k} p_i^{\alpha_i}} \\
&= \frac{1}{2}\left(\frac{S(2^{\alpha_1})}{2^{\alpha_1}}\right) \cdot \frac{\prod_{i=1}^{k} p_i^{\alpha_i}}{\prod_{i=2}^{k} p_i^{\alpha_i}} \\
&= \frac{1}{2}\frac{2^{\alpha_1+1}-1}{(2-1)\cdot 2^{\alpha_1}} \cdot \prod_{i=2}^{k} \frac{S(p_i^{\alpha_i})}{p_i^{\alpha_i}} \\
&= \frac{2^{\alpha_1+1}-1}{2^{\alpha_1+1}} \cdot \prod_{i=2}^{k} \frac{(1+p_i+p_i^2+\ldots+p_i^{\alpha_i})}{p_i^{\alpha_i}} \\
&= \frac{2^{\alpha_1+1}-1}{2^{\alpha_1+1}} \cdot \prod_{i=2}^{k} \frac{p_i^{\alpha_{i+1}-1}}{p_i^{\alpha_i}(p_i-1)}
\end{aligned}$$

Seja $d = 2^{\alpha_1+1} - 1$, logo $2^{\alpha_1+1} = d + 1$. Substituindo, temos:

$$\frac{S(N)}{2N} = \frac{2^{\alpha_1+1}-1}{2^{\alpha_1+1}} \cdot \prod_{i=2}^{k} \frac{(p_i^{\alpha_i} + p_i^{\alpha_{i-1}} + \ldots + p_i^3 + p_i^2 + p_i)}{p_i^{\alpha_i}} = 1$$

Logo

$$\prod_{i=2}^{k} \frac{(p_i^{\alpha_i} + p_i^{\alpha_{i-1}} + \ldots + p_i^3 + p_i^2 + p_i)}{p_i^{\alpha_i}} = \frac{2^{\alpha_i+1}}{2^{\alpha_1+1}-1} = \frac{d+1}{d} = 1 + \frac{1}{d}$$

Observe que

$$S(N) = S(2^{\alpha_1} \cdot \prod_{i=2}^{k} p_i^{\alpha_i}) = S(2^{\alpha_1}) \cdot \prod_{i=2}^{k} S(p_i^{\alpha_i}) = d \cdot \prod_{i=2}^{k} S(p_i^{\alpha_i}) = 2N = 2^{\alpha_1+1} \cdot \prod_{i=2}^{k} p_i^{\alpha_i}$$

Portanto, alguns p_i devem dividir d que é impar pois, temos uma fatoração completa em fatores primos.

Assim $p_i < d$ e $1 + \dfrac{1}{p_i}$ excede a desigualdade acima de daí $p_i = d$. Porém, a partir de $k = 2$ a desigualdade é novamente ultrapassada e, portanto N é perfeito. ■

Demonstração 6: Esta é a prova de Knopfmicher.
Já vimos que

$$S(N) = 2N = 2^{\alpha_1+1} \cdot \prod_{i=2}^{k} p_i^{\alpha_i}$$

Como $2^{\alpha_1+1} - 1$ é ímpar, não divide 2, divide, então N, e podemos escrever

$$2^{\alpha_1+1} - 1 = p_2^{\gamma_2} + p_3^{\gamma_3} + p_4^{\gamma_4} + \ldots + p_k^{\gamma_k} = \prod_{i=2}^{k} p_i^{\gamma_i}$$

Daí temos

$$\frac{2N}{2^{\alpha_1+1}-1} = 2^{\alpha_1+1} \cdot \prod_{i=2}^{k} \frac{p_i^{\alpha_i}}{\prod_{i=2}^{k} p_i^{\gamma_i}} = 2^{\alpha_1+1} \cdot \prod_{i=2}^{k} p_i^{\alpha_i-\gamma_i}$$

Observe que

$$2^{\alpha_1+1} - 1 = \prod_{i=2}^{k} p_i^{\gamma_i},$$

e assim

$$2^{\alpha_1+1} = 1 + \prod_{i=2}^{k} p_i^{\gamma_i}.$$

Portanto

$$\begin{aligned} 2^{\alpha_1+1} \cdot \prod_{i=2}^{k} p_i^{\alpha_i-\gamma_i} &= (1 + \prod_{i=2}^{k} p_i^{\gamma_i}) \cdot (\prod_{i=2}^{k} p_i^{\alpha_i-\gamma_i}) \\ &= \prod_{i=2}^{k} p_i^{\alpha_i-\gamma_i} + \prod_{i=2}^{k} p_i^{\alpha_i} \\ &= (1 + p_2 + \ldots + p_2^{\alpha_2}) \ldots (1 + p_k + \ldots + p_k^{\alpha_k}) \end{aligned}$$

onde $0 \leq \gamma_i \leq \alpha_i$ para todo i.
Tomando $k = 2$ e $\alpha_2 = 1$ e comparando termo a termo os termos correspondentes $p_2^{1-\gamma_2} + p_2 = 1 + p_2$ e, então $p_2^{1-\gamma_2} = 1 = p_2^0$ nos dá $1 - \gamma_2 = 0$,logo $\gamma_2 = 1$.
Daí concluí-se que $\gamma_i = 0$ para todos os valores de i, exceto um para que N seja perfeito.
Tomando $k = 2$ e $\alpha_3 = 1$, temos $p_3^{1-\gamma_3} + p_3 = 1 + p_3$ e novamente $\gamma_3 = 1$. ■

Observação 2.9. Os números perfeitos podem ser escritos numa progressão geométrica. Eles também podem ser derivados a partir de progressões aritméticas.

$$\sum_{i=1}^{k-1} 1 + 2 + 3 + \ldots + (k-1) = \frac{1}{2} \cdot k \cdot (k-1)$$

Exemplo 2.4. $6 = 1 + 2 + 3$

$28 = 1 + 2 + 3 + 4 + 5 + 6 + 7$
$496 = 1 + 2 + 3 + \ldots + 29 + 30 + 31.$

Proposição 2.9. *Se N for um número perfeito par, então N é triangular.*

Demonstração:

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

■

Proposição 2.10. *Se $N = 2^{n-1} \cdot (2^n - 1)$, então*

$$n = 1^3 + 3^3 + 5^3 + \ldots + (2m-1)^3,$$

com $m = 2^{\frac{n-1}{2}}$.

Demonstração: Observe que

$$\sum_{i=1}^{m} i^3 = \frac{m^2 \cdot (m+1)^2}{4}.$$

Basta escolher $m = 2^{\frac{n-1}{2}}$. De fato,

$$\begin{aligned} \sum_{i=1}^{m} i^3 &= 1^3 + 2^3 + \ldots + m^3 \\ &= 1^3 + 3^3 + 5^3 + \ldots + (2m-1)^3 + 2^3 + 4^3 + \ldots + (2m)^3. \end{aligned}$$

Então

$$\begin{aligned} 1^3 + 3^3 + 5^3 + \ldots + (2m-1)^3 &= [1^3 + 2^3 + 3^3 + \ldots + (2m-1)^3 + (2m)^3] \\ &\quad -[2^3 + 4^3 + 6^3 + \ldots + (2m)^3] \\ &= 1^3 + 2^3 + 3^3 + \ldots + (2m-1)^3 \\ &\quad +(2m)^3 - 2^3 \cdot (1^3 + 2^3 + 3^3 + \ldots + m^3) \\ &= \frac{(2m)^2(2m+1)^2}{4} - 8 \cdot \frac{m^2(m+1)^2}{4} \\ &= m^2 \cdot (2m^2 - 1). \end{aligned}$$

Logo

$$\begin{aligned} 1^3 + 3^3 + 5^3 + \ldots + (2 \cdot 2^{\frac{n-1}{2}} - 1)^3 &= \left(2^{\frac{n-1}{2}}\right)^2 \cdot \left[2 \cdot \left(2^{\frac{n-1}{2}}\right)^2 - 1\right] \\ &= 2^{n-1} \cdot (2 \cdot 2^{n-1} - 1) \\ &= 2^{n-1} \cdot (2^n - 1) = N. \end{aligned}$$

■

Capítulo 3

História e conjecturas

Apresentamos neste capítulo alguns aspectos históricos pitorescos e algumas conjecturas à respeito dos Números Primos, Primos de Mersenne e Números Perfeitos, nomeando cronologicamente os matemáticos que se interessaram pelo estudo dos Números Perfeitos.

Tales de Mileto (640 – 546 AC) introduziu o estudo da matemática na Grécia. Ele levou para a Grécia os rudimentos de geometria e da aritmética que aprendera com os sacerdotes egípcios, iniciando então uma intensa atividade matemática que ali se desenvolveu por mais de cinco séculos.

Os gregos deram à matemática um caráter científico, devido à atitude filosófica e especulativa que eles tinham em relação à vida.

Com Pitágoras de Samos (580 – 500 AC) através da escola pitagórica criada por ele e seus seguidores, que deram um caráter místico aos números, adotando a aritmética como fundamento de sua filosofia. Sobre esta escola, que apesar de durar vários séculos, poucos fragmentos dos escritos originais chegaram até nós por referências e comentários de matemáticos posteriores.

Por volta de 300 AC, em Alexandria, um tratado que se tornaria um dos marcos mais importantes da matemática surgia através da obra escrita pelo matemático grego Euclides (330 – 260 AC): Os Elementos.

Os Elementos de Euclides é considerado um tratado, por conter sistematicamente, todo o conhecimento matemático de sua época. Essa obra é composta por treze livros, dos quais três versam sobre a aritmética e dez sobre a geometria, chamada de Euclidiana.

Euclides, aparentemente não criou muitos resultados, mas teve o mérito de estabelecer um padrão de apresentação e rigor na matemática, jamais alcançado anteriormente.

Nos três livros referentes à aritmética, livros VII, VIII e IX, Euclides desenvolve a

teoria dos números naturais. No livro VII, são definidos conceitos de divisibilidade, de número primo, de números perfeitos, de máximo divisor comum e de mínimo múltiplo comum entre outros. Neste livro encontra-se, sem demonstração, a divisão Euclidiana com resto, através do uso iterado dessa divisão, Euclides estabelece o algoritmo que leva o seu nome e que é o método mais eficiente, até hoje conhecido, para o cálculo do máximo divisor comum de dois números naturais (Proposição 1 e 2 nos Elementos). No livro VIII, são estudadas propriedades de sequências de números em progressão. No livro IX, Euclides de maneira magistral nos mostra que a quantidade de números primos supera qualquer números dado, isto é, existem infinitos números primos (Proposição 20 nos Elementos). Nesse livro também se encontra o Teorema Fundamental da Aritmética (Proposição 14 nos Elementos).

Euclides também apresenta uma condição necessária para que um número natural seja perfeito (Proposição 35 nos Elementos).

Após a era de Euclides, a aritmética estagnou por cinco séculos, voltando a tona com os trabalhos de Diofanto de Alexandria, por volta de 250 DC.

Diofanto nos legou uma obra chamada Aritmética, escrita em treze volumes dos quais chegaram até nós apenas sete, com temas que, apesar de importantes, não vêm ao caso.

No período da renascença, movimento ocorrido entre os séculos XIII e XV na Europa, e que revolucionou as artes, as ciências e até os costumes, teve como uma de suas consequências, o renascimento da aritmética.

Este movimento atingiu a matemática um pouco mais tardialmente. Em 1575, através de Regiomanto que traduziu para o latim, o tratado Aritmética, de Diofanto. Em 1621, Bachet de Méziriac publicou uma edição francesa que possibilitou esse conhecimento a muitos matemáticos franceses, entre os quais convém destacar Pierre de Fermat (1601 – 1665), jurista Francês.

Nessa época, era comum os matemáticos divulgarem os resultados obtidos, lançando-os como desafio aos outros. Padre Marin Mersenne, que desenpenhava o papel de divulgador da matemática. Em uma de suas cartas de 1640, Fermat enuciou o seu pequeno teorema, dizendo que não escreveria a demonstração por ser longa demais.

Um problema cuja solução há muito era procurada pelos matemáticos é a fórmula para a determinação de todos os números primos. Fermat morreu com a convicção de que a expressão $2^{2^n} + 1$ representa um número primo (conjectura). Essa conjectura revelou-se posteriormente falsa para $n = 5$ através do matemático francês Leonhard Euler (1707 – 1783), que provou todos os resultados de Fermat, exceto, obviamente, o último teorema de Fermat.

Pelo Exposto até agora, muitos dos teoremas básicos da aritmética estancam na

investigação dos gregos acerca dos números perfeitos e pitagóricos. Aliás, foi através de Fermat, autor do mais antigo projeto (Teorema de Fermat), que a aritmética se desenvolveu.

Nesse trabalho nos importamos com os números perfeitos que proporcionam muitos aspectos pitorescos no desenvolvimento da teoria dos números.

A relação quase mística dos números perfeitos é tão antiga quanto à matemática em relação a eles. Os pitagóricos associaram o número perfeito seis ao casamento, à saúde e à beleza por conta da integridade e da concordância de suas partes.

Os matemáticos da Antiguidade fizeram várias afirmações sobre os números perfeitos baseados nos quatro que conheciam, mas a maior parte delas vieram a provar-se serem falsas. Uma dessas afirmações era que como $2, 3, 5$, e 7 são precisamente os quatro primeiros primos, o quinto número perfeito seria obtido com $n = 11$, que é o quinto primo. Todavia, $2^{11} - 1 = 2047 = 23 \times 89$ não é primo e daí $n = 11$ não gera um número perfeito.

Duas outras falsas afirmações são:

- O quinto número perfeito teria cinco algarismos pois os primeiros quatro têm, respectivamente, $1, 2, 3$, e 4 algarismos.

- Os números perfeitos alternam 6 e 8 no último algarismo. O quinto número perfeito ($33.550.336 = 2^{12}(2^{13} - 1)$) tem 8 algarismos, contrariando a primeira afirmação. Como termina em 6, a segunda afirmação parecia não ser falsa. Todavia, o sexto número perfeito (8.589.869.056) também termina em 6. É fácil provar que o último algarismo de um número perfeito par é sempre 6 ou 8.

Em meados do ano 100 DC, Nicômaco observou que números perfeitos atingem uma harmonia entre os extremos de excesso e deficiência. Observe que os números perfeitos 6, 28, 496 e 8128 são os único perfeitos no intervalo 1, 10, 100, 1000 e 10000 e eles terminam alternadamente em 6 e 8. No final do século XII, o rabino Josef B. Jehuda Ankin sugeriu que o estudo cuidadoso dos números perfeitos fosse uma parte essencial para a cura da alma. Erycius Puteanus em 1640 desenvolveu um trabalho atribuindo ao número perfeito e a Vênus, formada a partir da tríade (maculino, ímpar) e da dupla (feminino, par). Hrotsvit, uma beneditina de um convento da Saxônia listou os quatro primeiros números perfeitos em sua peça literária (Poesia) Sapietia no século X.

Santo Agostinho (entre outros, incluindo os antigos Hebreus) considerou 6 um número verdadeiramente perfeito, Deus fez a terra em exatamente esta quantidade de dias para significar a perfeição de sua obra.

Alcuino de York (732 – 804 DC) registrou que a segunda origem foi imperfeita como a que surgiu a partir do número deficiente 8 que é maior do que a soma dos seus

divisores próprios, significando as oito almas na arca de Noé (Noé, seus três filhos e suas quatro esposas conforme o livro de Gênesis, capítulo 7 sobre o surgimento da raça humana atual.

Philo, judeus no primeiro século da era cristã, chamava o número 6 de o mais produtivo de todos os números, sendo o menor número perfeito. Ao longo dos séculos que se seguiram, vários matemáticos cuidadosamente estudaram os números perfeitos.

Como vimos até o tempo de Descartes e Fermat, vários resultados importantes bem como mal interpretados tinham sido escritos.

3.1 Primos de Mersenne

Para que $2^n - 1$ seja primo, é necessário, mas não suficiente, que n seja primo. Os primos da forma $2^n - 1$ são conhecidos como primos de Mersenne, em honra ao monge, filósofo e matemático francés Marin Mersenne, que os estudou em 1644 junto com a teoria dos números e as propriedades dos números perfeitos.

Um milênio depois de Euclides, Ibn al-Haytham (Alhazen), por volta do ano 1000 percebeu que todo o número perfeito par é da forma $2^{n-1}(2^n - 1)$, onde $2^n - 1$ é um número primo, mas não conseguiu provar o resultado. Só no século XVIII, Leonhard Euler provou que a fórmula $2^{n-1}(2^n - 1)$ daria todos os números perfeitos pares. Portanto, todo primo de Mersenne gera um diferente número perfeito par, numa correspondência unívoca entre ambos os conjuntos. Este resultado é muitas vezes referido como o "teorema de Euclides-Euler".

À data de Setembro de 2009, eram conhecidos 47 primos de Mersenne, o que significa que há 47 números perfeitos pares conhecidos, sendo o maior $2^{43.112.608} \times (2^{43.112.609} - 1)$, um enorme número com 25.956.377 algarismos.

Os primeiros 39 números perfeitos pares são da forma $2^{n-1}(2^n - 1)$ para $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917$ (seqüência A000043 na OEIS).

Os outros oito conhecidos são para $n = 20996011, 24036583, 25964951, 30402457, 32582657, 37156667, 42643801, 43112609$. Não se sabe se há outros algures neste intervalo.

Encontrar números perfeitos pares ainda reduz-se simplesmente a encontrar números da forma $2^n - 1$, onde n é um número primo. Existem 47 números primos perfeitos de Mersenne, resumidos na tabela abaixo.

ordem	p	dígitos	ano	referência ao descobridor
1	2	1	antiguidade	
2	3	1	antiguidade	
3	5	2	antiguidade	
4	7	3	antiguidade	
5	13	4	1461	Reguis (1536), Cataldi (1603)
6	17	6	1588	Cataldi (1603)
7	19	6	1588	Cataldi (1603)
8	31	10	1750	Euler (1772)
9	61	19	1883	Pervouchine (1883), Seelhoff (1886)
10	89	27	1911	Powers (1911)
11	107	33	1913	Powers (1914)
12	127	39	1876	Lucas (1876)
13	521	157	Jan. 30, 1952	Robinson
14	607	183	Jan. 30, 1952	Robinson
15	1279	386	Jan. 30, 1952	Robinson
16	2203	664	Jan. 30, 1952	Robinson
17	2281	687	Jan. 30, 1952	Robinson
18	3217	969	Set. 8, 1957	Riesel
19	4253	1281	Nov. 3, 1961	Hurwitz
20	4423	1332	Nov. 3, 1961	Hurwitz
21	9689	2917	Mai 11, 1963	Gillies (1964)
22	9941	2993	Mai 11, 1963	Gillies (1964)
23	11213	3376	Jun. 2, 1963	Gillies (1964)
24	19937	6002	Mar. 4, 1971	Tuckerman (1971)
25	21701	6533	Out. 30, 1978	Noll and Nickel (1980)
26	23209	6987	Fev. 9, 1979	Noll (Noll & Nickel 1980)
27	44497	13395	Abr. 8, 1979	Nelson & Slowinski (Slowinski 1978-79)
28	86243	25962	Set. 25, 1982	Slowinski
29	11003	33265	Jan. 28, 1988	Colquitt & Welsh (1991)
30	132049	39751	Set. 20, 1983	Slowinski
31	216091	65050	Set. 6, 1985	Slowinski
32	756839	227832	Fev. 19, 1992	Slowinski & Gage
33	859433	258716	Jan. 10, 1994	Slowinski & Gage
34	1.257.787	378632	Set. 3, 1996	Slowinski & Gage
35	1.398.269	420921	Nov. 12, 1996	Joel Armengaud/GIMPS

36	2.976.221	895832	Ago. 24, 1997	Gordon Spence/GIMPS (Devlin 1997)
37	3.021.377	909526	Jan. 27, 1998	Roland Clarkson/GIMPS
38	6.972.593	2098960	Jun. 1, 1999	Nayan Hajratwala/GIMPS
39	13.466.917	4053946	Nov. 14, 2001	Michael Cameron/GIMPS
40	20.996.011	6320430	Nov. 17, 2003	Michael Shafer/GIMPS (Weisstein 2003)
41	24.036.583	7235733	Mai 15, 2004	Josh Findley/GIMPS (Weisstein 2004)
42	25.964.951	7816230	Fev. 18, 2005	Martin Nowak/GIMPS (Weisstein 2005)
43	30.402.457	9152052	Dez 15, 2005	Dr. Curtis Cooper e Dr. Steven Boone
44	32.582.657	9808358	Set. 4, 2006	Dr. Curtis Cooper e Dr. Steven Boone
45	37.156.667	11.185.272	Set. 6, 2008	GIMPS / Hans-Michael Elvenich
46	43.112.609	12.978.189	Ago. 23, 2008	GIMPS / Edson Smith
47	42.643.801	12.837.064	Abr. 12, 2009	GIMPS / Odd Magnar Strindmo

Com cada um desses primos, há uma história que se passa com a sua descoberta. Por exemplo, Peter Barlow em sua Teoria dos Números publicados em 1811, escreveu sobre o oitavo número perfeito: "É o maior que será descoberto, pois, como eles são meramente curiosos sem ser úteis, não é provável que qualquer pessoa irá tentar encontrar um mais além.

Os primos de Mersenne parecem ser distribuídos regularmente em grandes estimativas (ou seja, dentro de milhares de ordens de magnitude) pode ser dado [15], mas, em última análise, esses números devem ser checados um por um. Fechamos com um resultado interessante:

3.2 Conjectura Cunningham

Se $p = 2^x \pm 1$ ou $2^x \pm 3$ é primo, $p \equiv 3 \bmod 4$, e $2p+1$ é primo, então $2^p - 1$ é primo.

Todos conhecidos e conjecturados primos $2^p - 1$, com p primo, estão abrangidos por esta regra.

3.3 Conjectura de Goldbach

Goldbach escreveu uma carta para Euler em 1742 sugerindo que todo número inteiro $n > 5$ fosse a soma de três números primos. Euler respondeu dizendo que era equivalente a dizer que todo inteiro par $n > 2$ fosse a soma de dois números primos. Esta, assim formulada, passou a ser a chamada "'*Conjectura de Goldbach*".

$4 = 2 + 2$ $12 = 7 + 5$

$6 = 3 + 3$ $14 = 11 + 3$

$8 = 5 + 3$ $16 = 13 + 3$

$10 = 7 + 3$ $18 = 13 + 5$

3.3.1 Relação dos primeiros 1000 primos positivos, destacados os gêmeos

2, **3, 5, 7, 11, 13, 17, 19,** 23, **29, 31,** 37, **41, 43,** 47, 53, **59, 61,** 67, **71, 73,** 79, 83, 89, 97, **101, 103, 107, 109,** 113, 127, 131, **137, 139, 149, 151,** 157, 163, 167, 173,**179, 181, 191, 193, 197, 199,** 211, 223, **227, 229**, 233, 239, 241, 251, 257, 263,**269, 271,** 277, **281, 283,** 293, 307, **311, 313,** 317, 331, 337, **347, 349,** 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, **419, 421, 431, 433,** 439, 443, 449, 457, **461, 463,** 467, 479, 487, 491, 499, 503, 509, **521, 523**, 541, 547, 557, 563, **569, 571**, 577, 587, 593, **599, 601**, 607, 613, **617, 619**, 631, **641, 643**, 647, 653, **659, 661**, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, **809, 811,821, 823, 827, 829**, 839, 853, **857, 859**, 863, 877, **881, 883**, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997, 1009, 1013, **1019, 1021, 1031,1033**, 1039, **1049, 1051, 1061, 1063**, 1069, 1087, **1091, 1093**, 1097, 1103, 1109, 1117, 1123, 1129, **1151, 1153**, 1163, 1171, 1181, 1187, 1193, 1201, 1213, 1217, 1223,**1229, 1231**, 1237, 1249, 1259, **1277, 1279**, 1283, **1289, 1291**, 1297, **1301, 1303**,1307, **1319, 1321**, 1327, 1361, 1367, 1373, 1381, 1399, 1409, 1423, **1427, 1429**,1433, 1439, 1447,**1451, 1453**, 1459, 1471, **1481, 1483, 1487, 1489**, 1493, 1499, 1511, 1523, 1531, 1543, 1549, 1553, 1559, 1567, 1571, 1579, 1583, 1597, 1601, 1607, 1609, 1613, **1619, 1621**, 1627, 1637, 1657, 1663, **1667, 1669**, 1693, **1697, 1699**,1709, **1721, 1723**, 1733, 1741, 1747, 1753, 1759, 1777, 1783, **1787, 1789**, 1801, 1811, 1823, 1831, 1847, 1861, 1867, **1871, 1873, 1877, 1879**, 1889, 1901, 1907, 1913, **1931, 1933, 1949, 1951**, 1973, 1979, 1987, 1993, **1997, 1999**, 2003, 2011, 2017, **2027, 2029**, 2039, 2053, 2063, 2069, **2081, 2083, 2087, 2089**, 2099, **2111,2113**, 2129, 2131, 2137, **2141, 2143**, 2153, 2161, 2179, 2203, 2207, 2213, 2221,**2237, 2239**, 2243, 2251, **2267, 2269**, 2273, 2281, 2287, 2293, 2297, **2309, 2311**,2333, **2339, 2341**, 2347, 2351, 2357, 2371, 2377, **2381, 2383**, 2389, 2393, 2399, 2411, 2417, 2423, 2437, 2441, 2447, 2459, 2467, 2473, 2477, 2503, 2521, 2531, 2539, 2543, **2549, 2551**, 2557, 2579, 2591, 2593, 2609, 2617, 2621, 2633, 2647, **2657,2659**, 2663, 2671, 2677, 2683, 2687, 2689, 2693, 2699, 2707, **2711, 2713**, 2719, 2729, 2731, 2741, 2749, 2753, 2767, 2777, **2789, 2791**, 2797, **2801, 2803**, 2819, 2833, 2837, 2843, 2851, 2857, 2861, 2879, 2887, 2897, 2903, 2909, 2917, 2927, 2939, 2953, 2957, 2963, **2969, 2971, 2999, 3001**, 3011, 3019, 3023, 3037, 3041, 3049, 3061, 3067, 3079, 3083, 3089, 3109, **3119, 3121**, 3137, 3163, **3167, 3169**,

3181, 3187, 3191, 3203, 3209, 3217, 3221, 3229, **3251, 3253, 3257, 3259**, 3271, 3299, 3301, 3307, 3313, 3319, 3323, 3329, 3331, 3343, 3347, **3359, 3361, 3371, 3373, 3389,3391**, 3407, 3413, 3433, 3449, 3457, **3461, 3463, 3467, 3469**, 3491, 3499, 3511, 3517, **3527, 3529**, 3533, 3539, 3541, 3547, **3557, 3559**, 3571, **3581, 3583**, 3593, 3607, 3613, 3617, 3623, 3631, 3637, 3643, 3659, **3671, 3673**, 3677, 3691, 3697, 3701, 3709, 3719, 3727, 3733, 3739, 3761, **3767, 3769**, 3779, 3793, 3797, 3803, **3821,3823**, 3833, 3847, **3851, 3853**, 3863, 3877, 3881, 3889, 3907, 3911, **3917, 3919**,3923, **3929, 3931**, 3943, 3947, 3967, 3989, **4001, 4003**, 4007, 4013, **4019, 4021**,4027, **4049, 4051**, 4057, 4073, 4079, **4091, 4093**, 4099, 4111, **4127, 4129**, 4133, 4139, 4153, **4157, 4159**, 4177, 4201, 4211, **4217, 4219, 4229, 4231, 4241, 4243**,4253, **4259, 4261, 4271, 4273**, 4283, 4289, 4297, 4327, **4337, 4339**, 4349, 4357, 4363, 4373, 4391, 4397, 4409, **4421, 4423**, 4441, 4447, 4451, 4457, 4463, **4481,4483**, 4493, 4507, 4513, **4517, 4519**, 4523, **4547, 4549**, 4561, 4567, 4583, 4591, 4597, 4603, 4621, **4637, 4639**, 4643, **4649, 4651**, 4657, 4663, 4673, 4679, 4691, 4703, **4721, 4723**, 4729, 4733, 4751, 4759, 4783, **4787, 4789**, 4793, 4799, 4801, 4813, 4817, 4831, 4861, 4871, 4877, 4889, 4903, 4909, 4919,**4931, 4933**, 4937, 4943, 4951, 4957, 4967, 4969, 4973, 4987, 4993, 4999, 5003, **5009, 5011, 5021, 5023**,5039, 5051, 5059, 5077, 5081,**5087, 5099**, 5101, 5107, 5113, 5119, 5147, 5153, 5167, 5171, 5179, 5189, 5197, 5209, 5227,**5231, 5233**, 5237, 5261, 5273, **5279, 5281**,5297, 5303, 5309, 5323, 5333, 5347, 5351, 5381, 5387, 5393, 5399, 5407, 5413, **5417,5419**, 5431, 5437, **5441, 5443**, 5449, 5471, **5477, 5479**, 5483, **5501, 5503**, 5507, 5519, 5521, 5527, 5531, 5557, 5563, 5569, 5573, 5581, 5591, 5623, **5639, 5641**, 5647,**5651, 5653, 5657, 5659**, 5669, 5683, 5689, 5693, 5701, 5711, 5717, 5737, **5741**,5743, 5749, 5779, 5783, 5791, 5801, 5807, 5813, 5821, 5827, 5839, 5843, **5849, 5851**,5857, 5861, **5867, 5869, 5879, 5881**, 5897, 5903, 5923, 5927, 5939, 5953, 5981, 5987, 6007, 6011, 6029, 6037, 6043, 6047, 6053, 6067, 6073, 6079, 6089, 6091, 6101, 6113, 6121, **6131, 6133**, 6143, 6151, 6163, 6173, **6197, 6199**, 6203, 6211, 6217, 6221, 6229, 6247, 6257, 6263, **6269, 6271**, 6277, 6287, **6299, 6301**, 6311, 6317, 6323, 6329, 6337, 6343, 6353, **6359, 6361**, 6367, 6373, 6379, 6389, 6397, 6421, 6427,**6449, 6451**, 6469, 6473, 6481, 6491, 6521, 6529, 6547,**6551, 6553,** 6563, **6569,6571,** 6577, 6581, 6599, 6607, 6619, 6637, 6653, **6659, 6661,** 6673, 6679, **6689,6691, 6701, 6703,** 6709, 6719, 6733, 6737, **6761, 6763, 6779, 6781, 6791, 6793,**6803, 6823, **6827, 6829,** 6833, 6841, 6857, 6863, **6869, 6871,** 6883, 6899, 6907, 6911, 6917, **6947, 6949, 6959, 6961,** 6967, 6971, 6977, 6983, 6991, 6997, 7001, 7013, 7019, 7027, 7039, 7043, 7057, 7069, 7079, 7103, 7109, 7121, **7127, 7129,** 7151, 7159, 7177, 7187, 7193, 7207, **7211, 7213,** 7219, 7229, 7237, 7243, 7247, 7253, 7283, 7297, **7307, 7309,** 7321, **7331, 7333, 7349, 7351,** 7369, 7393, 7411, 7417, 7433, 7451, 7457, 7459, 7477, 7481,**7487, 7489,** 7499, 7507, 7517, 7523, 7529, 7537, 7541, **7547, 7549, 7559, 7561,** 7573, 7577, 7583,

7589, 7591, 7603, 7607, 7621, 7639, 7643, 7649, 7669, 7673, 7681, 7687, 7691, 7699, 7703, 7717, 7723, 7727, 7741, 7753,**7757, 7759,** 7789, 7793, 7817, 7823, 7829, 7841, 7853, 7867, 7873, **7877, 7879,**7883, 7901, 7907, 7919

Um pouco mais de sabor à sua curiosidade, The Electronic Frontier Foundation oferece um prêmio de US$100.000,00 à primeira pessoa ou ao grupo que descobrir um número primo de 10 milhões de casas decimais. O número de dígitos D de um número de Mersenne é dado por:

$$D = [\log(2^n - 1) + 1]$$

onde a função $[x]$ define o maior inteiro menor ou igual a x.

$$[45,678] = 45 \qquad\qquad [-8,250] = -9$$

$$[301] = 301$$

Referências Bibliográficas

[1] A. Hefez, *Elementos de Aritmética*. Textos Universitários, SBM, 2010.

[2] David Burton, *Elementary number theory*, 2010.

[3] Gareth A. Jones - J. Mary Jones, *Elementary number theory*. Springer Undergraduate Mathematics, 1998.

[4] Underwood Dudley, *Elementary number theory*, 2012.

[5] Willian Dunham, *Euler The Master of Us All*. The Mathematical Association of America, 1999.