Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Geociências e Ciências Exatas
Campus de Rio Claro

Números Primos e Divisibilidade: Estudo de Propriedades

Cristina Helena Bovo Batista Dias

Dissertação apresentada ao Programa de Pós-Graduação – Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) como requisito parcial para a obtenção do grau de Mestre

Orientadora
Profa. Dra. Eliris Cristina Rizziolli

2013

512.7 Dias, Cristina Helena Bovo Batista
D541n Números Primos e Divisibilidade: Estudo de Propriedades/ Cristina Helena Bovo Batista Dias. - Rio Claro: [s.n.], 2013.
49 f.: tab.

Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas.
Orientadora: Eliris Cristina Rizziolli

1. Teoria dos Números. 2. Conjetura de Goldbach. 3. Números Inteiros. 4. Fatoriais. I. Título

Ficha Catalográfica elaborada pela STATI - Biblioteca da UNESP
Campus de Rio Claro/SP

TERMO DE APROVAÇÃO

Cristina Helena Bovo Batista Dias

Números Primos e Divisibilidade: Estudo de Propriedades

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), pela seguinte banca examinadora:

Profa. Dra. Eliris Cristina Rizziolli
Orientadora

Prof. Dr. Aldicio José Miranda
Dpto. Matemática UNIFAL-Alfenas/MG

Prof. Dr. Thiago de Melo
Dpto. Matemática UNESP-Rio Claro/SP

Rio Claro, 28 de janeiro de 2013

Ao meu Deus, Jeová, aos meus pais,
ao meu querido esposo e aos meus filhos, à minha mãe e irmãos

Agradecimentos

Primeiramente, agradeço a Deus pela vida. A seguir, à minha orientadora, Eliris, aos membros da banca e, de modo geral, a todos os docentes e funcionários do Departamento de Matemática do IGCE, Rio Claro, por sua valiosa colaboração e apoio, sem os quais este trabalho não teria sido realizado. Em especial, agradeço ao Prof. Dr. Henrique Lazari e ao Prof. Dr. Rômulo Campos Lins, por sua ajuda na elaboração do Capítulo 5 desta dissertação. Agradeço, ainda, aos funcionários da UNESP, em especial, os que trabalham na Biblioteca, no Restaurante Universitário e na Cantina que, dos bastidores, dão suporte para que trabalhos como este sejam produzidos. Finalmente, agradeço a meus pais, ao meu esposo e aos meus filhos, e a todos meus familiares, amigos e irmãos.

Resumo

O objetivo deste trabalho é apresentar os fundamentos da divisibilidade, estudar as propriedades dos números primos, sua associação com fatoriais e com progressões aritméticas, além de apresentar alguns resultados equivalentes à Conjetura de Goldbach.

Palavras-chave: Teoria dos Números, Conjetura de Goldbach, Números Inteiros, Fatoriais.

Abstract

The objective of this paper is to present the fundamentals of divisibility, study the properties of prime numbers, their association with factorials and arithmetic progressions, and present some results equivalent to Goldbach's Conjecture.

Keywords: Number Theory, Goldbach's Conjecture, Integer Numbers, Factorial.

Lista de Tabelas

Sumário

1 Introdução

Este trabalho tem por objetivo analisar algumas das propriedades dos chamados números primos. Um número primo é aquele que somente é divisível por um ou por si mesmo. Um número inteiro n é divisível por um número inteiro m quando existe um inteiro q tal que $n = qm$.

Desde da Grécia Antiga os matemáticos se interessam pelos números primos: Quantos são? Como se distribuem? Como encontrá-los? Existe uma maneira simples de saber se um número é primo ou não? No decorrer dos séculos algumas destas perguntas foram respondidas, outras ainda permanecem sem resposta até os dias atuais.

Algumas afirmações sobre os números primos foram comprovadas há muitos séculos. O famoso matemático Euclides demonstrou que existem infinitos números primos. O matemático Eratóstenes inventou um método, conhecido como Crivo de Eratóstenes, para montar uma lista de primos até um determinado número. No entanto, ao passo que o número de elementos da lista aumenta, seu método se torna cada vez mais trabalhoso.

Por outro lado, outras afirmações envolvendo os números primos ainda não foram demonstradas. Por exemplo, até hoje não se sabe como os números primos se distribuem entre os números compostos (os que não são primos), nem como descobrir, de maneira simples, se um número é primo ou não. Por causa da dificuldade na identificação de um número primo, sistemas de segurança online têm utilizado, durante décadas, números primos para proteger senhas e outras informações pessoais daqueles que navegam pela internet.

Outra questão curiosa é sobre com que frequência um número primo aparece. Quando se observa uma lista de primos se nota, num breve olhar, que existem diversos pares de números primos que diferem por apenas duas unidades, tais como 3 e 5, 5 e 7, 11 e 13, 17 e 19, entre outros. Tais primos são chamados primos gêmeos e, até hoje, não se sabe se existem infinitos pares de primos gêmeos ou não.

Ainda sobre este tópico, por volta de 1900, J. Hadamard e Ch. de la Valleè-Poussin, provaram, trabalhando independentemente, um resultado sobre a frequência dos primos conhecido como Teorema dos Números Primos. A demonstração de tal Teorema foi simplificada em 1949 por A. Selberg. No entanto, a distribuição dos números primos ainda é bastante misteriosa e existem inúmeros problemas associados a ela aguardando

uma demonstração. Apresenta-se abaixo alguns dos mais famosos:

1. Existem infinitos primos gêmeos, ou seja, existem infinitos pares de números primos que diferem por apenas duas unidades?
2. Sempre existe um primo entre n^2 e $(n+1)^2$ para todo natural $n > 0$?
3. A sequência de Ficonacci $(1, 1, 2, 3, 5, 8, 13, ...)$ contém infinitos números primos?
4. Existem infinitos primos da forma $n^2 - n + 41$?
5. É verdade que, para todo $k \geq 4$, existe uma infinidade de progressões aritméticas constituídas por k números primos?

Os dois problemas mais famosos relacionados aos números primos e ainda em abertos são a Conjetura de Goldbach e a Hipótese de Riemman. A Conjetura de Goldbach relaciona-se a uma carta que o matemático Christian Goldbach escreveu a Leonhard Euler, em 1742, afirmando que todo número natural par, maior ou igual a quatro, pode ser escrito como a soma de dois números primos. Ivan Vinogradov, em 1937, demonstrou uma variante mais fraca desta conjetura, a saber, que todo número ímpar suficientemente grande pode ser escrito como a soma de três primos. A Conjetura de Goldbach, no entanto, permanece sem demonstração até hoje. O melhor resultado relacionado à conjetura de Goldbach foi obtido por Chen que demonstrou que todo número par, suficientemente grande, pode ser escrito como a soma de um primo com um 2-quase-primo. Um número 2-quase-primo é um número da forma $p_2 = p.q$, onde p e q são primos. Esse resultado é conhecido como Teorema de Chen.

Por sua vez, a Hipótese de Riemman é o maior problema matemático de todos os tempos e, resumidamente, consiste em demonstrar que todos os zeros não triviais da função zeta de Riemann encontram-se sobre uma determinada reta. Tal hipótese ainda permanece sem demonstração. Tão cedo quanto em 1900 foi oferecido um prêmio em dinheiro para quem a demonstrasse e muitos resultados importantes da Matemática dependem de sua veracidade. Trabalhar com estas importantes questões foi a motivação principal deste estudo.

Este trabalho está dividido em seis capítulos:

- Capítulo 1: Motivação histórica e resumo.
- Capítulo 2: Fundamentos da divisibilidade e conceitos ligados a ela.
- Capítulo 3: Números primos e suas propriedades básicas.
- Capítulo 4: Aplicações dos números primos em outros ramos da Matemática,
- Capítulo 5: Resultados relacionados à Conjetura de Goldbach e,
- Capítulo 6: Sugestão para Aplicação em Sala de Aula.

2 Números Inteiros e Divisibilidade

A linha da Matemática que estuda os números naturais é conhecida como aritmética. Os números naturais são os que aparecem naturalmente no dia a dia das pessoas e são conhecidos como $0, 1, 2, 3, 4, 5, ...$ Estes números foram reunidos em um conjunto a que os matemáticos chamam de $\mathbb{N}$. Estão definidas sobre este conjunto as operações adição $(+)$ e multiplicação $(.)$, que possuem às seguintes propriedades:

1. São bem definidas, ou seja, para todos a,b,a' e $b' \in \mathbb{N}$, se $a = b$ e $a' = b'$ então $a + b = a' + b'$ e $a \cdot b = a' \cdot b'$,
2. São comutativas, ou seja, para todos $a, b \in \mathbb{N}$ tem-se que $a+b = b+a$ e $a \cdot b = b \cdot a$,
3. São associativas, ou seja, para todos $a, b \in \mathbb{N}$ tem-se que $a + (b + c) = (a + b) + c$ e $a.(b.c) = (a.b).c$,
4. Possuem elementos neutros, ou seja, para todo $a \in \mathbb{N}$, $a + 0 = a$ e $a \cdot 1 = a$,
5. A multiplicação é distributiva com relação à adição, ou seja, para todos $a, b, c \in \mathbb{N}$ tem-se $a \cdot (b + c) = (a + b) \cdot (a + c)$.

Considera-se ainda que os números naturais possuem as seguintes propriedades:

6. Integridade, ou seja, dados $a, b \in \mathbb{N}$, com a, b diferentes de zero, tem-se que $a \cdot b$ é diferente de zero.

   De maneira equivalente pode-se dizer que se $a \cdot b = 0$ então $a = 0$ ou $b = 0$
7. Tricotomia: Dados $a, b \in \mathbb{N}$ se verifica apenas uma das seguintes possibilidades:

   (a) $a = b$

   (b) existe $c \in \mathbb{N}$, com $c \neq 0, b = a + c$, ou

   (c) existe $c \in \mathbb{N}$, com $c \neq 0, a = b + c$

Diz-se que a é menor do que b, e simboliza-se por $a < b$, sempre que se verifica a propriedade (b). Diz-se que a é maior do que b, e simboliza-se por $a > b$, sempre que se

verifica a propriedade (c). Adicionalmente, conclui-se, das definições acima, que $0 < a$, para todo $a \geq 1$, pois tem-se que $0 + a = a$, o que implica que $0 < a$.

Note ainda que, para a e b, números naturais, se $a + b = 0$ então, $a = b = 0$. Realmente, se $a \neq 0$ tem-se que $b < 0$, o que é absurdo. Portanto, $a = 0$. De maneira similar mostra-se que $b = 0$. Logo, se $a > 0$ ou $b > 0$ então $a + b > 0$.

Proposição 2.1. *Para todo $a \in \mathbb{N}$ tem-se que $a \cdot 0 = 0$.*

Demonstração. De fato, $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$. Se $a \cdot 0 > 0$ então, da afirmação anterior, segue que $a \cdot 0 > a \cdot 0$, o que é absurdo. Logo $a \cdot 0 = 0$. □

Proposição 2.2. *No que se refere à relação "menor do que" vale a lei do cancelamento para a adição, ou seja, para todo $a, b, c \in \mathbb{N}, a < b$ se, e somente se, $a + c < b + c$.*

Demonstração. Suponha $a < b$. Isso significa que existe $d > 0$, tal que $b = a + d$. Somando c a ambos os lados desta igualdade tem-se, pelas propriedades da adição:

$$b + c = c + b = c + (a + d) = (c + a) + d = (a + c) + d,$$

o que mostra que $a + c < b + c$. □

Proposição 2.3. *No que se refere à relação "menor do que" vale a lei do cancelamento para a multiplicação, ou seja, para todo $a, b, c \in \mathbb{N}$, com $c \neq 0$, tem-se que $a < b$ se, e somente se, $a \cdot c < b \cdot c$.*

Demonstração. Suponha $a < b$. Isso significa que existe $d > 0$, tal que $b = a + d$. Somando c a ambos os lados desta igualdade tem-se, pelas propriedades da adição e da multiplicação:

$$b \cdot c = c \cdot b = c \cdot (a + d) = (c \cdot a) + (c \cdot d) = (a \cdot c) + (c \cdot d),$$

o que mostra que $a \cdot c < b \cdot c$. □

Proposição 2.4. *No que se refere à "igualdade" vale a lei do cancelamento para a adição, ou seja, para todo $a, b, c \in \mathbb{N}, a = b$ se, e somente se, $a + c = b + c$.*

Demonstração. Pelo fato da adição ser bem definida vale que, se $a = b$ então $a + c = b + c$. Reciprocamente, supondo que $a + c = b + c$ existem três possibilidades:

(i) $a < b$. Pela Proposição 2.2, $a + c < b + c$, o que é absurdo.

(ii) $b < a$. Pela mesma proposição, $b + c < a + c$, o que também é absurdo.

(iii) Logo, $a = b$.

□

Proposição 2.5. *No que se refere à "igualdade" vale a lei do cancelamento para a multiplicação, ou seja, para todo $a, b, c \in \mathbb{N}$, com $c \neq 0$, tem-se que $a = b$ se, e somente se, $a \cdot c = b \cdot c$.*

Demonstração. Pelo fato da multiplicação ser bem definida vale que, se $a = b$ então $a \cdot c = b \cdot c$. Reciprocamente, supondo que $a \cdot c = b \cdot c$ existem três possibilidades:

(i) $a < b$. Pela Proposição 2.3, $a \cdot c < b \cdot c$, o que é absurdo.

(ii) $b < a$. Pela mesma proposição, $b \cdot c < a \cdot c$, o que também é absurdo.

(iii) Logo, $a = b$.

□

Observando-se em mais detalhes a relação "menor do que" percebe-se que não é reflexiva, pois não vale $a < a$. No entanto a relação "menor ou igual a", descrita abaixo, o é.

Diz-se que a é menor ou igual a b, e simboliza-se por $a \leq b$, sempre que $a < b$ ou $a = b$. Diz-se que a é maior ou igual a b, e simboliza-se por $a \geq b$, sempre que $a > b$ ou $a = b$.

A relação "menor ou igual a" é, de fato, uma relação de ordem, pois,

1. É reflexiva: para todo a, $a \leq a$.
2. É antissimétrica: para todos a, b, se $a \leq b$ e $b \leq a$ então $a = b$.
3. É transitiva: para todos a, b, e c, se $a \leq b$ e $b \leq c$, então $a \leq c$.

Antes de iniciar a discussão sobre divisibilidade é interessante considerar o princípio de indução finita, visto que é muito utilizado na demonstração de resultados importantes na teoria dos números.

A indução finita se baseia nos dois seguintes princípios:

Princípio 2.1. (Boa Ordem) Todo conjunto não-vazio de números naturais possui um menor elemento.

Princípio 2.2. (Indução Finita) Seja $A \subset \mathbb{N}$, com as seguintes propriedades:

i) $1 \in \mathbb{A}$;

ii) Se $k \in A$ então $k + 1 \in A$.

Então $A = \mathbb{N}$.

Observação 2.1. Observe que, de acordo com este princípio, para provar uma afirmação para todo número natural basta provar para 1 e, a seguir, supondo que a afirmação vale para um número natual n qualquer, provar que vale para $n+1$.

Corolário 2.1. *Não existe nenhum número natural n tal que $0 < n < 1$.*

Demonstração. A frase acima é equivalente à proposição $p(n) : n > 0$ então $n \geq 1$ vale para todo n. Uma vez que $0 > 0$ é falso segue-se que $p(0)$ é verdadeira, já que a implicação "$0 > 0$ então $0 \geq 1$" sempre é verdadeira. Além disso, $p(n+1)$ é sempre verdadeira pois, se $n+1 > 0$, então $n+1 \geq 1$ pela lei do cancelamento.

Portanto, $p(n)$ implica $p(n+1)$ para todo n e o resultado segue. □

Corolário 2.2. *Dado $n \in \mathbb{N}$ não existe nenhum número natural m tal que $n < m < n+1$.*

Demonstração. Se tal número existisse, existiria um natural k tal que $n+k = m < n+1$. Então, pelo cancelamento, tem-se que $0 < k < 1$ o que, pelo corolário anterior, é absurdo.

Portanto, não existe nenhum natural m entre n e $n+1$. □

Sequências são funções cujo domínio é o conjunto dos números naturais ($\mathbb{N}$) e cujo contradomínio é o conjunto dos números reais ($\mathbb{R}$). Para tratar do relacionamento entre os números primos e as progressões aritméticas apresenta-se a seguir o conceito de progressão. Progressões são sequências que seguem uma lei de formação determinada pelo seu primeiro elemento e por um número conhecido como razão. Essa lei de formação, em muitos casos, pode ser demonstrada através do princípio de indução finita. Para os fins deste trabalho serão utilizadas apenas progressões cujo contradomínio seja o conjunto dos números naturais.

Como exemplo, apresenta-se abaixo as definições de alguns tipos especiais de progressões:

Definição 2.1. *Uma progressão aritmética (PA) é uma sequência de números reais (a_n) tal que a_1 é dado e, para todo $n \in \mathbb{N}$, tem-se que*

$$a_{n+1} = a_n + r,$$

onde r é um número real fixado chamado razão.

Exemplo 2.1. A sequência 3, 7, 11, $\cdots$ é uma progressão aritmética na qual $a_1 = 3$ e $r = 4$.

Note que a razão de uma PA pode ser encontrada por se subtrair a_i de a_{i+1} para qualquer natural i. Assim, $a_2 - a_1 = a_3 - a_2 = a_{i+1} - a_i = r$. No exemplo dado $a_2 - a_1 = 4 = r$.

Definição 2.2. *Uma progressão geométrica (PG) é uma sequência de números reais* (a_n) *tal que* a_1 *é dado e, para todo* $n \in \mathbb{N}$*, tem-se que*

$$a_{n+1} = a_n \cdot q,$$

onde q *é um número real fixado,* $q \neq 0$ *e* $q \neq 1$*, chamado razão.*

Exemplo 2.2. A sequência 3, 6, 12, $\cdots$ é uma progressão geométrica na qual $a_1 = 3$ e $q = 2$.

Note que a razão de uma PG pode ser encontrada por se dividir a_{i+1} por a_i para qualquer natural i. Assim, $a_2 \div a_1 = a_3 \div a_2 = a_{i+1} \div a_i = q$. No exemplo dado $a_2 \div a_1 = 2 = q$.

Definição 2.3. *Uma progressão aritmético-geométrica (PAG) é uma sequência de números reais* (a_n) *tal que* a_1 *é dado e, para todo* $n \in \mathbb{N}$*, tem-se que*

$$a_{n+1} = a_n \cdot q + r,$$

onde r *e* q *são números reais fixados e* $q \neq 1$*.*

Exemplo 2.3. A sequência 4, 13, 31, $\cdots$ é uma progressão aritmético-geométrica na qual $a_1 = 4$, $r = 5$ e $q = 2$. De fato,

$$a_1 = 4, a_2 = 4 \cdot 2 + 5 = 13, a_3 = 13 \cdot 2 + 5 = 31, \cdots .$$

Note que as razões de uma PAG não são encontradas apenas por uma operação simples. Para que seja possível encontrá-las é necessário resolver um sistema de equações de duas incógnitas. No exemplo:

$$\begin{cases} 13 = 4 \cdot q + r \\ 31 = 13 \cdot q + r \end{cases},$$

Multiplicando a primeira equação por -1 obtem-se:

$$\begin{cases} -13 = -4 \cdot q - r \\ 31 = 13 \cdot q + r \end{cases},$$

Somando estas duas equações tem-se que $9 \cdot q = 18$, de onde $q = 2$. Substituindo este valor na primeira equação tem-se que $r = 5$.

Usando-se o princípio da indução finita é possível demonstrar as seguintes propriedades relacionadas a progressões:

Proposição 2.6. *Numa progressão aritmética tem-se que:*

1. $a_n = a_1 + (n-1)r$;

2. *Se* $S_n = a_1 + a_2 + \cdots + a_n$ *então* $S_n = \dfrac{(a_1 + a_n)n}{2}$.

Demonstração.

1. Para $n = 1$ tem-se que $a_1 = a_1$. Suponha que a propriedade vale para n. Então, pela definição de PA e pela hipótese de indução,

$$a_{n+1} = a_n + r = a_1 + (n-1)r + r = a_1 + nr.$$

2. Para $n = 1$ tem-se que $S_1 = a_1 = \dfrac{(a_1 + a_1) \cdot 1}{2}$. Suponha, agora, que o resultado vale para S_n. Então, pela definição de S_n, pelo item anterior e pela hipótese de indução tem-se que,

$$\begin{aligned} S_{n+1} = a_1 + a_2 + \cdots + a_n + a_{n+1} = \frac{(a_1 + a_n)n}{2} + a_{n+1} = \\ = \frac{a_1 n + a_n n}{2} + a_{n+1} = \frac{a_1 n + a_n n}{2} + \frac{2a_{n+1}}{2} = \frac{a_1 n + a_n n + 2a_{n+1}}{2} = \\ = \frac{a_1 n + a_n n + a_1 + nr + a_{n+1}}{2} = \frac{a_1 n + a_1 + a_n n + nr + a_{n+1}}{2} = \\ = \frac{a_1(n+1) + (a_n + r)n + a_{n+1}}{2} = \frac{a_1(n+1) + a_{n+1}n + a_{n+1}}{2} = \\ = \frac{a_1(n+1) + a_{n+1}(n+1)}{2}. \end{aligned}$$

□

Proposição 2.7. *Numa progressão geométrica tem-se que:*

1. $a_n = a_1 \cdot q^{n-1}$;

2. *Se* $S_n = a_1 + a_2 + \cdots + a_n$ *e* $q \neq 1$ *então* $S_n = a_1 \dfrac{q^n - 1}{q - 1}$.

Demonstração.

1. Para $n = 1$ tem-se que $a_1 = a_1$. Suponha que a propriedade vale para n. Então, pela definição de PG e pela hipótese de indução,

$$a_{n+1} = a_n q = a_1 q^{n-1} \cdot q = a_1 q^n.$$

2. Para $n = 1$ tem-se que $S_1 = a_1 = a_1 \dfrac{q^1 - 1}{q - 1}$. Suponha, agora, que o resultado vale para S_n. Então, pela definição de S_n, pelo item anterior e pela hipótese de indução tem-se que,

$$S_{n+1} = a_1 + a_2 + \cdots + a_n + a_{n+1} = a_1 \frac{q^n - 1}{q - 1} + a_{n+1} =$$

$$= \frac{a_1q^n - a_1}{q-1} + a_{n+1} = \frac{a_1q^n - a_1}{q-1} + \frac{a_{n+1}(q-1)}{q-1} = \frac{a_1q^n - a_1 + a_{n+1}q - a_{n+1}}{q-1} =$$

$$= \frac{a_{n+1} - a_1 + a_1q^nq - a_{n+1}}{q-1} = \frac{a_{n+1} - a_1 + a_1q^{n+1} - a_{n+1}}{q-1} =$$

$$= \frac{a_1q^{n+1} - a_1}{q-1} = a_1\frac{q^{n+1}-1}{q-1}.$$

□

Para terminar o tópico sobre indução finita apresenta-se abaixo alguns exemplos de fórmulas de indução.

Exemplo 2.4. Até onde se tem registro, o primeiro exemplo de utilização do Princípio de Indução Finita remonta ao ano de 1575, quando Francesco Maurolycus calculou a soma dos n primeiros números ímpares. Ele demonstrou que,para todo n natural tem-se que

$$1 + 3 + \cdots + (2n-1) = n^2$$

Primeiramente, observe que vale $p(1)$, pois, $1 = 1^2$. Suponha que vale $p(n)$, ou seja, que $1 + 3 + \cdots + (2n-1) = n^2$ para um determinado natural n. Então, vale $p(n+1$, pois

$$1 + 3 + \cdots + (2n-1) + (2n+1) = n^2 + 2n + 1 = (n+1)^1$$

e, portanto, a fórmula vale para todo n.

Exemplo 2.5. Mostre que $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdot + \frac{1}{n\cdot(n+1)} = \frac{n}{n+1}$.

Em primeiro lugar note que, $\frac{1}{1\cdot 2} = \frac{1}{1+1} = \frac{1}{2}$.

Suponha que vale $p(n)$, ou seja, que $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdot + \frac{1}{n\cdot(n+1)} = \frac{n}{n+1}$, para um determinado n. Então, pela hipótese de indução,

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

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

Exemplo 2.6. Encontre uma fórmula para a soma $2 + 4 + \cdots + 2n$.

Neste tipo de problema primeiro deve-se calcular alguns elementos a fim de conseguir encontrar a fórmula geral. Neste exemplo tem-se que:

$$S_1 = 2, S_2 = 6, S_3 = 12, S_4 = 20, S_5 = 10, \ etc$$

Organizando estas informações obtem-se:

$$\begin{aligned}
S_1 &= 2 \\
S_2 &= S_1 + 2 \cdot 2 \\
S_3 &= S_2 + 2 \cdot 3 \\
S_4 &= S_3 + 2 \cdot 4 \\
\vdots \quad &= \vdots + \vdots \\
S_n &= S_{n-1} + 2 \cdot n
\end{aligned}$$

Somando membro a membro estas equações chega-se a:

$$S_1 + S_2 + \cdots + S_n = 2 \cdot S_1 + S_2 + \cdots + S_{n-1} + 2(2 + \cdots + n)$$

$$S_n = S_1 + 2\frac{(2+n)(n-1)}{2} = 2 + (n-1)(n+2)$$

Logo, $S_n = 2 + (n-1)(n+2)$.

Observe que, neste caso, a maneira pela qual a fórmula foi encontrada constitui uma demonstração matemática de que esta soma é válida para um determinado n. Para garantir sua validade para todos os naturais é necessário aplicar o Princípio de Indução. Tem-se que $p(1)$ é verdadeira, pois $S_1 = 2 + (1-1)(1+2) = 2$. Suponha que $S_n = 2 + (n-1)(n+2)$, para um determinado n, ou seja, que vale $p(n)$. Então, pela definição da soma, pela construção da sequência e pela hipótese de indução, tem-se que

$$S_{n+1} = S_n + a_{n+1} = 2 + (n-1)(n+2) + 2(n+1) = 2 + n^2 + 2n - n - 2 + 2n + 2 =$$

$$= 2 + n^2 + 3n = 2 + n(n+3) = 2 + ((n+1)-1)((n+1)+2),$$

como queríamos demonstrar.

Observação 2.2. Chama-se de conjunto $\mathbb{Z}$ dos números inteiros ao conjunto dos números naturais $\mathbb{N}$, acrescido dos números negativos. Como em divisibilidade a maioria das propriedades vale quando restrita aos números naturais, neste trabalho, sempre que for interessante esta restrição será utilizada.

Definição 2.4. *Se a e b são inteiros, diz-se que a divide b, e denota-se por $a|b$, se existir um inteiro c tal que $b = ac$. Se a não divide b denota-se $a \nmid b$.*

Exemplo 2.7. Tem-se que 5 divide 65, pois $65 = 13 \cdot 5$. Por outro lado, 5 não divide 47, pois não existe nenhum inteiro k tal que $47 = 5k$.

Proposição 2.8. *Sejam a, b e c inteiros. Se $a|b$ e $b|c$ então $a|c$.*

Demonstração. De fato, uma vez que $a|b$ existe um inteiro k_1, tal que $b = k_1 a$. Analogamente, como $b|c$ existe um inteiro k_2, tal que $c = k_2 b$. Portanto, $c = k_2 k_1 a$, o que significa que $a|c$. □

Proposição 2.9. *Sejam a, b, c, m e n inteiros. Se $c|a$ e $c|b$ então $c|(ma \pm nb)$.*

Demonstração. Pela definição de divisibilidade se $c|a$ então $a = k_1 c$, para algum k_1, inteiro. Analogamente, se $c|b$ então $b = k_2 c$. Multiplicando-se estas duas equações, respectivamente, por m e n obtém-se $ma = mk_1 c$ e $nb = nk_2 c$. Somando-se membro a membro chega-se a $ma \pm nb = mk_1 c \pm nk_2 c = (mk_1 \pm nk_2)c$. Portanto $c|(ma+nb)$. □

Proposição 2.10. *Sejam $a, b, n \in \mathbb{N}$, com $a+b \neq 0$. Então $a+b$ divide $a^{2n+1} + b^{2n+1}$.*

Demonstração. Demonstra-se por indução sobre n. Para $n = 0$ a afirmação é verdadeira, pois $a^1 + b^1 = a + b$. Suponha que $a + b|a^{2n+1} + b^{2n+1}$. Então:

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

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

Uma vez que $a + b|a^2 - b^2$ e que, por hipótese, $a + b|(a^{2n+1} + b^{2n+1})$ o resultado segue, do acima e da Proposição 2.9. □

Teorema 2.1. ***(Divisão Euclidiana).*** *Sejam a e b dois números naturais tais que $0 < a < b$. Existem dois números naturais, unicamente determinados, tais que*

$$b = a \cdot q + r,$$

com $r < a$.

Demonstração. Considere o conjunto Q dos números da forma $b, b-a, b-2a, \cdots, b-n\cdot a$, enquanto $b - n \cdot a > 0$.

Pela Propriedade da Boa Ordem, existe $r = b - q \cdot a$, o menor elemento do conjunto Q. Se $a|b$, então $r = 0$ e o resultado segue. Caso contrário, se $a \nmid b$ então $r \neq 0$. Portanto, mostrando que $r < a$ chega-se ao resultado desejado. Então, suponha que $r > a$. Neste caso, existe $c < r$ tal que $r = c + a$. Logo, como $r = c + a = b - q \cdot a$ tem-se que:

$$c = b - (q+1) \cdot a \in Q.$$

Portanto, $c \in Q$ e é menor do que r, o que é absurdo, pois r foi tomado como o menor elemento de Q. Portanto, $r < a$ e a existência de q e r está demonstrada.

Quanto à unicidade, suponha que existam dois elementos distintos, $r = b - q \cdot a$ e $r' = b - q' \cdot a$, com $r < r' < a$. A diferença entre estes dois elementos é divisível por a e, portanto, $r - r' \geq a$. Então, $r' \geq r + a > a$, o que é absurdo. Logo, $r = r'$. □

Corolário 2.1. (Propriedade Arquimediana). Dados dois números naturais a e b com $1 < a < b$, existe um número natural n tal que

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

Demonstração. Pela Divisão Euclidiana tem-se que existem $q, r \in \mathbb{N}$, tais que $b = q \cdot a + r$, com $r < a$. Tome $n = q$. Então,

$$na = q \cdot a < q \cdot a + r = b.$$

Por outro lado,

$$b = q \cdot a + r < (q+1)a + r = (n+1)a + r.$$

Logo, $na < b < (n+1)a$. □

Definição 2.5. *Seja m um número natural diferente de zero. Dois números naturais a e b são congruentes módulo m quando os restos de sua divisão euclidiana por m são iguais. Notação: $a \equiv b \mod m$.*

Exemplo 2.8.

- 18 e 43 deixam resto 3 ao serem divididos por 5, então são congruentes módulo 5;
- 71 e 85 deixam resto 1 ao serem divididos por 7, então são congruentes módulo 7;
- 43 deixa resto 1 ao ser dividido por 6 e 46 deixa resto 4 ao ser dividido por 6. Portanto, 43 e 46 não são congruentes módulo 6.

Observação 2.3. Observe que dizer que $a \equiv b \mod m$ é o mesmo que dizer que $m|b-a$. De fato, suponha que a e b deixem resto r ao serem divididos por m. Então, pela divisão euclidiana tem-se que $a = mq_1 + r$ e $b = mq_2 + r$. Então $b - a = mq_2 + r - mq_1 - r = mq_2 - mq_1 = m(q_2 - q_1)$ e, portanto, $m|b-a$.

Proposição 2.11. *Sejam $a, b \in \mathbb{N}$ e n um número natural maior do que zero. Se $a \equiv b \mod m$, então $a^n \equiv b^n \mod m$.*

Demonstração. Inicialmente note que, para quaisquer números naturais tem-se que, se $a \equiv b \mod m$ e $c \equiv d \mod m$ então $ac \equiv bd \mod m$. De fato, $bd - ac = d(b-a) + a(d-c)$. Como $m|b-a$ e $m|d-c$, então $m|bd-ac$ e $ac \equiv b \mod m$.

Observado isto, a demonstração do resultado é feita por induçao sobre n. A afirmação é verdadeira para $n = 1$. Suponha, agora, que o resultado vale para n, então, pela hipótese de indução e pela Observação 2.3 tem-se que

$$a^{n+1} = a^n a \equiv b^n b \mod m.$$

Mas $b^n b = b^{n+1}$. Logo $a^{n+1} = a^n a \equiv b^{n+1} \mod m$. □

Definição 2.6. *Dados dois números inteiros a e b, distintos, diz-se que o número inteiro d é um divisor comum de a e b se $d|a$ e $d|b$.*

Exemplo 2.9. Por exemplo, 6 é um divisor comum de 84 e 96, pois $84 = 14 \cdot 6$ e $96 = 16 \cdot 6$, mas 7 não é um divisor comum de 84 e 96 pois, embora $84 = 12 \cdot 7$ não existe nenhum inteiro k tal que $96 = 7k$.

Definição 2.7. *O máximo divisor comum de dois inteiros a e b é o maior inteiro positivo que divide a e b. Notação:* (a, b).

Exemplo 2.10. Usando os mesmos números do Exemplo 2.10, 12 é o máximo divisor comum de 84 e 96, pois $84 = 12 \cdot 7$ e $96 = 12 \cdot 8$, e não existe nenhum outro número inteiro positivo que seja maior do que 12 e divisor comum de 84 e 96.

Proposição 2.12. *Seja $d = (a, b)$, então existem inteiros m e n tais que $d = ma + nb$.*

Demonstração. Seja $c = m_0a + n_0b$ o menor inteiro positivo que pode ser escrito nesta forma, então $c|a$ e $c|b$. De fato, se $c \nmid a$ existiriam, pela Divisão Euclidiana q_1 e r_1 tais que $a = cq_1 + r_1$, com $0 < r_1 < c$, de onde $r_1 = a - cq_1 = a - (m_0a + n_0b)q_1 = (1 - q_1m_0)a + (-qn_0)b$. Ou seja, r_1 é da forma $m_1a + n_1b$ e menor do que c, o que é absurdo por construção. Logo $c|a$. Da mesma maneira demonstra-se que $c|b$.

Como d é um divisor comum de a e b tem-se que existem inteiros m_1 e m_2 tais que $a = m_1d$ e $b = m_2d$. Logo, $c = m_0a + n_0b = m_0m_1d + n_0m_2d = d(m_0m_1 + n_0m_2)$, ou seja, $d|c$ e, portanto, $d \leq c$. Como d é o máximo divisor comum de a e b, $d < c$ é impossível. Logo $c = d$ e, portanto, existem m, n tais que $d = ma + nb$. □

Lema 2.1. ***(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 $d = (a, b - na)$. Pela definição de máximo divisor comum, $d|a$ e $d|b - na$. Uma vez que $d|a$ tem-se que $d|na$. Além disso, $d|b$, pois $b = b - na + na>$ então, d é um divisor comum de a e b. Finalmente, suponha que c seja um divisor comum de a e de b. Então $c|a$ e $c|b - na$. Portanto, pela definição de máximo divisor comum $c|d$. Logo, $d = (a, b)$. □

Definição 2.8. *Dois números naturais a e b são ditos primos entre si quando $(a, b) = 1$.*

Proposição 2.13. *Dois números naturais a e b são primos entre si se, e somente se, existem números naturais m e n tais que $ma - nb = 1$.*

Demonstração. Suponha, sem perda de generalidade, que $a > b$. Seja $c \in \mathbb{N}$ tal que $c|a$ e $c|b$. Logo, pela Proposição 2.9, $c|(ma - nb)$. Então, $c = d(ma - nb)$. Como $c = (a, b) = 1$ tem-se que $1 = d(ma - nb)$, de onde, $d = 1$ e $ma - nb = 1$, uma vez que tanto d, como $ma - nb$ foram tomados como números naturais. Portanto, existem m e n tais que $ma - nb = 1$.

Por outro lado, suponha que existam m e n tais que $ma - nb = 1$. Seja $d = (a, b)$. Então, pela Proposição 2.9, $d|(ma - nb) = 1$. Mas, então, $d|1$ e, portanto, $d = 1$. □

Teorema 2.2. *Sejam a, b e c números naturais. Se $a|b \cdot c$ e $(a,b) = 1$, então $a|c$.*

Demonstração. Como $a|b \cdot c$, existe um número natural e tal que $bc = ae$. Como $(a,b) = 1$, pela Proposição 2.13, existem números naturais m, n tais que $na - mb = 1$. Daí, segue que $c = nac - mbc = nac - mae = a(nc - me)$. Isto é, $a|c$. □

Proposição 2.14. *Sejam a, b e n números naturais. Então $d = (na, nb) = n(a,b)$.*

Demonstração. Pela Proposição 2.12 existem $u, v \in \mathbb{N}$ tais que $d = una + vnb$, é o menor valor possível para os números da forma $u_0na + v_0nb$. Seja $e = (a,b)$. Então, pela Proposição 2.12, e é igual ao menor valor dos números da forma $u_0a + v_0b$. Portanto, $d = una + vnb = n(ua + vb) = nc$ e $(na, nb) = n(a,b)$. □

Corolário 2.3. *Sejam a, b e n números naturais. Então* $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.

Demonstração. Usando a Proposição 2.14 tem-se que:

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

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

Proposição 2.15. *Dados a, b e $c \in \mathbb{N}$, se $(a,b) = 1$ então, $(a \cdot c, b) = (c,b)$.*

Proposição 2.16. *Dados a, b e $c \in \mathbb{N}$ então, $(a \cdot c, b) = 1$ se, e somente se, $(a,b) = (c,b) = 1$.*

Demonstração. Se $(a,b) = (c,b) = 1$ tem-se, pela Proposição 2.15, que $(a \cdot c, b) = (c,b) = 1$. Por outro lado, se $(a \cdot c, b) = 1$ então, pela Proposição 2.13 existem $m, n \in \mathbb{N}$ tais que $mac - nb = 1$. Logo, existem $m_1 = mc$ e $n_1 = n$ naturais, tais que $m_1a - n_1b = 1$. Daí segue, pela Proposição 2.13 que $(a,b) = 1$. Similarmente, concluí-se que $(c,b) = 1$. □

Proposição 2.17. *Dados $a, b \in \mathbb{N}$ então $a = (a,b)$ se, e somente se, $a|b$.*

Demonstração. De fato, se $a = (a,b)$ então, pela definição de máximo divisor comum $a|b$. Por outro lado, se $a|b$, então $b = na$, de onde, usando a Proposição 2.14, $(a,b) = (a, na) = a(1,n) = a$. □

Proposição 2.18. *Dada uma sequência $(a_n)_n$, tal que $\forall m \geq n$, $(a_m, a_n) = (a_n, a_r)$, onde r é o resto da divisão de m por n, então tem-se que $(a_m, a_n) = a_{m,n}$.*

Demonstração. Escrevendo $m = qn + r, r = q_1n_1 + r_1, r_1 = q_2n_2 + r_2, \cdot, r_s = q_{s+1}n_{s+1}$, onde $r_{s+1} = 0$, tem-se, pela Divisão Euclidiana, que $r_s = (m,n)$. Aplicando a propriedade de $(a_n)_n$ tem-se que:

$$(a_m, a_n) = (a_n, a_{r_1}) = (a_{r_1}, a_{r_2}) = \cdot = (a_{r_s}, a_{r_{s+1}}) = (a_s, 0) = a_{(m,n)}.$$

□

Definição 2.9. *O menor inteiro positivo que é, simultaneamente, múltiplo de a e b é chamado mínimo múltiplo de a e b. Notação:* $[a, b]$.

Exemplo 2.11. 30 é o mínimo múltiplo comum de 6 e 5, pois é o menor inteiro positivo que é múltiplo de 5 (pois $30 = 6 \cdot 5$) e de 6 (pois $30 = 5 \cdot 6$).

Note que 30 também é o mínimo múltiplo comum de 6 e 10, pois é o menor inteiro positivo que é múltiplo de 10 (pois $30 = 3 \cdot 10$) e de 6 (pois $30 = 5 \cdot 6$).

Proposição 2.19. *Dados dois números inteiros a e b, existe $[a, b]$ e*

$$[a, b](a, b) = ab.$$

Demonstração. Seja $m = \dfrac{ab}{(a, b)}$. Então $a|m$ e $b|m$. Por outro lado, tomando c um múltiplo comum de a e b tem-se que $c = n_1 a = n_2 b$, de onde, $n_1 \dfrac{a}{(a, b)} = n_2 \dfrac{b}{(a, b)}$. Mas, pelo Corolário 2.3, $\dfrac{a}{(a, b)}$ e $\dfrac{b}{(a, b)}$ são primos entre si. Segue do Teorema 2.2 que $\dfrac{a}{(a, b)}$ divide n_2 e, portanto, $m = \dfrac{a}{(a, b)} b$ divide $n_2 b = c$. □

Uma das aplicações interessantes do máximo divisor comum relaciona-se com a famosa sequência de Fibonacci. Nesta sequência um termo é a soma dos dois termos anteriores, sendo que os dois primeiros termos são 1. Representando os elementos da sequência de Fibonacci por f_i, onde i é a posição do termo na sequência é possível escrever:

$$f_1 = 1$$

$$f_2 = 1$$

$$f_i = f_{i-1} + f_{i-2}, \text{ para } i > 2,$$

ou seja, a sequência é dada por $1, 1, 2, 3, 5, 8, 13, 21, 33, \ldots$.

Apresenta-se, a seguir, algumas propriedades interessantes desta sequência relacionadas ao máximo divisor comum e à divisibilidade.

Proposição 2.20. *Dois termos consecutivos da sequência de Fibonacci são primos entre si.*

Demonstração. Demonstra-se o resultado por indução. Para $n = 1$ tem-se que $(f_1, f_2) = (1, 1) = 1$. Suponha que $(f_n, f_{n+1}) = 1$ Então, pelo Lema de Euclides:

$$(f_{n+1}, f_{n+2}) = (f_{n+1}, f_{n+2} - f_{n+1}) = (f_{n+1}, f_n) = 1.$$

□

Proposição 2.21. *Sejam $m, n \in \mathbb{N}^*$ e $m \geq 2$. Então*

$$f_{m+n} = f_{m-1}f_n + f_m f_{n+1}.$$

Demonstração. Demonstra-se o resultado primeiro por se fixar $n = 1$ e usar indução sobre m. Depois, fixa-se m e usa-se indução sobre n. Desta maneira demonstra-se que o resultado vale para todo m e para todo n.

Tomando $n = 1$ a igualdade escreve-se como:

$$f_{m+1} = f_{m-1}f_1 + f_m f_{1+1} = f_{m-1} + f_m,$$

que é verdadeira para todo m pela definição da sequência de Fibonacci.

Suponha, agora que, $f_{m+n} = f_{m-1}f_n + f_m f_{n+1}$. Então,

$$\begin{aligned} f_{m+(n+1)} = f_{m+n} + f_{m+(n-1)} = f_{m-1}f_n + f_m f_{n+1} + f_{m+(n-1)} = \\ = f_{m-1}(f_{n+1} - f_{n-1}) + f_m(f_{n+2} - f_n) + f_{m+(n-1)} = \\ = f_{m-1}f_{n+1} - f_{m-1}f_{n-1} + f_m f_{n+2} - f_m f_n + f_{m+(n-1)} = \\ = f_{m-1}f_{n+1} + f_m f_{n+2} - f_{m-1}f_{n-1} - f_m f_n + f_{m+(n-1)} = (*) \end{aligned}$$

Mas, usando a hipótese de indução uma segunda vez, tem-se que $f_{m+(n-1)} = f_{m-1}f_{n-1} + f_m f_n$. Substituindo em $(*)$ obtem-se

$$\begin{aligned} (*) = f_{m-1}f_{n+1} + f_m f_{n+2} - f_{m-1}f_{n-1} - f_m f_n + f_{m-1}f_{n-1} + f_m f_n = \\ = f_{m-1}f_{n+1} + f_m f_{n+2}. \end{aligned}$$

□

Proposição 2.22. *Sejam $m, n \in \mathbb{N}^*$. Se $m|n$ então $f_m|f_n$.*

Demonstração. Como $m|n$ tem-se que $n = km$ para algum inteiro k. Demonstra-se que o resultado vale para todo múltiplo de m pelo uso de indução sobre k. Para $k = 1$, tem-se que $m|m$ então $f_m|f_m$ verdadeiro. Suponha que o resultado vale para $n = km$, ou seja, que $f_m|f_{mk}$. Então, pela Proposição 2.21 tem-se que

$$f_{n(k+1)} = f_{nk+n} = f_{nk-1}f_n + f_{nk}f_{n+1}.$$

Mas, $f_n|f_{nk-1}f_n$ e, pela hipótese de indução, $f_n|f_{nk}f_{n+1}$, segue que f_n divide $f_{n(k+1)}$.

□

Teorema 2.3. *Na sequência de Fibonacci sempre vale $(f_m, f_n) = f_{(m,n)}$. Além disso, $f_n|f_m$ se, e somente se, $n|m$.*

Demonstração. Suponha que $m \geq n$. Então, pela Divisao Euclidiana, $m = nq + r$. Usando a Proposição 2.21 tem-se que

$$f_m = f_{nq+r} = f_{nq-1}f_r + f_{nq}f_{r+1}.$$

Mas, pela Proposição 2.22, $f_n | f_{nq}$. Então, pelo Lema de Euclides:

$$(f_n, f_m) = (f_{nq-1}f_r + f_{nq}f_{r+1}, f_n) = (f_{nq-1}f_r, f_n). \qquad (**)$$

Pela Proposição 2.20, $(f_{nq-1}, f_{nq}) = 1$, então, da Proposição 2.16 tem-se que $(f_{nq-1}, f_n) = 1$. Portanto, de $(**)$ e da Proposição 2.15 segue que $(f_m, f_n) = (f_n, f_r)$. Então, pela Proposição 2.18, $(f_m, f_n) = f_{(m,n)}$.

A segunda afirmação segue diretamente da primeira, pois, se $n|m$ então, pela Proposição 2.17, $(n, m) = n$, de onde, $f_n = f_{(n,m)} = (f_n, f_m)$, ou seja, $f_n = (f_n, f_m)$. Logo, $f_n | f_m$. Mostra-se a recíproca usando o mesmo argumento.

□

Uma das perguntas interessantes relacionadas à sequência de Fibonacci é se ela possui em seus termos, infinitos números primos (um número primo é o que é divisível apenas por um e por ele mesmo. Mais sobre os números primos será visto no capítulo 3). Esta pergunta não tinha sido respondida até à conclusão deste trabalho e encontra-se entre as afirmações não demonstradas sobre os números primos.

3 Sobre Números Primos

Neste capítulo, será apresentado o principal elemento matemático de estudo deste trabalho, os números primos. No próximo, serão apresentados algumas aplicações.

Definição 3.1. *Um número natural maior do que 1 e que só é divisível por 1 e por si próprio é chamado de número primo.*

Exemplo 3.1. Os números 7, 13 e 29 são primos, mas 85, 115 e 140 não são, pois são divisíveis por 5.

Definição 3.2. *Sejam, a e m números naturais tais que $(a, m) = 1$. O menor inteiro positivo k para o qual $a^k \equiv 1 \mod m$ é chamado de ordem de a módulo m e representado por $ord_m a$.*

Exemplo 3.2. Por exemplo, $3^4 = 81 \equiv 1 \mod 5$, $3^3 = 27 \equiv 2 \mod 5$, $3^2 = 9 \equiv 4 \mod 5$ e $3^1 = 3 \equiv 3 \mod 5$. Portanto, $ord_5 3 = 4$.

Definição 3.3. *Seja n um número natural. Chama-se função φ de Euler à que associa a cada número natural, o número de inteiros positivos m menores do que n, tais que $(m, n) = 1$.*

Exemplo 3.3. Calcule o valor da função φ para os números 24, 32 e 37.

Para 24 tem-se que $1, 5, 7, 9, 10, 11, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22$ e 23 são primos com 24. Logo $\varphi(24) = 17$.

Para 32 tem-se que 1, 3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28 ,29, 30 e 31 são primos com 32. Logo $\varphi(32) = 27$.

Finalmente, para 31, uma vez que ele é um número primo tem-se que $\varphi(31) = 30$, pois todos os números anteriores a 31 são primos com ele.

Definição 3.4. *Sejam, a e m números naturais tais que $(a, m) = 1$. O número a é chamado raiz primitiva módulo m quando $ord_m a = \varphi(m)$.*

Exemplo 3.4. Tem-se que 3 é uma raiz primitiva de 7, pois $729 = 3^6 \equiv 1 \mod 7$. Por outro lado, $3^5 = 243 \equiv 5 \mod 7$, $3^4 = 81 \equiv 4 \mod 7$, $3^3 = 27 \equiv 6 \mod 7$, $3^2 = 9 \equiv 2 \mod 7$ e $3^1 = 3 \equiv 3 \mod 7$. Portanto, $ord_7 3 = 6$.

Além disso, como 7 é um número primo tem-se que $\varphi(7) = 6$, o que prova que 3 é uma raiz primitiva de 7.

Definição 3.5. *Um sistema completo de resíduos módulo m é um conjunto de números naturais cujos restos pela divisão por m são os números $0, 1, 2, \cdots, m-1$, em qualquer ordem e sem repetições.*

Exemplo 3.5. O conjunto $\{31, 43, 82, 95, 14\}$ é um sistema completo de resíduos módulo 5 pois, dividindo estes números por 5 obtem-se, respectivamente, $1, 3, 2, 0$ e 4.

Definição 3.6. *Um sistema reduzido de resíduos módulo m é um conjunto de números naturais $r_1, \cdots, r_s$ tais que*

1. *$(r_i, m) = 1$, para todo $i = 1, \cdots, s$,*
2. *r_i não é congruente a r_j módulo m para $i \neq j$,*
3. *Para cada $n \in \mathbb{N}$ que seja primo com m, existe i tal que $n \equiv r_i \mod m$.*

Exemplo 3.6. Usando o mesmo conjunto do Exemplo 3.5 tem-se que $\{31, 43, 82, 14\}$ é um sistema reduzido de resíduos módulo 5, pois todos os seus elementos são primos com 5, nenhum deles é congruente ao outro módulo 5 e todo natural que seja primo com 5 é congruente a um dos elementos deste conjunto módulo 5, já que todos os restos maiores do que zero, possíveis numa divisão por 5 podem ser obtidos dos elementos deste conjunto.

Observação 3.1. Das definições anteriores percebe-se que $\varphi(m) \leq m - 1$ pois, os valores que tal função pode assumir são os valores que correspondem ao resto da divisão euclidiana de um número natural por m. Note ainda que, quando $\varphi(m) = m - 1$, m é primo, pois todos os números $1, 2, 3, \cdots, m - 1$ são primos com m.

Isso ajuda a concluir que, se um número a é raiz primitiva módulo p, com p primo, então $ord_p a = \varphi(p) = p - 1$. Além disso, é possível demonstrar que todo número primo p possui pelo menos uma raiz primitiva a, tal que $p \mid a$.

Nos artigos 73 e 74 das *Disquisitiones Arithmeticae*, Gauss descreveu um processo para o cálculo de raízes primitivas.

Observação 3.2. Durante os séculos os matemáticos têm observado classes de números com o objetivo de aprender sobre os números primos. Muitos dos problemas abertos da matemática relacionam-se a estas classes e, por isso, apresenta-se agora uma lista das mais conhecidas.

1. Números de Fermat : $F_n = 2^{2^n} + 1$;
2. Números de Mersenne: $M_n = 2^n - 1$;
3. Pseudoprimos: Números compostos que possuem propriedades que se espera encontrar apenas em números primos;

4. Números de Carmichael: Números compostos n tais que $a^{n-1} \equiv 1 \mod n$, para todo a, $1 < a < n$ com $(a, n) = 1$;

5. Números de Cullen: Números da forma $C_n = n \times 2^n + 1$

6. Números de Woodall: Números da forma $C_n = n \times 2^n - 1$

Além disso, diversas classes de números primos foram estudadas. Abaixo apresenta-se alguns exemplos.

1. Primos de Sophie-German: Números primos p tais que $2p + 1$ também sejam primos.

2. Primos de Wieferich: Um primo p que satisfaz a congruência $2^{p-1} \equiv 1 \mod p^2$.

3. Primos de Wilson: Um primo que satisfaz a congruência $(p-1)! \equiv -1 \mod p^2$.

Existem muitas conjeturas, ou seja, afirmações não demonstradas, sobre os números primos e relacionadas a eles. Abaixo apresenta-se algumas delas:

1. Existe uma infinidade de números de Mersenne compostos.

2. Se a é um número inteiro diferente de zero e que não é quadrado, então existe uma infinidade de números primos p tais que a é raiz primitiva módulo p. (Conjetura de Artin)

3. Para todo natural par $2k$, existe uma infinidade de pares de números primos consecutivos p_n, P_{n+1}, tais que $d_n = p_{n+1} - p_n = 2k$. (Conjetura de Polignac)

4. Todo inteiro par maior do que 4 é a soma de dois números primos. (Conjetura de Goldbach)

5. Seja M_p o p-ésimo número de Mersenne. M_p é primo, se é somente se, as sentenças $\dfrac{2^p + 1}{3}$ e p é um primo da forma $2^k \pm 1$ ou $4^k \pm 3$ (para algum $k \geq 1$) forem simultaneamente verdadeiras ou falsas. (Conjetura de Batman, Selfridge e Wagstaff)

Utilizando-se cálculos em computadores demonstra-se que várias conjeturas são válidas para milhares de números. No entanto, uma demonstração para todos os naturais ainda não foi encontrada para nenhuma delas. No capítulo 5 serão analisados alguns resultados relacionados com a Conjetura de Goldbach.

Observação 3.3. Da definição de número primos, dados p e q dois números primos e um número natural a qualquer, tem-se que:

1. Se $p|q$, então $p = q$.

2. Se $p \nmid a$, então $(p, a) = 1$.

1. Com efeito, por hipótese, q é primo e $p|q$, então pela definição de número primo, ou $p = 1$ ou $p = q$. Como p é primo tem-se, por definição, que $p > 1$. Logo $p = q$.

2. Seja $(p, a) = d$. Pela definição de máximo divisor comum tem-se que $d|p$ e $d|a$. Portanto, $d = p$ ou $d = 1$. Mas e se $d = p$ então se seguiria que $p|a$, o que é contrário à hipótese. Logo $d = 1$

Proposição 3.1. *Sejam a, b e p, números naturais com p um número primo. Se $p|a \cdot b$ então $p|a$ ou $p|b$.*

Demonstração. Suponha que $p \nmid a$. Logo, por definição, $(p, a) = 1$. Portanto, pelo Teorema 2.2, $p|b$.

□

Corolário 3.1. *Sejam $p, p_1, p_2, \cdots, p_n$ números primos. Se $p|p_1 \cdot p_2 \cdots p_n$, então $p = p_i$ para algum $i = 1, 2, \cdots, n$.*

Demonstração. Demonstra-se o resultado por indução sobre n. Se $n = 2$, o resultado vale pela Proposição 3.1. Como hipótese de indução suponha que o resultado vale para $n - 1$. Agora se, $p|p_1 \cdot p_2 \cdots p_n$ tem-se que $p|p_1 \cdot p_2 \cdots p_{n-1}$ ou $p|p_n$. Se $p|p_n$ o resultado segue. Se $p \nmid p_n$ então $p|p_1 \cdot p_2 \cdots p_{n-1}$ e, pela hipótese de indução $p = p_i$ para algum $i = 1, 2, \cdots, n - 1$. □

Teorema 3.1. ***(Teorema Fundamental da Aritmética)*** *Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos, distintos ou não.*

Demonstração. Usando o princípio de indução finita, tem-se que, para $n = 2$ o resultado vale. Suponha que o resultado vale para $k < n$. Mas então, ou n é primo, ou pode escrito como $n = n_1 n_2$ com $0 < n_1 < n$ e $0 < n_2 < n$. Então, pela hipótese de indução, existem primos $p_1, p_2, \cdots, p_r$ e $q_1, q_2, \cdots, q_s$, tais que $n_1 = p_1 \cdot p_2 \cdots p_r$ e $n_2 = q_1 \cdot q_2 \cdots q_s$ e, então $n = n_1 n_2 = p_1 \cdot p_2 \cdots p_r \cdot q_1 \cdot q_2 \cdots q_s$, onde os p_i não são todos necessariamente distintos dos q_j.

Falta, ainda, mostrar que esta decomposição é única. Suponha, agora que $n = p_1 \cdot p_2 \cdots p_t = q_1 \cdot q_2 \cdots q_u$, com os p_i e q_j, números primos. Evidentemente, se $n = 2$, tem-se $p_1 = q_1 = 2$. Suponha, que o resultado vale para todo natural menor do que n, ou seja, que caso se tenha $n > m = p_1 \cdot p_2 \cdots p_t = q_1 \cdot q_2 \cdots q_u$, com os p_i e q_j então, $t = u$ e cada um dos p_i é igual a um dos q_j para algum j.

Tem-se que $p_1|n = q_1 \cdot q_2 \cdots q_u$ e, portanto, $p_1 q_1 \cdot q_2 \cdots q_u$. Pelo Corolário 3.1 $p_1 = q_j$ para algum j. Reordenando os q_j pode-se supor que tem-se $q_1 = p1$. Então,

$$p_2 \cdots p_t = q_2 \cdots q_u.$$

Mas, como $p_2 \cdots p_t < n$ tem-se que, pela hipótese de indução, $t = u$ e cada um dos p_i é igual a um dos q_j para algum j. Portanto, o resultado segue. □

Teorema 3.2. *Se n não é primo, então n possui um fator primo menor ou igual a $\sqrt{n}$.*

Demonstração. Se n não é primo ele é, por definição, composto. Então, pode ser escrito como $n = n_1 \cdot n_2$. Suponha, sem perda de generalidade, que $n_1 < n_2$. Pode-se concluir, então, que $n_1 \leq \sqrt{n}$. De fato, se não for assim tem-se que $n = n_1 \cdot n_2 > \sqrt{n} \cdot \sqrt{n} = n$, o que é absurdo. Logo $n_1 \leq \sqrt{n}$.

Pelo Teorema Fundamental da Aritmética, n_1 possui pelo menos um fator primo p. Como esse fator é menor ou igual a n_1 ele é menor ou igual a $\sqrt{n}$. □

O famoso matemático grego Euclides, autor de *Os Elementos*, demonstrou o seguinte teorema:

Teorema 3.3. *Existem infinitos números primos.*

Demonstração. Suponha, por absurdo, que a sucessão de números primos seja finita e dada por $p_1, p_2, \cdots, p_n$. Seja $P = p_1 \cdot p_2 \cdots p_n + 1$. Seja p um número primo que divide P. Esse primo não pode ser igual a nenhum dos p_i pois, senão, dividiria P e dividiria $p_1 \cdot p_2 \cdots p_n$. Logo, dividiria, $P - p_1 \cdot p_2 \cdots p_n = 1$, o que é absurdo. Portanto, p é um número primo que não pertence à sucessão e, portanto, existe um primo diferente de $p_1, p_2, \cdots, p_n$. Esse raciocínio pode ser repetido quantas vezes for necessário. Portanto, existem infinitos números primos. □

Após a comprovação de que existiam infinitos primos diversos matemáticos começaram a procurar uma fórmula geral para a sequência dos primos. Esta procura levou à criação de vários testes de primalidade que, embora não sejam eficientes, pois exigem um grande número de operações, podem ajudar a determinar se um número possivelmente é primo. Os testes de primalidade podem ser classificados em seis categorias distintas:

1. Testes para números de forma particular
   (a) Teste APR
   (b) Testes com curvas elípticas
2. Testes para números genéricos
3. Testes baseados em teoremas
4. Testes baseados em conjecturas
   (a) Teste de Miller - baseado na hipótese de Riemann
5. Testes determinísticos

6. Testes de Monte Carlos

Proposição 3.2. *Se um número natural $n > 1$ não é divisível por nenhum número primo p tal que $p^2 \leq n$, então n é primo.*

Demonstração. Suponha, por absurdo, que não exista p primo, tal que $p|n$ com $p^2 \leq n$ e que n seja composto. Então pelo Teorema Fundamental da Aritmética, existe q,tal que q é o menor número primo que divide n. Então $n = qn_1$ e $q \leq n_1$. De onde, $q_2 \leq qn_1 = n$. Portanto, $q|n$ e $q_2 \leq n$, contrário à hipótese. □

Teorema 3.4. ***(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. Demonstra-se o resultado por indução sobre a. Para $a = 1$ o resultado vale, pois $p|0$. Suponha, que o resultado vale para a. Então tem-se que:

$$(a+1)^p - (a+1) = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a - a =$$

$$= a^p - a + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a,$$

que é, pela hipótese de indução e pelo Lema 4.1, divisível por p. □

Corolário 3.2. *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. Pelo Pequeno Teorema de Fermat tem-se que $p|a^p - a = a(a^{p-1} - 1)$. Por outro lado, por hipótese, $p \nmid a$, ou seja $(a, p) = 1$. Então, pelo Teorema 2.2, $p|a^{p-1} - 1$. □

Proposição 3.3. *Sejam $a, b, c, m \in \mathbb{N}$, com $c \neq 0$ e $m > 1$. Então*

$$ac \equiv bc \mod m \text{ se, e somente se } a \equiv b \mod \frac{m}{(c,m)}.$$

Demonstração. Supondo, sem perda de generalidade, que $bc \geq ac$ e uma vez que, pelo Corolário 2.3, $\frac{c}{(c,m)}$ e $\frac{m}{(c,m)}$ são primos entre si, tem-se que

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

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

□

Corolário 3.3. *Sejam $a, b, c, m \in \mathbb{N}$, com $c \neq 0$, $m > 1$ e $(c, m) = 1$. Então*

$$ac \equiv bc \mod m \text{ se, e somente se } a \equiv b \mod m.$$

Demonstração. Decorre, imediatamente da Proposição anterior, uma vez que $(c, m) = 1$. □

Proposição 3.4. *Seja $r_1, \cdots, r_{\varphi(m)}$ um sistema reduzido de resíduos módulo m e seja $a \in \mathbb{N}$, tal que $(a, m) = 1$. Então, $ar_1, \cdots, ar_{\varphi(m)}$ é um sistema reduzido de resíduos módulo m.*

Demonstração. Suponha que o sistema reduzido de resíduos módulo m, $r_1, \cdots, r_{\varphi(m)}$ tenha sido obtido a partir de um sistema completo de resíduos módulo m dado por $a_1, \cdots, a_m$. Então, para todo a_i com um r_i correspondente tem-se que $(a_i, m) = 1$. Então, pela Proposição 2.16 tem-se que $(aa_i, m) = 1$, o que demonstra o resultado. □

Teorema 3.5. *(De Euler) Sejam $m, a \in \mathbb{N}$, com $m > 1$ e $(a, m) = 1$. Então:*

$$a^{\varphi(m)} \equiv 1 \mod m.$$

Demonstração. Seja um sistema reduzido de resíduos módulo m dado por $r_1, \cdots, r_{\varphi(m)}$. Pela Proposicao 3.4, $ar_1, \cdots, ar_{\varphi(m)}$ também formam um sistema de resíduos módulo m. Então

$$a^{\varphi(m)} \cdot r_1 \cdot r_2 \cdots r_{\varphi(m)} = ar_1 \cdot ar_2 \cdots ar_{\varphi(m)} \equiv r_1 \cdot r_2 \cdots r_{\varphi(m)} \mod m.$$

Aplicando a Proposição 2.15 um número finito de vezes tem-se que $(r_1 \cdot r_2 \cdots r_{\varphi(m)}, m) = 1$. Então, pelo Corolário 3.3 tem-se que $a^{\varphi(m)} \equiv 1 \mod m$. □

Pode-se formular o Pequeno Teorema de Fermat utilizando a definição de congruência (Definição 2.5) da seguinte maneira:

Teorema 3.6. ***(Pequeno Teorema de Fermat)*** *Dado um número primo p, tem-se que p divide o número $a^p \equiv a \mod p$, para todo $a \in \mathbb{N}$. Se, $p \nmid a$, então $a^{p-1} \equiv 1 \mod p$.*

Demonstração. Consequência direta do Teorema de Euler já que, como p é primo $\varphi p = p - 1$. Então

$$a^{\varphi(p)} = a^{p-1} \equiv 1 \mod p.$$

□

4 Números Primos: Resultados e Aplicações

Definição 4.1. *Dado $x \in \mathbb{N}$ denota-se por $\pi(x)$ ao número de primos p tais que $p \leq x$. A função $\pi(x)$ é chamada função de contagem dos números primos.*

Em 1792, aos 15 anos de idade, Gauss conjeturou que $\pi(x)$ era assintoticamente igual à função logarítmica:

$$Li(x) = \int_2^x \frac{dt}{\log t}.$$

Com o tempo tal conjetura provou-se verdadeira e é hoje conhecida como:

Teorema 4.1. *(Teorema dos Números Primos). Nas condições da definição anterior,*

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

4.1 Números Primos e Fatoriais

Proposição 4.1. *Para todo natural $n \geq 2$, a sequência $(n+1)!+2, (n+1)!+3, \cdots, (n+1)!+n+1$ de números naturais é formada por n números consecutivos compostos.*

Demonstração. De fato, pela definição de fatorial, o número $(n+1)!$ possui todos os fatores de 2 até $n+1$. Logo, dado qualquer número da forma $(n+1)!+i$, com $i = 2, ..., n+1$, existirá o fator i no número $(n+1)!$, ou seja,

$$\begin{aligned}(n+1)!+i &= (2 \cdot 3 \cdot \ldots \cdot (i-1) \cdot i \cdot (i+1) \cdot \ldots \cdot (n+1)) + i = \\ &= i(2 \cdot 3 \cdot \ldots \cdot (i-1) \cdot (i+1) \cdot \ldots \cdot (n+1)) + i = \\ &= i(2 \cdot 3 \cdot \ldots \cdot (i-1) \cdot (i+1) \cdot \ldots \cdot (n+1) + 1)\end{aligned}$$

que é divisível por i e, portanto, um número composto. □

Lema 4.1. *Seja p um número primo. Os números $\binom{p}{i}$, onde $0 < i < p$, são todos divisíveis por p.*

Demonstração. Por definição,

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

Evidentemente, se $i = 1$ o resultado segue. Assim, supondo $1 < i < p$ tem-se $i!|p(p-1)\cdots(p-i+1)$. Uma vez que $i < p$ resulta que $(i!, p) = 1$, então $i!|(p-1)\cdots(p-i+1)$. Escrevendo

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

facilmente observa-se que o resultado vale.

□

Nesse tópico será utilizado o símbolo $\left[\frac{a}{b}\right]$ para designar o quociente da divisão de a por b na divisão euclidiana.

Proposição 4.2. *Seja $a \in \mathbb{N}$ e $b, c \in \mathbb{N}^*$. Então, o quociente da divisão por c do quociente da divisão de a por b é igual ao quociente da divisão de a por b vezes c, ou seja,*

$$\left[\frac{\left[\frac{a}{b}\right]}{c}\right] = \left[\frac{a}{bc}\right].$$

Demonstração. Considere

$$q_1 = \left[\frac{a}{b}\right] \quad e \quad q_2 = \left[\frac{\left[\frac{a}{b}\right]}{c}\right].$$

Então, pela divisão euclidiana, $a = bq_1 + r_1$, com $r_1 \leq b-1$. Por outro lado, também pela divisão euclidiana, $q_1 = \left[\frac{a}{b}\right] = cq_2 + r_2$, com $r_2 \leq c-1$.

Portanto, $a = bq_1 + r_1 = b(cq_2 + r_2) + r_1 = bcq_2 + br_2 + r_1$.

Observando ainda que, $br_2 + r_1 \leq b(c-1) + b - 1 = bc - 1$, concluí-se que q_2 é o quociente da divisão de a por bc, ou seja,

$$q_2 = \left[\frac{a}{bc}\right].$$

□

Observação 4.1. Dados p primo e m um número natural, denota-se por $E_p(m)$ ao expoente da maior potência de p que divide m, ou seja, ao expoente que aparece na decomposição de m em fatores primos.

Teorema 4.2. *(Legendre) Sejam n um número natural e p um número primo. Então*

$$E_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + ...$$

Demonstração. Observe que, pelo Princípio da Boa Ordem, existe um número natural r tal que $p^i > n$ para todo $i \geq r$. Então, $\left[\frac{n}{p^i}\right] = 0$, se $i \geq r$. Para demonstrar o resultado usa-se indução sobre n. Para $n = 0$ tem-se $E_p(0!) = 0$. Suponha, agora que o resultado vale para todo $m < n$. Os múltiplos de p entre 1 e n são

$$p, 2p, \ldots, \left[\frac{n}{p}\right] p.$$

Pode-se, então, escrever,

$$E_p(n!) = \left[\frac{n}{p}\right] + E_p\left(\left[\frac{n}{p}\right]!\right).$$

Mas, por hipótese de indução,

$$E_p\left(\left[\frac{n}{p}\right]!\right) = \left[\frac{\left[\frac{n}{p}\right]}{p}\right] + \left[\frac{\left[\frac{n}{p}\right]}{p^2}\right] + \ldots$$

Pela Proposição 4.2, $\dfrac{\left[\frac{n}{p}\right]}{p} = \left[\dfrac{n}{p^2}\right], \dfrac{\left[\frac{n}{p}\right]}{p^2} = \left[\dfrac{n}{p^3}\right]$, etc...

Portanto,

$$E_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$$

□

Exemplo 4.1. Encontrar a decomposição de 20! em fatores primos e descobrir com quantos zeros termina a representação decimal deste número.

Para resolver o problema é necessário encontrar o valor de $E_p(20!)$ para todo primo $p \leq 20$. Tem-se que:

$$E_2(20!) = \left[\frac{20}{2}\right] + \left[\frac{20}{4}\right] + \left[\frac{20}{8}\right] + \left[\frac{20}{16}\right] = 10 + 5 + 2 + 1 = 18$$

$$E_3(20!) = \left[\frac{20}{3}\right] + \left[\frac{20}{9}\right] = 6 + 2 = 8$$

$$E_5(20!) = \left[\frac{20}{5}\right] = 4$$

$$E_7(20!) = \left[\frac{20}{7}\right] = 2$$

$$E_{11}(20!) = \left[\frac{20}{11}\right] = 1$$

$$E_{13}(20!) = \left[\frac{20}{13}\right] = 1$$

$$E_{17}(20!) = \left[\frac{20}{17}\right] = 1$$

$$E_{19}(20!) = \left[\frac{20}{19}\right] = 1$$

Logo $20! = 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$. Como existem 4 fatores 5 neste número, ele termina com quatro zeros.

Definição 4.2. *Seja um número natural n, com $n > 0$. Chama-se representação n-ádica de um número natural m à sua representação na base n.*

Exemplo 4.2. Seja o número natural 295. Apresenta-se abaixo sua representação n-ádica para n de 2 a 9:

- $100100111_{(2)} = 1 \cdot 256 + 0 \cdot 128 + 0 \cdot 64 + 1 \cdot 32 + 0 \cdot 16 + 0 \cdot 8 + 1 \cdot 4 + 1 \cdot 2 + 1 = 256 + 0 + 0 + 32 + 0 + 0 + 4 + 2 + 1 = 295$
- $101221_{(3)} = 1 \cdot 243 + 0 \cdot 81 + 1 \cdot 27 + 2 \cdot 9 + 2 \cdot 3 + 1 = 243 + 0 + 27 + 18 + 6 + 1 = 295$
- $10213_{(4)} = 1 \cdot 256 + 0 \cdot 64 + 2 \cdot 16 + 1 \cdot 4 + 3 = 256 + 0 + 32 + 4 + 3 = 295$
- $2140_{(5)} = 2 \cdot 125 + 1 \cdot 25 + 4 \cdot 5 + 0 = 250 + 25 + 20 + 0 = 295$
- $1211_{(6)} = 1 \cdot 216 + 2 \cdot 36 + 1 \cdot 6 + 1 = 216 + 72 + 6 + 1 = 295$
- $601_{(7)} = 6 \cdot 49 + 0 \cdot 7 + 1 = 294 + 0 + 1 = 295$
- $447_{(8)} = 4 \cdot 64 + 4 \cdot 8 + 7 = 256 + 32 + 7 = 295$
- $357_{(9)} = 3 \cdot 81 + 5 \cdot 9 + 7 = 243 + 45 + 7 = 295$

Teorema 4.3. *Sejam $p, n \in \mathbb{N}^*$ com p primo. Suponha que*

$$n = n_r p^r + n_{r-1} p^{r-1} + ... + n_1 p + n_0.$$

seja a representação p-ádica de n. Então,

$$E_p(n!) = \frac{n - (n_0 + n_1 + ... + n_r)}{p - 1}.$$

Demonstração. Por definição, $0 \leq n_i < p$. Então:

$$\left[\frac{n}{p}\right] = n_r p^{r-1} + n_{r-1} p^{r-2} + ... + n_2 p + n_1$$

$$\left[\frac{n}{p^2}\right] = n_r p^{r-2} + n_{r-1}p^{r-3} + ... + n_2$$

$$\cdots$$

$$\left[\frac{n}{p^r}\right] = n_r.$$

Daí, usando a fórmula do Teorema de Legendre e somando e subtraindo n_0 na expressão resultante tem-se que:

$$E_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + ... + \left[\frac{n}{p^r}\right] = n_r\frac{p^r-1}{p-1} + n_{r-1}\frac{p^{r-1}-1}{p-1} + \cdots + n_1 =$$

$$= \frac{n_r p^r + n_{r-1}p^{r-1} + \cdots + n_1 p + n_0 - (n_r + n_{r-1} + \cdots + n_1 + n_0)}{p-1} =$$

$$= \frac{n - (n_0 + n_1 + \cdots + n_r)}{p-1}.$$

□

Exemplo 4.3. Encontre a decomposição de 20! utilizando a fórmula do Teorema 4.3 e compare com o resultado do Exemplo 4.1.

Para resolver este exercício é necessário encontrar a representação de 20 nas bases $2, 3, 5, 7, 11, 13, 17$ e 19. Tem-se que

- $10100_{(2)} = 1 \cdot 16 + 0 \cdot 8 + 1 \cdot 4 + 0 \cdot 2 + 0$
- $202_{(3)} = 2 \cdot 9 + 0 \cdot 3 + 2$
- $40_{(5)} = 4 \cdot 5 + 0 = 20 + 0$
- $26_{(7)} = 2 \cdot 7 + 6 = 14 + 6$
- $19_{(11)} = 1 \cdot 11 + 9$
- $17_{(13)} = 1 \cdot 13 + 7$
- $13_{(17)} = 1 \cdot 17 + 3$
- $11_{(19)} = 1 \cdot 19 + 1$

A partir daí tem-se que:

$$E_2(20!) = \frac{20 - (0+0+1+0+1)}{2-1} = 18$$

$$E_3(20!) = \frac{20-(2+0+2)}{3-1} = 8$$

$$E_5(20!) = \frac{20-(0+4)}{5-1} = 4$$

$$E_7(20!) = \frac{20-(6+2)}{7-1} = 2$$

$$E_{11}(20!) = \frac{20-(9+1)}{11-1} = 1$$

$$E_{13}(20!) = \frac{20-(7+1)}{13-1} = 1$$

$$E_{17}(20!) = \frac{20-(3+1)}{17-1} = 1$$

$$E_{19}(20!) = \frac{20-(1+1)}{19-1} = 1$$

4.2 Números Primos e Progressões Aritméticas

Teorema 4.4. *(Dirichlet) Se $d \geq 2$ e $a \neq 0$ são inteiros primos entre si então a progressão aritmética $a, a+d, a+2d, ..., a+(n-1)d$, contém uma infinidade de números primos.*

A demonstração foge do escopo deste trabalho, mas pode ser encontrada em HASSE, 1980.

O resultado abaixo está relacionado à conjetura de que existem infinitos números de Mersenne compostos.

Proposição 4.3. *(Powell-Israel) Sejam m, n números inteiros tais que, $m > 1$ e $mn > 2$ e p um número primo. Então existe uma infinidade de números compostos da forma $m_p - n$.*

Demonstração. Pelo Teorema Fundamental da Aritmética $mn - 1$ possui pelo menos um fator primo q. Então, $q \mid m$. Pelo Teorema de Dirichlet (4.4) existem infinitos primos p, tais que $p \equiv q - 2 \mod q - 1$. Portanto, existe uma infinidade de números inteiros compostos $m^p - n$ com p primo.

□

Observação 4.2. Em 2 de março de 1998, M. Topic, encontrou uma progressão aritmética que possui dez termos consecutivos primos. A razão da progressão aritmética é 210. O primeiro destes termos é o número

$$p = 100099697246971424763778665558796984032950932468919004180360341775890434170334888215906722971 9.$$

5 A Conjetura de Goldbach

Em 1742, em uma carta a Euler, Goldbach disse acreditar que todo inteiro maior do que 5, ou seja, todo inteiro maior ou igual a 6, podia ser escrito como a soma de três primos. Euler respondeu que era fácil ver que essa afirmação era equivalente à:

Todo inteiro par maior ou igual a 4 é a soma de dois números primos.

De fato, se a segunda afirmação for suposta verdadeira tem-se que, para todo $n \geq 3$, $2n-2 = p_1+p_2$, onde p_1 e p_2 são primos. Portanto, $2n = 2+p_1+p_2$ e $2n+1 = 3+p_1+p_2$, o que demonstra a primeira afirmação.

Reciprocamente, suposta verdadeira a primeira afirmação tem-se que, para $2n \geq 4$, $2n+2 = p_1+p_2+p_3$, onde p_1, p_2 e p_3 são primos. Como $2n+2$ é par, um destes primos é necessariamente par, ou seja, é igual a 2. Supondo, $p_2 = 2$ tem-se $2n = p_1 + p_2$.

No entanto, a validade da segunda afirmação, agora conhecida como Conjetura de Goldbach, permanece sem demonstração até a conclusão deste trabalho. Pelo fato de existirem infinitos primos, facilmente nota-se que vale a seguinte variação da Conjetura de Goldbach:

Proposição 5.1. *Existe uma quantidade enumerável de naturais tais que a Conjetura de Goldbach é válida.*

Demonstração. Tome $b \geq 3$, um número natural. Como existem infinitos números primos, quando b percorre o conjunto dos naturais, obtém-se a sequência $p_1 + 3, p_2 + 3, p_2 + 3, ..., p_i + 3, ...$, com os p_i's primos distintos e ímpares. Sendo assim, as somas $p_i + 3$ são números pares, ou seja, $2n_i = p_i + 3$, para uma quantidade enumerável de n_i. Portanto, a Conjetura de Goldbach vale para uma quantidade enumerável de naturais. □

Generalizando este resultado, tem-se que escolhendo $2 < p < q \leq p_i$, primos, a sequência,

$$p_1 + p, p_2 + p, p_3 + p, ..., p_i + p, ...,$$

com os $p_i's$ primos distintos, também tem por elementos apenas números pares, valendo a Conjetura de Goldbach para os n_i da forma $2n_i = p_i + p$.

Apesar disso, as dificuldades para demonstrar a Conjetura permanecem. Durante o ano de 2011 cursava o Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), quando, na disciplina de Fundamentos da Aritmética me deparei com o seguinte exercício (Hefez, pg 95, ex 7.S.6)

Existe uma correspondência biunívoca entre pares de primos gêmeos e números n tais que $n^2 - 1$ possui quatro divisores.

O problema imediatamente me interessou, pois relacionava-se diretamente a um outro problema em aberto da matemática, a saber: *Existem infinitos primos gêmeos*? Então decidi resolver o exercício, pois demonstrar que existem infinitos valores de n para os quais $n^2 - 1$ tem quatro divisores equivale a responder afirmativamente a questão acima. A resolução do exercício é:

Dado um par de primos gêmeos p e q, tome $n = p + 1$. Então, $p = n - 1$. Por outro lado, $n = q - 1$ e, portanto, $q = n + 1$. Tem-se então que $p \cdot q = (n-1)(n+1) = n^2 - 1$. Os divisores de $n^2 - 1$ são $1, p, q$ e $n^2 - 1$, ou seja, quatro divisores.

Reciprocamente, se $n^2 - 1$ possui quatro divisores ele é da forma $p \cdot q = n^2 - 1$, com p e q primos. Então,

$$p \cdot q = n^2 - 1 = (n + 1)(n - 1).$$

Como p e q são primos tem-se, supondo, sem perda de generalidade, $p < q$, que $p = n - 1$ e $q = n + 1$. Logo, p e q são primos gêmeos. A unicidade é garantida pelo Teorema Fundamental da Aritmética.

Resolver o exercício foi simples, no entanto, demonstrar a existência de infinitos n para os quais tal propriedade vale mostrou-se tão inatingível quanto a demonstração da afirmação original sobre se existem infinitos pares de primos gêmeos. No entanto, analisando o exercício, imaginei o que aconteceria se em vez de considerar as diferenças de quadrado $n^2 - 1$ fossem estudadas as diferenças $n^2 - a^2$ para um número natural a qualquer.

Uma primeira ideia foi de que o resultado do exercício pudesse ser estendido para o caso geral, ou seja, que existisse uma correspondência biunívoca entre primos equidistantes de um determinado n e as diferenças de quadrados $n^2 - a^2$ que possuíssem quatro divisores. Observe que tal diferença pode ser fatorada como $(n + a)(n - a)$. No entanto, ao estudar tal diferença para diversos valores percebi, com a ajuda do Prof. Dr. Rômulo Campos Lins e Prof Dr. Henrique Lazari, que em alguns determinados casos o resultado não era válido.

Por exemplo, se for escolhido $n = 6$ e $a = 3$ tem-se que $n^2 - a^2 = 6^2 - 3^2 = 27 = (6 + 3)(6 - 3) = 9 \cdot 3$, que possui quatro divisores, a saber 1, 3, 9 e 27, mas 9 e 3 não

são primos equidistantes de 6.

Portanto, para o caso geral, é necessário colocar, como hipótese, que $n+a$ e $n-a$ sejam primos entre si. Observe que esta condição é satisfeita no caso em que $a = 1$. Adicionalmente, perceba que se $a = n-1$ obtem-se que $n+a = 2n-1$ e $n-a = 1$ e, uma vez que 1 não é primo, estes casos também precisam ser excluídos.

Levando em conta estas restrições formulei o seguinte resultado geral:

Proposição 5.2. *Para cada número natural $n > 3$, suponha que exista um número natural a, $0 < a < n-1$, tal que $(n-a, n+a) = 1$. Nestas condições, para cada par n e a, existe uma correspondência biunívoca entre pares de primos equidistantes de n e os números da forma $n^2 - a^2$ que possuem quatro divisores.*

Demonstração. De fato, dado um par de primos p e q equidistantes de n, suponha, sem perda de generalidade, que $p < n$ e tome $a = n-p$. Então, $n = p+a$ e $p = n-a$. Como p e q são equidistantes de n, $n = q-a$ e tem-se que $q = n+a$. Então $p \cdot q = (n-a)(n+a) = n^2 - a^2$. Como, por hipótese, $(n-a, n+a) = 1$, os divisores de $n^2 - a^2$ são 1, p, q e $n^2 - a^2$, ou seja, quatro divisores.

Reciprocamente, se $n^2 - a^2$ possui quatro divisores e $(n-a, n+a) = 1$, então $n^2 - a^2$ é da forma $p \cdot q = n^2 - a^2$. Além disso,

$$p \cdot q = n^2 - a^2 = (n+a)(n-a).$$

Como $(n-a, n+a) = 1$ e $n-a > 1$ (pois, $0 < a < n-1$), tem-se que p e q são primos. De fato, suponha, por absurdo, que um deles, por exemplo p, seja composto. Então, pelo Teorema Fundamental da Aritmética, ele seria escrito como $p = p_1 p_2$. Logo, $p_1 | n^2 - a^2$, $p_2 | n^2 - a^2$, $p | n^2 - a^2$, $q | n^2 - a^2$, $p_1 p_2 q | n^2 - a^2$ e $1 | n^2 - a^2$ e $n^2 - a^2$ teria seis divisores, o que é contrário à hipótese.

Supondo, sem perda de generalidade, $p < q$, tem-se que $p = n-a$ e $q = n+a$. Logo, p e q são primos equidistantes de n. A unicidade de a para p e q é garantida pelo Teorema Fundamental da Aritmética.

□

Após demonstrar essa proposição percebi que havia uma ligação entre ela e a Conjetura de Goldbach, pois, considerando-se os primos p e q da proposição acima tem-se que $p = n-a$ e $q = n+a$, de onde $p+q = n-a+n+a = 2n$. Ou seja, $p+q = 2n$. Desta maneira, demonstrar que para todo n existe um número a nas condições da Proposição 5.2 é equivalente a demonstrar a Conjetura de Goldbach. Estudando ainda mais o assunto percebi, então, que falar sobre $p+q = 2n$ para $2n \geq 4$ era equivalente a falar sobre $\frac{p+q}{2} = n$, $n \geq 2$. Essa conclusão equivale à afirmar que para todo $n \geq 2$ ou n é primo, ou existem primos equidistantes de n. Em resumo significa que, para todo número $n \geq 2$ pode-se afirmar que n é a média aritmética de 2 primos. Chegando a esta conclusão, por volta de agosto de 2012, resolvi entrar em contato com alguns pesquisadores do Departamento de Matemática da UNESP/RC. Conversei com a Profa.

Dra. Eliris Cristina Rizziolli e com o Prof. Dr. Henrique Lazari sobre meus estudos e enviei para eles, via e-mail, parte de minhas conclusões. A partir do incentivo deles prossegui as pesquisas.

Encontrei, num artigo da Wikipedia, em inglês [7] uma afirmação similar à de que para todo número $n \geq 2$, n é a média aritmética de 2 primos. Tal afirmação, citada como Conjetura de Lawson, dizia *"Para todo I maior do que 2 existe um par de primos equidistantes de I"*. No entanto, a Conjetura de Lawson falha para $I = 3$. É necessário, então complementar esta afirmação por dar a I a possibilidade de ser primo. Quando se faz isto a ampliação da Conjetura de Lawson, expressa abaixo é equivalente à Conjetura de Goldbach. Formalizando:

Proposição 5.3. *A Conjetura de Golbach é equivalente a afirmação de que todo natural $n \geq 2$ é a média aritmética de dois números primos, distintos ou não.*

Demonstração. De fato, suponha válida a Conjetura de Goldbach. Então, para todo $n \geq 2$ tem-se que $2n \geq 4$ e, por Goldbach, existem primos p e q, tais que $2n = p + q$. Portanto, $n = \dfrac{p+q}{2}$.

Reciprocamente, se vale que, para todo $n \geq 2$, n é a média aritmética de, no máximo, dois números primos, existem p e q, primos, distintos ou não, tais que $n = \dfrac{p+q}{2}$. Ou seja, $2n = p + q$, com $2n \geq 4$ e vale a Conjetura de Goldbach. □

Uma vez provado este resultado, demonstra-se agora que essa afirmação é equivalente à Proposição 5.2 e, portanto, as duas afirmações são equivalentes à Conjetura de Goldbach. Apenas, neste caso, os primos p e q devem ser distintos para se conseguir satisfazer a hipótese de que $a > 0$. Formalizando:

Proposição 5.4. *Se para todo $n \geq 2$, existir $0 < a < n - 1$ tal que $(n + a, n - a) = 1$ e $n^2 - a^2$ tenha 4 divisores, então existem p e q primos, tais que, $n = \dfrac{p+q}{2}$.*

Demonstração. Se existe $a < n - 1$ tal que $n^2 - a^2$ tem quatro divisores então, pela Proposição 5.2, existem p e q primos tais que $pq = n^2 - a^2$, com $p = n - a$ e $q = n + a$. Logo $p + q = n - a + n + a = 2n$ e $n = \dfrac{p+q}{2}$.

Reciprocamente, se $n = \dfrac{p+q}{2}$ com p e q primos, tome $a = \dfrac{q-p}{2}$. Então

$$n^2 - a^2 = \frac{(p+q)^2}{4} - \frac{(q-p)^2}{4} = \frac{4pq}{4} = pq,$$

e, portanto, $n^2 - a^2$ tem quatro divisores.

□

Continuando os estudos, percebi que existe um relacionamento entre as diferenças de quadrados, nas condições da Proposição 5.2, e as equações quadráticas da forma $x^2 - (p + q)x + pq = 0$, com p e q primos distintos. Observe que, p e q são as raízes da equação e, portanto, existe uma correspondência biunívoca entre estas diferenças

de quadrados e as equações quadráticas nas quais o coeficiente do termo x^2 é igual a 1 e cujas raízes são primos p e q, distintos.

Proposição 5.5. *Para cada número natural $n > 3$, seja um número natural a, $0 < a < n-1$, tal que $(n-a, n+a) = 1$. Nestas condições, existe uma correspondência biunívoca entre diferenças de quadrados que possuem quatro divisores e equações quadráticas da forma $x^2 - (p+q)x + pq = 0$, com p e q primos distintos.*

Demonstração. De fato, dado $n^2 - a^2$ com quatro divisores tem-se, pela Proposição 5.2, que $n^2 - a^2 = pq$. Toma-se então $x^2 - (p+q)x + pq = 0$ para a equação.

Reciprocamente, dada a equação $x^2 - (p+q)x + pq = 0$, com p e q primos distintos, tome $n = \dfrac{p+q}{2}$ e $a = \dfrac{q-p}{2}$. Então, como demonstrado na Proposição 5.4, tem-se que $n^2 - a^2 = pq$. □

Observação 5.1. Um ponto interessante a se observar é que, dada uma função quadrática da forma $f(x) = x^2 - (p+q)x + pq = 0$, com p e q primos, tomando-se $n = \dfrac{p+q}{2}$ e $n^2 - a^2 = pq$ tem-se que o vértice da parábola que representa esta função tem coordenadas $(n - a^2)$. Ou seja, demonstrar que para todo $n > 2$ encontra-se um a, tal que $0 < a < n - 1$, com $(n + a, n - a) = 1$,$n^2 - a^2$ tenha quatro divisores e $(n, -a^2)$ seja o vértice da parábola que representa a função $f(x) = x^2 - 2nx + (n^2 - a^2)$, também se relaciona com demonstrar a Conjetura de Goldbach.

Simplificando, se para todo $n > 2$, existir um número natural a, tal que $0 < a < n - 1$, de maneira que a função quadrática $f(x) = x^2 - 2n + (n^2 - a^2)$ tenha por raízes dois números primos distintos, então a Conjetura de Goldbach é verdadeira.

A Tabela 5.1 mostra que para muitos valores de n (o número da coluna) é possível encontrar um a (o número da linha) e primos p e q que satisfazem a igualdade acima. Por exemplo, quando se escolhe $n = 13$ e $a = 6$ tem-se que $n^2 - a^2 = 13^2 - 6^2 = 169 - 36 = 133 = 7 \cdot 19$. Então, 7 e 19 são os primos de Goldbach para $n = 13$. Estes primos podem ser localizados na tabela por se seguir as diagonais a partir do número que se encontra no cruzamento da linha 13 com a coluna 6. Na tabela n, a e $n^2 - a^2$ estão sublinhados. As diagonais percorridas para encontrar p e q estão em itálico e os primos p e q estão em negrito.

Utilizando o mesmo processo para outros valores de n e de a para os quais $n^2 - a^2$ possuam quatro divisores o leitor perceberá que pode encontrar diversos primos de Goldbach. No entanto, a demonstração de que existe um a para todo $n > 2$, nas condições da Proposição 5.4 , equivalente à verificação da Conjetura de Goldbach, ainda não foi possível.

Pelos estudos que fiz concluí que tal demonstração é tão complexa quanto a própria Conjetura de Goldbach, mas deixo aos interessados o incentivo para procurar respostas e caminhos adicionais.

	1	2	3	4	5	6	7	8	9	10	11	12
1	0	-3	-8	-15	-24	-35	-48	-63	-80	-99	-120	-143
2	3	0	-5	-12	-21	-32	-45	-60	-77	-96	-117	-140
3	8	5	0	-7	-16	-27	-40	-55	-72	-91	-112	- 135
4	15	12	7	0	-9	-20	-33	-48	-65	-84	-105	-128
5	24	21	16	9	0	-11	-24	-39	-56	-75	-96	-119
6	35	32	27	20	11	0	-13	-28	-45	-64	-85	-108
7	48	45	40	33	24	13	0	-15	-32	-51	-72	-95
8	*63*	60	55	48	39	28	15	0	-17	-36	-57	-80
9	80	*77*	72	65	56	45	32	17	0	-19	-40	-63
10	99	96	*91*	84	75	64	51	36	19	0	-21	-44
11	120	117	112	*105*	96	85	72	57	40	21	0	-23
12	143	140	135	128	*119*	108	95	80	63	44	23	0
13	168	165	160	153	144	133	120	105	88	69	48	25
14	195	192	187	180	*171*	160	147	132	115	96	75	52
15	224	221	216	*209*	200	189	176	161	144	125	104	81
16	255	252	*247*	240	231	220	207	192	175	156	135	112
17	288	*285*	280	273	264	253	240	225	208	189	168	145
18	*323*	320	315	308	299	288	275	260	243	224	203	180
19	360	357	352	345	336	325	312	297	280	261	240	217
20	399	396	391	384	375	364	351	336	319	300	279	256
21	440	437	432	425	416	405	392	377	360	341	320	296
22	483	480	475	468	459	448	435	420	403	384	363	340
23	528	525	520	513	504	493	480	465	448	429	408	385
24	575	572	567	560	551	540	527	512	495	476	455	432
25	624	621	616	609	600	589	576	561	544	525	504	481
26	675	672	667	660	651	640	627	612	595	576	555	532
27	728	725	720	713	704	693	680	665	648	629	608	585
28	783	780	775	768	759	748	735	720	703	684	663	640
29	840	837	832	825	816	805	792	777	760	741	720	697
30	899	896	891	894	885	874	861	846	829	800	869	756
31	960	957	952	945	936	925	912	897	880	861	840	907
32	1023	1020	1015	1008	999	988	975	960	943	924	903	880
33	1088	1085	1080	1073	1064	1053	1040	1025	1008	989	968	945
34	1155	1152	1147	1140	1131	1120	1107	1092	1075	1056	1035	1012
35	1224	1221	1216	1209	1200	1189	1176	1161	1144	1125	1104	1081
36	1295	1292	1287	1280	1271	1260	1247	1232	1215	1196	1175	1152
37	1368	1365	1360	1353	1344	1333	1320	1305	1288	1269	1248	1225
38	1443	1440	1435	1428	1419	1408	1395	1380	1363	1344	1323	1300
39	1520	1517	1512	1505	1496	1485	1472	1457	1440	1421	1400	1377
40	1599	1596	1591	1584	1575	1564	1551	1536	1519	1500	1479	1456

Tabela 5.1: Tabela de Diferenças de Quadrados

6 Aplicação do Tema Divisibilidade em Sala de Aula

Apresenta-se agora uma sugestão para a utilização do tema divisibilidade na Escola Básica. O objetivo é mostrar aos alunos como diferentes áreas da Matemática estão interligadas e como entender esta ligação é de ajuda para uma melhor compreensão e aplicação dos conteúdos estudados em sala de aula.

No Capítulo 4 deste trabalho foram analisadas algumas ligações entre fatoriais e divisibilidade. Em especial o Exemplo 4.1, que mostra como encontrar a decomposição de 20! utilizando a função $E_p(m)$, na qual p é um número primo e m é um número natural, fornece um tema bastante interessante para utilização em uma classe do segundo ano do Ensino Médio, associado ao ensino de Análise Combinatória.

Essa função, definida na Observação 4.1, e que retorna o expoente da maior potência de p que divide m, ou seja, o expoente que aparece na decomposição de m em fatores primos, é simples o suficiente para ser trabalhada com os alunos do Ensino Médio. Uma sequência didática para trabalhar o tema é:

1. Recordar a ideia da decomposição de um número em fatores primos;
2. Como motivação, explicar o relacionamento entre a decomposição de números muito grandes e a segurança na internet;
3. Revisar o conceito de fatorial, trabalhado anteriormente no estudo da Análise Combinatória e do Binômio de Newton;
4. Definir a função $E_p(m)$ e trabalhar exemplos para uma melhor compreensão do conceito;
5. Tornar claro como a função está associada à decomposição de fatoriais em fatores primos, conforme explicado no Teorema 4.2 (De Legendre);
6. Apresentar a fórmula do Teorema e exemplos com números pequenos;
7. Calcular a decomposição do fatorial de 20 usando o Exemplo 4.1. Essa decomposição é dada por $2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$.

8. Comentar o trabalho envolvido no cálculo desta decomposição utilizando o algoritmo tradicional, destacando que, antes deste ser aplicado, é necessário calcular o valor de 20!;

9. Escolhendo um fatorial menor, por exemplo, 10! (veja Exemplo 6.1), mostrar como encontrar a decomposição utilizando o teorema de Legendre e utilizando o algoritmo tradicional da decomposição em fatores primos;

10. Aplicar alguns exercícios para fixação os conceitos.

Se o professor tiver tempo e achar interessante poderá ainda mostrar aos alunos como descobrir com quantos zeros termina 20! ou outro fatorial qualquer, conforme explicado no Exemplo 4.1.

Concluindo, apresenta-se abaixo uma comparação entre os dois processos e alguns exercícios para aplicação em sala de aula.

Exemplo 6.1. Decomponha 10! pelo método tradicional e usando o Teorema de Legendre.

Resolução:

Para utilizar o algoritmo tradicional inicialmente calcula-se o valor de 10!, ou seja, $10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 = 3628800$. Depois divide-se este número pelos números primos em ordem crescente até que o resultado seja 1.

3628800	2
1814400	2
907200	2
453600	2
226800	2
113400	2
56700	2
28350	2
14175	3
4725	3
1575	3
525	3
175	5
35	5
7	7
1	

Então $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$.

Usando o Teorema de Legendre é necessário encontrar o valor de $E_p(10!)$ para todo primo $p \leq 10$. Tem-se que:

$$E_2(10!) = \left[\frac{10}{2}\right] + \left[\frac{10}{4}\right] + \left[\frac{10}{8}\right] = 5 + 2 + 1 = 8$$

$$E_3(10!) = \left[\frac{10}{3}\right] + \left[\frac{10}{9}\right] = 3 + 1 = 4$$

$$E_5(10!) = \left[\frac{10}{5}\right] = 2$$

$$E_7(10!) = \left[\frac{10}{7}\right] = 1$$

Logo $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$.

Observe que, calculando pelo Teorema não é necessário encontrar o valor do fatorial, o que facilita, em muito, encontrar a decomposição do fatorial para números grandes.

Exercício 6.1. Resolva os exercícios abaixo utilizando a função $E_p(m)$ e o Teorema de Legendre (Teorema 4.2).

1. Quais as maiores potências de 3 e 7 que dividem 10000!?
2. Com quantos zeros termina a representação decimal de 10000!?
3. Ache a maior potência de 108 que divide 10000!.
4. Ache o menor valor de n tal que a maior potência de 7 que divide $n!$ seja 7^{34}.

Referências

[1] GAUSS, C. F., *Disquisitiones arithmeticae.* Tradução para o inglês de Clarke, A. A.; Waterhouse, W. C. Londres: Springer-verlag, 1966.

[2] HEFEZ, A., *Elementos de aritmética.* Rio de Janeiro: SBM, 2011. 176 p. (Coleção do Professor de Matemática; 2).

[3] MAYER, R., *Teoria dos Números*, 2005. Disponível em: $< http://www.mat.unb.br/\ maierr/tnotas.pdf >$. Acesso em: 18 jan. 2013.

[4] OLIVEIRA, K.; CORCHO, A. J., *Iniciação à Matemática.* 1. ed. Maceió: SBM, 2010.

[5] RIBENBOIM, P., *Números Primos: Mistérios e Recordes.* Rio de Janeiro: IMPA, 2001.

[6] SANTOS, J. P. O., *Introdução à Teoria dos Números.* 1. ed. Rio de Janeiro: IMPA, 2007.

[7] TALK:GOLDBACH'S conjecture. , 2003. Disponível em: $< http://en.wikipedia.org/wiki/Talk:Goldbach\%27s\_conjecture >$. Acesso em: 18 jan. 2013.