Universidade Estadual de Campinas
Instituto de Matemática, Estatística e Computação Científica

Dissertação de Mestrado

# Tópicos de Teoria dos Números
# e
# Teste de Primalidade

Por

**Jackson Martins Reis**

Mestrado Profissional em Matemática – Campinas – SP

**Orientador: Prof. Dr. José Plínio de Oliveira Santos**

# TÓPICOS DE TEORIA DOS NÚMEROS E TESTE DE PRIMALIDADE

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por **Jackson Martins Reis** e aprovada pela comissão julgadora.

Campinas, 29 de julho de 2009.

Prof. Dr. José Plínio de Oliveira Santos
Orientador

**Banca Examinadora:**

Prof. Dr. José Plínio de Oliveira Santos
Prof. Dr. Emerson Alexandre de Oliveira Lima
Prof. Dr. Eduardo Henrique de Mattos Brietzke

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica, Unicamp, como requisito para a obtenção de título de Mestre em Matemática.

**FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP**
Bibliotecária: Maria Fabiana Bezerra Müller – CRB8 / 6162

Reis, Jackson Martins
R277t Tópicos de teoria dos números e teste de primalidade/Jackson Martins Reis-- Campinas, [S.P. : s.n.], 2009.

Orientador : José Plínio de Oliveira Santos
Dissertação (mestrado profissional) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1.Congruências e restos. 2.Números - Divisibilidade. 3.Números naturais. 4.Números primos. I. Santos, J. Plínio O. (José Plínio de Oliveira). II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: Topics of numbers theory and primality test

Palavras-chave em inglês (Keywords): 1. Congruences and residues. 2. Numbers,, Divisibility of. 3. Whole numbers. 4. Prime numbers.

Área de concentração: Teoria dos Números

Titulação: Mestre em Matemática

Banca examinadora: José Plínio de Oliveira Santos – (IMECC- UNICAMP)
Emerson Alexandre de Oliveira Lima (UFRPE)
Eduardo Henrique de Mattos Brietzke (UFRGS)

Data da defesa: 29/07/2009

Programa de Pós-Graduação: Mestrado profissional em Matemática

**Dissertação de Mestrado Profissional defendida em 29 de julho de 2009 e Aprovada pela Banca Examinadora composta pelos Profs. Drs.**

**Prof. (a). Dr (a). JOSÉ PLÍNIO DE OLIVEIRA SANTOS**

**Prof. (a). Dr (a). EMERSON ALEXANDRE DE OLIVEIRA LIMA**

**Prof. (a). Dr (a). EDUARDO HENRIQUE DE MATTOS BRIETZKE**

A minha amada esposa Marília Martins

e aos meus queridos filhos Maria Carolina Martins e Lucas Martins,

Dedico

“Uma vida sem busca não é digna de ser vivida.” (Sócrates)

# Agradecimentos

A Deus, em primeiro lugar, indispensável em minha vida.

Ao meu querido pai Manoel Martins e a minha amada mãe Raimunda Martins, pelo ensino contínuo através de bons exemplos.

Ao meu sogro Antônio Vanderly e a minha sogra Maria Theresa, pelos ensinamentos de luta, persistência e determinação.

Aos meus queridos tios Joaquim Neves e Maria Assunção, pelo amor a mim e a minha família dedicados. Sinto-me confortavelmente como um filho.

Aos queridos compadres, Neto e Cristiane, pelo companheirismo de todas as horas.

Ao amigo Anselmo Raposo, pelo empenho no projeto ora realizado.

Ao professor Plínio, pela capacidade no cumprimento de sua função de mestre e pela aceitação de orientar-me na realização desta tarefa.

A professa Sueli, pela incansável dedicação e por acreditar neste projeto pioneiro de capacitação de docentes.

Ao meu ex-aluno Agnaldo, por ajudar-me na solução de problemas com o LATEX.

A Universidade Estadual do Maranhão e a Universidade Estadual de Campinas, pela oportunidade concedida para a realização do presente curso.

Aos amigos e professores do Mestrado, pelos ensinamentos e pelo bom convívio.

# Resumo

Neste trabalho foram abordados tópicos de Teoria dos Números e alguns testes de primalidade. Mostramos propriedades dos números inteiros, bem como alguns critérios de divisibilidade. Apresentamos também, além das propriedades do Máximo Divisor Comum e Mínimo Múltiplo Comum, interpretações geométricas dos mesmos. Foram estudados Tópicos da Teoria de Congruências e por fim trabalhamos alguns Testes de Primalidade, com respectivos exemplos.

**Palavras-chave**: Congruência, Divisibilidade, Números inteiros, Primalidade.

# Abstract

In this work were discussed topics of the theory of numbers and some primality tests. We show properties of whole numbers, and some criteria for divisibility. We also present, beyond the properties of the Common Dividing Maximum and Minimum Common Multiple, geometric interpretations of the same ones. They had been study topics of theory of congruences and finally we work some of primality tests, whith respective applications.

**Keywords**: Congruence, Divisibility, Whole Numbers, Primality.

# Sumário

# Introdução

Considerando a proposta do programa, que é o estudo de temas relevantes e que tenham conexão com as disciplinas da Matemática do Ensino Superior, neste trabalho foram estudados tópicos da Teoria dos números e Testes de Primalidade.

No primeiro capítulo, são apresentados os números inteiros e suas propriedades, além de diversas aplicações. Convém lembrar que, além da demonstração, foram feitas aplicações da primeira e segunda forma do princípio de indução finita.

No segundo capítulo, foram abordados diversos tópicos de divisibilidade, tais como, Máximo Divisor Comum e Mínimo Múltiplo Comum, além dos critérios de divisibilidade.

No terceiro capítulo, foi introduzida a definição de congruência e suas propriedades, além de resoluções de congruências lineares e sistemas de congruências lineares.

No quarto capítulo, foram apresentadas algumas fórmulas que geram números primos e alguns dos testes de primalidade.

# Capítulo 1

# Conjunto dos Números Inteiros

Os números inteiros formam um conjunto, que denotamos por $\mathbb{Z}$, o qual é munido de duas operações que chamamos de adição e multiplicação e denotamos por + e $\cdot$, respectivamente. Considerar que + e $\cdot$ são duas operações em $\mathbb{Z}$, significa que + e $\cdot$ são duas funções:

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \quad \text{e} \quad \cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$

sendo que a adição (+) associa a cada par ordenado de inteiros $(x,\ y)$, um único inteiro $x + y$, chamado soma de $x$ e $y$ e a multiplicação ($\cdot$) associa a cada par de inteiros um único inteiro $x \cdot y$, chamado produto de $x$ e $y$.

## 1.1 Conjunto dos números inteiros e subconjuntos especiais

### 1.1.1 Conjuntos dos números inteiros

O conjunto dos números inteiros, representado pela letra $\mathbb{Z}$, é o conjunto dado por:

$$\mathbb{Z} = \{\ldots,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \ldots\}\,.$$

### 1.1.2 Subconjuntos especiais de $\mathbb{Z}$

**a)** Conjunto dos números inteiros não nulos:

$$\mathbb{Z}^* = \{\ldots,\ -3,\ -2,\ -1,\ 1,\ 2,\ 3,\ \ldots\} = \{x \in \mathbb{Z} \,/\, x \neq 0\}\,.$$

**b)** Conjunto dos números inteiros não negativos:

$$\mathbb{Z}_+ = \{0,\ 1,\ 2,\ 3,\ \ldots\} = \{x \in \mathbb{Z} \ / \ x \geq 0\}\,.$$

**c)** Conjunto dos números inteiros positivos:

$$\mathbb{Z}_+^* = \{1,\ 2,\ 3,\ \ldots\} = \{x \in \mathbb{Z} \ / \ x > 0\}\,.$$

**d)** Conjunto dos números inteiros não positivos:

$$\mathbb{Z}_- = \{0,\ -1,\ -2,\ -3,\ \ldots\} = \{x \in \mathbb{Z} \ / \ x \leq 0\}\,.$$

**e)** Conjunto dos números inteiros negativos:

$$\mathbb{Z}_-^* = \{-1,\ -2,\ -3,\ \ldots\} = \{x \in \mathbb{Z} \ / \ x < 0\}\,.$$

## 1.2 Propriedades dos números inteiros

Inicialmente, introduzimos algumas propriedades de $\mathbb{Z}$ de forma axiomática, isto é, a partir de um conjunto de axiomas ou postulados, que caracterizam as operações de adição e multiplicação em $\mathbb{Z}$. A partir desses axiomas ou postulados, apresentaremos outras propriedades de $\mathbb{Z}$.

### 1.2.1 Axiomas ou postulados em $\mathbb{Z}$

Para cada $x,\ y,\ z \in \mathbb{Z}$, tem-se:

**($A_1$)** Associativa em relação à adição:

$$x + (y + z) = (x + y) + z.$$

**($A_2$)** Comutativa em relação à adição:

$$x + y = y + x.$$

**($A_3$)** Elemento neutro da adição:

$$x + 0 = 0 + x = x,$$

isto é, o zero é o elemento neutro da adição em $\mathbb{Z}$.

($A_4$) Existência do elemento oposto:

Existe um elemento $-x$ em $\mathbb{Z}$, chamado oposto de $x$ ou inverso aditivo de $x$, ou ainda simétrico de $x$ relativamente à operação de adição, satisfazendo:

$$x + (-x) = (-x) + x = 0.$$

($M_1$) Associativa em relação à multiplicação:

$$x(yz) = (xy)z.$$

($M_2$) Comutativa em relação à multiplicação:

$$xy = yx.$$

($M_3$) Elemento neutro da multiplicação:

$$1 \cdot x = x \cdot 1 = x.$$

($M_4$) Distributiva em relação à adição:

$$x(y + z) = xy + xz.$$

**Definição 1.1** ( Subtração em $\mathbb{Z}$ )**.** *Chama-se diferença de dois números inteiros $x$ e $y$ à soma $x + (-y)$. A subtração em $\mathbb{Z}$ é a operação:*

$$- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z},$$

*que associa a cada par ordenado de inteiros $(x,\ y)$ a diferença $x - y$.*

### 1.2.2 Outras propriedades de $\mathbb{Z}$

Sejam $x,\ y$ e $z$ números inteiros quaisquer, temos que:

($P_1$) $x + y = x \Rightarrow y = 0$.

Obs.: Esta propriedade indica que o "0" é o único elemento neutro da adição em $\mathbb{Z}$.

$(P_2)$ $x + y = 0 \Rightarrow y = -x$.

Obs.: Esta propriedade indica que o elemento oposto de um número inteiro $x$ é único.

$(P_3)$ $x + y = x + z \Rightarrow y = z$ (Lei do cancelamento da adição).

$(P_4)$ $-(-x) = x$.

$(P_5)$ $-(x + y) = -x - y$.

$(P_6)$ $x \cdot 0 = 0$.

$(P_7)$ $(-x) \cdot y = -xy$.

$(P_8)$ $(-x) \cdot (-y) = xy$.

$(P_9)$ $(x - y)z = xz - yz$.

$(P_{10})$ $x \cdot y = x \cdot z$ e $x \neq 0 \Rightarrow y = z$.

**Demonstrações**

$(P_1)$ $x + y = x \Rightarrow (-x) + (x + y) = (-x) + x$. Por $(A_1)$, $(A_2)$ e $(A_3)$ temos que:
$[(-x) + x] + y = 0 \Rightarrow 0 + y = 0 \Rightarrow y = 0$.

$(P_2)$ Se $x + y = 0 \Rightarrow (-x) + (x + y) = (-x) + 0$. Por $(A_1)$, $(A_2)$ e $(A_4)$ temos que:
$[(-x) + x] + y = (-x) \Rightarrow 0 + y = -x \Rightarrow y = -x$.

$(P_3)$ Se $x + y = x + z \Rightarrow (-x) + (x + y) = (-x) + (x + z)$. Por $(A_1)$
$[(-x) + x] + y = [(-x) + x] + z$, por $(A_4)$
$0 + y = 0 + z$ e, finalmente, por $(A_3)$ $y = z$.

$(P_4)$ Por $(A_4)$, temos que $-(-x) + (-x) = 0$, logo $[-(-x) + (-x)] + x = 0 + x$. Aplicando $(A_1)$ e $(A_3)$, temos: $-(-x) + [(-x) + x] = x \Rightarrow -(-x) + 0 = x \Rightarrow -(-x) = x$.

$(P_5)$ Queremos provar que $-(x + y) = -x - y$. Para isso, primeiro provamos que a soma $S = (x + y) + [(-x) + (-y)] = 0$.
Por $(A_1)$ $S = (x + y) + [(-x) + (-y)] = (x + y + (-x)) + (-y)$.

Por $(A_2)$ $S = (x + y) + [(-x) + (-y)] = (y + x + (-x)) + (-y)$.

Por $(A_4)$ $S = y + 0 + (-y) = y + (-y) = 0 \Rightarrow S = 0$.

Então, $(x + y) + [(-x) + (-y)] = 0$ e, portanto, $(x + y)$ e $(-x) + (-y)$ são opostos, logo $-(x + y) = (-x) + (-y) = (-x) - y \Rightarrow -(x + y) = -x - y$.

**$(P_6)$** Fazendo $x \cdot 0 = y$.

Por $(A_3)$ e $(M_4)$, temos:

$y = x \cdot 0 \Rightarrow y = x(0 + 0) = x \cdot 0 + x \cdot 0 = y + y$.

Logo, $y + y = y + 0$ e, portanto, pela propriedade de $(P_3)$, temos que $y = 0$, ou seja, $x \cdot 0 = 0$.

**$(P_7)$** $(-x) \cdot y = -x \cdot y$.

i) Temos que: $[(-x) + x] \cdot y = (-x) \cdot y + x \cdot y$.

ii) Também que: $[(-x) + x] \cdot y = 0 \cdot y = 0$. Logo, por (i) e (ii) temos:

$(-x) \cdot y + x \cdot y = 0$, ou seja, $xy$ e $(-x)y$ são simétricos $(P_2)$, portanto, $(-x) \cdot y = -xy$.

**$(P_8)$** $(-x) \cdot (-y) = xy$.

i) $(-x) \cdot (-y) = -[x \cdot (-y)]$ $(P_7)$.

ii) $x \cdot (-y) = -xy$ $(P_7)$.

De (i) e (ii), temos que $(-x) \cdot (-y) = -(-xy)$ e, finalmente, por $(P_4)$, $(-x) \cdot (-y) = xy$.

**$(P_9)$** $(x - y) \cdot z = xz - yz$

$(x - y) \cdot z + yz = [(x - y) + y]z = [x + ((-y) + y)]z = (x + 0)z = xz$.

Então, $(x - y) \cdot z + yz = xz \Rightarrow (x - y) \cdot z + yz + (-yz) = xz + (-yz)$

$\Rightarrow (x - y) \cdot z + 0 = xz - yz \Rightarrow (x - y) \cdot z = xz - yz$.

**$(P_{10})$** $xy = xz$ e $x \neq 0 \Rightarrow y = z$

$xy = xz \Rightarrow xy + (-xz) = xz + (-xz)$

$\Rightarrow xy - xz = 0$ e, como $x(y - z) = xy - xz$, temos $x(y - z) = 0$ e ainda, como $x \neq 0$

$\Rightarrow y - z = 0 \Rightarrow y - z + z = 0 + z \Rightarrow y + 0 = z \Rightarrow y = z$.

**Observação 1.1.** *Os axiomas e propriedades apresentados não são suficientes para caracterizar o conjunto dos números inteiros de maneira única, isto é, existem outras estruturas algébricas que*

*também satisfazem as referidas propriedades, como exemplo, podemos citar o conjunto dos números racionais* ($\mathbb{Q}$) *e o conjunto dos números reais* ($\mathbb{R}$)*, que embora tendo propriedades adicionais, satisfazem todos os axiomas e propriedades citados anteriomente.*

## 1.3 Relação de ordem em $\mathbb{Z}$

Sejam $x$ e $y$ números inteiros quaisquer, dizemos que "$x$" é menor do que ou igual a "$y$" e indicamos $x \leq y$, se $y - x$ é um número inteiro não negativo, isto é, $(y - x) \in \mathbb{Z}_+$. Se $y - x$ é número inteiro positivo (estritamente positivo), isto é, $(y - x) \in \mathbb{Z}_+^*$, então dizemos que "$x$" é menor do que "$y$" e indicamos $x < y$.

**Observação 1.2.** *Escrever $x \leq y$ é equivalente a dizer que $y \geq x$ ($y$ é maior do que ou igual a $x$) e para $x < y$ é equivalente a dizer que $y > x$ ($y$ maior do que $x$).*

### 1.3.1 Axiomas para a relação de ordem em $\mathbb{Z}$

Admitiremos que a relação de ordem satisfaz os seguintes axiomas para quaisquer $x,\ y,\ z \in \mathbb{Z}$.

($R_1$) Lei da Tricotomia em $\mathbb{Z}$

Sejam $x$ e $y$ números inteiros quaisquer, vale uma, e somente uma, das afirmações:

$$x = y\,; \quad x < y \quad \text{ou} \quad x > y.$$

($R_2$) Se $x \leq y$ e $y \leq z \Rightarrow x \leq z$ (transitiva).

($R_3$) Se $x \leq y \Rightarrow x + z \leq y + z$.

($R_4$) Se $x \geq 0$ e $y \geq 0 \Rightarrow xy \geq 0$.

### 1.3.2 Outras propriedades da relação de ordem em $\mathbb{Z}$

Sejam $x,\ y,\ z$ e $w$ inteiros quaisquer, temos:

$P_1$) $x \leq x$ (reflexiva);

$P_2$) $x \leq y$ e $y \leq x \Rightarrow x = y$ (anti-simétrica);

$P_3$) $x \leq y \Leftrightarrow x - y \leq 0$;

$P_4$) $x \leq 0 \Leftrightarrow -x \geq 0$;

$P_5$) Se $x + y \leq y + z \Rightarrow x \leq z$;

$P_6$) Se $x \leq y$ e $z \leq w \Rightarrow x + z \leq y + w$;

$P_7$) Se $x \leq 0$ e $y \geq 0 \Rightarrow xy \leq 0$;

$P_8$) Se $x \leq 0$ e $y \leq 0 \Rightarrow xy \geq 0$;

$P_9$) Se $x \neq 0 \Rightarrow x^2 > 0$;

$P_{10}$) $1 > 0$;

$P_{11}$) Se $x \leq y$ e $z > 0 \Rightarrow xz \leq yz$;

$P_{12}$) Se $x \leq y$ e $z < 0 \Rightarrow xz \geq yz$;

$P_{13}$) $x \leq y$ ou $y \leq x$;

$P_{14}$) Se $x \neq 0 \Rightarrow x < 0$ ou $x > 0$;

$P_{15}$) Se $x > y > 0$ e $z > w > 0 \Rightarrow xz > yw > 0$;

$P_{16}$) (Leis do cancelamento para a multiplicação):

i) Se $xz \leq yz$ e $z > 0 \Rightarrow x \leq y$.

ii) Se $xz \leq yz$ e $z < 0 \Rightarrow x \geq y$.

**Demonstrações**

**Observação 1.3.** *Devido à grande quantidade de propriedades, demonstraremos apenas algumas.*

$P_3$) $x \leq y \Leftrightarrow x - y \leq 0$

$x \leq y \Leftrightarrow x + (-y) \leq y + (-y) \Leftrightarrow x - y \leq 0.$

$P_4$) $x \leq 0 \Leftrightarrow -x \geq 0$

$x \leq 0 \Leftrightarrow x + (-x) \leq 0 + (-x) \Leftrightarrow 0 \leq -x \Leftrightarrow -x \geq 0$.

$P_6$) Se $x \leq y$ e $z \leq w \Rightarrow x + z \leq y + w$.

Se $x \leq y \Rightarrow x+z \leq y+z$; do mesmo modo, se $z \leq w \Rightarrow y+z \leq y+w$. Logo, $x+z \leq y+z \leq y+w$ e pelo axioma ($R_2$), temos que $x + z \leq y + w$.

$P_7$) Se $x \leq 0$ e $y \geq 0 \Rightarrow xy \leq 0$.

Se $x \leq 0$ e $y \geq 0$. Por ($P_4$) $-x \geq 0$ e $y \geq 0$ e por ($R_4$) $(-x) \cdot y \geq 0 \Rightarrow -(xy) \geq 0$ e, portanto, novamente por ($P_4$) $xy \leq 0$.

$P_8$) Se $x \leq 0$ e $y \leq 0 \Rightarrow xy \geq 0$.

Se $x \leq 0$ e $y \leq 0$. Por ($P_4$) $(-x) \geq 0$ e $(-y) \geq 0$ e ainda por ($R_4$) $(-x)(-y) \geq 0$ e, portanto, $xy \geq 0$.

$P_{10}$) Por $P_9$ temos que, se $x \neq 0 \Rightarrow x^2 > 0$ e daí temos que $1^2 > 0 \Rightarrow 1 \cdot 1 > 0 \Rightarrow 1 > 0$.

$P_{11}$) Se $x \leq y$ e $z > 0 \Rightarrow xz \leq yz$.

Se $x \leq y$ e $z > 0$, então por ($P_3$) $x - y \leq 0$ e $z > 0$. Por ($P_7$), temos ainda que $(x - y) \cdot z \leq 0 \Rightarrow xz - yz \leq 0 \Rightarrow xz \leq yz$.

$P_{12}$) Se $x \leq y$ e $z < 0 \Rightarrow xz \geq yz$.

Se $x \leq y$ e $z < 0$, então por ($P_3$) $x - y \leq 0$ e $z < 0$ e por ($P_8$) $(x - y) \cdot z \geq 0 \Rightarrow xz - yz \geq 0 \Rightarrow xz \geq yz$.

$P_{16}$) (i) Se $xz \leq yz$ e $z > 0 \Rightarrow x \leq y$.

Se $xz \leq yz$ e $z > 0$, então necessariamente $x \leq y$ pois, caso contrário, teremos $x > y$ o que contraria a nossa hipótese ($xz \leq yz$), pois se $x > y$ e como $z > 0$, teríamos $xz > yz$ ($P_{11}$).

ii) Se $xz \leq yz$ e $z < 0 \Rightarrow x \geq y$.

De modo análogo ao anterior, se $xz \leq yz$ e $z < 0$, então necessariamente $x \geq y$ pois, caso contrário, teremos $x < y$, o que contraria a nossa hipótese ($xz \leq yz$), pois se $x < y$ e como $z < 0$, teríamos $xz > yz$ ($P_{12}$).

**Teorema 1.1.** *Se $x$ e $y$ são números inteiros, com $x \neq 0$ e $y \neq 0$, então $xy \neq 0$. Equivalentemente, $xy = 0 \Rightarrow x = 0$ ou $y = 0$.*

**Demonstração**

Se $x \neq 0$ e $y \neq 0$, então pela Lei da tricotomia, temos $x < 0$ ou$x > 0$ e $y < 0$ ou $y > 0$ e, portanto, temos que $x \cdot y < 0$ ou $xy > 0$.

**Definição 1.2.** *Seja $A$ um subconjunto não vazio de $\mathbb{Z}$. Dizemos que $A$ é limitado inferiormente se existe um número $a \in \mathbb{Z}$, tal que $a \leq x$, qualquer que seja o elemento $x \in A$, isto é, $a$ é menor do que ou igual a qualquer elemento de $A$.*

**Definição 1.3.** *Seja $A$ um subconjunto não vazio de $\mathbb{Z}$, limitado inferiormente. Chama-se de limite inferior de $A$ todo número $a \in \mathbb{Z}$, tal que $a \leq x$, para todo $x \in A$.*

**Definição 1.4.** *Seja $A$ um subconjunto não vazio de $\mathbb{Z}$. Chama-se mínimo de $A$, notação "$\min A$", um elemento $a \in A$ tal que $a \leq x$, para todo $x \in A$.*

$$\min A = a \Leftrightarrow a \in A \text{ e } \forall x \in A \Rightarrow a \leq x.$$

**Exemplos:**

I) $A = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

- A é limitado inferiormente.
- Limites inferiores de A: $-5, -6, -7, -8, \ldots$
- $\min A = -5$.

II) $B = \{0, -1, -2, -3, -4, \ldots\}$ não é limitado inferiormente, logo não tem mínimo, pois não existe nenhum número inteiro que seja menor do que todo elemento de B.

**Teorema 1.2.** *Se $a$ é elemento mínimo de $A$, então este elemento é único.*

**Demonstração**

Sejam $a$ e $b$ elementos mínimos de A, temos:

i) $a \leq b$, pois $a = \min A$.

ii) $b \leq a$, pois $b = \min A$, logo pela propriedade $(P_2)$ ($a \leq b$ e $b \leq a \Rightarrow a = b$) temos que $a = b$.

## 1.4 Princípio da Boa Ordem ou da Boa Ordenação ou do Menor Inteiro

Todo conjunto não vazio de inteiros não negativos possui um elemento mínimo.

Simbolicamente:

$$\forall\, A \subset \mathbb{Z}_+,\ A \neq \phi \Rightarrow \exists \min\ A.$$

**Observação 1.4.** *As propriedades e axiomas da adição e multiplicação de números inteiros, bem como as propriedade da relação de ordem em $\mathbb{Z}$, apresentadas até o momento, são igualmente válidas para o conjunto dos números racionais $\mathbb{Q}$ e reais $\mathbb{R}$, porém, o princípio de boa ordenação não é válido para os referidos conjuntos, considerando que nem todo subconjunto dos números racionais não negativos (por exemplo) possui um primeiro elemento.*

**Exemplo:** O conjunto $A = \{x \in \mathbb{R}/x > 2\}$ não possui primeiro elemento.

**Teorema 1.3.** *Seja A um subconjunto não vazio de $\mathbb{Z}$.*

*i) Se A é limitado inferiormente por $m \in \mathbb{Z}$, então A possui um primeiro (menor) elemento, isto é, existe $a_0$ em A tal que $a \geq a_0$ para todo $a \in A$. ( Tal $a_0$ é chamado mínimo de A).*

*ii) Se A é limitado superiormente por $M \in \mathbb{Z}$, então A possui um último (maior) elemento, isto é, existe $b_0$ em A tal que $a \leq b_0$ para todo $a \in A$. (Tal $b_0$ é chamado máximo de A).*

**Demonstração**

i) Considere o conjunto

$$A' = \{x \in \mathbb{Z}/x = a - m,\ \text{com}\ a \in A\}.$$

Para cada $a \in A$, temos $a \geq m$, logo $a - m \geq 0$, o que implica que cada elemento $x$ de $A'$ é um número natural. Como $A' \subset \mathbb{N}$ e $A' \neq \phi$ (pois $A \neq \phi$), pelo princípio da boa ordenação, existe $n_0 \in A'$ tal que $x \geq n_0$ para cada $x \in A'$.

Sendo $n_0$ um elemento de $A'$, temos que $n_0 = a_0 - m$ para algum inteiro $a_0 \in A$. Logo, para cada $x \in A'$, $x \geq a_0 - m$. Isto significa que para cada $a \in A$, $a - m \geq a_0 - m$, ou seja, $a \geq a_0$.

ii) Considere o conjunto

$$A'' = \{x \in \mathbb{Z}/x = -a, \text{ com } a \in A\}.$$

Para cada $a \in A$, temos $a \leq M$, ou equivalente $-a \geq -M$. Logo, para cada elemento $x \in A''$ temos $x \geq -M$. Pelo item anterior, $A''$ tem um primeiro elemento, isto é, existe $c_0 \in A''$ tal que $x \geq c_0$ para cada $x \in A''$. Pela caracterização dos elementos de $A''$, $c_0 = -b_0$ para algum $b_0 \in A$. Daí, $-a \geq -b_0$ para cada $a \in A$, ou seja, $a \leq b_0$ para cada $a \in A$.

**Teorema 1.4** (Archimedes)**.** *Se a e b são dois inteiros positivos quaisquer, então existe um inteiro positivo k, tal que* $ka \geq b$.

**Demonstração**

Por contradição, consideremos dois inteiros positivos $a$ e $b$ tais que $ka < b$ para todo inteiro positivo $k$. Então, todos os elementos do conjunto

$$A = \{b - ka/k \in \mathbb{N}\}$$

são inteiros positivos e pelo princípio da boa ordem, possui um elemento mínimo, digamos que $\min A = b - ra$, com $r \in \mathbb{N}$ e como $b - (r + 1)a$ pertence a $A$, pois $A$ contém todos os inteiros positivos. Desta forma, temos:

$$b - (r + 1)a = (b - ra) - a < b - ra.$$

Logo, $b - ra$ não é elemento mínimo de $A$, o que é uma contradição. Portanto, a propriedade archimediana é verdadeira.

**Exemplos:**

Se $a = 3$ e $b = 16 \Rightarrow k = 6$, pois $6 \cdot 3 \geq 16$.

Se $a = 20$ e $b = 5 \Rightarrow k = 1$, pois $20 \cdot 1 \geq 5$.

**Corolário 1.1.** *Não existe nenhum número inteiro n, tal que* $0 < n < 1$.

**Demonstração**

Vamos supor por contradição que existam números $n \in \mathbb{Z}$ tais que $0 < n < 1$. Observando que todos estes números são positivos e considerando que $A$ é o conjunto formado por todos esses números, temos:

Pelo princípio da boa ordenação, temos que $A$ possui um menor elemento $k$ e $0 < k < 1$. Multiplicando por $k$, temos $0 < k^2 < k$, o que contraria o fato de $k$ ser o menor elemento de $A$. Logo, 1 é o menor inteiro positivo.

**Corolário 1.2.** *Dado um número inteiro positivo qualquer n, não existe nenhum número inteiro n tal que* $n < m < n + 1$.

**Demonstração**

Supondo por absurdo, que existe um número inteiro positivo $m$ tal que $n < m < n + 1$. Logo, $\Rightarrow 0 < m - n < 1$, isto é, teríamos um número inteiro entre 0 e 1, o que contraria o corolário 1. Portanto, não existe número inteiro positivo entre dois números inteiros positivos.

## 1.5 Indução finita

### 1.5.1 Primeira forma do princípio de indução finita

**Teorema 1.5.** *Seja* $n_0$ *um número inteiro e suponhamos que a cada inteiro n,* $n \geq n_0$ *está associada uma afirmação* $A(n)$*, a qual possui, para cada n, um valor lógico V (quando verdadeira) ou F(quando falsa). Suponhamos que as condições 1 e 2 abaixo sejam verificadas:*

1. A afirmação $A(n)$ é verdadeira para $n = n_0$;

2. Para cada $k \geq n_0$, se $A(k)$ é verdadeira (hipótese de indução), então, (é possível demonstrar que) $A(k + 1)$ é também verdadeira. Então, a afimação $A(n)$ é verdadeira para cada $n \geq n_0$.

**Demonstração**

Suponha que estejam estabelecidas as hipóteses do teorema 1.5 e que as condições 1 e 2 estejam ocorrendo.

Suponhamos ainda que, além disso, contrariamente a tese do teorema, exista um número inteiro $s \geq n_0$ tal que a afirmação $A(s)$ é falsa.

Seja

$$S = \{n \in \mathbb{Z} / n \geq n_0 \quad \text{e} \quad A(n) \text{ é falsa}\}.$$

$S$ é não vazio, pois $s \in S$.

Sendo $S \subset \mathbb{Z}$ e limitado inferiormente por $n_0$, podemos afirmar que $S$ possui um menor elemento $s_0$. (Princípio do menor inteiro).

Como $n_0 < s_0$ e $A(n_0)$ é verdadeira, temos $n_0 < s_0$, e então $n_0 \leq s_0 - 1$.

Seja $k = s_0 - 1$. Então $A(k)$ é verdadeira, pois $k < s_0$ e $s_0$ é o menor inteiro $n$ com $A(n)$ falsa.

Mas como $k \geq n_0$ e $A(k)$ é verdadeira, temos então $A(k+1)$ verdadeira, porém, $k + 1 = s_0$ e $A(s_0)$ é falsa.

Assim, temos uma contradição decorrente do fato de existir um inteiro $s \geq n_0$ para o qual $A(s)$ é falsa.

Portanto, $A(n)$ é verdadeira para cada número inteiro $n \geq n_0$.

**Exemplo:**

**Teorema 1.6.** *Provar que para todo $n \in \mathbb{Z}$ e $n \geq 0$, o número inteiro $9^n - 1$ é múltiplo de 8.*

**Demonstração**

A afirmação $A(n)$, que queremos provar ser verdadeira para todo inteiro $n \geq 0$, é a seguinte:

$$A(n): \text{ “}9^n - 1 \text{ é divisível por 8.”}$$

I) Se $n = 0 \Rightarrow A(n) = A(0)$ é a afirmação $9^0 - 1$ é divisível por 8, que é verdadeira, pois:

$$9^0 - 1 = 1 - 1 = 0,$$

e “0” é divisível por 8.

II) Seja então $k$ um inteiro $k \geq 0$, e admitamos a hipótese de indução de que $A(k)$ é verdadeira, isto é, $9^k - 1$ é divisível por 8. Provaremos, então, que $A(k+1)$ também é verdadeira, ou seja, $9^{k+1} - 1$ é divisível por 8.

Temos então:

$$9^{k+1} - 1 = 9^k \cdot 9 - 1 = 9^k \cdot 9 - 9 + 8 = 9(9^k - 1) + 8,$$

e como $9^k - 1$ é divisível por 8, podemos escrever que

$$9^{k+1} - 1 = 9 \cdot 8p + 8, \ p \in \mathbb{Z} \Rightarrow 9^{k+1} - 1 = 8(9p + 1)$$

e, portanto, concluímos que $9^{k+1} - 1$ é múltiplo inteiro de 8, isto é, também é divisível por 8.

Provamos, portanto, que a validade da afirmação $A(k)$ implica na validade da afirmação $A(k+1)$.

Sendo assim, provamos, pelo princípio de indução finita, que $A(n)$ é válida para todo $n \in \mathbb{Z}$ e $n \geq 0$, ou seja, que $9^n - 1$ é divisível por 8 para todo $n \geq 0$.

### 1.5.2 Segunda forma do princípio de indução finita

**Teorema 1.7.** *Seja $n_0$ um número inteiro e suponhamos que a cada inteiro n, $n \geq n_0$ está associada uma afirmação $A(n)$, a qual possui, para cada n, um valor lógico V (quando verdadeira) e F (quando falsa). Suponhamos que as condições 1 e 2 abaixo sejam verificadas:*

1. A afirmação $A(n)$ é verdadeira para $n = n_0$.

2. Para cada inteiro $k \geq n_0$, se $A(n)$ é verdadeira para $n_0 \leq n \leq k$, então $A(k+1)$ é também verdadeira. Então, a afirmação $A(n)$ é verdadeira para cada $n \geq n_0$.

**Demonstração**

De forma idêntica à Primeira forma do princípio de indução, temos que:

Suponhamos que estejam estabelecidas as hipótese do teorema 1.7 e que as condições 1 e 2 estejam ocorrendo. Suponhamos ainda que, além disso, contrariamente à tese do teorema, exista um número inteiro $s \geq n_0$ tal que a afirmação $A(s)$ é falsa.

Seja

$$S = \{n \in \mathbb{Z} / n \geq n_0 \text{ e } A(n) \text{ é falsa}\},$$

$S$ é não vazio pois $s \in S$.

Sendo $S \subset \mathbb{Z}$ e limitado inferiormente por $n_0$, podemos afirmar que S possui um menor elemento $s_0$ (Princípio do menor inteiro).

Como $n_0 \leq s_0$ e $A(n_0)$ é verdadeira, temos $n_0 < s_0$, e então $n_0 \leq s_0 - 1$. Como $s_0$ é o menor inteiro $n$ com $A(n)$ falsa, temos então $A(n)$ verdadeira para cada $n$ tal que $n_0 \leq n \leq s_0 - 1$. Tomando $k = s_0 - 1$, temos então $A(n)$ verdadeira para cada $n$ satisfazendo $n_0 \leq n \leq k$. Pelo item 2 da hipótese, isto acarreta $A(k+1)$ verdadeira mas $k + 1 = s_0$ e novamente temos uma contradição.

Portanto, $A(n)$ é verdadeira para cada inteiro $n \geq n_0$.

**Exemplo:**

**Teorema 1.8** (Representação decimal de números naturais)**.** *Para cada inteiro $n \geq 1$, existem números naturais $a_0, a_1, \ldots, a_s$, $(S \geq 0)$, com os "algarismos" $a_0, a_1, \ldots, a_s$ tomados no conjunto $\{0, 1, 2, \ldots, 9\}$ e $a_s \neq 0$, tais que*

$$n = \sum_{i=0}^{s} a_i \cdot 10^i = a_0 10^0 + a_1 10^1 + \ldots + a_s 10^s$$

*ou*

$$n = \sum_{i=0}^{s} a_i \cdot 10^i = a_s 10^s + \ldots + a_1 10^1 + a_0 10^0.$$

**Demonstração**

Se $n = 1$, podemos tomar $n = a_0$. Seja $k \geq 1$ um inteiro e suponhamos que o resultado do teorema seja verdadeiro para cada inteiro $n$, com $1 \leq n \leq k$. Mostraremos que isto acarreta a validade da mesma propriedade para $n = k + 1$.

Com efeito, realizando a divisão euclidiana de $k + 1$ por 10,

$$\begin{array}{r|l} k+1 & 10 \\ \hline \text{r} & \text{q} \end{array},$$

obtemos um quociente $q \in \mathbb{N}$ e um resto $r \in \mathbb{N}$, satisfazendo $k + 1 = 10q + r$, com $0 \leq r < 10$.

Se $q = 0$, então $k + 1 = r = a_0$, com $a_0 \in \{0, 1, 2, \ldots, 9\}$.

Se $q > 0$, então $q \leq k$, pois se $q > k$, então $k + 1 = 10q + r > 10k + r \geq 10k$, e assim $k + 1 > 10k$ e então $1 > 9k \geq 9$, o que é impossível.

Sendo $1 \leq q \leq k$, pela hipótese de indução $q = b_t \cdot 10^t + \ldots + b_0 10^0$ para certos algarismos $b_t, \ldots, b_0$, todos em $\{0, 1, 2, \ldots, 9\}$.

Então:

$$\begin{aligned} k + 1 &= 10q + r \\ \Rightarrow k + 1 &= 10(b_t \cdot 10^t + \ldots + b_0 10^0) + r \\ \Rightarrow k + 1 &= b_t \cdot 10^{t+1} + \ldots + b_0 10^1 + r, \end{aligned}$$

com $b_t, \ldots, b_0$ e $r$ todos em $\{0, 1, 2, \ldots, 9\}$. Logo, pela segunda forma do princípio de indução finita, a representação decimal de $n$ é possível para cada inteiro $n \geq 1$.

**Observação 1.5.** *Ilustrando o teorema anterior quando escrevemos, por exemplo, 670325, queremos dizer:*

$$6 \cdot 10^5 + 7 \cdot 10^4 + 0 \cdot 10^3 + 3 \cdot 10^2 + 2 \cdot 10^1 + 5 \cdot 10^0.$$

**Observação 1.6.** *O que difere a segunda forma do princípio de indução finita da primeira é a forma como é formulada a hipótese de indução. Na primeira forma, supomos que a afirmação*

*$A(n)$ é verdadeira para $n = k$ somente, enquanto que no segundo, supomos $A(n)$ é válida para cada n satisfazendo $n_0 \leq n \leq k$. Em ambas as formas, devemos provar que a hipótese de indução acarreta a validade de $A(n)$ para $n = k + 1$.*

# Capítulo 2

# Divisibilidade

**Definição 2.1.** *Sejam a e b números inteiros, diz-se que "a" divide "b", notação a | b, se, e somente se, existir um número inteiro c tal que*

$$b = a \cdot c.$$

**Observação 2.1.** *Se a divide b diz-se também que a é um divisor de b ou que b é múltiplo de a ou a é um fator de b ou ainda que b é divisível por a.*

**Observação 2.2.** *Para indicar que a não divide b, escrevemos* $a \nmid b$.

**Observação 2.3.** *Se a divide b, então* $(-a)$ *também divide b, pois a igualdade* $b = a \cdot c$ *pode ser escrita como* $b = (-a) \cdot (-c)$.

**Exemplos:**

- $5 \mid 20$, pois $20 = 5 \cdot 4$.
- $-3 \mid 12$, pois $12 = (-3) \cdot (-4)$.
- $6 \mid -18$, pois $-18 = 6 \cdot (-3)$.
- $5 \nmid 14$, pois não existe $c \in \mathbb{Z}$ tal que $14 = 5 \cdot c$.
- $0 \mid 0$, pois $0 = c \cdot 0 \quad \forall c \in \mathbb{Z}$.
- $3 \mid 0$, pois $0 = 3 \cdot 0$.

**Teorema 2.1.** *Sejam a, b, c* e *d números inteiro quaisquer tem-se:*

*I)* $a \mid 0, \quad 1 \mid a \quad$ e $\quad a \mid a$.

**Demonstração**

Com efeito

$0 = a \cdot 0$.

$a = 1 \cdot a$.

$a = a \cdot 1$.

**Exemplos:**

- $2 \mid 0$, pois $0 = 2 \cdot 0$.
- $1 \mid 5$, pois $5 = 1 \cdot 5$.
- $6 \mid 6$, pois $6 = 6 \cdot 1$.

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

**Demonstração**

i) Se $a \mid b \Rightarrow$ existe $k_1 \in \mathbb{Z}$; $\quad b = a \cdot k_1$.

ii)Se $b \mid c \Rightarrow$ existe $k_2 \in \mathbb{Z}$; $\quad c = b \cdot k_2$.

Substituindo (i) em (ii), temos:

$c = ak_1k_2$ e como $k_1,\ k_2 \in \mathbb{Z},\ k_1 \cdot k_2 = k \in \mathbb{Z} \Rightarrow c = a \cdot k$, o que prova que $a \mid c$.

**Exemplo:** $5 \mid 15$ e $15 \mid 30$, então $5 \mid 30$.

III) Se $a \mid 1$, então $a = \pm 1$.

**Demonstração**

Com efeito, se $a \mid 1$ então existe $c \in \mathbb{Z};\ 1 = a \cdot c \Rightarrow a = 1$ e $c = 1$ ou $a = -1$ e $c = -1$, ou seja, $a = \pm 1$.

IV) Se $a \mid b$ e se $c \mid d$, então $ac \mid bd$.

**Demonstração**

i) Se $a \mid b \Rightarrow b = a \cdot k_1, \quad k_1 \in \mathbb{Z}$.

ii) Se $c \mid d \Rightarrow d = c \cdot k_2, \quad k_2 \in \mathbb{Z}$.

$\Rightarrow bd = ak_1 \cdot ck_2 = (k_1k_2)(ac) = k(ac), \quad k \in \mathbb{Z}$. Logo, $ac \mid bd$.

**Exemplo:** $2 \mid 8$ e $3 \mid 12 \Rightarrow 2 \cdot 3 \mid 8 \cdot 12$, isto é, $6 \mid 96$.

V) Se $a \mid b$, então $ca \mid cb$.

**Demonstração**

$a \mid b \Rightarrow b = a \cdot k_1, \quad k_1 \in \mathbb{Z}$

$\Rightarrow cb \mid cak_1 \Rightarrow ca \mid cb.$

**Exemplo:** $4 \mid 20 \Rightarrow 4 \cdot 2 \mid 20 \cdot 2 \Rightarrow 8 \mid 40$.

VI) Se $a \mid b$ e $b \mid a$, então $a = \pm b$ ou $|a| = |b|$.

**Demonstração**

i) $a \mid b \Rightarrow b = k_1 \cdot a, \quad k_1 \in \mathbb{Z}$.

ii) $b \mid a \Rightarrow a = k_2 \cdot b, \quad k_2 \in \mathbb{Z}$.

Substituindo (i) em (ii), temos:

$a = k_2 \cdot k_1 \cdot a \Rightarrow k_2 \cdot k_1 = 1 \Rightarrow k_1 \mid 1 \Rightarrow k_1 = \pm 1 \Rightarrow a = \pm b.$

VII) Se $ab \mid ac$ e $a \neq 0 \Rightarrow b \mid c$.

**Demonstração**

$ab \mid ac \Rightarrow ac = ab \cdot k_1, \quad k_1 \in \mathbb{Z}$ e como $a \neq 0 \Rightarrow c = b \cdot k_1$, o que prova que $b \mid c$.

**Exemplo:** $2 \cdot 3 \mid 2 \cdot 12 \Rightarrow 3 \mid 12$.

VIII) Se $a \mid b$, com $b \neq 0$, então $|a| \leq |b|$.

**Demonstração**

$a \mid b, \quad b \neq 0 \Rightarrow b = ak_1, \quad k_1 \in \mathbb{Z}^* \Rightarrow |b| = |a| \cdot |k_1|$ e como $k_1 \neq 0 \Rightarrow |k_1| \geq 1$ e, portanto, $|b| \geq |a|$ ou $|a| \leq |b|$.

IX) Se $a \mid b$ e $a \neq 0$, então $\left(\frac{b}{a}\right) \mid b$.

**Demonstração**

$a \mid b \Rightarrow b = a \cdot k, \quad k \in \mathbb{Z}$. Como $a \neq 0 \Rightarrow k = \dfrac{b}{a}$ e, portanto, $\dfrac{b}{a}$ é um número inteiro. Como $\left(\frac{b}{a}\right) \cdot a = b$, temos da definição $\left(\frac{b}{a}\right) \mid b$.

**Exemplo:** $3 \mid 12 \Rightarrow \left(\frac{12}{3}\right) \mid 12$ ou $4 \mid 12$.

X) Se $a \mid b$ e se $a \mid c$, então $a \mid (bx + cy), \quad \forall x, y \in \mathbb{Z}$.

**Demonstração**

i) $a \mid b \Rightarrow b = a \cdot k_1, \ k_1 \in \mathbb{Z}$.

ii) $a \mid c \Rightarrow c = a \cdot k_2, \ k_2 \in \mathbb{Z}$.

Multiplicando-se (i) por $x \in \mathbb{Z}$ e (ii) por $y \in \mathbb{Z}$, temos:

$bx = a \cdot k_1 x$

$cy = a \cdot k_2 y$ e somando-se membro a membro, encontra-se:
$bx + cy = ak_1 x + ak_2 y \Rightarrow bx + cy = a(k_1 x + k_2 y)$ e como $k_1 \in \mathbb{Z},\ k_2 \in \mathbb{Z},\ x \in \mathbb{Z}$ e $y \in \mathbb{Z}$, temos então que $k_1 x + k_2 y = k,\ k \in \mathbb{Z} \Rightarrow bx + cy = ak,\ k \in \mathbb{Z}$. Logo, concluimos que $a \mid (bx + cy)$.

**Observação 2.4.** *Esta propriedade admite uma generalização, isto é, se* $a \mid b_k$, *para* $k = 1,\ 2,\ \ldots,\ n$, *então, para quaisquer inteiro* $x_1,\ x_2,\ \ldots,\ x_n$, *temos que* $a \mid (b_1 x_1 + b_2 x_2 + \ldots + b_n x_n)$.

**Exemplo:**

$3 \mid 6, \quad 3 \mid 9, \quad 3 \mid 18$, então $3 \mid (5 \cdot 6 + 2 \cdot 9 - 4 \cdot 18) \Rightarrow 3 \mid (-24)$.

**Teorema 2.2** (Teorema de EUDOXIUS)**.** *Dados dois números inteiros* $a$ e $b$, *com* $b \neq 0$, *então* $a$ *é múltiplo de* $b$ *ou está entre dois múltiplos consecutivos de* $b$, *isto é, sendo* $a$ e $b$ *números inteiros com* $b \neq 0$, *existe um número inteiro* $q$, *tal que, para* $b \geq 0$, *tem-se*

$$qb \leq a < (q + 1)b$$

*e para* $b < 0$, *tem-se*

$$qb \leq a < (q - 1)b.$$

**Exemplos**

- Se $a = 20$ e $b = 5$, devemos tomar $q = 4$
  $\Rightarrow a = 4 \cdot 5$, portanto, $a$ é múltiplo de $b$.

- Se $a = 15$ e $b = 8$, devemos tomar $q = 1$
  $1 \cdot 8 < 15 < (1 + 1) \cdot 8 \Rightarrow 8 < 15 < 16$.

- Se $a = 4$ e $b = 11$, devemos tomar $q = 2$
  $2 \cdot 4 < 11 < (2 + 1) \cdot 4 \Rightarrow 8 < 11 < 12$.

- Se $a = 7$ e $b = -3$, devemos tomar $q = -2$
  $(-2) \cdot (-3) < 7 < (-2 - 1) \cdot (-3) \Rightarrow 6 < 7 < 9$.

## 2.1 Algoritmo da divisão de Euclides

**Teorema 2.3.** *Sejam a e b dois números inteiros com* $b > 0$*, então existem e são únicos os números inteiros q* e *r tais que*

$$a = qb + r \quad e \quad 0 \leq r < b,$$

*onde "q" chama-se quociente e "r" o resto na divisão de a por b.*

**Demonstração**

I) A existência de $q$ e $r$.

Sejam $a$ e $b$ números inteiros quaisquer com $b > 0$ e consideremos o conjunto $A$ de todos os inteiros não negativos que são da forma $a - bx$, com $x \in \mathbb{Z}$, isto é,

$$A = \{a - bx / \ x \in \mathbb{Z}, \ a - bx \geq 0\}.$$

Este conjunto $a$ é não vazio ($A \neq \phi$), pois sendo $b > 0 \Rightarrow b > 1$ e, portanto, para $x = -|a|$, temos que

$$a - bx = a - b(-|a|) = a + b|a| \geq a + |a| \geq 0.$$

Logo, pelo "princípio da boa ordenação", existe um elemento mínimo ($r$) de $A$. Como $r \in A$, existe um $x = q \in \mathbb{Z}$, tal que

$$r = a - bq \Rightarrow a = bq + r.$$

Prova-se agora que $0 \leq r < b$.

Como $r \in A \Rightarrow r \geq 0$. Supondo por contradição que $r \geq b$, temos que

$$a - bq - b = r - b \geq 0, \text{ ou seja,}$$

$$r > a - bq - b \Rightarrow r > a - (q + 1)b \in A,$$

o que contradiz a minimalidade do $r \in A$. Logo, concluímos que $r \geq b$ é falso e, portanto, $r < b$.

II) A unicidade de $q$ e $r$.

Vamos supor que $q,\ r,\ q_1$ e $r_1$ são números inteiros tais que:

$$a = bq + r \quad \text{e} \quad a = bq_1 + r_1$$

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

$r_1 - r = bq - bq_1 = b(q - q_1) \Rightarrow b \mid (r_1 - r) \quad (I)$

$\Rightarrow |r_1 - r| = |b(q - q_1)| \Rightarrow |r_1 - r| = b\,|q - q_1|.$

Por outro lado, temos:

$$\begin{cases} 0 \leq r_1 < b \\ \\ -b < -r \leq 0 \end{cases} \Rightarrow -b < r_1 - r < b \Rightarrow |r_1 - r| < b. \quad (II)$$

Assim, de (I) e (II), temos que

$r_1 - r = 0 \Rightarrow r = r_1$ e como $b \neq 0$, temos que

$r_1 - r = (q - q_1)b \Rightarrow\ 0 = (q - q_1)b \ \Rightarrow\ q - q_1 = 0 \ \Rightarrow\ q = q_1.$

**Observação 2.5.** *Embora o teorema anterior tenha feito a restrição $b > 0$, podemos enunciá-lo também da seguinte forma:*

**Teorema 2.4** (Algoritmo da divisão de Euclides)**.** *Sejam a e b dois números inteiros, com $b \neq 0$, então existem e são únicos os números inteiros q e r tais que:*

$$a = qb + r\ ,\ com\ 0 \leq r < |b|\,.$$

**Demonstração**

I) Se $b > 0$ (já foi demonstrado - Teorema anterior).

II) Se $b < 0$.

$|b| > 0$ e, portanto, existem e são únicos os inteiros $q_1$ e $r$ tais que

$$a = |b|\,q_1 + r \quad \text{e} \quad 0 \leq r < |b|\,.$$

Como neste caso $|b| = -b$, podemos considerar $q = (-q_1) \Rightarrow a = (-b)q_1 + r \Rightarrow a = b(-q_1) + r$ $\Rightarrow a = bq + r$, portanto, existem e são únicos $q = (-q_1)$ e $r$, tais que

$$a = qb + r\ , \quad \text{e} \quad 0 \leq r < |b|\,.$$

**Exemplos:**

- Divisão de 43 por 10, temos:

$$\begin{array}{r|l} 43 & 10 \\ \hline 3 & 4 \end{array}$$

$$43 = 4 \cdot 10 + 3.$$

- Divisão de $-43$ por 10.

Neste exemplo, devemos ter cuidado para que o resto atenda às condições do algoritmo da divisão, isto é, $0 \leq r < |b|$. Veja:

$$\begin{array}{r|l} -43 & 10 \\ \hline -3 & -4 \end{array}$$

É lógico que $-43 = (-4) \cdot 10 + (-3)$, porém, o resto não atende às condições do algoritmo da divisão e, portanto, devemos proceder da seguinte forma:

$$\begin{array}{r|l} -43 & 10 \\ \hline 7 & -5 \end{array}$$

$$-43 = (-5) \cdot 10 + 7 \quad \text{e} \quad 0 \leq 7 < |10|\,.$$

Variando os sinais do dividendo e do divisor, temos:

$$\begin{array}{r|l} -43 & 10 \\ \hline 3 & -4 \end{array} \Rightarrow 43 = (-4)\cdot(-10) + 3$$

$$\begin{array}{r|l} -43 & -10 \\ \hline 7 & 5 \end{array} \Rightarrow -43 = 5\cdot(-10) + 7$$

Com os exemplos apresentados, verificamos que para atender às exigências do algoritmo de Euclides em $\mathbb{Z}$ devemos fazer algumas adaptações.

**Observação 2.6.** *Uma consequência interessante do algoritmo da divisão é que o conjunto $\mathbb{Z}$ dos números inteiros pode ser decomposto em n subconjuntos disjuntos, da seguinte forma:*

*a) considerando $b = 2$, temos que para qualquer $a \in \mathbb{Z}$, existe um $q \in \mathbb{Z}$, com $a = 2q$ ou $a = 2q + 1$ e, consequentemente,*

$$\mathbb{Z} = \{2q/q \in \mathbb{Z}\} \cup \{2q + 1/q \in \mathbb{Z}\},$$

*com*

$$\{2q/q \in \mathbb{Z}\} \cap \{2q + 1/q \in \mathbb{Z}\} = \phi,$$

*isto é, o conjuntos $\mathbb{Z}$ foi decomposto em dois subconjuntos disjuntos, os inteiros pares e os inteiros ímpares.*

*b) Considerando agora $b = 3$, temos para qualquer $a \in \mathbb{Z}$, existe um $q \in \mathbb{Z}$ com $a = 3q$, $a = 3q + 1$ ou $a = 3q + 2$ e, consequentemente,*

$$\mathbb{Z} = \{3q/q \in \mathbb{Z}\} \cup \{3q + 1/q \in \mathbb{Z}\} \cup \{3q + 2/q \in \mathbb{Z}\},$$

*uma decomposição em três subconjuntos disjuntos.*

*c) Para $b = 4$, temos*

$$\mathbb{Z} = \{4q/q \in \mathbb{Z}\} \cup \{4q + 1/q \in \mathbb{Z}\} \cup \{4q + 2/q \in \mathbb{Z}\} \cup \{4q + 3/q \in \mathbb{Z}\}.$$

*d) Generalizando para $b = n \in \mathbb{N}$, temos*

$$\mathbb{Z} = \{nq/q \in \mathbb{Z}\} \cup \{nq + 1/q \in \mathbb{Z}\} \cup \ldots \cup \{nq + (n-1)/q \in \mathbb{Z}\}.$$

*Estes n conjuntos $\{nq/q \in \mathbb{Z}\}$, $\{nq + 1/q \in \mathbb{Z}\}$, $\ldots$, $\{nq + (n-1)/q \in \mathbb{Z}\}$ chamam-se as classes de resto módulo n, que veremos no capítulo 3.*

## 2.2 Conjunto dos divisores de um inteiro

Chama-se conjunto dos divisores de um número inteiro "a", notação $D(a)$, ao conjunto formado por todos os divisores do número $a$, isto é,

$$D(a) = \{x \in \mathbb{Z}^* / x \mid a\}.$$

**Exemplos:**

$D(10) = \{x \in \mathbb{Z}/x \mid 10\} = \{\pm 1,\ \pm 2,\ \pm 5,\ \pm 10\}$.

$D(-20) = \{x \in \mathbb{Z}/x \mid -20\} = \{\pm 1,\ \pm 2,\ \pm 4,\ \pm 5; \pm 10; \pm 20\}$.

$D(1) = \{x \in \mathbb{Z}/x \mid 1\} = \{\pm 1\}$.

$D(0) = \{x \in \mathbb{Z}/x \mid 0\} = \mathbb{Z}$.

**Observação 2.7.** *O número de divisores positivos de a é igual ao número de divisores negativos de a, isto é,*

$$n\left[D_+(a)\right] = n\left[D_-(a)\right].$$

**Observação 2.8.** *Para todo inteiro a, tem-se que* $D(a) = D(-a)$.

**Observação 2.9.** *Seja a um número inteiro qualquer, tem-se que* $1; -1$*; a e* $-a$ *são divisores de a e daí temos que:*

*i)* $D(a) \neq \phi$.

*ii) Se a é um número inteiro e* $a \neq 0$, *tem-se que se* $x \mid a$, *então* $-a \leq x \leq a$ *e, portanto,* $D(a) \subset [-a,\ a]$. *Isto significa que qualquer inteiro* $a \neq 0$ *possui um número finito de divisores.*

## 2.3 Divisores comuns de dois inteiros

Chamam-se divisores comuns de dois inteiros $a$ e $b$, todo número inteiro $d$, tal que $d \mid a$ e $d \mid b$.

Notação: $D(a,\ b)$

$$D(a,\ b) = \{x \in \mathbb{Z}/\ x \in D(a) \quad \text{e} \quad x \in D(b)\}$$

ou

$$D(a,\ b) = \{x \in \mathbb{Z}/\ x \mid a \quad \text{e} \quad x \mid b\}$$

ou

$$D(a,\ b) = D(a) \cap D(b).$$

**Observação 2.10.** *O conjunto dos divisores comuns de a e b é sempre diferente do vazio, pois* 1 *e* $-1$ *são divisores de quaisquer números inteiros a e b.*

$$D(a,\ b) \neq \phi$$

**Exemplo**:

$a = 20$ e $b = -16$

$D(20) = \{\pm 1;\ \pm 2;\ \pm 4;\ \pm 5;\ \pm 10;\ \pm 20\}$

$D(-16) = \{\pm 1;\ \pm 2;\ \pm 4;\ \pm 8;\ \pm 16\}$

$D(20,\ -16) = \{\pm 1;\ \pm 2;\ \pm 4\}$.

## 2.4 Máximo Divisor Comum

Dados dois números inteiros $a$ e $b$ não nulos simultaneamente ($a \neq 0$ ou $b \neq 0$), chama-se Máximo Divisor Comum de $a$ e $b$, denotado por MDC $(a,\ b)$ ou $(a,\ b)$, o maior número inteiro que divide $a$ e $b$.

Por definição, se $(a,\ b) = d$, temos que:

**I)** $d \mid a$ e $d \mid b$.

**II)** Se $c \mid a$ e $c \mid b$, então $c \leq d$.

**Observação 2.11.** *É imediato que:*

**i)** $(a,\ b) = (b,\ a)$.

**ii)** $(a,\ 1) = 1$.

**iii)** $(0,\ 0)$ *não existe.*

**iv)** *Se* $a \neq 0$*, então* $(a,\ 0) = |a|$.

**v)** *Se* $a \mid b$*, então* $(a,\ b) = |a|$.

**Exemplos:**

$(10,\ 1) = 1$.

$(-10,\ 0) = |-10| = 10$.

$(15,\ 5) = 5$.

$D(24) = \{\pm 1;\ \pm 2;\ \pm 3;\ \pm 4;\ \pm 6;\ \pm 8;\ \pm 12;\ \pm 24\}$

$D(60) = \{\pm 1;\ \pm 2;\ \pm 3;\ \pm 4;\ \pm 5;\ \pm 6;\ \pm 10;\ \pm 12;\ \pm 15;\ \pm 20;\ \pm 30;\ \pm 60\}$

$D(24) \cap D(60) = \{\pm 1;\ \pm 2;\ \pm 3;\ \pm 4;\ \pm 6;\ \pm 12\}$

$$(24,\ 60) = 12.$$

### 2.4.1 Existência e unicidade do MDC

**Teorema 2.5.** *Se $a$ e $b$ são dois inteiros não nulos simultaneamente ($a \neq 0$ ou $b \neq 0$), então existe e é único o $(a,\ b)$; além disso, existem inteiros $x$ e $y$ tais que:*

$$(a,\ b) = ax + by,$$

*isto é, $(a,\ b)$ é uma combinação linear de $a$ e $b$.*

**Demonstração**

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

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

Este conjunto $S$ é não vazio ($S \neq \phi$), porque por exemplo, se $a \neq 0$, então um dos dois inteiros $a = a \cdot 1 + b \cdot 0$ ou $-a = a \cdot (-1) + b \cdot 0$ é positivo e pertence a $S$. Logo, pelo princípio da boa ordenação, existe e é único o elemento mínimo de $S$, que chamaremos de $d$. Portanto,

$$\min\ S = d > 0.$$

Pela definição do conjunto $S$ e como $d \in S$, podemos garantir que existem inteiros $x$ e $y$ tais que $d = ax + by$.

Provaremos agora que $d = (a,\ b)$.

Se $d > 0$, pelo algoritmo da divisão em $\mathbb{Z}$, existem inteiros $q$ e $r$ tais que:

$$\begin{aligned} a &= dq + r \text{ e } 0 \leq r < d = |d| \Rightarrow r = a - dq \\ \Rightarrow r &= a - (ax + by)q = a - aqx - bqy \Rightarrow r = (1 - qx) \cdot a - qy \cdot b \\ \Rightarrow r &= k_1 \cdot a + k_2 \cdot b, \end{aligned}$$

com $k_1,\ k_2 \in \mathbb{Z}$. Logo, $r$ é também uma combinação linear de $a$ e $b$ e daí como $0 \leq r < d$ e $d > 0$ e é o elemento mínimo de $S$, concluímos que $r = 0$ e, portanto, $a = dq$, ou $d \mid a$.

De forma análoga, concluímos também que $d \mid b$ e então podemos afirmar que $d > 0$ é um divisor comum de $a$ e $b$.

Finalmente, seja $k \in \mathbb{Z}_+^*$ um divisor comum qualquer de $a$ e $b$, isto , $k \mid a,\ k \mid b$ e $k > 0$, então pelo teorema 2.1, item "X", temos que $k \mid (xa + yb),\ \forall x,\ y \in \mathbb{Z}$. Assim, $k \mid d$ e, portanto, $k \leq |d|$ ou $k \leq d$, isto é, $d$ é o maior divisor comum de $a$ e $b$ ou $(a,\ b) = d = ax + by,\ \forall x,\ y \in \mathbb{Z}$.

**Observação 2.12.** *A demonstração do teorema anterior nos mostra não apenas que o Máximo Divisor Comum de a e b pode ser expresso como uma combinação linear deste números, mas que este número é o menor valor positivo dentre todas essas combinações. Esta representação do* $(a,\ b)$ *como combinação linear de a e b não é única.*

**Exemplo**: $(24,\ 60) = 12$.

- $12 = -2 \cdot 24 + 1 \cdot 60$;
- $12 = 58 \cdot 24 - 23 \cdot 60$;
- $12 = -62 \cdot 24 + 25 \cdot 60$.

**Corolário 2.1.** *Sejam dois números inteiros a e b (não nulos simultaneamente) e* $(a,\ b) = d$. *Sejam ainda*

$$A = \{x \in \mathbb{Z} / x = k_1 a + k_2 b,\ com\ k_1,\ k_2 \in \mathbb{Z}\}$$

*e*

$$B = \{y \in \mathbb{Z} / y = \lambda d,\ com\ \lambda \in \mathbb{Z}\}.$$

*Então,* $A = B$, *isto é, as combinações lineares* $k_1 a + k_2 b$, *com* $k_1,\ k_2 \in \mathbb{Z}$ *são, na verdade, os inteiros múltiplos de d.*

**Demonstração**

$a \neq 0$ ou $b \neq 0$.

(i) Vamos provar que $A \subset B$.

Seja $x$ um elemento qualquer de $A \Rightarrow x = k_1a + k_2b,\ k_1,\ k_2 \in \mathbb{Z}$. Como $d = (a,\ b)$, temos que $d \mid a$ e $d \mid b \Rightarrow d \mid (k_1a + k_2b) \Rightarrow d \mid x \Rightarrow x = \lambda d, \lambda \in \mathbb{Z} \Rightarrow x \in B$. Logo $A \subset B$.

(ii) Vamos provar que $B \subset A$.

Seja $y$ um elemento qualquer de $B \Rightarrow y = \lambda d,\ \lambda \in \mathbb{Z}$. Como $d = ra + sb,\ r,\ s \in \mathbb{Z}$ (teorema 2.5), temos que $y = \lambda \cdot (ra + sb) = (\lambda r)a + (\lambda s)b \Rightarrow y \in A$ e, portanto, $B \subset A$. E, finalmente por (i) e (ii), temos que $A = B$.

## 2.5 Números primos entre si

Sejam $a$ e $b$ dois números inteiros, dizemos que $a$ e $b$ são primos entre si ou relativamente primos ou ainda co-primos quando $(a,\ b) = 1$.

**Exemplo**: 4 e 15 são primos entre si, pois $(4,\ 15) = 1$.

**Proposição 2.1.** *Sejam a, b números inteiros quaisquer e* $k \in \mathbb{Z}_+^*$, *temos que* $(ka,\ kb) = k(a,\ b)$.

**Demonstração**

Pelo teorema 2.5, tem-se que $(ka,\ kb)$ é o menor valor positivo de $xka + ykb$, com $x,\ y \in \mathbb{Z}$ que é igual a $k$ vezes o menor valor positivo de $xa + yb \Rightarrow (ka,\ kb) = k(a,\ b)$.

**Exemplo**:

$(2 \cdot 36,\ 2 \cdot 60) = (72,\ 120) = 24$

$(2 \cdot 36,\ 2 \cdot 60) = 2 \cdot (36,\ 60) = 2 \cdot 12 = 24$.

**Proposição 2.2.** *Sejam a, b e c números inteiros. Se* $c > 0$ *e a e b são divisíveis por c, então*

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

**Demonstração**

Como $c \mid a$ e $c \mid b$, então $\dfrac{a}{c} \in \mathbb{Z}$ e $\dfrac{b}{c} \in \mathbb{Z}$. Para provarmos a proposição em questão, basta, pela

proposição 2.1, substituir $a$ por $\frac{a}{c}$ e $b$ por $\frac{b}{c}$ e tomar $k = c$. Logo,

$$\begin{aligned} \left(c \cdot \frac{a}{c},\ c \cdot \frac{b}{c}\right) &= c \cdot \left(\frac{a}{c},\ \frac{b}{c}\right) \\ \Rightarrow \qquad (a,\ b) &= c \cdot \left(\frac{a}{b},\ \frac{b}{c}\right) \\ \Rightarrow \qquad \left(\frac{a}{b},\ \frac{b}{c}\right) &= \frac{1}{c}(a,\ b)\,. \end{aligned}$$

**Exemplo**: $(60,\ 36) = 12$.

- $\left(\frac{60}{6},\ \frac{36}{6}\right) = (10,\ 6) = 2$
- $\left(\frac{60}{6},\ \frac{36}{6}\right) = \frac{1}{6}(60,\ 36) = \frac{1}{6} \cdot 12 = 2.$

**Corolário 2.2.** *Sejam a e b números inteiros. Se* $(a,\ b) = d$, *então* $\left(\frac{a}{d},\ \frac{b}{d}\right) = 1$.

**Demonstração**

Considerando na proposição 2.2, $c$ é divisor comum de $a$ e $b$. Se fizermos $c = (a,\ b) = d$, teremos:

$$\begin{aligned} \left(\frac{a}{d},\ \frac{b}{d}\right) &= \frac{1}{d} \cdot (a,\ b) = \frac{1}{d} \cdot d \\ \Rightarrow \left(\frac{a}{d},\ \frac{b}{d}\right) &= 1 \end{aligned}$$

**Exemplo**: $(80,\ 24) = 8$.

$$\left(\frac{80}{8},\ \frac{24}{8}\right) = (10,\ 3) = 1.$$

**Teorema 2.6.** *Se* $a \mid bc$ *e* $(a,\ b) = 1$, *então* $a \mid c$.

**Demonstração**

$a \mid bc \Rightarrow bc = aq$, com $q \in \mathbb{Z}$. $(a,\ b) = 1$, logo existem $x$ e $y$ inteiros tais que $xa + yb = 1$ (Teorema 2.1, item X). Multiplicando-se os dois membros da igualdade por c, temos

$$acx + bcy = c,$$

portanto,

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

**Exemplo**: $6 \mid (25 \cdot 12)$, logo $6 \mid 12$ uma vez que $(6,\ 25) = 1$.

**Observação 2.13.** *É importante verificar que somente a condição $a \mid bc$ não garante que $a \mid c$.*

**Exemplo**: $15 \mid (25 \cdot 6)$, porém, $15 \nmid 25$ e $15 \nmid 6$, $(15,\ 6) = 5 \neq 1$ e $(15,\ 6) = 3 \neq 1$.

**Teorema 2.7.** *Sejam $a$ e $b$ números inteiros e $a = qb + r$, onde $q \in \mathbb{Z}$ e $r \in \mathbb{Z}$, então $(a,\ b) = (b,\ r)$.*

**Demonstração**

Da relação $a = bq + r$ concluímos que todo divisor de $b$ e $r$ é um divisor de $a$ (Teorema 2.1 - item X).

Fazendo agora $r = a - bq$, concluímos também que todo divisor de $a$ e $b$ é um divisor de $r$. Logo, o conjunto de divisores comuns de $a$ e $b$ é igual ao conjunto dos divisores de $b$ e $r$. Portanto, podemos concluir que $(a,\ b) = (b,\ r)$.

**Exemplo**: $60 = 1 \cdot 36 + 24$.

$$(60, 36) = (36, 24) = 12.$$

## 2.6 Algoritmo de Euclides

**Teorema 2.8.** *Sejam $r_0 = a$ e $r_1 = b$ inteiros não negativos com $b \neq 0$. Se o algoritmo da divisão for aplicado sucessivamente para se obter*

$$r_j = q_{j+1} \cdot r_{j+1} + r_{j+2}, \quad 0 \leq r_{j+2} < r_{j+1}$$

*para $j = 0, 1, 2, \ldots, n-1$ e $r_{n+1} = 0$, então $(a,\ b) = r_n$, o último resto não nulo.*

**Demonstração**

Aplicando o algoritmo da divisão inicialmente para dividirmos $a = r_0$ por $b = r_1$, obtemos $r_0 = r_1 q_1 + r_2$, em seguida dividimos $r_1$ por $r_2$ e obtemos $r_1 = r_2 q_2 + r_3$ e assim, sucessivamente, até a obtenção do resto $r_{n+1} = 0$. Como em cada passo o resto é sempre menor do que o anterior e estamos lidando com números inteiros positivos, é claro que após um número finito de aplicações do algoritmo da divisão, teremos resto nulo.

Temos, pois, a seguinte sequência de equações:

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2, & 0 < r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3, & 0 < r_3 < r_2 \\
r_2 &= q_3 r_3 + r_4, & 0 < r_4 < r_3 \\
r_3 &= q_4 r_4 + r_5, & 0 < r_5 < r_4 \\
&\vdots & \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} &= q_n r_n + 0. &
\end{aligned}$$

E portanto, a última das equações nos diz, pelo teorema 2.7, que o máximo divisor comum de $r_n$ e $r_{n-1}$ é $r_n$. A penúltima, que este número é igual a $(r_{n-1},\ r_{n-2})$ e prosseguindo desta maneira, teremos por repetida aplicações do teorema 2.7 a sequência

$$r_n = (r_{n-1},\ r_n) = (r_{n-2},\ r_{n-1}) = \ldots = (r_1,\ r_2) = (r_0,\ r_1) = (a,\ b).$$

Portanto, o máximo divisor comum de $a$ e $b$ é o último resto não nulo da sequência de divisões descrita.

**Observação 2.14.** *O algoritmo de Euclides é, portanto, um processo prático para cálculo do Máximo Divisor Comum entre dois inteiros positivos a e b e também é denominado processo das divisões sucessivas. É usual o seguinte dispositivo de cálculo no emprego do algoritmo de Euclides:*

| | $q_1$ | $q_2$ | $q_3$ | | $q_{n-2}$ | $q_{n-1}$ | $q_n$ |
|---|---|---|---|---|---|---|---|
| $a = r_0$ | $b = r_1$ | $r_2$ | $r_3$ | $\ldots$ | $r_{n-2}$ | $r_{n-1}$ | $r_n$ |
| $r_2$ | $r_3$ | $r_4$ | $r_5$ | | $r_n$ | 0 | |

$$\Rightarrow (a,\ b) = (r_0,\ r_1) = (r_1,\ r_2) = \ldots = (r_{n-2},\ r_{n-1}) = (r_{n-1},\ r_n) = r_n.$$

**Exemplo**: Calcular o Máximo Divisor Comum entre 1764 e 360, usando o algoritmo de Euclides.

$$1764 = 4 \cdot 360 + 324$$

$$360 = 1 \cdot 324 + 36$$

$$324 = 9 \cdot 36.$$

| | 4 | 1 | 9 |
|---|---|---|---|
| 1764 | 360 | 324 | 36 |
| 324 | 36 | 0 | |

$$(1764,\ 360) = (360,\ 324) = (324,\ 36) = 36.$$

## 2.7 Máximo Divisor Comum de vários inteiros

O conceito do Máximo Divisor Comum, definido para dois inteiros $a$ e $b$, estende-se de maneira natural a mais de dois inteiros. No caso, por exemplo, de três inteiros $a$, $b$ e $c$, não todos nulos, o Máximo Divisor Comum de $a$, $b$ e $c$, mdc$(a,\ b,\ c)$ ou $(a,\ b,\ c)$ é o inteiro positivo $d$ $(d > 0)$ que satisfaz às seguintes condições:

I) $d \mid a, \quad d \mid b \quad$ e $\quad d \mid c$.

II) Se $e \mid a$, se $e \mid b$ e se $e \mid c$, então $e \leq d$.

**Teorema 2.9.** *Sejam a, b e c números inteiros,* $(a,\ b,\ c) = ((a,\ b),\ c)$.

**Demonstração**

Com efeito, seja $(a,\ b,\ c) = d$ e $(a,\ b) = e$ , então, $d \mid a$, $d \mid b$ e $d \mid c$ e como existem inteiros $x$ e $y$, tais que $ax + by = e$, segue que $d \mid (ax + by)$ ou $d \mid e$, isto é, $d$ é um divisor comum de $e$ e $c$ $(d \mid e$ e $d \mid c)$.

Por outro lado, se $f$ é divisor comum qualquer de $e$ e $c$ $(f \mid e$ e $f \mid c)$, então $f \mid a$, $f \mid b$ e $f \mid c$, o que implica $f \leq d$. Assim sendo, $(e,\ c) = d$, isto é, $((a,\ b),\ c) = (a,\ b,\ c)$.

**Exemplo**: Calcular $(2100,\ 1890,\ 900)$.

i) $(2100,\ 1890) = 210$

| | 1 | 9 |
|---|---|---|
| 2100 | 1890 | 210 |
| 210 | 0 | |

ii) $(210,\ 900) = 30$

| | 4 | 3 | 2 |
|---|---|---|---|
| 900 | 210 | 60 | 30 |
| 60 | 30 | 0 | |

Portanto, $(2100,\ 1890,\ 900) = ((2100,\ 1890),\ 900) = (210,\ 900) = 30$.

**Definição 2.2.** *Seja $a_1,\ a_2,\ a_3,\ \ldots,\ a_n$ uma coleção finita de inteiros não todos nulos. O Máximo Divisor Comum dessa coleção é o maior inteiro d que divide simultaneamente todos os inteiros da coleção e será denotado por:*

$$\text{MDC}\,(a_1,\ a_2,\ a_3,\ \ldots,\ a_n) \quad \text{ou} \quad (a_1,\ a_2,\ a_3,\ \ldots,\ a_n).$$

**Exemplo:** $(100, 80, 40, 36) = 4$.

**Teorema 2.10.** *Se $a_1,\ a_2,\ a_3,\ \ldots,\ a_n$ é uma coleção finita de inteiros, não todos nulos, então*

$$(a_1,\ a_2,\ a_3,\ \ldots,\ a_{n-2},\ a_{n-1},\ a_n) = (a_1,\ a_2,\ a_3,\ \ldots,\ a_{n-2}, (\ a_{n-1},\ a_n)).$$

**Demonstração**

Qualquer divisor comum dos inteiros $a_1,\ a_2,\ a_3,\ \ldots,\ a_n$ é, em particular, um divisor de $a_{n-1}$ e $a_n$ e, portanto, um divisor comum dos inteiros $a_1,\ a_2,\ \ldots,\ a_{n-2}$ e $(a_{n-1},\ a_n)$.

Reciprocamente, todo divisor comum de $a_1,\ a_2,\ a_3,\ \ldots,\ a_{n-2}$ e $(a_{n-1},\ a_n)$ é um divisor comum dos inteiros $a_1,\ a_2,\ a_3,\ \ldots,\ a_n$, pois, para dividir $(a_{n-1},\ a_n)$, terá necessariamente que dividir $a_{n-1}$ e $a_n$. Como as duas listas de inteiros $a_1,\ a_2,\ a_3,\ \ldots,\ a_n$ e $a_1,\ a_2,\ a_3,\ \ldots,\ a_{n-2}, (a_{n-1},\ a_n)$ possuem o mesmo conjunto de divisores comuns, concluímos então que

$$(a_1,\ a_2,\ a_3,\ \ldots,\ a_{n-2},\ a_{n-1},\ a_n) = (a_1,\ a_2,\ a_3,\ \ldots,\ a_{n-2},\ (a_{n-1},\ a_n)).$$

**Exemplo:** $(2700,\ 1764,\ 648,\ 360) = 36$.

$$(2700,\ 1764,\ 648,\ 360) = (2700,\ 1764,\ (648,\ 360)) =$$

$$(2700,\ 1764,\ 72) = (2700,\ (1764,\ 72)) = (2700,\ 36) = 36.$$

## 2.8 Números primos

Diz-se que um número inteiro positivo $p (p > 1)$ é um número primo se, e somente se, 1 e $p$ são os seus únicos divisores positivos.

**Exemplos:**

$D_+(2) = \{1,\ 2\} \Rightarrow 2$ é primo.

$D_+(5) = \{1,\ 5\} \Rightarrow 5$ é primo.

**Observação 2.15.** *Alguns autores referem-se a um número primo como sendo um número inteiro qualquer e definem-o da seguinte forma:*

*Dizemos que um inteiro p é primo se* $p \neq 0$, $p \neq \pm 1$ *e os únicos inteiros divisores de p são 1,* $p$, $-1$ *e* $-p$. *Portanto, por exemplo,* $-2$ *é primo,* $-5$ *é primo.*

*No presente trabalho, trataremos apenas o caso em que* $p > 1$. *Em caso contrário, faremos a devida citação.*

**Observação 2.16.** *Se* $p > 1$ *não é primo, dizemos que p é composto.*

**Teorema 2.11.** *Se um número inteiro primo p não divide a, então a e p são primos entre si.*

**Demonstração**

Seja $(a,\ p) = d \Rightarrow d \mid a$ e $d \mid p$.

Como $p$ é primo e $d \mid p$, temos que $d = 1$ ou $d = p$. Como a segunda igualdade $(d = p)$ não pode ocorrer, pois $p \nmid a$, segue-se que $d = 1$, ou seja, $(a,\ p) = 1$, logo $a$ e $p$ são primos entre si.

**Corolário 2.3.** *Se p é um número primo e* $p \mid ab$, *então* $p \mid a$ *ou* $p \mid b$.

**Demonstração**

Se $p \mid a$, não há nada o que demonstrar, porém, se $p \nmid a$, então pelo teorema anterior, $(a,\ p) = 1$ e então teremos que $p \mid ab$ e $(a,\ p) = 1$ e, portanto, pelo Teorema 2.6, $p \mid a$.

**Exemplo:** $3 \mid (4 \cdot 6)$; $3 \nmid 4$ e $3 \mid 6$.

**Teorema 2.12** (Teorema Fundamental da Aritmética)**.** *Todo número inteiro maior do que* 1 *pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

**Demonstração**

Seja $n$ um número inteiro, $n > 1$, temos:

Se $n$ é primo, não há o que demonstrar.

Se $n$ é composto, considerando $p_1 (p_1 > 1)$ o menor dos divisores positivos de $n$, podemos afirmar então que $p_1$ é primo, pois se não fosse, existiria $p$, $1 < p < p_1$ com $p \mid n$, contradizendo a escolha de $p_1$ (menor dos divisores positivos de $n$), logo $n = p_1 \cdot n_1$.

Se $n_1$ for primo, a prova está completada, pois $n$ será um produto de primos. Caso contrário, tomamos $p_2$ como menor fator de $n_1$ e pelo mesmo argumento anterior, $p_2$ é primo e temos que $n = p_2 p_2 n_2$.

Repetindo este procedimento, obtemos uma sequência decrescente de inteiros $n_1, n_2, \ldots, n_r$. Como todos eles são inteiros maiores do que 1, este processo deve terminar. Como os primos na sequência $p_1, p_2, p_3, \ldots, p_k$ não são, necessariamente, distintos, $n$ terá, em geral, a forma

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_k^{a_k}.$$

Para mostrarmos a unicidade usamos a indução em $n$. Para $n = 2$, a afirmação é verdadeira. Assumimos, então, que ela se verifica para todos os inteiros maiores que 1 e menores do que $n$. Vamos provar, então, que ela também é verdadeira para $n$.

Se $n$ é primo, não há o que provar. Vamos supor, então, que $n$ seja composto e que tenha duas fatorações, isto é,

$$n = p_1 p_2 \ldots p_s = q_1 q_2 \ldots q_r.$$

Vamos provar que $s = r$ e que cada $p_i$ é igual a algum $q_j$. Como $p_1$ divide o produto $q_1 \cdot q_2 \cdot \ldots \cdot q_r$ ele divide pelo menos um dos fatores $q_j$. Sem perda de generalidade, podemos supor que $p_1 \mid q_1$. Como são ambos primos, isto implica que $p_1 = q_1$. Logo,

$$\frac{n}{p_1} = p_2 \cdot p_3 \cdot \ldots \cdot p_s = q_2 \cdot q_3 \cdot \ldots \cdot q_r.$$

Como $1 < \dfrac{n}{p_1} < n$, a hipótese de indução nos diz que as duas fatorações são idênticas, isto é, $s = r$ e, a menos da ordem, as fatorações $p_1 p_2 \ldots p_s$ e $q_1 q_2 \ldots q_r$ são iguais.

**Exemplo:**

$480 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 2^5 \cdot 3 \cdot 5.$

**Observação 2.17.** *É importante lembrar que a fatoração em fatores primos de um número inteiro n qualquer não necessariamente deve obdecer a ordem crescente dos fatores primos. Por exemplo:*

| | |
|---|---|
| 480 | 2 |
| 240 | 5 |
| 48 | 2 |
| 24 | 2 |
| 12 | 3 |
| 4 | 2 |
| 2 | 2 |

$480 = 2 \cdot 5 \cdot 2 \cdot 2 \cdot 3 \cdot 2 \cdot 2 = 2^5 \cdot 3 \cdot 5.$

**Teorema 2.13.** *Seja o número inteiro* $n = \prod_{i=1}^{r} p_i^{a_i}$, *isto é,* $n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_r^{a_r}$. *O conjunto dos divisores positivos de n é o conjunto de todos os números da forma*

$$\prod_{i=1}^{r} p_i^{c_i}, \quad 0 \leq c_i \leq a_i, \quad i = 1, 2, 3, \ldots, r,$$

*isto é, se d é divisor de n, então, d é da forma* $d = p_1^{c_1} \cdot p_2^{c_2} \cdot p_3^{c_3} \cdot \ldots \cdot p_r^{c_r}$, onde $0 \leq c_i \leq a_i, \quad i = 1, 2, 3, \ldots, r.$

**Demonstração**

Qualquer que seja o número $d$ da forma $d = p_1^{c_1} \cdot p_2^{c_2} \cdot p_3^{c_3} \cdot \ldots \cdot p_r^{c_r}$, com $0 \leq c_i \leq a_i$, é divisor positivo de $n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_r^{a_r}$, pois $(p_i^{c_i}) \mid (p_i^{a_i})$, considerando $0 \leq c_i \leq a_i$, portanto, $d \mid n$. Se o $c_i$ não estiver no intervalo $0 \leq c_i \leq a_i$, d não será divisor de $n$.

**Exemplo:** Divisores positivos de 120.

$D_+ = (120) = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}$

$120 = 2^3 \cdot 3^1 \cdot 5^1$

$0 \leq c_1 \leq 3 \Rightarrow c_1 \in \{0, 1, 2, 3\}$

$0 \leq c_2 \leq 1 \Rightarrow c_2 \in \{0, 1\}$

$0 \leq c_3 \leq 1 \Rightarrow c_3 \in \{0, 1\}$.

| $c_1$ | $c_2$ | $c_3$ | Divisores |
|---|---|---|---|
| 0 | 0 | 0 | $2^0 \cdot 3^0 \cdot 5^0 = 1$ |
| 0 | 0 | 1 | $2^0 \cdot 3^0 \cdot 5^1 = 5$ |
| 0 | 1 | 0 | $2^0 \cdot 3^1 \cdot 5^0 = 3$ |
| 0 | 1 | 1 | $2^0 \cdot 3^1 \cdot 5^1 = 15$ |
| 1 | 0 | 0 | $2^1 \cdot 3^0 \cdot 5^0 = 2$ |
| 1 | 0 | 1 | $2^1 \cdot 3^0 \cdot 5^1 = 10$ |
| 1 | 1 | 0 | $2^1 \cdot 3^1 \cdot 5^0 = 6$ |
| 1 | 1 | 1 | $2^1 \cdot 3^1 \cdot 5^1 = 30$ |
| 2 | 0 | 0 | $2^2 \cdot 3^0 \cdot 5^0 = 4$ |
| 2 | 0 | 1 | $2^2 \cdot 3^0 \cdot 5^1 = 20$ |
| 2 | 1 | 0 | $2^2 \cdot 3^1 \cdot 5^0 = 12$ |
| 2 | 1 | 1 | $2^2 \cdot 3^1 \cdot 5^1 = 60$ |
| 3 | 0 | 0 | $2^3 \cdot 3^0 \cdot 5^0 = 8$ |
| 3 | 0 | 1 | $2^3 \cdot 3^0 \cdot 5^1 = 40$ |
| 3 | 1 | 0 | $2^3 \cdot 3^1 \cdot 5^0 = 24$ |
| 3 | 1 | 1 | $2^3 \cdot 3^1 \cdot 5^1 = 120$ |

Portanto,

$$D_+(120) = \{1, 5, 3, 15, 2, 10, 6, 30, 4, 20, 12, 60, 8, 40, 24, 120\}$$

ou

$$D_+(120) = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}$$

e

$$D(120) = \{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm8, \pm10, \pm12, \pm15, \pm20, \pm24, \pm30, \pm40, \pm60, \pm120\}.$$

**Observação 2.18.** *Se denotarmos a sequência de primos em ordem crescente* $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $\ldots$, $p_m =$ enésimo primo, *então, todo inteiro positivo pode ser escrito na forma*

$$n = \prod_{i=1}^{\infty} p_i^{a_i}, \quad a_i \geq 0$$

*e os divisores positivos de n são, agora, todos os números da forma*

$$\prod_{i=1}^{\infty} p_i^{c_i}, \quad 0 \leq c_i \leq a_i.$$

*Todos estes produtos são finitos, pois o número de fatores primos de qualquer inteiro é finito.*

**Teorema 2.14.** *Sejam a e b dois números inteiros positivos que possuem as seguintes fatorações:*

$$a = \prod_{i=1}^{\infty} p_i^{a_i} \quad \text{e} \quad b = \prod_{i=1}^{\infty} p_i^{b_i},$$

*então o Máximo Divisor Comum de a e b é igual a*

$$(a,\ b) = \prod_{i=1}^{\infty} p_i^{c_i},\ \text{onde } \mathrm{c_i} = \min\{\mathrm{a_i},\ \mathrm{b_i}\}.$$

**Demonstração**

Para que um produto de fatores primos comuns seja um divisor comum de $a$ e $b$, nenhum expoente $c_i$ de $p_i$ poderá superar nem $a_i$ e nem $b_i$. Como estamos interessados no maior dos divisores positivos, basta tomarmos, para $c_i$, o menor desses dois, isto é,

$$c_i = \min\{a_i,\ b_i\}.$$

**Observação 2.19.** *O Teorema anterior nos fornece a regra seguinte para o cálculo do Máximo Divisor Comum de dois números inteiros positivos a e b.*

**Regra:** *Conhecidas as fatorações de a e b, o Máximo Divisor Comum de a e b é o produto dos fatores primos comuns às duas fatorações tomadas cada um com o menor expoente.*

**Exemplos:**

i) $4500 = 2^2 \cdot 3^2 \cdot 5^3 = 2^2 \cdot 3^2 \cdot 5^3 \cdot 7^0$

$2016 = 2^5 \cdot 3^2 \cdot 7 = 2^5 \cdot 3^2 \cdot 5^0 \cdot 7$

$(4500,\ 2016) = 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^0 = 36.$

ii) $756000 = 2^5 \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 11^0 \cdot 13^0$

$39600 = 2^4 \cdot 3^2 \cdot 5^2 \cdot 7^0 \cdot 11 \cdot 13^0$

$42120 = 2^3 \cdot 3^4 \cdot 5 \cdot 7^0 \cdot 11^0 \cdot 13$

$(756000,\ 39600,\ 42120) = 2^3 \cdot 3^2 \cdot 5 \cdot 7^0 \cdot 11^0 \cdot 13^0 = 360.$

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

**Demonstração**

Suponhamos, por absurdo, que exista uma quantidade finita de números primos, sejam eles $p_1,\ p_2,\ p_3,\ \ldots,\ p_n$. Consideremos um número $k$, tal que $k = p_1p_2p_3 \cdots p_n + 1$, é claro que $k$ é maior que qualquer um dos primos $p_1, p_2, p_3, \cdots, p_n$.

Mas nenhum primo dessa lista pode dividir $k$, pois se $p$ fosse primo que divide $k$, então $p$ teria que dividir 1 também, já que $1 = k - p_1p_2p_3 \cdots p_n$, o que é um absurdo, pois $p > 1$ e o único divisor positivo de 1 é 1. Logo, qualquer que seja o número primo $p_n$, existe um primo maior do que $p_n$, isto é, o conjunto $\{2, 3, 5, 7, 11, 13, 17, \cdots\}$ dos números primos é um conjunto infinito.

## 2.9 Conjunto dos múltiplos de um número inteiro

Chama-se conjunto dos múltiplos de um número inteiro qualquer, $a \neq 0$, indica-se por $M(a)$, ao conjunto formado por todos os múltiplos de $a$, isto é,

$$M(a) = \{x \in \mathbb{Z} / x = k \cdot a,\ k \in \mathbb{Z}\}$$

ou

$$M(a) = \{x \in \mathbb{Z} / a \mid x\}.$$

**Exemplos:**

$M(5) = \{0; \pm5; \pm10; \pm15; \ldots\}$.

$M(1) = \{0; \pm1; \pm2; \pm3; \ldots\}$.

$M(7) = \{0; \pm7; \pm14; \pm21; \ldots\}$.

**Observação 2.20.** *É imediado que, para todo inteiro* $a \neq 0$, *se tem* $M(a) = M(-a)$.

**Definição 2.3.** *Sejam a e b dois números inteiros não nulos (*$a \neq 0$ e $b \neq 0$*). Chama-se múltiplo comum de a e b e indica-se por* $M(a,\ b)$ *todo o inteiro x tal que* $a \mid x$ *e* $b \mid x$, *isto é,*

$$M(a,\ b) = \{x \in \mathbb{Z} / a \mid x \text{ e } b \mid x\}$$

*ou*

$$M(a,\ b) = \{x \in \mathbb{Z} / x \in M(a) \text{ e } x \in M(b)\}$$

*ou ainda*

$$M(a,\ b) = M(a) \cap M(b).$$

**Exemplo:**

$M(6) = \{0; \pm6; \pm12; \pm18; \pm24; \ldots\}$

$M(4) = \{0; \pm4; \pm8; \pm12; \pm16; \ldots\}$

$M(6,\ 4) = M(6) \cap M(4) = \{0; \pm12; \pm24; \pm36; \ldots\}$.

## 2.10 Mínimo Múltiplo Comum

Sejam $a$ e $b$ dois números inteiros não nulos ($a \neq 0$ e $b \neq 0$). Chama-se Mínimo Múltiplo Comum de $a$ e $b$, o menor inteiro positivo que é divisível por $a$ e $b$.

Notação: $\text{mmc}(a,\ b) = [a\ b]$.

**Exemplo:** Achar o Mínimo Múltiplo Comum de 8 e 12.

$M(8) = \{0; \pm8; \pm16; \pm24; \pm32; \pm40; \pm48; \pm56 \ldots\}$

$M(12) = \{0; \pm12; \pm24; \pm36; \pm48; \ldots\}$

$M(8,\ 12) = M(8) \cap M(12) = \{0; \pm24; \pm48 \ldots\}$

$[8,\ 12] = 24$.

**Proposição 2.3.** *Sejam a e b inteiros positivos, com decomposição em fatores primos da seguinte forma:*

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_n^{a_n}$$

*e*

$$b = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdot \ldots \cdot p_n^{b_n},$$

*onde* $a = p_1, p_2, p_3 \ldots p_n$ *são os primos que ocorrem na fatoração de a e b, então*

$$[a,\ b] = p_1^{\max\{a_1,\, b_1\}},\ p_2^{\max\{a_2,\, b_2\}},\ \ldots,\ \ p_n^{\max\{a_n,\, b_n\}}$$

*ou*

$$[a,\ b] = \prod_{i=1}^{n} p_i^{\max\{a_i,\, b_i\}}.$$

**Demonstração**

Da definição de Mínimo Múltiplo Comum nenhum fator primo $p_i$ deste mínimo poderá ter um expoente que seja inferior a $a_i$ e nem a $b_i$. Se tomarmos, pois, o maior destes dois expoentes de $p_i$ teremos, não apenas um múltiplo comum, mas o menor possível dentre todos eles, o que conclui a demonstração.

**Exemplo:**

$500 = 2^2 \cdot 3^0 \cdot 5^3 \cdot 7^0$

$630 = 2 \cdot 3^2 \cdot 5^1 \cdot 7$

$[630,\ 500] = 2^2 \cdot 3^2 \cdot 5^3 \cdot 7 = 31500.$

**Observação 2.21.** *O Teorema anterior nos fornece a regra seguinte para o cálculo do Mínimo Múltiplo Comum de dois números inteiros positivos a e b.*

**Regra:** *Conhecidas as fatorações de a e b, o Mínimo Múltiplo Comum de a e b é o produto dos fatores primos comuns e não comuns às duas fatorações tomadas cada um com o maior expoente.*

**Observação 2.22.** *Para calcularmos o Mínimo Múltiplo Comum entre dois inteiros positivos, utilizamos o algoritmo seguinte que é uma consequência imediata do Teorema anterior.*

**Exemplo:** Calcular o Mínimo Múltiplo Comum de 500 e 630.

| | | | |
|---|---|---|---|
| 500, | 630 | 2 | |
| 250, | 315 | 2 | |
| 125, | 315 | 3 | |
| 125, | 105 | 3 | |
| 125, | 35 | 5 | |
| 25, | 7 | 5 | |
| 5, | 7 | 5 | |
| 1, | 7 | 7 | × |
| 1, | 1 | 31500 | |

$500 = 2^2 \cdot 5^3$

$630 = 2 \cdot 3^2 \cdot 5 \cdot 7$

$[500,\ 630] = 2^2 \cdot 3^2 \cdot 5^3 \cdot 7^1$.

**Proposição 2.4.** *Se $x$ e $y$ são números reais, então*

$$\max\{x,\ y\} + \min\{x,\ y\} = x + y.$$

**Demonstração**

i) Se $x = y \Rightarrow \max\{x, y\} = \min\{x, y\} = x = y$ e, portanto, $\max\{x,\ y\} + \min\{x,\ y\} = x + y$.

ii) Se $x \neq y$, podemos considerar $x < y$ sem perda de generalidade.

Então, $\max\{x, y\} = y$ e $\min\{x, y\} = x$, portanto, $\max\{x,\ y\} + \min\{x,\ y\} = x + y$ como queríamos demonstrar.

**Teorema 2.16.** *Se $a$ e $b$ são dois números inteiros positivos, então*

$$[a,\ b] \cdot (a,\ b) = a \cdot b.$$

**Demonstração**

Sejam $a$ e $b$, dados por

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_n^{a_n} \quad \text{e} \quad b = p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_n^{b_n}.$$

Sabemos que

$$(a,\ b) = \prod_{i=1}^{n} p_i^{\min\{a_i,\ b_i\}} \quad \text{(Teorema 2.14)}$$

e

$$[a,\ b] = \prod_{i=1}^{n} p_i^{\max\{a_i,\ b_i\}} \quad \text{(Proposicão 2.3)},$$

logo,

$(a,\ b) = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_n^{r_n}$

$[a,\ b] = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_n^{s_n}$,

sendo que, para cada índice $i$, $r_i = \min\{a_i,\ b_i\}$ e $s_i = \max\{a_i,\ b_i\}$.

Pela Proposição 2.4, temos ainda que, para cada índice $i$, $r_i + s_i = \min\{a_i.\ b_i\} + \max\{a_i,\ b_i\} = a_i + b_i$

$\Rightarrow (a,\ b) \cdot [a,\ b] = (p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_n^{r_n}) \cdot (p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_n^{s_n})$

$\Rightarrow (a,\ b) \cdot [a,\ b] = p_1^{r_1+s_1} \cdot p_2^{r_2+s_2} \cdot \ldots \cdot p_n^{r_n+s_n}$

$\Rightarrow (a,\ b) \cdot [a,\ b] = p_1^{a_1+b_1} \cdot p_2^{a_2+b_2} \cdot \ldots \cdot p_n^{a_n+b_n}$

$\Rightarrow (a,\ b) \cdot [a,\ b] = (p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_n^{a_n}) \cdot (p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_n^{b_n})$

$\Rightarrow [a,\ b] \cdot (a,\ b) = a \cdot b.$

**Exemplo:**

$60 = 2^2 \cdot 3 \cdot 5$

$126 = 2 \cdot 3^2 \cdot 7$

$(60, 126) = 2 \cdot 3 = 6$

$[60, 126] = 2^2 \cdot 3^2 \cdot 5 \cdot 7 = 1260$

$60 \cdot 126 = 7560$

$(60, 126)[60, 126] = 6 \cdot 1260 = 7560.$

**Observação 2.23.** *Podemos encontrar também o Mínimo Múltiplo Comum ou Máximo Divisor Comum usando a relação*

$$[a,\ b] = \frac{ab}{(a,\ b)}.$$

## 2.11 Mínimo Múltiplo Comum de vários inteiros

Seja $a_1,\ a_2,\ a_3,\ \ldots,\ a_n$ uma coleção finita de números inteiros não nulos ($a_i \neq 0$). O Mínimo Múltiplo Comum dessa coleção é o menor inteiro positivo que é divisível simultaneamente por

todos os inteiros da coleção e será denotado por

$$\text{MMC}(a_1,\ a_2,\ a_3,\ \ldots,\ a_n) \text{ ou } [a_1,\ a_2,\ a_3,\ \ldots,\ a_n].$$

**Exemplo:** Calcular $[15, 20, 35, 50]$.

$15 = 3 \cdot 5$

$20 = 2^2 \cdot 5$

$35 = 5 \cdot 7$

$50 = 2 \cdot 5^2$

$[15, 20, 35, 50] = 2^2 \cdot 3 \cdot 5^2 \cdot 7 = 2100.$

## 2.12 Interpretação geométrica do MDC e do MMC

Com o intuito de enriquecer as aplicações do Máximo Divisor Comum (MDC) e do Mínimo Múltiplo Comum (MMC), apresentamos duas interpretações geométricas dadas, respectivamente, por Oliveira (1995) e Cardoso e Gonçalves (1996).

### 2.12.1 Interpretação geométrica do Máximo Divisor Comum

**Método:**

Dados dois números inteiros positivos $a$ e $b$, construímos um retângulo com essas dimensões. Cobrindo esse retângulo com os maiores quadrados possíveis, o lado do menor quadrado será o Máximo Divisor Comum entre $a$ e $b$.

**Exemplos:**

a) $(55, 15) = 5$.

Constrói-se um retângulo de dimensões 55 e 15 (Figura 2.1). Cobrindo o retângulo com os maiores quadrados possíveis, teremos três quadrados de lados 15, um quadrado de lado 10 e dois quadrados de lado 5. Logo, $(55, 15) = 5$.

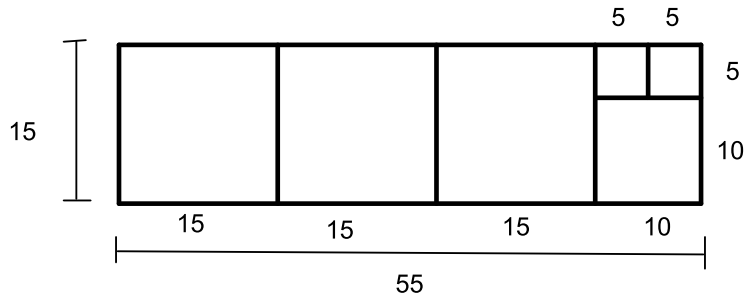


Figura 2.1: Método geométrico do MDC (55, 15).

b) $(40, 12) = 4$.

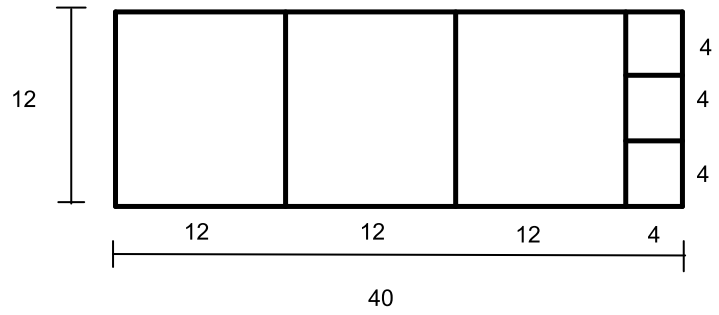


Figura 2.2: Método geométrico do MDC (40, 12).

c) (24, 16) = 8.

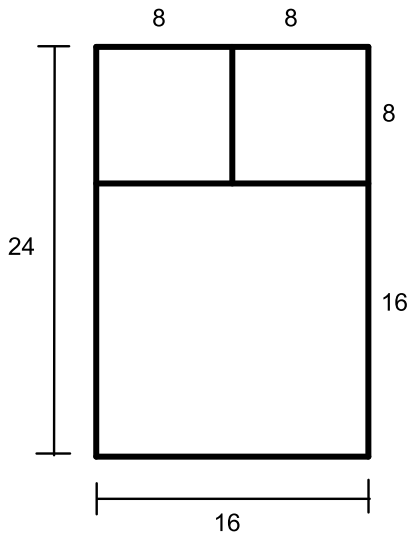


Figura 2.3: Método geométrico do MDC (24, 16).

O autor faz uma referência ao livro de Euclides que contém essencialmente o método.

### 2.12.2 Interpretação geométrica do Mínimo Múltiplo Comum

Para a interpretação do Mínimo Múltiplo Comum, os autores citados apresentaram o seguinte método:

Dados dois números inteiros positivos *m* e *n*:

1. Toma-se um retângulo ABCD de lados *m* e *n*. O retângulo deverá ser subdividido em quadrados unitários;

2. Partindo de um dos vértices do retângulo, traça-se as diagonais do quadrado unitário observando a seguinte ordem;

   a) Traça-se a diagonal do quadrado que tem vértice coincidente com o vértice escolhido do retângulo;

b) Traça-se, a partir do vértice no qual paramos, as diagonais dos quadrados que têm um ângulo oposto pelo vértice com o quadrado anterior ou, na ausência desse quadrado, traça-se a diagonal do quadrado ao lado e a partir do vértice onde paramos;

c) As diagonais dos quadrados unitários devem ser traçadas até que se chegue a um dos outros vértices do retângulo ABCD;

d) Conta-se quantos quadrados tiveram suas diagonais traçadas. O número encontrado é o Mínimo Múltiplo Comum de $m$ e $n$.

**Exemplo:**

I) MMC de 5 e 10 (iniciando, por exemplo, em A).

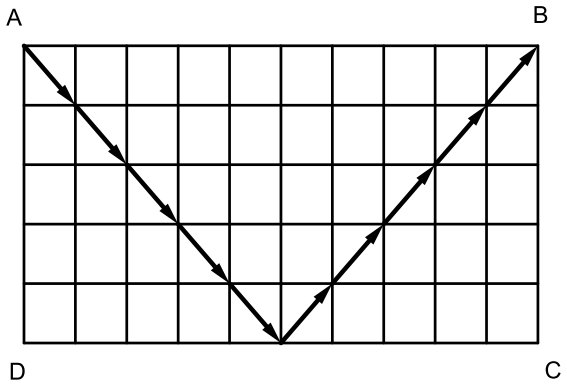


Figura 2.4: Método geométrico do MMC (5, 10).

Observa-se que 10 quadrados tiveram duas diagonais traçadas, o que implica que $[10,\ 5] = 10$.

II) MMC de 3 e 5 (iniciando, por exemplo, em C).

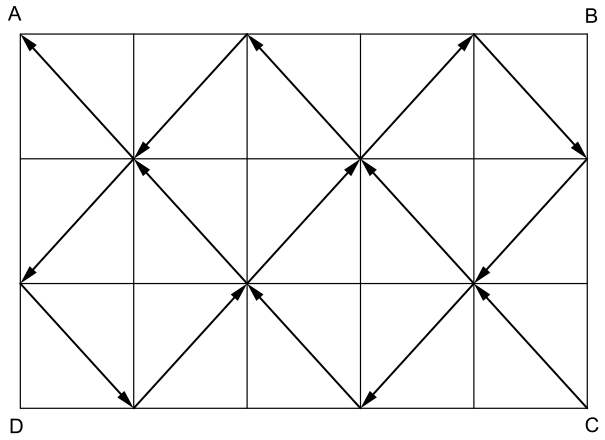


Figura 2.5: Método geométrico do MMC (3, 5).

Observa-se que 15 quadrados tiveram duas diagonais traçadas, o que implica que $[3,\ 5] = 15$.

III) MMC de 4 e 6 (iniciado, por exemplo, em D).

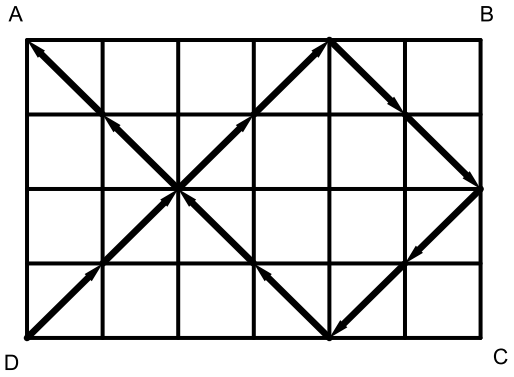


Figura 2.6: Método geométrico do MMC (4, 6).

Observa-se que 12 quadrados tiveram duas diagonais traçadas, o que implica que $[4,\ 6] = 12$.

Segundo os autores Cardoso e Gonçalves (1996), o referido método baseia-se nos seguintes fatos: ao partirmos de um vértice do retângulo e chegarmos a um outro vértice desse mesmo retângulo, traçamos diagonais de um número de quadrados que corresponde a um múltiplo tanto de $m$ quanto de $n$; parando no primeiro, outro vértice do retângulo ABCD, estamos determinando o mínimo dentre os múltiplos comuns entre $m$ e $n$.

Como estamos traçando os múltiplos tanto de $m$ quanto de $n$, quando chegamos num outro vértice, encontramos, na realidade, um múltiplo comum de $m$ e $n$ que é o menor, pois é o primeiro múltiplo comum encontrado.

## 2.13 Critério de divisibilidade por 2,3,4,5,6,7,8,9,10,11,12,13

Chama-se critério de divisibilidade todo conjunto de condições que permitem reconhecer se um dado inteiro é divisível por outro.

**Critério de divisibilidade por 2**

Um número natural $a$ é divisível por 2 se, e somente se, o algarismo das unidades de $a$ for divisível por 2, isto é, $a$ é divisível por 2 se $a$ é par.

**Demonstração**

Seja o número natural $a$ dado por

$$a = 10^n \cdot a_n + 10^{n-1} \cdot a_{n-1} + \ldots + 10^2 \cdot a_2 + 10 \cdot a_1 + a_0$$

em que $a_i$ tomam valores de 0 a 9.

Colocando 10 em evidência, temos

$$a = 10(10^{n-1} \cdot a_n + 10^{n-2} \cdot a_{n-1} + \ldots + 10 \cdot a_2 + a_1) + a_0.$$

Como $10^{n-1} \cdot a_n + 10^{n-2} \cdot a_{n-1} + \ldots + 10 \cdot a_2 + a_1$ é um inteiro $k$, temos que

$$a = 10k + a_0.$$

- Se $2 \mid a \Rightarrow \exists q \in \mathbb{Z};\ a = 2q \Rightarrow 2q = 10k + a_0 \Rightarrow a_0 = 2(q - 5k) = 2 \cdot q_2;\ q_2 \in \mathbb{Z},$ logo $2 \mid a_0$.

- Reciprocamente, se $2 \mid a_0 \Rightarrow \exists q;\ a_0 = 2q$
  $\Rightarrow a = 10k + 2q \Rightarrow a = 2(5k + q) \Rightarrow a = 2k_2,$ onde $k_2 \in \mathbb{Z}$, logo $2 \mid a$.

**Exemplo:** 345678 é divisível por 2 pois é um número par.

**Critério de divisibilidade por 3**

Se $a \in \mathbb{N},\ a = 10^n \cdot a_n + 10^{n-1} \cdot a_{n-1} + \ldots + 10^2 \cdot a_2 + 10 \cdot a_1 + a_0$.

Fazendo

$$\begin{aligned}
10 &= 9+1 = 3k_1+1, && k_1 = 3\\
10^2 &= 100 = 99+1 = 3k_2+1 && k_2 = 33\\
10^3 &= 1000 = 999+1 = 3k_3+1, && k_3 = 333\\
&\vdots\\
10^n &= 1\underbrace{00\ldots0}_{n\ zeros} = \underbrace{99\ldots9}_{n\ noves}+1 = 3k_n+1, && k_n = \underbrace{33\ldots3}_{n\ três}
\end{aligned}$$

e substituindo, temos:

$$\begin{aligned}
a &= a_n\cdot(3k_n+1)+a_{n-1}(3k_{n-1}+1)+\ldots+a_2(3k_2+1)+a_1(3k_1+1)+a_0\\
\Rightarrow\ a &= 3a_n\cdot k_n+3a_{n-1}k_{n-1}+\ldots+3a_2k_2+3a_1k_1+a_n+a_{n-1}+\ldots+a_2+a_1+a_0\\
\Rightarrow\ a &= 3(a_n\cdot k_n+a_{n-1}k_{n-1}+\ldots+a_2k_2+a_1k_1)+a_n+a_{n-1}+\ldots+a_2+a_1+a_0\\
\Rightarrow\ a &= 3k+a_n+a_{n-1}+\ldots+a_2+a_1+a_0,
\end{aligned}$$

com $k = a_n\cdot k_n+a_{n-1}k_{n-1}+\ldots+a_2k_2+a_1k_1$ e $k\in\mathbb{Z}$. Logo, concluímos que se $3\mid a$, como $3\mid 3k$, pelo teorema 2.1 item X, 3 divide $(a_n+a_{n-1}+\ldots+a_0)$.

Reciprocamente, se $3\mid(a_n+a_{n-1}+\ldots+a_0)$, então $3\mid a$, uma vez que $3\mid 3k$. Logo, concluímos que um número natural é divisível por 3 se, e somente se, a soma de seus algarismos é divisível por 3.

**Exemplo:** 2357841 é divisível por 3, pois $2+3+5+7+8+4+1 = 30$ e 30 é múltiplo de 3.

**Critério de divisibilidade por 4**

Seja um número natural $a$, dado por

$$\begin{aligned}
a &= 10^n\cdot a_n+10^{n-1}\cdot a_{n-1}+\ldots+10^2\cdot a_2+10\cdot a_1+a_0\\
\Rightarrow\ a &= 100\cdot(10^{n-2}\cdot a_n+10^{n-3}\cdot a_{n-1}+\ldots+\cdot a_2)+10\cdot a_1+a_0\\
\Rightarrow\ a &= 100\cdot k+a_1a_0,\ \text{onde } k = 10^{n-2}\cdot a_n+10^{n-3}\cdot a_{n-1}+\ldots+\cdot a_2
\end{aligned}$$

e, portanto, $k\in\mathbb{N}$ e $a_1a_0$ é o número formado pelos dois últimos dígitos de $a$, isto é, o algarismo das dezenas e o algarismo das unidades.

Como 100 é múltiplo de 4, temos que o número $a$ é múltiplo de 4 se, e somente se, $a_1a_0$ é divisível por 4.

i) Se $4 \mid a \Rightarrow a = 4q,\ q \in \mathbb{Z}$ e como $a = 100k + a_1a_0$

$\Rightarrow 4q = 100k + a_1a_0 \Rightarrow a_1a_0 = 4(q - 25k)$

e como $q - 25k$ é inteiro $\Rightarrow a_1a_0 = 4k_2,\ k_2 \in \mathbb{Z}$ e, portanto, $a_1a_0$ é múltiplo de 4.

ii) Reciprocamente, se $4 \mid a_1a_0 \Rightarrow a_1a_0 = 4q$

$\Rightarrow a = 100k + 4q \Rightarrow a = 4(25k + q)$ e como 25k+q é inteiro $\Rightarrow a = 4k_2,\ k_2 \in \mathbb{Z}$.

**Exemplos:**

- 4577844 é divisível por 4, pois 44 é múltiplo de 4.
- 37280 é divisível por 4, pois 80 é múltiplo de 4.
- 82500 é divisível por 4, pois 00 é múltiplo de 4.
- 352918 não é divisível por 4, pois 18 não é múltiplo de 4.

**Critério de divisibilidade por 5**

Como todo número inteiro pode ser escrito da forma $10k + a_0$, onde $a_0$ é o algarismo das unidades, temos que $a = 10k + a_0$ é divisivel por 5 se, e somente se, $a_0$ é múltiplo de 5, isto é, se $a_0 = 0$ ou $a_0 = 5$.

i) Se $5 \mid a \Rightarrow a = 5q, q \in \mathbb{Z}$ e como $a = 10k + a_0$

$\Rightarrow 5q = 10k + a_0 \Rightarrow a_0 = 5q - 10k \Rightarrow a_0 = 5(q - 2k)$, portanto, $a_0$ é múltiplo de 5 e ainda como $a_0$ é o algarismo das unidades de $a$, então $a_0 \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ e, portanto, $a_0 = 0$ ou $a_0 = 5$.

ii) Se $a_0 = 0$ ou $a_0 = 5$.

Para $a_0 = 0$. Como $a = 10k + a_0 \Rightarrow a = 10k = 5 \cdot 2k$, portanto, a é múltiplo de 5.

Para $a_0 = 5$. Novamente, como $a = 10k + a_0 \Rightarrow a = 5(2k + 1)$, portanto, $a$ é múltiplo de 5, então se $a_0 = 0$ ou $a_0 = 5 \Rightarrow 5 \mid a$.

Portanto, seja $a = 10k + a_0 \Rightarrow 5 \mid a \Leftrightarrow a_0 = 0$ ou $a_0 = 5$.

**Exemplos:**

- 345085 é divisível por 5, pois termina em 5.
- 72040 é divisível por 5, pois termina em 0.

- 45728 não é divisível por 5, pois não termina nem em 0 e nem em 5.

**Critério de divisibilidade por 6**

Um número natural é divisível por 6 se, e somente se, é divisível simultaneamente por 2 e 3.

**Demonstração**

i) Se $6 \mid a \Rightarrow a = 6k,\ k \in \mathbb{Z} \Rightarrow a = 2 \cdot 3k$, portanto, $a$ é múltiplo de 2 e $a$ é múltiplo de 3.

ii) Se $2 \mid a \Rightarrow a = 2p$, $p \in \mathbb{Z}$ e se $3 \mid a \Rightarrow a = 3q$, $q \in \mathbb{Z}$.

Como 2 e 3 são primos entre si, é sempre possível escrever $a = 2 \cdot 3k$, onde $k = (p,\ q)$. Logo, $a = 6k$ e, portanto, divisível por 6.

**Exemplos:**

- 235422 é divisível por 6, pois é divisível por 2 (par) e é divisível por 3 $(2 + 3 + 5 + 4 + 2 + 2 = 18)$, simultaneamente.

- 4335 não é divisível por 6, pois não é divisível por 2.

- 52732 não é divisível por 6, pois não é divisível por 3.

**Critério de divisibilidade por 7**

Seja $a = 10k + a_0,\ k \in \mathbb{Z}$ e $a_0$ é o algarismo das unidades, então $a$ é múltiplo de $7 \Leftrightarrow k - 2a_0$ é múltiplo de 7.

**Demonstração**

($\Rightarrow$) Se $10k + a_0$ é múltiplo de 7, então existe inteiro q tal que $10k + a_0 = 7q$ e, portanto, $k - 2a_0 = k - 2(7q - 10k) = k - 14q + 20k \Rightarrow k - 2a_0 = 21k - 14q = 7(3k - 2q)$, logo $k - 2a_0$ é múltiplo de 7.

($\Leftarrow$) Se $k - 2a_0$ é múltiplo de 7, então existe inteiro $p$, tal que $k - 2a_0 = 7p$ e, portanto,

$$10k + a_0 = 10 \cdot (7p + 2a_0) + a_0 = 70p + 20a_0 + a_0 \Rightarrow 10k + a_0 = 70p + 21a_0 = 7 \cdot (10p + 3a_0).$$

Logo, $10k + a_0$ é múltiplo de 7.

**Observação 2.24.** *O número $k - 2a_0$ não é retirado da cartola simplesmente, existe uma explicação para tal fato, vejamos:*

*Seja* $a = 10k + a_0$. *A ideia deste e de outros critérios de divisibilidade é subtrair de* $k$ *um múltiplo conveniente de* $a_0$. *Assim*

$$\begin{aligned} & a = 10k + a_0 \\ \Rightarrow \quad & a = 10k - 10\lambda a_0 + 10\lambda a_0 + a_0 \\ \Rightarrow \quad & a = 10(k - \lambda a_0) + a_0(10\lambda + 1). \end{aligned}$$

*A ideia é procurar um* $\lambda$ *de tal forma que* $10\lambda + 1$ *seja divisível por 7. A possibilidade mais simples é 2. De fato,* $10 \cdot 2 + 1 = 21$ *é múltiplo de 7. Como* $(7,\ 10) = 1$, *temos*

$$7|a \Leftrightarrow 7|(a - 21a_0) \Leftrightarrow 7|10(k - 2a_0) \Leftrightarrow 7|(k - 2a_0).$$

**Regra:** Um número é divisível por 7 se o dobro do último algarismo, subtraído do número sem o último algarismo, resultar um número divisível por 7. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisibilidade por 7.

**Exemplos:**

**a)** 33523

$3352 - 2 \cdot 3 = 3346$

$334 - 2 \cdot 6 = 322$

$32 - 2 \cdot 2 = 28.$

Como 28 é múltiplo de 7, então 33523 é divisível por 7.

**b)** 398898

$39889 - 2 \cdot 8 = 39873$

$3987 - 2 \cdot 3 = 3981$

$398 - 2 \cdot 1 = 396$

$39 - 2 \cdot 6 = 27.$

Como 27 não é múltiplo de 7, então 398898 não é divisível por 7.

**Critério de divisibilidade por 8**

Seja um número natural $a$, dado por

$$a = 10^n \cdot a_n + 10^{n-1} \cdot a_{n-1} + \ldots + 10^4 \cdot a_4 + 10^3 \cdot a_3 + 10^2 \cdot a_2 + 10 \cdot a_1 + a_0$$

$$\Rightarrow a = 10^3(10^{n-3} \cdot a_n + 10^{n-4} \cdot a_{n-1} + \ldots + 10 \cdot a_4 + a_3) + 10^2 \cdot a_2 + 10 \cdot a_1 + a_0$$

$$\Rightarrow a = 1000k + a_2a_1a_0, \text{ onde } k \in \mathbb{N} \text{ e } k = 10^{n-3} \cdot a_n + 10^{n-4} \cdot a_{n-1} + \ldots + 10 \cdot a_4 + \cdot a_3$$

e $a_2a_1a_0$ é o número formado pelos três últimos dígitos de $a$, isto é, os algarismos das centenas, dezenas e unidades, respectivamente. Como 1000 é múltiplo de 8, $a$ é múltiplo de 8 se, e somente se, $a_2a_1a_0$ é múltiplo de 8.

**Demonstração**

($\Rightarrow$) Se $8 \mid a \Rightarrow a = 8q,\ q \in \mathbb{Z}$

$a = 1000k + a_2a_1a_0 \Rightarrow 8q - 1000k = a_2a_1a_0 \Rightarrow a_2a_1a_0 = 8 \cdot (q - 125k)$. Logo, $a_2a_1a_0$ é múltiplo de 8, pois $q - 125k$ é um número inteiro.

($\Leftarrow$) Se $a_2a_1a_0$ é múltiplo de 8, então $a_2a_1a_0 = 8q,\ q \in \mathbb{Z}$. Logo, temos

$a = 1000k + 8q = 8(125k + q)$, portanto, $a$ é múltiplo de 8.

**Exemplos:**

- 3671384 é divisível por 8, pois 384 é múltiplo de 8.
- 457841 não é divisível por 8, pois 841 não é múltiplo de 8.

**Critério de divisibilidade por 9**

Seja $a$ um número natural, dado por

$$a = 10^n \cdot a_n + 10^{n-1} \cdot a_{n-1} + \ldots + 10 \cdot a_1 + a_0.$$

Fazemos a seguir as seguintes substituições:

$$\begin{aligned} 10 &= 9 + 1 \\ 100 &= 99 + 1 \\ 1000 &= 999 + 1 \\ &\vdots \\ 10^n &= \underbrace{99\ldots9}_{n\ 9's} + 1 \end{aligned}$$

obtendo

$a = a_n(\underbrace{99\ldots9}_{n\ 9's}+1) + a_{n-1}(\underbrace{99\ldots9}_{n-1\ 9's}+1) + \ldots + a_2(99+1) + a_1(9+1) + a_0$

$\Rightarrow a = a_n\underbrace{99\ldots9}_{n\ 9's} + a_n + a_{n-1}\underbrace{99\ldots9}_{n-1\ 9's} + a_{n-1} + \ldots + a_2 99 + a_2 + a_1 9 + a_1 + a_0$

$\Rightarrow a = 9(a_n\underbrace{11\ldots1}_{n\ 1's} + a_{n-1}\underbrace{11\ldots1}_{n-1\ 1's} + \ldots + a_2 11 + a_1) + a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0$

$\Rightarrow a = 9k + a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0,\ k \in \mathbb{N}$. Logo, $a$ é divisível por 9 se, e somente se, $a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0$ é múltiplo de 9, isto é, um número natural $a$ é múltiplo de 9 se, e somente se, a soma dos algarismos é um número divisível por 9.

**Demonstração**

i) Se $9 \mid a \Rightarrow a = 9q,\ q \in \mathbb{Z}$

$\Rightarrow a = 9k + a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0$

$\Rightarrow 9q = 9k + a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0$

$\Rightarrow a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0 = 9q - 9k$

$\Rightarrow a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0 = 9(q-k)$

$\Rightarrow a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0$ é múltiplo de 9, pois $(q-k) \in \mathbb{Z}$.

ii) Se $9 \mid (a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0) \Rightarrow a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0 = 9p,\ p \in \mathbb{Z}$. Como $a = 9k + a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0 \Rightarrow a = 9k + 9p \Rightarrow a = 9(k+p) \Rightarrow a$ é múltiplo de 9.

**Exemplos:**

- 2354211 é múltiplo de 9, pois $2 + 3 + 5 + 4 + 2 + 1 + 1 = 18$ que é múltiplo de 9.
- 4235 não é múltiplo de 9, pois $4 + 2 + 3 + 5 = 14$ que não é múltiplo de 9.

**Critério de divisibilidade por 10**

Um número natural é divisível por 10 se, e somente se, o algarismo da unidade é 0 (zero).

**Demonstração**

Seja $a = 10k + a_0$, onde $a_0$ é o algarismo das unidades de $a$.

- Se $10 \mid a \Rightarrow a = 10q,\ q \in \mathbb{Z} \Rightarrow 10q = 10k + a_0 \Rightarrow a_0 = 10q - 10k = 10(q-k)$, logo $a_0$ é múltiplo de 10 e, como $a_0 \in \{0,1,2,3,4,5,6,7,8,9\}$, temos que $a_0 = 0$.
- Se $a_0 = 0$

  $a = 10k + a_0 \Rightarrow a = 10k + 0 \Rightarrow a = 10k$. Logo, $a$ é múltiplo de 10.

**Exemplos:**

- 356980 é múltiplo de 10, pois termina em zero.
- 4579 não é múltiplo de 10, pois não termina em zero.

**Critério de divisibilidade por 11**

Antes de provarmos o critério de divisibilidade por 11, devemos provar as seguintes proposições:

**Proposição 2.5.** *Todo número da forma* $99\ldots9$*, onde o número de "9"s é par, é divisível por 11.*

**Demonstração**

Seja $a = 99\ldots9$, com $2n$ "9"$s$ queremos provar que $11 \mid a$.

Por indução, temos:

i)p/$n = 1$, temos que o número de algarismo 9 é 2, logo $a = 99 = 9 \cdot 11 \cdot q$, portanto, $11 \mid a$.

ii) Vamos supor que $a = 99\ldots9$ com $2n$ algarismos 9 é múltiplo de 11, ou seja, $a = 11q_1,\ q_1 \in \mathbb{Z}$ (Hipótese de indução).

iii) Vamos provar que $a = 999\ldots9$ com $2n + 2$ algarismos 9 também é múltiplo de 11.

$a = 999\ldots9 = \underbrace{99\ldots900}_{2k\ algarismos\ 9} + 99 \Rightarrow a = \underbrace{999\ldots9}_{2kalgarismos9} \cdot 100 + 99$

e como $99\ldots9$ com $2k$ algarismos 9 é múltiplo de 11 (Hipótese de indução), temos que

$a = 11q_1 \cdot 100 + 11 \cdot 9 \Rightarrow a = 11(100 \cdot q_1 + 9) \Rightarrow a = 11q_2,\ q_2 \in \mathbb{Z}$. Logo, $a$ é múltiplo de 11.

**Proposição 2.6.** *Todo número da forma* $1000\ldots01$*, onde o número de "0"s entre os dois "1"s é par, é múltiplo de 11.*

**Demonstração**

Seja $a = 100\ldots01$ com $2n$"0"$s$ entre os dois "1"$s$, queremos provar que $11 \mid a$.

Por indução:

i) p/$n = 1$ temos que o número de algarismos "0"s entre os dois 1's é 2, logo $a = 1001 = 990 + 11 \Rightarrow a = 11 \cdot 90 + 11 \Rightarrow a = 11(90 + 1) \Rightarrow a = 11 \cdot 91$. Portanto, $11 \mid a$

ii) Vamos supor que $a = 100\ldots1$, com $2k$ "0" $s$ entre os dois "1"$s$ é múltiplo de 11, isto é, $a = 1\underbrace{00\ldots0}_{2k\ zeros}1 = 11q$.

iii) Vamos provar que $a = 1\underbrace{00\ldots0}_{2k+2\ zeros}1$ também é múltiplo de 11.

$\Rightarrow a = 1000\ldots01 = \underbrace{999\ldots9}_{2k+2\ noves} + 11$.

Pela proposição anterior, provou-se que $99\ldots9$, com $2k+2$ algarismos 9's é múltiplo de 11, isto é, $99\ldots9 = 11q_2$ e, portanto, $a = 11q_2 \cdot 10 + 11 \Rightarrow a = 11(10q_2 + 1)$. Logo, $a$ é múltiplo de 11.

**Critério:**

Seja $a$ um número natural, dado por

$$a = 10^n \cdot a_n + 10^{n-1} \cdot a_{n-1} + \ldots + 10^3 \cdot a_3 + 10^2 \cdot a_2 + 10 \cdot a_1 + a_0.$$

i) Se $n$ é par

Fazendo as seguintes substituições:

$$\begin{aligned}
10 &= 11 - 1\\
100 &= 99 + 1\\
1000 &= 1001 - 1\\
10000 &= 9999 + 1\\
&\vdots\\
10^{n-1} &= 1000\ldots01 - 1 \quad (n-2\ zeros)\\
10^n &= 99\ldots9 + 1 \quad (n\ noves),
\end{aligned}$$

obtemos

$$\begin{aligned}
a = a_n \cdot (\underbrace{999\ldots9}_{n\ 9's} + 1) &+ a_{n-1} \cdot (\underbrace{100\ldots01}_{n-2\ 0's} - 1) + \ldots + a_3 \cdot (1001 - 1) +\\
&+ a_2 \cdot (99 + 1) + a_1 \cdot (11 - 1) + a_0
\end{aligned}$$

$$\begin{aligned}
\Rightarrow a = a_n \cdot 99\ldots9 &+ a_n + a_{n-1} \cdot 100\ldots01 - a_{n-1} + \ldots + a_3 \cdot 1001 - a_3 +\\
&+ a_2 \cdot 99 + a_2 + a_1 \cdot 11 - a_1 + a_0.
\end{aligned}$$

Como $99\ldots9$, $100\ldots01$, $1001$, $99$ e $11$ são múltiplos de 11 (Proposições 2.5 e 2.6), temos que

$$a = 11k + a_n - a_{n-1} + \ldots - a_3 + a_2 - a_1 + a_0$$

$$\Rightarrow a = 11k + (a_n + a_{n-2} + \ldots + a_2 + a_0) - (a_{n-1} + a_{n-3} + \ldots + a_3 + a_1).$$

ii) Se n é ímpar

Fazendo as seguintes substituições:

$$\begin{aligned}
10 &= 11 - 1\\
100 &= 99 + 1\\
1000 &= 1001 - 1\\
10000 &= 9999 + 1\\
&\vdots\\
10^{n-1} &= 99\ldots9 + 1 \ (n-1 \text{ noves})\\
10^{n} &= 1000\ldots01 - 1 \ (n-1 \text{ zeros}),
\end{aligned}$$

obtemos

$$\begin{aligned}
a = a_n \cdot (\underbrace{100\ldots01}_{n-1\ 0's} - 1) &+ a_{n-1} \cdot (\underbrace{99\ldots9}_{n-1\ 9's} + 1) + a_{n-2} \cdot (\underbrace{100\ldots01}_{n-3\ 0's} - 1) + a_{n-3} \cdot (\underbrace{99\ldots9}_{n-3\ 9's} + 1)\ldots +\\
&+ a_4 \cdot (9999 + 1) + a_3 \cdot (1001 - 1) + a_2 \cdot (99 + 1) + a_1 \cdot (11 - 1) + a_0
\end{aligned}$$

$$\begin{aligned}
\Rightarrow a &= a_n \cdot 100\ldots01 - a_n + a_{n-1} \cdot 99\ldots9 + a_{n-1} + a_{n-2} \cdot 100\ldots01 - a_{n-2} + a_{n-3} \cdot 99\ldots9 +\\
&+ a_{n-3} + \ldots + a_4 \cdot 9999 + a_4 + a_3 \cdot 1001 - a_3 + a_2 \cdot 99 + a_2 + a_1 \cdot 11 - a_1 + a_0.
\end{aligned}$$

Como $100\ldots01,\ 99\ldots9,\ \ldots,\ 9999,\ 1001,\ 99$ e $11$ são múltiplos de 11 (Proposições 2.5 e 2.6), temos que

$$a = 11q - a_n + a_{n-1} - a_{n-2} + a_{n-3} - \ldots + a_4 - a_3 + a_2 - a_1 + a_0$$

$$\Rightarrow a = 11q + (a_{n-1} + a_{n-3} + \ldots + a_4 + a_2 + a_0) - (a_n + a_{n-2} + \ldots + a_3 + a_1).$$

Em (i), tem-se que $a_n,\ a_{n-2},\ \ldots,\ a_2,\ a_0$ são algarismos de ordem ímpar de $a$ e $a_{n-1},\ a_{n-3},\ \ldots,\ a_3,\ a_1$ são os algarismos de ordem par de $a$.

Em (ii), tem-se que $a_{n-1},\ a_{n-3},\ \ldots,\ a_4,\ a_2,\ a_2,\ a_0$ são os termos de ordem ímpar e $a_n,\ a_{n-2},\ \ldots,\ a_3,\ a_1$ são os termos de ordem par.

Fazendo em (i) e (ii) $S_i$ como a soma dos algarismos de ordem ímpar e $S_p$ a soma dos algarismos de ordem par, temos que nos dois casos

$$a = 11k + S_i - S_p.$$

Portanto, $a$ é divisível por 11 se, e somente se, a diferença entre a soma dos algarismos de ordem ímpar e a soma dos algarismos de ordem par for múltipla de 11.

**Demonstração**

- Se $11 \mid a \Rightarrow a = 11q,\ q \in \mathbb{Z}$ e como $a = 11k + S_i - S_p$
  $\Rightarrow 11q - 11k = S_i - S_p \Rightarrow S_i - S_p = 11(q - k)$, portanto, $S_i - S_p$ é múltiplo de 11.

- Se $11 \mid (S_i - S_p) \Rightarrow S_i - S_p = 11q,\ q \in \mathbb{Z}$
  $\Rightarrow a = 11k + S_i - S_p \Rightarrow a = 11k + 11q \Rightarrow a = 11(k + q)$. Logo, $a$ é múltiplo de 11.

**Exemplos:**

- 10885985 é múltiplo de 11, pois
  $S_i = 5 + 9 + 8 + 0 = 22$
  $S_p = 8 + 5 + 8 + 1 = 22$
  $S_i - S_p = 0$ e "0" é múltiplo de 11.

- 87549 é múltiplo de 11, pois
  $S_i = 9 + 5 + 8 = 22$
  $S_p = 4 + 7 = 11$
  $S_i - S_p = 22 - 11 = 11$ e 11 é múltiplo de 11.

- 845032 não é múltiplo de 11, pois
  $S_i = 2 + 0 + 4 = 6$
  $S_p = 3 + 5 + 8 = 16$
  $S_i - S_p = -10$, então $S_i - S_p$ não é múltiplo de 11.

**Critério de divisibilidade por 12**

Um número natural $a$ é divisível por 12 se, e somente se, é divisível por 3 e 4 simultaneamente.

i) Se $12 \mid a \Rightarrow a = 12k,\ k \in \mathbb{Z} \Rightarrow a = 3 \cdot 4 \cdot k$, portanto, $a$ é múltiplo de 3 e 4 simultaneamente.

ii) Se $3 \mid a \Rightarrow a = 3p,\ p \in \mathbb{Z}$. Se $4 \mid a \Rightarrow a = 4q,\ q \in \mathbb{Z}$

Como 3 e 4 são primos entre si, é sempre possível escrever $a = 3 \cdot 4 \cdot k$, onde $k = (p,\ q)$. Logo, $a = 12 \cdot k$ e, portanto, divisível por 12.

**Exemplos:**

- 219588 é divisível por 12, pois é múltiplo de 4 e de 3.
- 315423 não é divisível por 12, pois não é múltiplo de 4.
- 804110 não é divisível por 12, pois não é múltiplo de 3.

**Critério de divisibilidade por 13**

Seja $a = 10k + a_0,\ k \in \mathbb{N}$ e $a_0$ é o algarismo das unidades de $a$, dizemos que $a$ é múltiplo de 13 se, e somente se, $k + 4a_0$ é múltiplo de 13.

**Demonstração:**

($\Rightarrow$) Se $10k + a_0$ é múltiplo de 13, então $10k + a_0 = 13q$ e, portanto, $a_0 = 13q - 10k$. Logo, $k + 4a_0 = k + 4(13q - 10k) = k + 52q - 40k = 52q - 39k \Rightarrow k + 4a_0 = 13(4q - 3k) \Rightarrow k + 4a_0$ é múltiplo de 13.

($\Leftarrow$) Se $k + 4a_0$ é múltiplo de 13, então

$$k + 4a_0 = 13p \Rightarrow k = 13p - 4a_0.$$

Logo, $10k + a_0 = 10(13p - 4a_0) + a_0$

$130p - 40a_0 + a_0 = 130p - 39a_0 \Rightarrow 10k + a_0 = 13(10p - 3a_0)$. Portanto, conclui-se que $10k + a_0$ é múltiplo de 13.

**Regra:** Um número natural é divisível por 13 se, e somente se, o quádruplo do algarismo das unidades somado ao número sem o último algarismo, resultar em um número divisível por 13. Se o número obtido for grande, repete-se o processo até que se possa verificar a divisibilidade por 13.

**Exemplos:**

- 856323

  $856323 + 4 \cdot 3 = 85644$

  $8564 + 4 \cdot 4 = 8580$

  $858 + 4 \cdot 0 = 858$

  $85 + 4 \cdot 5 = 117$

  $11 + 4 \cdot 7 = 39$ (múltiplo de 13). Portanto, 856323 é múltiplo de 13.

- 26846

  $2684 + 4 \cdot 6 = 2708$

  $270 + 4 \cdot 8 = 302$

  $30 + 4 \cdot 2 = 38$ (não é múltiplo de 13). Portanto, 26846 não é múltiplo de 13.

Poderíamos enunciar e demonstrar outros critérios de divisibilidade, porém, o que interessa é saber que eles existem.

A Tabela abaixo apresentada por Guedes (1988) permite verificar se um dado número natural $n$, é ou não divisível por um número primo $p$, $7 \leq p < 100$.

| Nº primo | Forma aditiva | Forma subtrativa |
|---|---|---|
| 7 | a+5b | a-2b |
| 11 | a+10b | a-b |
| 13 | a+4b | a-9b |
| 17 | a+12b | a-5b |
| 19 | a+2b | a-17b |
| 23 | a+7b | a-16b |
| 29 | a+3b | a-26b |
| 31 | a+90b * | a-3b |
| 37 | a+26b | a-11b |
| 41 | a+37b | a-4b |
| 43 | a+13b | a-30b |
| 47 | a+80b * | a-14b |
| 53 | a+16b | a-90b * |
| 59 | a+6b | a-53b |
| 61 | a+55b | a-6b |
| 67 | a+47b | a-20b |
| 71 | a+64b | a-7b |
| 73 | a+22b | a-51b |
| 79 | a+8b | a-71b |
| 83 | a+25b | a-58b |

∗ 90, 80 e 90 foram colocados na tabela no lugar dos números menores 28, 33 e 37, respectivamente, porque dão maior agilidade ao processo.

Exemplificando o uso da tabela, considere um número natural $n$, temos que:

**b** é o algarismo das unidades de $n$;

**a** é o número formado pelos demais algarismos de $n$.

Para facilitar a compreensão, por exemplo, um dado número é divisível por 19 (ver tabela) se, e somente se, é divisível por $a + 2b$ ou $a - 17b$.

**Exemplo:** Verificar se o número 695362 é divisível por 19.

**i)** Forma aditiva

$\underbrace{69536}_{a} + 2 \cdot \underbrace{2}_{b} = 69540$

$6954 + 2 \cdot 0 = 6954$

$695 + 2 \cdot 4 = 703$

$70 + 2 \cdot 3 = 76$

$7 + 2 \cdot 6 = 19$(múltiplo de 19). Logo, 695362 é divisível por 19

**ii)** Forma subtrativa

$69536 - 17 \cdot 2 = 69502$

$6950 - 17 \cdot 2 = 6916$

$691 - 17 \cdot 9 = 589$

$58 - 17 \cdot 9 = -95$(múltiplo de 19). Portanto, 695362 é múltiplo de 19.

**Observação 2.25.** *Como podemos garantir que o método funciona?*

*Como o a e b foram definidos, temos que*

$$n = 10a + b.$$

*O processo consiste em achar um número k tal que* $n = 10a + b$ *seja um múltiplo do número primo p se, e somente se,* $m = a + kb$ *for múltiplo de p.*

*Das duas igualdades,*

$$n = 10(m - kb) + b \Rightarrow n = 10m - 10kb + b \Rightarrow n = 10m + (1 - 10k)b,$$

*temos ainda que se* $1 - 10k$ *for divisível pelo número primo p, então:*

*i) Se p* ($p \neq 2$ e $p \neq 5$) *dividir n então p dividirá m.*

*Se* $p|n \Rightarrow n = q_1 p,\ q - 1 \in \mathbb{Z}$*, daí*

$$n = 10m + (1 - 10k)b \Rightarrow q_1 p = 10m + (1 - 10k)b$$

*e como* $1 - 10k$ *é múltiplo de p, temos que*

$$\begin{aligned} & 1 - 10k = q_2 p, \quad q_2 \in \mathbb{Z} \ \Rightarrow \ q_1 p = 10m + q_2 p \ \Rightarrow \ q_1 p - q_2 p = 10m \\ \Rightarrow \ & (q_1 - q_2)p = 10m \ \Rightarrow \ qp = 10m, \quad q \in \mathbb{Z}. \end{aligned}$$

*Como* $p \neq 2$ *e* $p \neq 5$*, o que implica* $p|m$*.*

*ii) Reciprocamente, se p dividir m, então, p dividirá n* ($m = k_1 p$).

$$\begin{aligned} & n = 10m + (1 - 10k)b \ \Rightarrow \ n = 10k_1 p + q_2 pb \\ \Rightarrow \ & n = (10k_1 + q_2 b)p \ \Rightarrow \ n = k_2 p, \quad k_2 \in \mathbb{Z} \end{aligned}.$$

*Logo, p dividirá n.*

*Então, para concluir que um número primo p,* $p \neq 2$ *e* $p \neq 5$ *é um divisor de n se, e somente se, ele for um divisor de m, podemos escolher k de modo que p seja um divisor de* $1 - 10k$ *e este é o segundo da Tabela.*

**Observação 2.26.** *Veremos no capítulo seguinte que também podemos usar a congruência para estabelecer critérios de divisibilidade, de forma muito mais simples.*

# Capítulo 3

# Congruência

O conceito de congruência foi introduzido por Karl Friedrich Gauss (1777 - 1855), em sua obra Disquisitiones arithmeticae, publicada em 1801, quando tinha apenas 24 anos.

A teoria das congruências é, sem dúvida, uma das ferramentas mais poderosas da teoria dos números.

**Definição 3.1.** *Dados três inteiros a, b e m ($m > 0$), dizemos que a é congruente a b módulo m e denotamos $a \equiv b (\mathrm{mod}\ m)$ ou $a \underset{m}{\equiv} b$, se $m \mid (a - b)$. Se a não for congruente a b módulo m, dizemos que a é incongruente a b módulo m e denotamos $a \not\equiv b (mod\, m)$ ou ainda $a \underset{m}{\not\equiv} b$. Neste caso, $m \nmid (a - b)$.*

**Exemplos:**

$10 \equiv 14 (mod\ 2)$, pois $2 \mid (10 - 14)$.

$-32 \equiv 10 (mod\ 7)$, pois $7 \mid (-32 - 10)$.

$8 \not\equiv 5 (mod\ 7)$, pois $7 \nmid (8 - 5)$.

**Proposição 3.1.** *Se a e b são inteiros, temos que $a \equiv b (\mathrm{mod}\, m)$ se, e somente se, existir um inteiro k tal que $a = b + km$.*

**Demonstração**

($\Rightarrow$) Se $a \equiv b (\mathrm{mod}\, m)$, então $m \mid (a - b)$, o que implica que existe $k \in \mathbb{Z};\ (a - b) = k \cdot m$, isto é, $a = b + km$

($\Leftarrow$) Se existe $k \in \mathbb{Z};\ a = b + km$, temos que

$(a - b) = km$, ou seja, $m$ é divisor de $(a - b)$, isto é, $m \mid (a - b)$ e, portanto, $a \equiv b (\mathrm{mod}\, m)$.

**Proposição 3.2.** *Se a, b, c e m são números inteiros, $m > 0$, então, o conjunto*

$$R = \{(a,\ b) \in \mathbb{Z} \times \mathbb{Z} \ / \ a \equiv b (\mathrm{mod}\, m)\}$$

*é uma relação de equivalência sobre o conjunto dos números inteiros.*

**Demonstração**

Para demonstrarmos que um dado conjunto $R$ é uma relação de equivalência em $\mathbb{Z}$, precisamos demonstrar que $R$ satisfaz as propriedades reflexiva, simétrica e transitiva que, no caso em questão, se escreve, respectivamente, da seguinte forma:

**(i)** $a \equiv a (\mathrm{mod}\, m)$.

**(ii)** Se $a \equiv b (\mathrm{mod}\, m)$, então, $b \equiv a (\mathrm{mod}\, m)$.

**(iii)** Se $a \equiv b (\mathrm{mod}\, m)$ e $b \equiv c (\mathrm{mod}\, m)$, então, $a \equiv c (\mathrm{mod}\, m)$.

**Demonstração**

**(i)** $m \mid 0$, então $m \mid (a - a)$, o que implica que $a \equiv a (\mathrm{mod}\, m)$.

**(ii)** Se $a \equiv b (\mathrm{mod}\, m)$, então $m \mid (a - b)$, isto é, existe $q_1 \in \mathbb{Z}$, tal que $a - b = q_1 \cdot m$. Multiplicando-se ambos os membros por $-1$ temos que $b - a = -q_1 \cdot m$, ou seja, $m \mid (b - a)$ e, portanto, $b \equiv a (\mathrm{mod}\, m)$.

**(iii)** Se $a \equiv b (\mathrm{mod}\, m)$ e $b \equiv c (\mathrm{mod}\, m)$, temos que:

$$a - b = m \cdot q_1, \quad q_1 \in \mathbb{Z} \quad (I)$$

$$b - c = m \cdot q_2, \quad q_2 \in \mathbb{Z} \quad (II)$$

Somando-se membro a membro (I) e (II), temos que

$$\begin{aligned} a - c &= m(q_1 + q_2) \quad \text{e como } (q_1 + q_1) \in \mathbb{Z} \\ \Rightarrow \quad a - c &= m \cdot k,\ k \in \mathbb{Z}. \quad \text{Logo, } a \equiv c (\mathrm{mod}\, m), \end{aligned}$$

o que finaliza a demonstração.

**Exemplos:**

- $2 \equiv 2 \pmod 4$, pois $4 \mid (2-2)$.
- $\begin{cases} 15 \equiv 3 \pmod 6, & \text{pois } 6 \mid (15-3) \\ 3 \equiv 15 \pmod 6, & \text{pois } 6 \mid (3-15). \end{cases}$
- $\begin{cases} 20 \equiv 15 \pmod 5 \quad \text{e} \quad 15 \equiv 40 \pmod 5, \text{ logo} \\ 20 \equiv 40 \pmod 5. \end{cases}$

**Teorema 3.1.** *Dois inteiros a e b são congruentes módulo m, ($m > 0$), se, e somente se, a e b deixam o mesmo resto quando divididos por m.*

**Demonstração**

($\Rightarrow$) Suponhamos que $a \equiv b \pmod m$, então $a - b = q_1 \cdot m,\ q_1 \in \mathbb{Z} \Rightarrow a = q_1 m + b$. $(I)$

Seja $r$ o resto da divisão de $b$ por $m$, então, pelo algoritmo da divisão

$$b = m \cdot q_2 + r, \quad 0 \leq r < m \quad \text{e} \quad q_2 \in \mathbb{Z}. \quad (II)$$

Substituindo $(II)$ em $(I)$, temos

$a = q_1 m + q_2 m + r \Rightarrow a = m(q_1 + q_2) + r$, o que significa que $r$ também é o resto da divisão de $a$ por $m$.

($\Leftarrow$) Reciprocamente, suponhamos que $a$ e $b$, quando divididos por $m$, deixam o mesmo resto, isto é,

$$a = q_1 m + r, \quad 0 \leq r < m, \quad q_1 \in \mathbb{Z} \quad (I)$$
$$b = q_2 m + r, \quad 0 \leq r < m, \quad q_2 \in \mathbb{Z}. \quad (II)$$

Subtraindo-se membro a membro $(I)$ e $(II)$, temos

$$\begin{aligned} a - b &= q_1 m + r - q_2 - r \\ \Rightarrow \quad a - b &= (q_1 - q_2)m, \end{aligned}$$

isto é, $m \mid (a - b)$ e, portanto, $a \equiv b \pmod m$, o que finaliza a demonstração.

**Teorema 3.2.** *Sejam a, b, c, d e m números inteiros, temos que:*

$P_1$) Se $a \equiv b \,(\text{mod})\, m$, então $a + c \equiv b + c \,(\text{mod}\, m)$.

**Demonstração**

Como $a \equiv b \,(\text{mod}\, m)$, então $a - b = q_1 m, \quad q_1 \in \mathbb{Z}$ e como $a - b = (a + c) - (b + c)$, então $(a + c) - (b + c) = q_1 m$. Logo, $(a + c) \equiv (b + c) \,(\text{mod}\, m)$.

**Exemplo:** $-31 \equiv 11 \,(\text{mod}\, 6) \Rightarrow -31 + 4 \equiv 11 + 4 \,(\text{mod}\, 6)$ ou $-27 \equiv 15 \,(\text{mod}\, 6)$.

$P_2$) Se $a \equiv b \,(\text{mod}\, m)$, então $a - c \equiv b - c \,(\text{mod}\, m)$.

**Demonstração**

De forma análoga a ($\mathbf{P_1}$), $a-b = (a-c)-(b-c)$. Como $a-b = q_1 m \Rightarrow (a-c)-(b-c) = q_1 m$. Logo, $a - c \equiv b - c \,(\text{mod}\, m)$.

**Exemplo:** $54 \equiv 5 \,(\text{mod}\, 7) \Rightarrow 54 - 8 \equiv 5 - 8 \,(\text{mod}\, 7)$ ou $46 \equiv -3 \,(\text{mod}\, 7)$.

$P_3$) Se $a \equiv b \,(\text{mod}\, m)$, então $ac \equiv bc \,(\text{mod}\, m)$.

**Demonstração**

Como $a - b = q_1 m, \ q_1 \in \mathbb{Z}$, então $ac - bc = cq_1 m$, o que implica que $m \mid (ac - bc)$. Logo, $ac \equiv bc \,(\text{mod}\, m)$.

**Exemplo:** $30 \equiv 8 \,(\text{mod}\, 11) \Rightarrow 30 \cdot 2 \equiv 8 \cdot 2 \,(\text{mod}\, 11)$ ou $60 \equiv 16 \,(\text{mod}\, 11)$, pois $11 \mid (60-16)$.

$P_4$) Se $a \equiv b \,(\text{mod}\, m)$ e $c \equiv d \,(\text{mod}\, m)$, então $a + c \equiv b + d \,(\text{mod}\, m)$.

**Demonstração**

Da hipótese, temos que $a - b = q_1 m, \ q_1 \in \mathbb{Z}$ e $c - d = q_2 m, \ q_2 \in \mathbb{Z}$. Somando-se membro a membro, temos que $a - b + c - d = q_1 m + q_2 m$, o que implica que $(a + c) - (b + d) = (q_1 + q_2)m$, portanto, $m \mid [(a + c) - (b + d)]$ ou $a + c \equiv b + d \,(\text{mod}\, m)$.

**Exemplo:** $45 \equiv 15 \,(\text{mod}\ 10)$ e $30 \equiv 20 \,(\text{mod}\ 10) \Rightarrow 45 + 30 \equiv 15 + 20 \,(\text{mod}\ 10)$ ou $75 \equiv 35 \,(\text{mod}\, 10)$.

$P_5$) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a - c \equiv b - d \pmod{m}$.

**Demonstração**

Da hipótese, $a - b = q_1 m$ e $c - d = q_2 m$, $q_1, q_2 \in \mathbb{Z}$. Subtraindo-se membro a membro, temos $(a - b) - (c - d) = q_1 m - q_2 m \Rightarrow (a - c) - (b - d) = (q_1 - q_2)m$, portanto, $m \mid [(a - c) - (b - d)]$ ou $a - c \equiv b - d \pmod{m}$.

**Exemplo:** $45 \equiv 15 \pmod{10}$ e $30 \equiv 20 \pmod{10}$, logo $45 - 30 \equiv 15 - 20 \pmod{10}$ ou $15 \equiv -5 \pmod{10}$.

$P_6$) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $ac \equiv bd \pmod{m}$.

**Demonstração**

Da hipótese, $a - b = q_1 m$, $q_1 \in \mathbb{Z}$ $(I)$

e

$c - d = q_2 m$, $q_2 \in \mathbb{Z}$. $(II)$

Multiplicando-se ambos os membros de $(I)$ por $c$ e de $(II)$ por $b$, temos

$ac - bc = cq_1 m$ e $bc - bd = bq_2 m$. Somando-se agora membro a membro as duas igualdades, obtemos

$ac - bd = cq_1 m + bq_2 m$ ou $ac - bd = (cq_1 + bq_2)m$. Logo, $m \mid (ac - bd)$ ou $ac \equiv bd \pmod{m}$.

**Exemplo:** $45 \equiv 12 \pmod{3}$ e $28 \equiv 7 \pmod{3} \Rightarrow 45 \cdot 28 \equiv 12 \cdot 7 \pmod{3}$ ou $1260 \equiv 84 \pmod{3}$.

$P_7$) Se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m}$ para todo inteiro positivo $n$.

**Demonstração**

Por indução, temos:

i) p/$n = 1 \Rightarrow a^1 \equiv b^1 \pmod{m}$ ou $a \equiv b \pmod{m}$ (hipótese), portanto, a proposição é verdadeira para $n = 1$.

ii) Vamos supor que a proposição seja verdadeira para $n = k$, isto é, $a^k \equiv b^k \pmod{m}$, devemos provar que a proposição é válida para $n = k + 1$.

Sabemos que $a^k \equiv b^k \pmod{m}$ e $a \equiv b \pmod{m}$, então, por $(\mathbf{P}_6)$ temos que $a^k \cdot a \equiv b^k \cdot b \pmod{m} \Rightarrow a^{k+1} \equiv b^{k+1} \pmod{m}$, isto é, a proposição é verdadeira para o inteiro positivo $k+1$. Logo, podemos afirmar que a proposição é verdadeira para todo inteiro positivo $n$.

**Exemplo:** $-8 \equiv 2 \pmod 5 \Rightarrow (-8)^3 \equiv 2^3 \pmod 5$ ou $-512 \equiv 8 \pmod 5$.

**Teorema 3.3.** *Se $a$, $b$, $c$ e $m$ são inteiros e $ac \equiv bc \pmod{m}$, então, $a \equiv b \left(\mathrm{mod}\ \frac{m}{d}\right)$, onde $d = (c,\ m)$.*

**Demonstração**

Da hipótese, temos $ac - bc = q_1 m$ ou $c(a-b) = q_1 m$. Se dividirmos os dois membros por $d$, teremos

$\left(\frac{c}{d}\right) \cdot (a-b) = q_1 \cdot \left(\frac{m}{d}\right)$, logo $\left(\frac{m}{d}\right) \mid \left(\frac{c}{d}\right) \cdot (a-b)$ e como $\left(\frac{m}{d},\ \frac{c}{d}\right) = 1$, pelo Teorema 3.6, $\left(\frac{m}{d}\right) \mid (a-b)$ o que implica $a \equiv b \left(\mathrm{mod}\ \frac{m}{d}\right)$.

**Corolário 3.1.** *Se $ac \equiv bc \pmod m$ e se $(c,\ m) = 1$, então, $a \equiv b \pmod m$.*

**Demonstração**

Do teorema anterior, se $ac \equiv bc \pmod{m} \Rightarrow a \equiv b \pmod{\frac{m}{d}}$, onde $d = (c,\ m)$, logo, como $d = 1$, temos que $a \equiv b \pmod{\frac{m}{1}}$ ou $a \equiv b \pmod m$.

Este corolário diz que é permitido cancelar fatores de ambos os membros de uma congruência, desde que sejam primos entre si com o módulo.

**Corolário 3.2.** *Se $ac \equiv bc \pmod{m}$, com $m$ primo e se $m$ não divide $c$ ($m \nmid c$), então $a \equiv b \pmod m$.*

**Demonstração**

Com efeito, as condições $m$ não divide $c$ e $m$ é primo, implicam que $(m,\ c) = 1$ e, pelo Corolário anterior, $ac \equiv bc \pmod m$ e $(m,\ c) = 1 \Rightarrow a \equiv b \pmod m$.

**Exemplos:**

- $48 \equiv 12 \pmod{18}$ ou $6 \cdot 8 \equiv 6 \cdot 2 \pmod{18}$ e como $(18,\ 6) = 6$, então, $8 \equiv 2 \pmod{\frac{18}{6}}$ ou $8 \equiv 2 \pmod 3$ (Teorema 3.3).

- $-45 \equiv 35 \pmod 8$ ou $5 \cdot (-9) \equiv 5 \cdot 7 \pmod 8$ e como $(5,\ 8) = 1$, temos pelo Corolário 3.1 que $-9 \equiv 7 \pmod 8$.

**Observação 3.1.** *Temos que ter bastante cuidado para fazer o cancelamento de um número de ambos os lado de uma congruência, isto é,*

$ac \equiv bc \pmod m \Rightarrow a \equiv b \pmod m$ *só será verdade se* $(c,\ m) = 1$.

**Exemplo:** $44 \equiv 60 \pmod 8$ ou $4 \cdot 11 \equiv 4 \cdot 15 \pmod 8$. Neste caso, não podemos cancelar o fator 4, pois $(4,\ 8) = 4 \neq 1$. De fato, $11 \not\equiv 15 \pmod 8$.

**Teorema 3.4.** *Se* $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$*, onde* $a$, $b$, $m_1$, $m_2, \ldots, m_k$ *são inteiros com* $m_i$ *positivos,* $i = 1, 2, \ldots, k$*, então* $a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}$ *onde* $[m_1, m_2, \ldots, m_k]$ *é o Mínimo Múltiplo Comum.*

**Demonstração**

Seja $P_n$ o maior primo que aparece nas fatorações de $m_1, m_2, \ldots, m_k$. Cada $m_i,\ i = 1, 2, \ldots, k$, pode então ser expresso como $m_i = P_1^{\alpha_{1i}} \cdot P_2^{\alpha_{2i}} \cdot \ldots P_n^{\alpha_{ni}}$ (alguns $\alpha_{ji}$ podem ser nulos).

Como $m_i \mid (a - b),\ \ i = 1, 2, \ldots, k$, temos que $p_j^{\alpha_{ji}} \mid (a - b),\ \ i = 1, 2, \ldots, k$ e $j = 1, 2, \ldots, n$. Logo, se tomarmos $\alpha_j = \max\{\alpha_{ji}\}$ temos que $P_1^{\alpha_{1i}} \cdot P_2^{\alpha_{2i}} \cdot \ldots P_n^{\alpha_{ni}} \mid (a - b)$, mas, $P_1^{\alpha_{1i}} \cdot P_2^{\alpha_{2i}} \cdot \ldots P_n^{\alpha_{ni}} = [m_1, m_2, \ldots, m_k]$ o que implica

$$a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}.$$

**Exemplo:**

$$\left.\begin{array}{c} 70 \equiv 30 \pmod 8 \\ 70 \equiv 30 \pmod 5 \\ 70 \equiv 30 \pmod{10} \\ 70 \equiv 30 \pmod{20} \end{array}\right\} \Rightarrow 70 \equiv 30 \pmod{[8,\ 5,\ 10,\ 20]} \text{ ou } 70 \equiv 30 \pmod{40}.$$

**Teorema 3.5.** *Se* $a \equiv b \pmod m$ *e se* $P(x) = \sum_{i=0}^{n} c_i x^i = c_0 + c_1 x + c_2 x^2 + \ldots + c_n x^n$ *é um polinômio em* $x$ *com coeficientes inteiros* $c_i$*, então*

$$P(a) \equiv P(b) \pmod m.$$

**Demonstração**

Pela hipótese, temos $a \equiv b \,(\text{mod } m)$ e por $(\mathbf{P}_7)$ $a^i \equiv b^i \,(\text{mod } m)$, para $i = 0, 1, 2, \ldots, n$, o que implica por $(\mathbf{P}_3)$ $c_i \cdot a^i \equiv c_i \cdot b^i \,(\text{mod } m)$, para $i = 0, 1, 2, \ldots, n$.

Somando-se ordenadamente as $n + 1$ congruências, obtemos

$$\sum_{i=0}^{n} c_i a^i \equiv \sum_{i=0}^{n} c_i b^i \,(\text{mod } m),$$

ou seja,

$$P(a) \equiv P(b) \,(\text{mod } m).$$

**Exemplo:**

Seja $P(x) = 2x^3 - 5x^2 + 2x - 1$.

- $5 \equiv -3 \,(\text{mod } 4)$
- $P(5) = 2 \cdot 5^3 - 5 \cdot 5^2 + 2 \cdot 5 - 1 = 250 - 125 + 10 - 1 \Rightarrow P(5) = 134$
- $P(-3) = 2 \cdot (-3)^3 - 5 \cdot (-3)^2 + 2 \cdot (-3) - 1 = -54 - 45 - 6 - 1 \Rightarrow P(-3) = -106$
- $P(5) \equiv P(-3) \,(\text{mod } 4)$ ou $134 \equiv -106 \,(\text{mod } 4)$.

**Definição 3.2.** *Se $h$ e $k$ são dois inteiros com $h \equiv k \,(\text{mod } m)$, dizemos que $k$ é um resíduo de $h$ módulo $m$.*

**Definição 3.3.** *Chama-se sistema completo de resíduos (resto) módulo $m$ todo conjunto $S = \{r_1, r_2, \ldots, r_m\}$ de $m$ inteiros tal que um inteiro qualquer $a$ e congruente módulo $m$ a um único elemento $r_i \,(1 \leq i \leq m)$ de $S$.*

**Teorema 3.6.** *O conjunto $S = \{0,\ 1,\ 2, \ldots,\ m - 1\}$ é um sistema completo de resíduos módulo $m$.*

**Demonstração**

Com efeito, o conjunto $S$ tem $m$ elementos e, além disso, qualquer que seja o inteiro $a$ temos, pelo algoritmo da divisão,

$$a = mq + r,\ q \in \mathbb{Z} \quad \text{e} \quad 0 \leq r < m,$$

o que implica que $a \equiv r \,(\text{mod } m)$, e como $r$ só pode assumir os $m$ valores $0, 1, 2, \ldots, m - 1$, segue-se que o inteiro $a$ é congruente módulo $m$ a um único elemento do conjunto $S$, e por conseguinte, esse conjunto é um sistema completo de restos módulo $m$.

**Exemplo:** O conjunto $S = \{0, 1, 2, 3, 4, 5, 6\}$ é um sistema completo de resíduos módulo 7.

**Teorema 3.7.** *Se* $S = \{r_1, r_2, \ldots, r_m\}$ *é um sistema completo de resto módulo m, então, os elementos de* $S$ *são congruentes módulo m aos inteiros* $0, 1, 2, \ldots, m-1$*, numa certa ordem.*

**Demonstração**

Com efeito, qualquer que seja o inteiro $a$, temos

$$a \equiv r_i \,(\text{mod } m), \quad \text{com } r_i \in S \quad \text{e} \quad a \equiv k \,(\text{mod } m), \text{com } 0 \leq k \leq m-1.$$

Logo, pela propriedade transitiva da "congruência" módulo $m$, temos $r_i \equiv k \,(\text{mod } m)$.

**Exemplo:** $S = \{-28, -15, -6, 11, 15, 22, 101, 800\}$ é um sistema completo de resíduo módulo 8. Assim, temos

$$\begin{array}{ll} -28 \equiv 4 \,(\text{mod } 8) & 15 \equiv 7 \,(\text{mod } 8) \\ -15 \equiv 1 \,(\text{mod } 8) & 22 \equiv 6 \,(\text{mod } 8) \\ -6 \equiv 2 \,(\text{mod } 8) & 101 \equiv 5 \,(\text{mod } 8) \\ 11 \equiv 3 \,(\text{mod } 8) & 800 \equiv 0 \,(\text{mod } 8), \end{array}$$

isto é, os elementos de $S$ são congruentes módulo 8 aos inteiros 4, 1, 2, 3, 7, 6, 5, 0.

**Teorema 3.8.** *Um conjunto* $S = \{a_1, a_2, \ldots, a_m\}$ *de m inteiro é um sistema completo de resíduos módulo m se, e somente se, dois elementos quaisquer de* $S$ *são incongruentes módulo m.*

**Demonstração**

($\Rightarrow$) Suponhamos que o conjunto $S$ é um sistema completo de resíduos. Então, se dois elementos distintos de $S$ $a_i$ e $a_j$ fossem congruentes módulo $m$, teríamos

$a \equiv a_i \,(\text{mod } m)$ e $a \equiv a_j \,(\text{mod } m)$, sendo $a$ um inteiro, o que é impossível (definição 3.3). Logo, dois elementos distintos quaisquer do conjunto $S$ são incongruentes módulo $m$.

($\Leftarrow$) Reciprocamente, suponhamos que dois elementos distintos quaisquer do conjunto $S$ são incongruentes módulo $m$. Então, um inteiro qualquer "$a$" é necessariamente congruente módulo $m$ a um único elemento de $S$ e pela definição 3.3, o conjunto $S$ é um sistema completo de resíduos módulo $m$.

**Exemplos:** O conjunto $S = \{26,\ -33,\ 13,\ -11,\ -15\}$ é um sistema completo de resíduo módulo 5 porque contém 5 elementos e dois quaisquer deles são incongruentes módulo 5.

O conjunto $S = \{-5,\ 0,\ 6,\ 22\}$ não é um sistema completo de resíduo módulos 4, porque os elementos 6 e 22 são congruentes módulo 4.

$$6 \equiv 22 \,(\text{mod } 4) \quad \text{ou} \quad 4 \mid (6 - 22).$$

## 3.1 Determinação de resto com uso de congruência

Uma das grandes utilidades da teoria das congruências módulo $m$ é calcular restos de uma divisão onde o dividendo é um número muito grande.

**Exemplo:** Calcule o resto da divisão de $2364^{638564}$ por 7.

**Solução:**

O que queremos achar é um inteiro $r$ $(0 \leq r < 7)$ satisfazendo $2364^{638564} \equiv r \,(\text{mod } 7)$. Então, temos que 2364 quando dividido por 7 deixa resto 5 e, portanto,

$$\begin{aligned}
& 2364 \equiv 5 \,(\text{mod } 7) \\
\Rightarrow \quad & 2364^2 \equiv 5^2 \,(\text{mod } 7) \\
\Rightarrow \quad & 2364^2 \equiv 25 \,(\text{mod } 7) \quad e \quad 25 \equiv 4 \,(\text{mod } 7) \\
\Rightarrow \quad & 2364^2 \equiv 4 \,(\text{mod } 7) \quad (*)
\end{aligned}$$

$$\left.\begin{array}{l} 2364 \equiv 5 \,(\text{mod } 7) \\ 2364^2 \equiv 4 \,(\text{mod } 7) \end{array}\right\} \Rightarrow 2364^3 \equiv 20 \,(\text{mod } 7) \text{ e } 20 \equiv 6 \,(\text{mod } 7) \Rightarrow 2364^3 \equiv 6 \,(\text{mod } 7)$$

$$\left.\begin{array}{l} 2364 \equiv 5 \,(\text{mod } 7) \\ 2364^3 \equiv 6 \,(\text{mod } 7) \end{array}\right\} \Rightarrow 2364^4 \equiv 30 \,(\text{mod } 7) \text{ e } 30 \equiv 2 \,(\text{mod } 7) \Rightarrow 2364^4 \equiv 2 \,(\text{mod } 7)$$

$$\left.\begin{array}{l} 2364 \equiv 5 \,(\text{mod } 7) \\ 2364^4 \equiv 2 \,(\text{mod } 7) \end{array}\right\} \Rightarrow 2364^5 \equiv 10 \,(\text{mod } 7) \text{ e } 10 \equiv 3 \,(\text{mod } 7) \Rightarrow 2364^5 \equiv 3 \,(\text{mod } 7)$$

$$\left.\begin{array}{l} 2364 \equiv 5 \,(\text{mod } 7) \\ 2364^5 \equiv 3 \,(\text{mod } 7) \end{array}\right\} \Rightarrow 2364^6 \equiv 15 \,(\text{mod } 7) \text{ e } 15 \equiv 1 \,(\text{mod } 7) \Rightarrow 2364^6 \equiv 1 \,(\text{mod } 7).$$

Se escrevermos $638564 = 6q + r$, temos que

$$2364^{638564} = 2364^{6q+r} = 2364^{6q} \cdot 2364^{r} \Rightarrow 2364^{638564} = (2364^{6})^{q} \cdot 2364^{r}$$

- $2364^{6} \equiv 1 \pmod 7 \Rightarrow (2364^{6})^{q} \equiv 1^{q} \pmod 7$

$\Rightarrow (2364^{6})^{q} \cdot 2364^{r} \equiv 2364^{r} \pmod 7$

$\Rightarrow 2364^{638564} \equiv 2364^{r} \pmod 7$

e como $638564 = 6m + 2$, temos $2364^{638564} \equiv 2364^{2} \pmod 7$ e em $(*)$ vimos que $2364^{2} \equiv 4 \pmod 7$, temos que $2364^{638564} \equiv 4 \pmod 7$ e, portanto, o resto da divisão de $2364^{638564}$ por 7 é igual a 4.

**Exemplo:** Calcular o resto da divisão de $7^{34}$ por 51 e o resto da divisão de $5^{63}$ por 29.

(I) Resto da divisão de $7^{34}$ por 51

$$\begin{aligned} & 49 \equiv -2 \pmod{51} \Rightarrow 7^{2} \equiv -2 \pmod{51} \\ \Rightarrow \quad & (7^{2})^{17} \equiv (-2)^{17} \pmod{51} \Rightarrow 7^{34} \equiv (-2)^{17} \pmod{51}. \quad (*) \end{aligned}$$

Sabemos ainda que

$$\begin{aligned} & (-2)^{8} \equiv 1 \pmod{51} \Rightarrow [(-2)^{8}]^{2} \equiv 1^{2} \pmod{51} \\ \Rightarrow \quad & (-2)^{16} \equiv 1 \pmod{51} \Rightarrow (-2)^{16} \cdot (-2) \equiv (-2)1 \pmod{51} \\ \Rightarrow \quad & (-2)^{17} \equiv -2 \pmod{51}. \quad (**) \end{aligned}$$

De $(*)$ e $(**)$, temos que

$$\begin{aligned} & 7^{34} \equiv -2 \pmod{51} \Rightarrow 7^{34} + 2 = 51q, \quad q \in \mathbb{Z} \\ \Rightarrow \quad & 7^{34} = 51q - 2 \Rightarrow 7^{34} = 51q - 2 - 49 + 49 \\ \Rightarrow \quad & 7^{34} = 51(q-1) + 49 \text{ e como } (q-1) \in \mathbb{Z} \\ \Rightarrow \quad & 7^{34} = 51k + 49, \quad k \in \mathbb{Z}, \end{aligned}$$

portanto, o resto da divisão de $7^{34}$ por 51 é 49.

(II) Resto da divisão de $5^{63}$ por 29

- $5^{3} \equiv 9 \pmod{29} \Rightarrow (5^{3})^{21} \equiv (3^{2})^{21} \pmod{29} \Rightarrow 5^{63} \equiv 3^{42} \pmod{29} \quad (*)$

- $3^{3} \equiv -2 \pmod{29} \Rightarrow (3^{3})^{14} \equiv (-2)^{14} \pmod{29} \Rightarrow 3^{42} \equiv (-2)^{14} \pmod{29} \quad (**)$

- $(-2)^5 \equiv -3 \pmod{29} \Rightarrow [(-2)^5]^2 \equiv (-3)^2 \pmod{29}$
  $(-2)^{10} \equiv 9 \pmod{29} \Rightarrow (-2)^{10} \cdot (-2)^4 \equiv 9 \cdot (-2)^4 \pmod{29}$
  $\Rightarrow (-2)^{14} \equiv 9(-2)^4 \pmod{29}. \quad (***)$

De $(**)$ e $(***) \Rightarrow 3^{42} \equiv 9 \cdot (-2)^4 \pmod{29}$ ou $3^{42} \equiv 144 \pmod{29}$ e como $5^{63} \equiv 144 \pmod{29}$, isto é,

$$\begin{aligned} & 5^{63} = 29q + 144 && q \in \mathbb{Z} \\ \Rightarrow \quad & 5^{63} = 29q + 4 \cdot 29 + 28 \\ \Rightarrow \quad & 5^{63} = 29(q+4) + 28 \\ \Rightarrow \quad & 5^{63} = 29k + 28 && k \in \mathbb{Z} \end{aligned}$$

e, portanto, o resto da divisão de $5^{63}$ por 29 é 28.

## 3.2 Critérios de divisibilidade

Já vimos alguns critérios de divisibilidade no capítulo 2 e apresentaremos alguns destes critérios utilizando a congruência.

### 3.2.1 Critério de divisibilidade por 3

Seja $a = a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_1 10 + a_0$, com $0 \leq a_i < 10$, a representação no sistema decimal do inteiro $a$ e seja $S_n$ a soma dos seus algarismos, isto é, $S_n = a_0 + a_1 + \ldots + a_{n-1} + a_n$. Então, $a$ é divisível por 3 se, e somente se, $S_n$ é divisível por 3.

**Demonstração**

Considere o polinômio de coeficientes inteiros

$$P(x) = \sum_{i=0}^{n} a_i x^i.$$

Observa-se que $P(10) = a$ e $P(1) = S_n$.

Sabe-se que $10 \equiv 1 \pmod{3}$ e pelo Teorema 3.5 temos que $P(10) \equiv P(1) \pmod{3}$, logo, $a \equiv S_n \pmod{3}$ e, portanto,

$$a = 3q + S_n.$$

Então, concluímos que $a$ é múltiplo de 3 se, e somente se, $S_n$ é múltiplo de 3.

($\Rightarrow$) Se $a$ é múltiplo de 3, $a = 3q_1$, $q_1 \in \mathbb{Z}$ e então $3q_1 = 3q + S_n$ $\Rightarrow S_n = 3(q_1 - q)$. Portanto, $S_n$ é múltiplo de 3.

($\Leftarrow$) Se $S_n$ é múltiplo de 3 $\Rightarrow S_n = 3k$, $k \in \mathbb{Z}$ o que implica $a = 3q + 3k \Rightarrow a = 3(q + k)$. Logo, $a$ é múltiplo de 3.

**Exemplo:** 235671 é múltiplo de 3, pois 2+3+5+6+7+1=24 e 3 | 24.

### 3.2.2 Critério de divisibilidade por 8

Seja $a = a_n 10^n + a_{n-1}10^{n-1} + \ldots + a_2 10^2 + a_1 10 + a_0$, $0 \leq a_i < 10$, a representação no sistema decimal do inteiro positivo $a$. Temos:

i) $10 \equiv 2 \,(\text{mod } 8) \Rightarrow 10a_1 \equiv 2a_1 \,(\text{mod } 8)$.

ii) $10 \equiv 2 \,(\text{mod } 8) \Rightarrow 10^2 \equiv 4 \,(\text{mod } 8) \Rightarrow 10^2 a_2 \equiv 4a_2 \,(\text{mod } 8)$.

iii) $a_i 10^i \equiv 0 \,(\text{mod } 8)$, $\quad i \geq 3 \Rightarrow a_i 10^i + a_0 \equiv 0 + a_0 \,(\text{mod } 8) \Rightarrow a_i 10^i + a_0 \equiv a_0 \,(\text{mod } 8)$.

De (i), (ii) e (iii), tem-se

$(10a_1 + 10^2 a_2 + 10^i a_i + a_0) \equiv 2a_1 + 4a_2 + a_0 \,(\text{mod } 8) \Rightarrow a \equiv 2a_1 + 4a_2 + a_0 \,(\text{mod } 8)$

$\Rightarrow a \equiv 8q + 4a_2 + 2a_1 + a_0 \,(\text{mod } 8)$ e, para mantermos a mesma regra do capítulo 2, temos:

$$\begin{aligned} & a = 8q + 4a_2 + 96a_2 - 96a_2 + 2a_1 + 8a_1 - 8a_1 + a_0 \\ \Rightarrow \quad & a = 8q - 96a_2 - 8a_1 + 100a_2 + 10a_1 + a_0 \\ \Rightarrow \quad & a = 8(q - 12a_2 - a_1) + 100a_2 + 10a_1 + a_0 \\ \Rightarrow \quad & a = 8k + 100a_2 + 10a_1 + a_0, \end{aligned}$$

isto é,

$a$ é múltiplo de 8 se, e somente se, o número formado pelos três últimos algarismos de $a$ é múltiplo de 8, isto é, $8 \mid a_2 a_1 a_0$.

($\Rightarrow$) Se $a$ é múltiplo de 8, então $a = 8q_1$, $\quad q_1 \in \mathbb{Z}$ e daí $8q_1 = 8k + 100a_2 + 10a_1 + a_0$, logo $100a_2 + 10a_1 + a_0 = 8(q_1 - k)$. Portanto, o número $a_2 a_1 a_0 = 100a_2 + 10a_1 + a_0$ é múltiplo de 8.

($\Leftarrow$) Se $100a_2 + 10a_1 + a_0$ é múltiplo de 8, temos $100a_2 + 10a_1 + a_0 = 8q_2$, $q_2 \in \mathbb{Z}$, então $a = 8k + 8q_2$, logo $a = 8(k + q_2)$. Portanto, $a$ é múltiplo de 8.

**Exemplo:** 4329184 é múltiplo de 8, pois 184 é múltiplo de 8.

### 3.2.3 Critério de divisibilidade por 11

Seja $a = a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_2 10^2 + a_1 10 + a_0$, $0 \leq a_i < 10$, a representação no sistema decimal do inteiro positivo $a$ e seja

$$S_n = a_0 - a_1 + a_2 - \ldots + (-1)^n \cdot a_n,$$

então, $a$ é divisível por 11 se, e somente se, $S_n$ é divisível por 11.

**Demonstração**

Considere o polinômio com coeficientes inteiros

$$P(x) = \sum_{i=0}^{n} a_i x^i.$$

Observa-se que $P(10) = a$ e $P(-1) = S_n$.

Sabe-se que $10 \equiv (-1) \pmod{11}$ e, portanto, $P(10) \equiv P(-1) \pmod{11}$, (Teorema 3.5), o que implica em $a \equiv S_n \pmod{11}$ e, portanto, $a = 11q + S_n,\ q \in \mathbb{Z}$. Daí, concluímos que $a$ é múltiplo de 11 se, e somente se, $S_n$ é múltiplo de 11.

($\Rightarrow$) Se $a$ é múltiplo de 11 $\Rightarrow a = 11q_1,\ q_1 \in \mathbb{Z} \Rightarrow 11q_1 = 11q + S_n \Rightarrow S_n = 11(q_1 - q)$. Logo, $S_n$ é múltiplo de 11.

($\Leftarrow$) Se $S_n$ é múltiplo de 11, então $S_n = 11k,\ k \in \mathbb{Z}$, logo $a = 11q + S_n = 11q + 11k \Rightarrow a = 11(q + k)$. Logo $a$ é múltiplo de 11.

## 3.3 Congruência linear

Chama-se congruência linear em uma variável a toda congruência (equação) da forma

$$ax \equiv b \pmod{m}, \qquad (I)$$

onde $a$ e $b$ são inteiros, $m$ um inteiro positivo e $x$ é uma incógnita.

Diz-se que um número inteiro $x_0$ é solução da equação $(I)$ se

$$ax_0 \equiv b \pmod{m}$$

e, portanto, $m \mid (ax_0 - b)$, isto é, existe $y_0 \in \mathbb{Z}$ tal que $ax_0 - b = y_0 \cdot m$, de modo que o problema de achar todos os inteiros que satisfazem a congruência $(I)$, reduz-se a obter todas as soluções da equação diofantina linear $ax - my = b$.

Toda equação da forma $ax + by = c$, onde $a$, $b$ e $c$ são inteiros é chamada equação diofantina linear (nome dado em referência a Diofanto de Alexandria).

É importante observar que, se $x_0$ é uma solução da congruência linear $(I)$, então todos os inteiros da forma $x_0 + km$, onde $k$ é um inteiro qualquer, também são soluções da congruência linear $(I)$, pois

$$a(x_0 + km) \equiv ax_0 \equiv b \,(\text{mod } m).$$

**Exemplo:** Considere a congruência linear $5x \equiv 6 \,(\text{mod } 9)$.

Observe que $x_0 = 3$ é solução pois $5 \cdot 3 \equiv 6 \,(\text{mod } 9)$ e, portanto, todo inteiro sob a forma $x_0 + km,\ k \in \mathbb{Z}$, isto é, $3 + k \cdot 9$ é também solução. Vejamos:

- $x_1 = 3 + 1 \cdot 9 = 12$ é solução, pois

$$5 \cdot 12 \equiv 6 \,(\text{mod } 9) \quad \text{ou} \quad 60 \equiv 6 \,(\text{mod } 9).$$

- $x_2 = 3 - 1 \cdot 9 = -6$ é solução, pois

$$5 \cdot (-6) \equiv 6 \,(\text{mod } 9) \quad \text{ou} \quad -30 \equiv 6 \,(\text{mod } 9).$$

- $x_3 = 3 + 2 \cdot 9 = 21$ é solução, pois

$$5 \cdot 21 \equiv 6 \,(\text{mod } 9) \quad \text{ou} \quad 105 \equiv 6 \,(\text{mod } 9).$$

Assim, os inteiros $\ldots, -15,\ -6,\ 3,\ 12,\ 21,\ 30,\ 39,\ \ldots$ são todos soluções da congruência linear.

Observando o exemplo anterior, conclui-se que para cada solução particular podemos encontrar uma infinidade de soluções, todas mutuamente congruentes módulo $m$. Porém, estas soluções encontradas a partir da solução particular, isto é, $x_0 \equiv x_1 \equiv x_2 \ldots \equiv x_n \,(\text{mod } m)$, não são consideradas soluções distintas da congruência linear $ax \equiv b \,(\text{mod } m)$, isto é, só são consideradas soluções distintas de $(I)$ aquelas que são mutuamente incongruentes módulo $m$ e a satisfazem e, portanto, o número de soluções da congruência linear $ax \equiv b \,(\text{mod } m)$ é dado pelo número de soluções mutuamente incongruentes módulo $m$ que a satisfazem.

**Teorema 3.9.** *Sejam $a$, $b$ e $c$ inteiros e $d = (a, b)$. Se $d \nmid c$, então a equação $ax + by = c$ não possui nenhuma solução inteira. Se $d \mid c$ ela possui infinitas soluções e se $x = x_0$ e $y = y_0$ é uma solução particular, então, todas as soluções são dadas por:*

$$x = x_0 + \left(\frac{b}{d}\right) \cdot k$$

$$x = x_0 + \left(\frac{a}{d}\right) \cdot k,$$

*onde $k$ é um número inteiro.*

**Demonstração**

i) Se $d \nmid c$, então a equação $ax + by = c$ não possui solução inteira pois, como $d \mid a$ e $d \mid b$, $d$ deveria dividir $c$, pois $c$ é uma combinação linear de $a$ e $b$ (Teorema 3.1, item X).

ii) Suponhamos agora que $d \mid c$. Pelo Teorema 3.1 item X, existem inteiros $n_0$ e $m_0$, tais que

$$an_0 + bm_0 = d, \qquad (I)$$

Como $d \mid c$, existe um inteiro $k$ tal que $c = kd$. Se multiplicarmos ambos os membros de $(I)$ por $k$, teremos

$$an_0k + bm_0k = dk.$$

Então,

$$a(n_0k) + b(m_0k) = c.$$

Isto nos diz que o par $(x_0, y_0)$, com $x_0 = n_0k$ e $y_0 = m_0k$ é uma solução de $ax + by = c$.

iii) Vamos provar agora que conhecida uma solução particular $(x_0, y_0)$, podemos, a partir dela, gerar uma infinidade de soluções. Fazendo

$$x = x_0 + \left(\frac{b}{d}\right)k \quad \text{e} \quad y = y_0 - \left(\frac{a}{d}\right)k,$$

temos

$$\begin{aligned} ax + by &= a\left(x_0 + \frac{b}{d}k\right) + b\left(y_0 - \frac{a}{d}k\right) \\ &= ax_0 + \frac{abk}{d} + by_0 - \frac{abk}{d} \\ &= ax_0 + by_0 = c. \end{aligned}$$

Portanto, se $(x_0,\ y_0)$ é solução, então todo par $\left(x_0 + \frac{b}{d}k,\ y_0 - \frac{a}{d}k\right)$ também é solução, sendo $k \in \mathbb{Z}$.

iv) Vamos mostrar que toda solução da equação $ax + by = c$ é da forma

$$x = x_0 + \frac{b}{d}k,\ y = y_0 - \frac{a}{d}k.$$

Vamos supor que $(x,\ y)$ seja uma solução inteira da equação, isto é, $ax + by = c$. Mas como $ax_0 + by_0 = c$, obtemos subtraindo membro a membro, que

$$ax + by - ax_0 - by_0 = 0.$$

Então,

$$a(x - x_0) + b(y - y_0) = 0,$$

o que implica

$$a(x - x_0) = -b(y - y_0),$$

isto é,

$$a(x - x_0) = b(y_0 - y).$$

Como $d = (a,\ b)$, temos pelo Corolário 3.2, que

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

Portanto, dividindo os dois membros da igualdade por $d$, teremos

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y). \qquad (II)$$

Logo, pelo Teorema 3.6, $\left(\frac{b}{d}\right) \mid (x - x_0)$ e, portanto, existe um inteiro $k$ satisfazendo $x - x_0 = k \cdot \left(\frac{b}{d}\right)$ ou $x = x_0 + k \cdot \left(\frac{b}{d}\right)$.

Substituindo em $(II)$, temos que

$$\frac{a}{d}\left[x_0 + \frac{kb}{d} - x_0\right] = \frac{b}{d}(y_0 - y) \Rightarrow \frac{akb}{d^2} = \frac{by_0}{d} - \frac{b}{d}y \Rightarrow \frac{by}{d} = \left(\frac{b}{d}\right)y_0 - \left(\frac{b}{d}\right) \cdot \left(\frac{a}{d}\right)k.$$

Dividindo os dois membros por $\frac{b}{d}$, obtemos

$$y = y_0 - k \cdot \left(\frac{a}{d}\right),$$

o que conclui a demonstração.

**Exemplos:** Achar as soluções inteiras das equações.

a) $4x + 6y = 15$.

$(4,\ 6) = 2$ e como $2 \not| 15$, então, pelo Teorema anterior, temos que a equação não possui soluções inteiras.

b) $6x + 15y = 12$.

$(6, 15) = 3$ e como $3 \mid 12$, temos uma infinidade de soluções.

Para encontrarmos uma solução particular, usamos o algoritmo de Euclides da seguinte forma:

$$15 = 6 \cdot 2 + 3 \Rightarrow 6(-2) + 15 \cdot 1 = 3.$$

Multiplicando-se por 4 os dois membros da igualdade temos $6 \cdot (-8) + 15 \cdot 4 = 12$. Portanto, uma solução é o par $(-8,\ 4)$ e daí podemos achar outras soluções sabendo que

$$x = x_0 + \left(\frac{b}{d}\right)k \quad \text{e} \quad y = y_0 - \left(\frac{a}{d}\right)k.$$

Então,

$$x = -8 + \left(\frac{15}{3}\right)k \Rightarrow x = -8 + 5k$$

e

$$y = 4 - \left(\frac{6}{3}\right)k \Leftarrow y = 4 - 2k.$$

$p/k = 1 \Rightarrow x = -3$ e $y = 2 \Rightarrow (-3,\ 2)$ é solução.

$p/k = -1 \Rightarrow x = -13$ e $y = 6 \Rightarrow (-13,\ 6)$ é solução.

$p/k = 2 \Rightarrow x = 2$ e $y = 0 \Rightarrow (2,\ 0)$ é solução.

$p/k = -2 \Rightarrow x = -18$ e $y = 8 \Rightarrow (-18,\ 8)$ é solução.

$\vdots$

**Teorema 3.10.** *Sejam $a$, $b$ e $m$ inteiros tais que $m > 0$ e $(a,\ m) = d$. No caso em que $d \nmid b$ a congruência linear $ax \equiv b \pmod{m}$ não possui nenhuma solução e quando $d \mid b$, possui exatamente $d$ soluções incongruentes módulo $m$.*

**Demonstração**

Pela Proposição 3.1, o inteiro $x$ é solução de $ax \equiv b \pmod{m}$ se, e somente se, existe um inteiro $y$ tal que $ax = b + my$, ou equivalentemente, $ax - my = b$. Do Teorema 3.9, sabemos que

esta equação não possui nenhuma solução inteira caso $d \nmid b$ , e que se $d \mid b$ ela possui infinitas soluções inteiras dadas por

$$x = x_0 - \left(\frac{m}{d}\right)k \quad \text{e} \quad y = y_0 - \left(\frac{a}{d}\right)k,$$

onde $k \in \mathbb{Z}$ e $(x_0,\ y_0)$ é uma solução particular de $ax - my = b$. Logo, a congruência $ax \equiv b \pmod{m}$ possui infinitas soluções dadas por $x = x_0 - \left(\frac{m}{d}\right)k$. Como estamos interessados em saber o número de soluções incongruentes, vamos tentar descobrir sob que condições

$$x_1 = x_0 - \left(\frac{m}{d}\right)k_1 \quad \text{e} \quad x_2 = x_0 - \left(\frac{m}{d}\right)k_2$$

são congruentes módulo $m$.

Se $x_1$ e $x_2$ são congruentes módulos $m$, então

$$x_0 - \left(\frac{m}{d}\right)k_1 \equiv x_0 - \left(\frac{m}{d}\right)k_2 \pmod{m}.$$

Isto implica

$$\left(\frac{m}{d}\right)k_1 \equiv \left(\frac{m}{d}\right)k_2 \pmod{m}$$

e como $\left(\frac{m}{d}\right) \mid m$, temos $\left(\frac{m}{d},\ m\right) = \frac{m}{d}$, o que nos permite o cancelamento de $\frac{m}{d}$, resultando pelo Teorema 3.3, $k_1 \equiv k_2 \left(\mod \frac{m}{\frac{m}{d}}\right)$, isto é, $k_1 \equiv k_2 \pmod{d}$. Isto nos mostra que soluções incongruentes serão obtidas ao tomarmos $x = x_0 - \left(\frac{m}{d}\right)k$, onde $k$ percorre um sistema completo de resíduos módulo $d$, o que conclui a demonstração.

**Exemplo:** Resolver a congruência linear $12x \equiv 30 \pmod{18}$.

Como $(12,\ 18) = 6$ e como $6 \mid 30$, a congruência linear dada possui exatamente 6 soluções mutuamente incongruentes módulo 18. Achar as soluções da congruência é o mesmo que achar as soluções inteiras da equação

$$12x - 30 = 18y \quad \text{ou} \quad 12x - 18y = 30.$$

Como $(12,\ 18) = 6$ e $6 \mid 30$, temos pelo algoritmo da divisão

$$18 = 1 \cdot 12 + 6 \Rightarrow -1 \cdot 12 + 1 \cdot 18 = 6.$$

Multiplicando ambos os membros por 5, obtemos

$$-5 \cdot 12 + 5 \cdot 18 = 30 \Rightarrow 12 \cdot (-5) - 18 \cdot (-5) = 30.$$

Portanto, $(-5,\ -5)$ é solução da equação diofantina $12x - 18y = 30$ e daí temos que $x_0 = -5$ é uma solução particular da congruência linear $12x \equiv 30 \pmod{18}$. Logo, as seis soluções mutuamente incongruentes módulo 18, são dadas por

$$x = x_0 + \left(\frac{m}{d}\right)k.$$

$x = -5\left(\frac{18}{6}\right)k \Rightarrow x = -5 - 3k$, onde $k \in \{0,\ 1,\ 2,\ 3,\ 4,\ 5\}$

$p/k = 0 \quad \Rightarrow \quad x_0 = -5 - 3 \cdot 0 \quad \Rightarrow \quad x_0 = -5$

$p/k = 1 \quad \Rightarrow \quad x_1 = -5 - 3 \cdot 1 \quad \Rightarrow \quad x_0 = -8$

$p/k = 2 \quad \Rightarrow \quad x_2 = -5 - 3 \cdot 2 \quad \Rightarrow \quad x_0 = -11$

$p/k = 3 \quad \Rightarrow \quad x_3 = -5 - 3 \cdot 3 \quad \Rightarrow \quad x_0 = -14$

$p/k = 4 \quad \Rightarrow \quad x_4 = -5 - 3 \cdot 4 \quad \Rightarrow \quad x_0 = -17$

$p/k = 5 \quad \Rightarrow \quad x_5 = -5 - 3 \cdot 5 \quad \Rightarrow \quad x_0 = -20.$

**Definição 3.4.** *Dizemos que uma solução $x_0$ de $ax \equiv b \pmod{m}$ é única módulo m quando qualquer outra solução $x_1$ for congruente a $x_0$ módulo m.*

**Definição 3.5.** *Uma solução $\bar{a}$ de $ax \equiv 1 \pmod{m}$ é chamada de um inverso de a módulo m.*

**Exemplo:** Achar o inverso de 2 módulo 5.

$2x \equiv 1 \pmod{5} \Rightarrow x = 3$, portanto, 3 é o inverso de 2 módulo 5.

**Teorema 3.11.** *Se $(a,\ m) = 1$, então a tem um único inverso módulo m.*

**Demonstração**

Com efeito, se $(a,\ m) = 1$, então a congruêmcia $ax \equiv 1 \pmod{m}$ tem uma única solução $x_0$ (Teorema 3.10), isto é, $ax_0 \equiv 1 \pmod{m}$. Portanto, $a$ tem um único inverso módulo $m$ que é $x_0 = \bar{a}$.

**Exemplo:** $4x \equiv 1 \pmod{15}$.

Como $(4,\ 15) = 1$, temos uma única solução $x_0 = 4$, isto é, o inverso de 4 módulo 15 é $\bar{a} = x_0 = 4$. É bom lembrar que $\ldots,\ -26,\ -11,\ 4,\ 19,\ 34,\ \ldots$ são soluções da congruência linear acima, porém isto não é inconsistente com a unicidade do inverso de 4 módulo 15.

**Proposição 3.3.** *Seja p um número primo. O inteiro positivo a é o seu próprio inverso módulo p se, e somente se,* $a \equiv 1 \pmod{p}$ *ou* $a \equiv -1 \pmod{p}$.

**Demonstração**

($\Rightarrow$) Se $a$ é o seu próprio inverso módulo $p$, temos que $a \cdot a \equiv 1 \pmod{p}$, o que significa que $p \mid (a^2 - 1)$ ou $p \mid (a+1)(a-1)$ e como $p$ é primo, $p \mid (a+1)$ ou $p \mid (a-1)$, o que implica $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$.

($\Leftarrow$) Se $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$, então $p \mid (a-1)$ ou $p \mid (a+1)$.

Portanto, $p \mid (a-1)(a+1)$ ou $p \mid (a^2-1)$ ou ainda $a^2 \equiv 1 \pmod{p}$, o que conclui a demonstração.

**Exemplo:** $8x \equiv 1 \pmod{7}$.

8 é o seu próprio primo inverso módulo 7, pois $8 \cdot 8 \equiv 1 \pmod{7}$.

## 3.4 Sistemas de congruências lineares

Chama-se sistema de congruências lineares, com uma incógnita, todo sistema da forma

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \\ a_3 x \equiv b_3 \pmod{m_3} \\ \vdots \quad \vdots \quad \vdots \\ a_k x \equiv b_k \pmod{m_k}, \end{cases} \qquad (1)$$

onde $a_1,\ a_2,\ \ldots,\ a_k$ e $b_1,\ b_2,\ \ldots,\ b_k$ são inteiros quaisquer e $m_1,\ m_2,\ \ldots,\ m_k$ são inteiros positivos.

Todo inteiro $x_0$ tal que $a_i x_0 \equiv b_i \pmod{m_i}$, para $i = 1,\ 2,\ \ldots,\ k$, diz-se solução do sistema (1), isto é, $x_0$ é solução de (1) se satisfaz simultaneamente todas as congruências do sistema.

Mesmo que todas as congruências $a_i x \equiv b_i \pmod{m_i}$, $i = 1,\ 2,\ \ldots,\ k$, tenham solução não podemos garantir que o sistema possua solução, porém, se pelo menos uma das congruências não possui solução, podemos afirmar que o sistema não possui solução.

**Teorema 3.12.** *No sistema de congruências lineares*

$$\begin{cases} a_1x & \equiv & b_1 \pmod{m_1} \\ a_2x & \equiv & b_2 \pmod{m_2} \\ a_3x & \equiv & b_3 \pmod{m_3} \\ \vdots & \vdots & \vdots \\ a_kx & \equiv & b_k \pmod{m_k}, \end{cases} \qquad (2)$$

*se* $d_i = (a_i,\ m_i)$*, para* $i = 1,\ 2,\ \ldots,\ k$*, e se* $x_i$ *é uma solução da congruência* $a_ix \equiv b_i \pmod{m_i}$*, para* $i = 1,\ 2,\ \ldots,\ k$*, então o inteiro* $x_0$ *é uma solução do sistema (2) se, e somente se,* $x_0$ *é uma solução do seguinte sistema:*

$$\begin{cases} x & \equiv & x_1 \pmod{m_1/d_1} \\ x & \equiv & x_2 \pmod{m_2/d_2} \\ x & \equiv & x_3 \pmod{m_3/d_3} \\ \vdots & \vdots & \vdots \\ x & \equiv & x_k \pmod{m_k/d_k}. \end{cases} \qquad (3)$$

**Demonstração**

($\Rightarrow$) Suponha que o inteiro $x_0$ é uma solução do sistema (2). Então, pelo Teorema 3.10, o conjunto de todas as soluções da congruência $a_ix \equiv b_i \pmod{m_i}$ é

$$S_i = \{x \mid x \equiv x_i \pmod{m_i/d_i}\}$$

e, portanto, o inteiro $x_0$ pertence a cada um dos conjuntos $S_i$, para $i = 1,\ 2,\ \ldots,\ k$, isto é, $x_0 \equiv x_i \pmod{m_i/d_i}$, para $i = 1,\ 2,\ \ldots,\ k$. Isto significa que $x_0$ é solução do sistema (3).

($\Leftarrow$) Reciprocamente, suponhamos que o inteiro $x_0$ é uma solução do sistema (3), isto é, $x_0 \equiv x_i \pmod{m_i/d_i}$, para $i = 1,\ 2,\ \ldots,\ k$. Então, pelo mesmo Teorema 3.10, $x_0$ é uma solução de cada uma das congruências do sistema (2), logo $x_0$ é uma solução do sistema (2).

**Exemplo:** Resolva o sistema de congruências lineares

$$\begin{cases} 10x & \equiv & 22 \pmod{24} \\ 9x & \equiv & 15 \pmod{84} \\ 15x & \equiv & 123 \pmod{126}. \end{cases}$$

Sendo $d_1 = (10, 24) = 2$, $d_2 = (9, 84) = 3$ e $d_3 = (15, 123) = 3$, temos ainda que

$$\frac{m_1}{d_1} = \frac{24}{2} = 12, \quad \frac{m_2}{d_2} = \frac{84}{3} = 28 \quad \text{e} \quad \frac{m_3}{d_3} = \frac{126}{3} = 42.$$

Como $x_1 = 7$, $x_2 = 11$ e $x_3 = 25$ são soluções, respectivamente, das três congruências lineares do sistema dado, então pelo Teorema 3.12, as soluções deste sistema são as mesmas do sistema seguinte:

$$\begin{cases} x \equiv 7 \,(\text{mod } 12) & (I) \\ x \equiv 11 \,(\text{mod } 28) & (II) \\ x \equiv 25 \,(\text{mod } 42), & (III) \end{cases}$$

que iremos resolver.

De $(I)$, temos $x = 7 + a \cdot 12$, $a \in \mathbb{Z}$. Substituindo em $(II)$, encontramos $7 + a \cdot 12 \equiv 11 \,(\text{mod } 28)$, o que implica $12 \cdot a + 7 - 11 = b \cdot 28$, $b \in \mathbb{Z}$ ou $12a = 4 + 28b \Rightarrow 12a \equiv 4 \,(\text{mod } 28)$ e $a \equiv 5 \,(\text{mod } 28)$. Portanto, $a = 5 + 28b$, $b \in \mathbb{Z}$ e $x = 7 + 12(5 + 28b)$, logo $x = 67 + 336b$. Substituindo agora em $(III)$, temos $67 + 336b \equiv 25 \,(\text{mod } 42)$, o que implica $336b \equiv -42 \,(\text{mod } 42)$ e $b \equiv 1 \,(\text{mod } 42)$. Portanto, $b = 1 + 42c$, $c \in \mathbb{Z}$ e $x = 67 + 336(1 + 42c) \Rightarrow x = 403 + 14112c$. Isto significa que todo inteiro congruente a 403 módulo 14112 é uma solução do sistema dado, isto é, a solução geral deste sistema é

$$x \equiv 403 \,(\text{mod } 14112).$$

### 3.4.1 Teorema Chinês dos Restos

O nome dado ao Teorema seguinte se deve ao fato de que este resultado já era conhecido na antiguidade pelos matemáticos chineses.

**Teorema 3.13** (Teorema Chinês dos Restos)**.** *Se* $(a_i, m_i) = 1$, $(m_i, m_j) = 1$ *para* $i \neq j$ *e* $c_i$ *um inteiro, então o sistema*

$$\begin{cases} a_1 x \equiv c_1 \,(\text{mod } m_1) \\ a_2 x \equiv c_2 \,(\text{mod } m_2) \\ a_3 x \equiv c_3 \,(\text{mod } m_3) \\ \vdots \quad \vdots \quad \vdots \\ a_r x \equiv c_r \,(\text{mod } m_r) \end{cases}$$

*possui solução e a solução é única módulo m, onde* $m = m_1 \cdot m_2 \cdot m_3 \cdot \ldots \cdot m_r$.

**Demonstração**

Do fato de $(a_i,\ m_i) = 1$, o Teorema 3.10 nos diz que $a_i x \equiv c_i \pmod{m_i}$ possui uma única solução que denotaremos por $b_i$. Se definirmos $y_i = \frac{m}{m_i}$, onde $m = m_1 \cdot m_2 \cdot m_3 \cdot \ldots \cdot m_r$, teremos $(y_i,\ m_i) = 1$, uma vez que $(m_i,\ m_j) = 1$ para todo $i \neq j$. Novamente, o Teorema 3.10 nos garante que cada uma das congruências $y_i \equiv 1 \pmod{m_i}$ possui única solução que denotamos por $\bar{y}_i$. Logo, $\bar{y}_i y_i \equiv 1 \pmod{m_i}$, $i = 1,\ 2,\ \ldots,\ r$. Afirmamos, então, que o número $x$ dado por $x = b_1 y_1 \bar{y}_1 + b_2 y_2 \bar{y}_2 + \ldots + b_r y_r \bar{y}_r$ é uma solução simultânea para nosso sistema de congruência. De fato,

$$\begin{aligned} a_i x &= a_i b_1 y_1 \bar{y}_1 + a_i b_2 y_2 \bar{y}_2 + \ldots + a_i b_i y_i \bar{y}_i + \ldots + a_i b_r y_r \bar{y}_r \\ &\equiv a_i b_i y_i \bar{y}_i \pmod{m_i} \equiv a_i b_i \pmod{m_i} \equiv c_i \pmod{m_i}, \end{aligned}$$

uma vez que $y_j$ é divisível por $m_i$ para $i \neq j$, $y_i \bar{y}_i \equiv 1 \pmod{m_i}$ e $b_i$ é solução de $a_i x \equiv c_i \pmod{m_i}$.

Provamos, a seguir, que esta solução é única módulo $m$. Se $\bar{x}$ é uma outra solução para o sistema dado, então $a_i \bar{x} \equiv c_i \equiv a_i x \pmod{m_i}$ e, sendo $(a_i,\ m_i) = 1$ obtemos $\bar{x} \equiv x \pmod{m_i}$. Logo, $m_i \mid (\bar{x} - x)$, $i = 1,\ 2,\ \ldots,\ r$. Mas, como $(m_i,\ m_j) = 1$ para $i \neq j$, temos que

$$[m_1,\ m_2,\ m_3\ \ldots,\ m_r] = m_1 \cdot m_2 \cdot m_3 \cdot \cdots \cdot \ldots \cdot m_r.$$

Portanto, pelo Teorema 3.4, $m_1 \cdot m_2 \cdot m_3 \cdot \cdots \cdot \ldots \cdot m_r \mid (\bar{x} - x)$ ou seja $\bar{x} \equiv x \pmod{m_i}$, o que conclui a demonstração.

**Exemplo:** Resolver o sistema de congruências lineares

$$\begin{cases} 2x \equiv 1 \pmod 5 \\ 3x \equiv 2 \pmod 7 \\ 4x \equiv 3 \pmod{11}. \end{cases}$$

Como $(5, 7) = (5, 11) = (7, 11) = 1$ e $(2, 5) = (3, 7) = (4, 11) = 1$ logo, utilizando o Teorema Chinês dos Restos, temos que o sistema dado tem uma única solução módulo $m = 5 \cdot 7 \cdot 11 = 385$.

As congruências lineares $2x \equiv 1 \pmod 5$, $3x \equiv 1 \pmod 7$ e $4x \equiv 1 \pmod{11}$ tem como soluções, respectivamente, $\bar{y}_1 = 3$, $\bar{y}_2 = 5$ e $\bar{y}_3 = 3$ e por conse-

guinte o sistema dado é equivalente (mesma solução) ao sistema de congruências lineares

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 10 \pmod 7 \\ x \equiv 11 \pmod{11}, \end{cases}$$

o qual tem, pelo Teorema Chinês dos Restos , como única solução $x \equiv 108 \pmod{385}$.

# Capítulo 4

# Números Primos e Testes de Primalidade

Os números primos fascinam muito os estudiosos desde o surgimento dos mesmos.

Discutiu-se nos capítulos anteriores definições, propriedades e teoremas relacionados aos números primos e deste modo percebe-se o quão importante é o estudo dos números primos para a teoria dos números.

Como reconhecer se um dado número é primo ou não é uma das questões de ampla discussão no estudo da teoria dos números. Essas discussões deram origem aos testes de primalidade dos quais apresentaremos alguns neste capítulo. Entretanto, antes de apresentá-los, abordaremos alguns tópicos importantes no estudo dos números primos.

## 4.1 A função $\pi(x)$

Para cada número real $x$, define-se $\pi(x)$ como sendo a quantidade de números primos $p$ satisfazendo $2 \leq p \leq x$.

**Exemplo:**

- $\pi(10) = 4$, pois os números primos menores do que ou iguais a 10 são 2, 3, 5, 7.

- $\pi(15) = 6$, pois os números primos menores do que ou iguais a 15 são 2, 3, 5, 7, 11, 13.

**Teorema 4.1.** *Para todo número natural $n \geq 2$ existem n números compostos consecutivos.*

**Demonstração**

A sequência $(n+1)! + 2,\ (n+1)! + 3,\ \ldots,\ (n+1)! + n,\ (n+1)! + (n+1)$ é formada apenas por números compostos, pois $i \mid (n+1)! + i$, para todo $i$ tal que $2 \leq i \leq n+1$, pois

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

o que prova o teorema.

**Exemplo:** para $n = 5$, temos:

- $(5+1)! + 2 = 6! + 2 = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 + 2 = 2 \cdot (6 \cdot 5 \cdot 4 \cdot 3 \cdot 1 + 1) = 2 \cdot 361 = 722$
- $(5+1)! + 3 = 6! + 3 = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 + 3 = 3 \cdot (6 \cdot 5 \cdot 4 \cdot 2 \cdot 1 + 1) = 3 \cdot 241 = 723$
- $(5+1)! + 4 = 6! + 4 = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 + 4 = 4 \cdot (6 \cdot 5 \cdot 3 \cdot 2 \cdot 1 + 1) = 4 \cdot 181 = 724$
- $(5+1)! + 5 = 6! + 5 = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 + 5 = 5 \cdot (6 \cdot 4 \cdot 3 \cdot 2 \cdot 1 + 1) = 5 \cdot 145 = 725$
- $(5+1)! + 6 = 6! + 6 = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 + 6 = 6 \cdot (5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 + 1) = 6 \cdot 121 = 726.$

Logo, temos que 722, 723, 724, 725 e 726 são números compostos consecutivos.

**Teorema 4.2.** *Para valores suficientemente grandes de x, verifica-se que* $\dfrac{\pi(x)}{x/\ln x}$ *é aproximadamente igual a 1. Mais precisamente, na linguagem de limites,*

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} = 1.$$

Exibiremos uma tabela, (Tabela 4.1), segundo Sampaio e Caetano (2008), para que tenhamos evidências numéricas a respeito do Teorema 4.2, pois não iremos demonstrá-lo.

Tabela 4.1: Comparações de $\pi(x)$ com $\frac{(x)}{\ln x}$ ($\ln x = \log_e x$)

| x | $\pi(x)$ | $\frac{(x)}{\ln x}$ | $\frac{\pi(x)}{x/\ln x}$ |
|---|---|---|---|
| 1000 | 168 | 144,8 | 1,160 |
| 10000 | 1229 | 1085,7 | 1,132 |
| 100000 | 9592 | 8685,7 | 1,104 |
| 1000000 | 78498 | 72382,4 | 1,085 |
| $10^{10}$ | 455052512 | 434294481,9 | 1,048 |
| $10^{12}$ | 37607912018 | 36191206825,3 | 1,039 |
| $10^{14}$ | 3204941750802 | 3102103442166 | 1,033 |

Pelo Teorema 4.2, quando $x$ tende ao infinito, temos que $\dfrac{\pi(x)\cdot \ln x}{x}$ tende a 1. Por outro lado, $\ln x$ tende ao infinito.

Assim, temos que $\dfrac{\pi(x)}{x} = \dfrac{\frac{\pi(x)\cdot \ln x}{x}}{\ln x}$ tende a 0 quando $x$ tende ao infinito.

Dessa maneira, a porcentagem de primos positivos até $x$, dada aproximadamente pela fração decimal $\dfrac{\pi(x)}{x}$, tende a zero à medida que $x$ cresce. Isto nos revela que é cada vez mais difícil encontrar números primos à medida que avançamos nos inteiros positivos.

Para valores inteiros $x$ muito grande, este percentual é dado aproximadamente por

$$\frac{\pi(x)}{x} = \frac{\frac{\pi(x)}{x}}{\frac{\ln x}{\ln x}} \approx \frac{1}{\ln x}.$$

Tabela 4.2: Densidade dos números primos entre os primeiros inteiros positivos. Porcentagens de primos positivos até $x$ e comparações com $\frac{1}{\ln x}$

| x | $\pi(x)$ | $\frac{\pi(x)}{x}$ | $\frac{1}{\ln x}$ |
|---|---|---|---|
| $10^3$ | 168 | 0,168 | 0,1447648273 |
| $10^6$ | 78498 | 0,078498 | 0,0723824136 |
| $10^9$ | 50847534 | 0,050847534 | 0,04825494243 |
| $10^{10}$ | 455052512 | 0,0455052512 | 0,04342944819 |
| $10^{14}$ | 3204941750802 | 0,03204941750802 | 0,0310210344216608 |

Fonte: Sampaio e Caetano, (2008).

Observando a Tabela 4.2, notamos que são primos aproximadamente 16,8% dos inteiros positivos até $10^3$, 7,85% dos inteiros positivos até $10^6$ e aproximadamente 3,2% dos inteiros positivos até $10^{14}$.

Uma aproximação ainda melhor para $\pi(x)$ para $x \geq 2$, é dada por

$$\pi(x) \cong \int_2^x \frac{1}{\ln t} dt,$$

isto é,

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = \lim_{x\to\infty} \frac{\pi(x)}{\int_2^x \frac{dt}{\ln t}} = 1.$$

**Exemplo:** Para $x = 10^{14}$.

$$\frac{\pi(x)}{\int_2^x \frac{1}{\ln(t)} dt} \approx 0,9999999, \text{ enquanto que } \frac{\pi(x)}{\frac{x}{\ln x}} \approx 1,033.$$

O teorema dos números primos foi conjecturado por Gauss em 1796, mas demonstrado somente em 1896, pelos matemáticos Jacques Handamard e C.J. de la Vallée Poussin, em trabalhos independentes.

## 4.2 Números especiais

Alguns números merecem destaque na teoria dos números, pelas suas características, propriedades e fatos históricos que giram em torno deles, dos quais apresentaremos alguns.

### 4.2.1 Números de Fermat

Chama-se número de Fermat, todo número da forma

$$F_n = 2^{2^n} + 1, \ (n \geq 0).$$

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

Em 1640, Fermat observando que os inteiros $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, e $F_4 = 65537$ são todos primos conjecturou: $F_n$ é primo para todo inteiro $n \geq 0$. Entretanto, Euler, em 1730 derruba esta conjectura, provando que $F_5$ é composto, ou seja, $F_5 = 2^{2^5} + 1 = 2^{32} + 1$, o que implica $F_5 = 4294967297 = 641 \cdot 6700417$. Como até hoje não se encontrou outro número de Fermat que seja primo e não se provou tal fato, temos a seguinte conjectura:

Só existem cinco primos de Fermat, $F_0, \ F_1, \ F_2, \ F_3, \ F_4$ ou equivalentemente, todos os números de Fermat $F_n > F_4$ são compostos.

### 4.2.2 Números de Mersenne

Chama-se número de Mersenne todo inteiro positivo da forma

$$M(n) = 2^n - 1.$$

Se $M(n)$ é primo, diz-se que é um primo de Mersenne.

A denominação "Números de Mersenne" dada aos números inteiros $M(n)$ é uma homenagem ao matemático do século XVII Marin Mersenne (1588 - 1648).

Como resultado das suas pesquisas, Mersenne fez em 1644 a seguinte afirmação:

Todo inteiro $M(p) = 2^p - 1$ é primo para $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ e é composto para todos outros primos $p < 257$. Esta afirmação é falsa, pois provou-se que $M_{67}$ e $M_{257}$ são compostos e $M_{61}$, $M_{89}$ e $M_{107}$ são primos.

### 4.2.3 Primos gêmeos

Chamam-se primos gêmeos dois inteiros positivos ímpares e consecutivos que são ambos primos.

**Exemplos:** (3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73) são primos gêmeos.

Uma outra questão em aberto até hoje é que não se sabe se existem infinitos primos gêmeos.

### 4.2.4 Conjectura de Goldbach

No século XVIII, em 1742, o matemático Christian Goldbach, em uma carta escrita a Euler, conjecturou que todo inteiro par, maior do que dois, pode ser escrito como soma de dois primos positivos. Assim, por exemplo, temos:

$$
\begin{aligned}
4 &= 2 + 2 \\
6 &= 3 + 3 \\
8 &= 3 + 5 \\
10 &= 3 + 7 = 5 + 5 \\
12 &= 5 + 7 \\
14 &= 3 + 11 = 7 + 7 \\
16 &= 3 + 13 = 5 + 11 \\
18 &= 5 + 13 = 7 + 11 \\
20 &= 3 + 17 = 7 + 13 \\
&\vdots
\end{aligned}
$$

Outra famosa conjectura de Goldbach diz que todo inteiro ímpar, maior do que 5, é soma de três primos positivos.

Um grande número de problemas interessantes relacionados com os primos ainda permanecem sem solução. Vejamos, por exemplo:

(1) Há um número infinito de primos da forma $n^2 + 1$, onde $n$ é um inteiro;

(2) Existe sempre pelo menos um primo entre $n^2$ e $n^2 + n$ para todo inteiro $n > 1$.

**Teorema 4.3** (Pequeno Teorema de Fermat)**.** *Seja p um número primo. Se p não divide a* ($p \nmid a$)*, então*

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

**Demonstração**

Sabemos que o conjunto formado pelos $p$ números $0, 1, 2, \ldots, p-1$ constitui um sistema completo de resíduos módulo $p$. Isto significa que qualquer conjunto contendo no máximo $p$ elementos incongruentes módulo $p$ pode ser colocado em correspondência biunívoca com um subconjunto de $\{0, 1, 2, \ldots, p-1\}$. Vamos, agora, considerar os números $a, 2a, 3a, \ldots, (p-1)a$. Como $(a, p) = 1$, nenhum destes números $ia$, $1 \leq i \leq p-1$, é divisível por $p$, ou seja, nenhum é congruente a zero módulo $p$. Quaisquer dois deles são incongruentes módulo $p$, pois $aj \equiv ak (\text{mod } p)$ implica $j \equiv k (\text{mod} p)$ e isto só é possível se $j = k$, uma vez que ambos $j$ e $k$ são positivos e menores do que $p$. Temos, portanto, um conjunto de $p-1$ elementos incongruentes módulo $p$ e não divisíveis por $p$. Logo, cada um deles é congruente a exatamente um dentre os elementos $1, 2, 3, \ldots, p-1$. Se multiplicarmos essas congruências, membro a membro, obtemos $a \cdot (2a) \cdot (3a) \ldots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot p - 1 (\text{mod } p)$, ou seja, $a^{p-1} \cdot (p-1)! \equiv (p-1)! (\text{mod } p)$. Mas, como $((p-1)!, p) = 1$, podemos cancelar o fator $(p-1)!$ em ambos os lados, obtendo

$$a^{p-1} \equiv 1 (\text{mod} p),$$

o que conclui a demonstração.

**Corolário 4.1.** *Se p é um primo e a é um inteiro positivo, então* $a^p \equiv a (\text{mod } p)$.

**Demonstração**

Temos que analisar dois casos, se $p \mid a$ e se $p \nmid a$.

(i) Se $p \mid a$, então $p \mid (a \cdot (a^{p-1} - 1))$ e, portanto, $a^p \equiv a (\text{mod } p)$.

(ii) Se $p \nmid a$, pelo Teorema 4.3, $p \mid (a^{p-1} - 1)$ e, portanto, $p \mid (a^p - a)$. Logo, em ambos os casos, $a^p \equiv a (\text{mod } p)$, o que conclui a demonstração.

**Exemplos:**

a) Mostrar que $13|(2^{70} + 3^{70})$.

Pelo Teorema de Fermat, temos

$2^{12} \equiv 1(\text{mod } 13)$ e, portanto, $(2^{12})^5 \equiv 1^5(\text{mod } 13) \Rightarrow 2^{60} \equiv 1(\text{mod } 13)$. $(I)$

Obviamente, $2^5 = 32 \equiv 6(\text{mod}13) \Rightarrow (2^5)^2 \equiv 6^2(\text{mod}13) \Rightarrow 2^{10} \equiv 36(\text{mod } 13)$ e como $36 \equiv -3(\text{mod } 13) \Rightarrow 2^{10} \equiv -3(\text{mod } 13)$. $(II)$

De (I) e (II), temos $2^{60} \cdot 2^{10} \equiv 1 \cdot (-3)(\text{mod}13) \Rightarrow 2^{70} \equiv -3(\text{mod}13)$. $(III)$

Temos ainda que

$3^3 \equiv 1(\text{mod}13) \Rightarrow (3^3)^{23} \equiv 1^{23}(\text{mod}13) \Rightarrow 3^{69} \equiv 1(\text{mod}13)$, o que implica

$3^{69} \cdot 3 \equiv 1 \cdot 3(\text{mod}13) \Rightarrow 3^{70} \equiv 3(\text{mod}13)$. $(IV)$

Somando ordenadamente as congruências (III) e (IV), temos

$2^{70} + 3^{70} \equiv (-3 + 3)(\text{mod } 13) \Rightarrow 2^{70} + 3^{70} \equiv 0(\text{mod } 13)$, isto é,

$2^{70} + 3^{70} = 13q,\ q \in \mathbb{Z}$ ou $13|(2^{70} + 3^{70})$.

b) Calcular o resto da divisão de $5^{63}$ por 29.

Queremos achar um $x$, tal que $5^{63} \equiv x(\text{mod } 29)$ pelo Teorema de Fermat, fazendo $p = 29$ e $a = 5$, temos

$$\begin{aligned} & 5^{29-1} \equiv 1(\text{mod } 29) \\ \Rightarrow\ & 5^{28} \equiv 1(\text{mod } 29) \\ \Rightarrow\ & (5^{28})^2 \equiv 1^2(\text{mod } 29) \\ \Rightarrow\ & 5^{56} \equiv 1(\text{mod } 29) \\ \Rightarrow\ & 5^{56} \cdot 5^7 \equiv 5^7(\text{mod } 29) \\ \Rightarrow\ & 5^{63} \equiv 5^7(\text{mod } 29) \text{ e como } 5^7 \equiv 28(\text{mod } 29) \\ \Rightarrow\ & 5^{63} \equiv 28(\text{mod } 29). \end{aligned}$$

Portanto, o resto da divisão de $5^{63}$ por 29 é 28.

**Teorema 4.4** (Teorema de Wilson)**.** *Se p é primo, então* $(p-1)! \equiv -1(\text{mod}p)$.

**Demonstração**

Como $(2-1)! \equiv -1(\text{mod}2)$, o resultado é válido para $p = 2$. Pelo Teorema 3.10, a congruência $ax \equiv 1(\text{mod}p)$ tem única solução para todo $a$ no seguinte conjunto $\{1, 2, 3, \ldots, (p-1)\}$ e como, destes elementos, somente 1 e $p-1$ são seus próprios inversos módulo $p$, podemos agrupar os números $2, 3, 4, \ldots, p-2$ em $(p-3)/2$ pares cujos produtos sejam congruentes a 1 módulo $p$.

Se multiplicarmos estas congruências, membro a membro, teremos pelo Teorema 3.2 ($\mathbf{P_6}$) que $2 \cdot 3 \cdot 4 \cdot 5 \cdot \ldots \cdot (p-2) \equiv 1(\text{mod}p)$. Multiplicando-se ambos os lados desta congruência por $p-1$, teremos $2 \cdot 3 \cdot 4 \cdot 5 \cdot \ldots \cdot (p-2) \cdot (p-1) \equiv (p-1)(\text{mod}p)$, isto é, $(p-1)! \equiv -1(\text{mod}p)$ uma vez que $(p-1) \equiv -1(\text{mod}p)$.

**Exemplo:** Vamos utilizar um exemplo para ilustrar a ideia usada na demonstração. Seja $p = 13$, observe que

$(13-1)! \equiv -1(\text{mod } 13) \Rightarrow (12)! \equiv -1(\text{mod } 13)$ ou $479001600 \equiv -1(\text{mod } 13)$.

Dentre os números $1, 2, 3, \ldots, 12$, somente 1 e 12 são os seus próprios inversos módulo 13, pois $1 \equiv 1(\text{mod } 13)$ e $12 \equiv -1(\text{mod } 13)$ (Proposição 3.3) e nenhum dos números $2, 3, 4, \ldots, 11$ é congruente a 1 ou $-1$ módulo 13. Mas, como os números $2, 3, 4, \ldots, 11$ são todos relativamente primos com 13, cada um deles possui, pelo Teorema 3.10, um único inverso módulo 13. Eles podem, portanto, ser agrupados em 5 pares $\left(5 = \dfrac{13-2}{2}\right) = \left(\dfrac{p-2}{2}\right)$ que são os seguintes:

$$2 \cdot 7 \equiv 1(\text{mod } 13)$$
$$3 \cdot 9 \equiv 1(\text{mod } 13)$$
$$4 \cdot 10 \equiv 1(\text{mod } 13)$$
$$5 \cdot 8 \equiv 1(\text{mod } 13)$$
$$6 \cdot 11 \equiv 1(\text{mod } 13)$$

e pelo Teorema 3.2 podemos multiplicar estas congruências, membro a membro, obtendo $2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \equiv 1(\text{mod } 13)$ e se multiplicarmos ainda os dois lados por 12, teremos $2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \equiv 12(\text{mod } 13)$ ou $12! \equiv 12(\text{mod } 13)$ e como$12 \equiv -1(\text{mod } 13)$. Podemos afirmar que $12! \equiv -1(\text{mod } 13)$ ou ainda $(13-1)! \equiv -1(\text{mod } 13)$.

**Teorema 4.5** (Recíproco do Teorema de Wilson)**.** *Se n é um inteiro tal que* $(n-1)! \equiv -1(\text{mod } n)$*, então n é primo.*

**Demonstração**

A prova é feita por contradição. Vamos supor então que $(n-1)! \equiv -1(\text{mod } n)$, isto é, $n \mid ((n-1)! + 1)$ e que $n$ não seja primo, ou seja, $n = rs$, $1 < r < n$ e $1 < s < n$. Nestas condições, $r \mid (n-1)!$ e, sendo $r$ um divisor de $n$, $r \mid ((n-1)! + 1)$ e, portanto, $r$ deve dividir a diferença $(n-1)! + 1 - (n-1)! = 1$, o que é um absurdo, uma vez que $r > 1$. Logo, um $n$ satisfazendo $(n-1)! \equiv -1(\text{mod } n)$ é primo.

**Exemplo:** Verificar se 7 é primo.

Basta verificar se 7 satisfaz o Teorema 4.5.

$$(7-1)! = 6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$$
$$(7-1)! + 1 = 6! + 1 = 721 = 7 \cdot 103,$$

ou seja,

$$(7-1)! \equiv -1 (\text{mod } 7).$$

Portanto, 7 é primo.

**Definição 4.1** (Função de Euler)**.** *Seja n um inteiro positivo, a função $\phi$ de Euler ou simplesmente Função de Euler, denotada por $\phi(n)$, é definida como sendo o número de inteiros positivos menores do que ou iguais a n que são relativamente primos com n, em outras palavras, $\phi(n)$ é igual ao número de elementos do conjunto*

$$\{x \in \mathbb{N} / 1 \leq x \leq n \text{ e } (x,\ n) = 1\}.$$

**Exemplos:**

- $\phi(1) = 1$, pois $(1, 1) = 1$.
- $\phi(10) = 4$, pois o conjunto $\{x \in \mathbb{N} / 1 \leq x \leq 10 \text{ e } (x,\ 10) = 1\} = \{1, 3, 7, 9\}$.
- $\phi(15) = 8$, pois o conjunto $\{x \in \mathbb{N} / 1 \leq x \leq 15 \text{ e } (x,\ 15) = 1\} = \{1, 2, 4, 7, 8, 11, 13, 14\}$.

**Definição 4.2.** *Um sistema reduzido de resíduos módulo m é um conjunto de $\phi(m)$ inteiros $r_1, r_2, \ldots, r_{\phi(m)}$, tais que cada elemento do conjunto é relativamente primo com m, e se $i \neq j$, então $r_i \not\equiv r_j (\text{mod } m)$.*

**Exemplo:** O conjunto $\{0, 1, 2, 3, 4, 5, 6, 7\}$ é um sistema completo de resíduos módulo 8, portanto, $\{1, 3, 5, 7\}$ é um sistema reduzido de resíduo módulo 8. A fim de se obter um sistema reduzido de resíduos de um sistema completo de resíduos módulo $m$, basta retirar os elementos do sistema completo que não são relativamente primos com $m$.

**Teorema 4.6.** *Seja a um inteiro positivo tal que* $(a,\ m) = 1$ *se* $r_1, r_2, \ldots, r_{\phi(m)}$ *é um sistema reduzido de resíduo módulo m, então* $ar_1, ar_2, \ldots, ar_{\phi(m)}$ *é, também, um sistema reduzido de resíduos módulo m.*

**Demonstração**

Como na sequência $ar_1, ar_2, \ldots, ar_{\phi(m)}$ temos $\phi(m)$ elementos, devemos mostrar que todos eles são relativamente primos com $m$ e, dois a dois, incongruentes módulo $m$. Como $(a,\ m) = 1$ e $(r_i,\ m) = 1$, temos que $(ar_i,\ m) = 1$. Logo, nos resta mostrar que $ar_i \not\equiv ar_j (\text{mod } m)$ se $i \neq j$. Mas como $(a,\ m) = 1$, de $ar_i \equiv ar_j (\text{mod } m)$ temos que $r_i \equiv r_j (\text{mod } m)$, o que implica $i = j$, uma vez que $r_1, r_2, \ldots, r_{\phi(m)}$ é um sistema reduzido de resíduos módulo $m$, o que conclui a demonstração.

**Exemplo:** Sejam $m = 8$ e $a = 5$. Sabemos que o conjunto $\{1, 3, 5, 7\}$ é um sistema reduzido de resíduos módulo 8 e que $(8, 5) = 1$. Consideremos o conjunto $\{5\cdot 1, 5\cdot 3, 5\cdot 5, 5\cdot 7\}$ ou $\{5, 15, 25, 35\}$, observe que $(5,\ 8) = (15,\ 8) = (25,\ 8) = (35,\ 8) = 1$. Assim, $15 \not\equiv 5 (\text{mod } 8)$, $25 \not\equiv 15 (\text{mod } 8)$, $25 \not\equiv 5 (\text{mod } 8)$, $35 \not\equiv 5 (\text{mod } 8)$, $35 \not\equiv 15 (\text{mod } 8)$ e $35 \not\equiv 25 (\text{mod } 8)$.

**Teorema 4.7.** *Se m é um inteiro positivo e a um inteiro com* $(a,\ m) = 1$*, então*

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

**Demonstração**

No Teorema 4.6 mostramos que os elementos $ar_1, ar_2, \ldots, ar_{\phi(m)}$ constituem um sistema reduzido de resíduos módulo $m$ se $(a,\ m) = 1$ e $r_1, r_2, \ldots, r_{\phi(m)}$ for um sistema reduzido de resíduos módulo $m$. Isto significa que $ar_i$ é congruente a exatamente a um dos $r_j,\ 1 \leq j \leq \phi(m)$, e, portanto, o produto dos $ar_i$ deve ser congruente ao produto dos $r_j$ módulo $m$, isto é,

$$ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\phi(m)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(m)} (\text{mod } m),$$

ou seja,

$$a^{\phi(m)} r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(m)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(m)} (\text{mod } m)$$

e como $\left( \prod_{j=1}^{\phi(m)} r_j,\ m \right) = 1$, podemos cancelar $\prod_{i=j}^{\phi(m)} r_j$ em ambos os lados para obter

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

**Exemplo:** Vamos utilizar um exemplo para ilustrar a ideia da demonstração.

Sejam $m = 8$ e $a = 5$, observamos que $(8,\ 5) = 1$ e que $\{1, 3, 5, 7\}$ é um sistema reduzido de resíduos módulo 8. Consideremos o conjunto $\{5 \cdot 1, 5 \cdot 3, 5 \cdot 5, 5 \cdot 7\}$ ou $\{5, 15, 25, 35\}$. Pelo Teorema 4.6, vimos que este conjunto também é um sistema reduzido de resíduos módulo 8. Isto significa que cada um dos elementos do conjunto $\{5 \cdot 1, 5 \cdot 3, 5 \cdot 3, 5 \cdot 7\}$ é congruente módulo 8 a exatamente um dos elementos 1, 3, 5, 7. Temos, então, que

$$5 \cdot 1 \equiv 5 (\text{mod } 8)$$
$$5 \cdot 3 \equiv 7 (\text{mod } 8)$$
$$5 \cdot 5 \equiv 1 (\text{mod } 8)$$
$$5 \cdot 7 \equiv 3 (\text{mod } 8).$$

Multiplicando-se, membro a membro, estas congruências, obtemos:

$5 \cdot 1 \cdot 5 \cdot 3 \cdot 5 \cdot 5 \cdot 5 \cdot 7 \equiv 5 \cdot 7 \cdot 1 \cdot 3 (\text{mod } 8)$ ou $5^4 \cdot 1 \cdot 3 \cdot 5 \cdot 7 \equiv 5 \cdot 7 \cdot 1 \cdot 3 (\text{mod } 8)$ e ainda como $(1 \cdot 3 \cdot 5 \cdot 7,\ 8) = 1$, podemos cancelar o fator $(1 \cdot 3 \cdot 5 \cdot 7)$ obtendo $5^4 \equiv 1 (\text{mod } 8)$ ou $5^{\phi(8)} \equiv 1 (\text{mod } 8)$.

**Teorema 4.8.** *Seja o inteiro $n > 1$, então $\phi(n) = n - 1$ se, e somente se, $n$ é primo.*

**Demonstração**

($\Rightarrow$) Se $n > 1$ é primo, então cada um dos inteiros positivos menores do que $n$ é relativamente primo com $n$ e, portanto,

$$\phi(n) = n - 1.$$

($\Leftarrow$) Reciprocamente, se $\phi(n) = n - 1$, com $n > 1$, então $n$ é primo, pois, se $n$ fosse composto, teria pelo menos um divisor $d$ tal que $1 < d < n$, de modo que pelo menos dois dos inteiros $1, 2, 3, \ldots, n$ não seriam relativamente primos com $n$, isto é, $\phi(n) \leq n - 2$. Logo, $n$ é primo.

**Exemplo:** $\phi(13) = 13 - 1 = 12$, pois $\{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12\}$ são todos relativamente primos com 13.

**Observação 4.1.** *Como para p primo, $\phi(p) = p - 1$, o Teorema de Euler nada mais é que uma generalização do pequeno Teorema de Fermat. Se p é primo e se $p \nmid a$, então $a^{p-1} \equiv 1 (\text{mod } p)$.*

## 4.3 Testes de primalidade

Testar a primalidade de um número nada mais é que comprovar, através de um algoritmo, se um dado número $n$ é primo ou não.

Muitos estudiosos, desde a antiguidade, vem se dedicando a este problema e, portanto, surgiram muitos métodos até hoje. Apresentaremos alguns destes neste capítulo.

### 4.3.1 Fórmulas que resultam números primos

Os números primos aparecem com muita irregularidade na sequência dos números inteiros positivos e por isso muitas fórmulas que resultam números primos foram construídas.

- $f(n) = n^2 + n + 41$

  Esta fórmula fornece primos para $n = 0, 1, 2, \ldots, 39$. Para $n = 40$ e $n = 41$ os inteiros que se obtém são compostos, pois temos:

  - $f(40) = 40^2 + 40 + 41 = 40(40+1) + 41 = 40 \cdot 41 + 41 \Rightarrow f(40) = 41(40+1) = 41 \cdot 41$. Portanto, $f(40)$ é composto.
  - $f(41) = 41^2 + 41 + 41 \Rightarrow f(41) = 41(41 + 1 + 1) \Rightarrow f(41) = 41 \cdot 43$. Portanto, $f(41)$ é composto.

  A fórmula $f(n) = n^2 + n + 41$ é chamada de fórmula de Euler.

- $f(n) = 2n^2 + 29$

  Fornece primos para $n = 0,\ 1,\ 2,\ \ldots, 28$. Para $n = 29$ o inteiro que se obtém é composto, pois

  $f(29) = 2 \cdot 29^2 + 29 \Rightarrow f(29) = 29 \cdot (2 \cdot 29 + 1) \Rightarrow f(29) = 29 \cdot 59$. Portanto, $f(29)$ é composto.

- $f(n) = n^2 + n + 17$

  Para a fórmula acima obtém-se primos para $n = 0,\ 1,\ 2,\ \ldots,\ 16$. Para $n = 17$ o inteiro que se obtém é composto, pois

  $f(17) = 17^2 + 17 + 17 = 17(17 + 1 + 1) = 17 \cdot 19$.

- $f(n) = 3n^2 + 3n + 23$

  Com essa fórmula obtemos primos para $n = 0,\ 1,\ \ldots,\ 21$. Para $n = 22$ e $n = 23$ os inteiros que se obtém são compostos, pois temos:

  - $f(22) = 3 \cdot 22^2 + 3 \cdot 22 + 23 = 3 \cdot 22(22 + 1) + 23$
    $\Rightarrow f(22) = 3 \cdot 22 \cdot 23 + 23 = 23(3 \cdot 22 + 1) = 23 \cdot 67$. Portanto, $f(22)$ é composto.
  - $f(23) = 3 \cdot 23^2 + 3 \cdot 23 + 23 = 23(3 \cdot 23 + 3 + 1) = 23 \cdot 73$. Portanto, $f(23)$ é composto.

Observando as fórmulas anteriores, nos vem a cabeça o seguinte questionamento: será que é possível encontrarmos alguma expressão polinomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,$$

com coeficientes inteiros, que forneça a sequência dos números primos ou pelo menos forneça somente primos?

Infelizmente a resposta é negativa. Isto será demonstrado no teorema seguinte.

**Teorema 4.9.** *Seja* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ *uma expressão polinomial com coeficientes* $a_0,\ a_1,\ \ldots,\ a_n$ *todos inteiros e* $a_n > 0$ *e* $n \geq 1$. *Então, a sequência* $(f(x))_{x \in \mathbb{N}}$ *assume infinitos valores naturais compostos.*

**Demonstração**

$f(x)$ pode assumir finitos valores negativos, pois $a_n > 0$. Se $f(x)$ sempre é composto, não há o que provar. Podemos supor então que exista $x_0 \in \mathbb{N}$ tal que $f(x_0) = p$ é primo e $f(x) > 0$, para $x \geq x_0$. Para todo $t \in \mathbb{N}$, temos

$$\begin{aligned} f(x_0 + t \cdot p) &= a_n(x_0 + t \cdot p)^n + a_{n-1}(x_0 + t \cdot p)^{n-1} + \ldots + a_1(x_0 + t \cdot p) + a_0 \\ &= a_n x_0^n + a_{n-1}x_0^{n-1} + \ldots + a_1 x_0 + a_0 + k_t \cdot p \end{aligned}$$

e como $p = f(x_0) = a_n x_0^n + a_{n-1}x_0^{n-1} + \ldots + a_1 x_0 + a_0$, temos que

$$f(x_0 + t \cdot p) = p + k_t \cdot p = p(1 + k_t) \quad \text{com} \quad k_t \in \mathbb{N}$$

apropriado. Segue então que os valores$f(x_0 + t \cdot p) = p(1 + k_t) \quad \text{com} \quad k_t \in \mathbb{N}$ são números compostos. Como $k_t = a_n \cdot^n \cdot t^n \pm \ldots$ assume infinitos valores naturais distintos quando $t \in \mathbb{N}$, concluímos a afirmação.

**Fórmula dada por Willans em 1964**

A fórmula de Willans é $p_n = 1 + \sum_{m=1}^{2^n} \left[ \sqrt[n]{\frac{n}{1+\pi(m)}} \right]$, onde $[x]$ é a parte inteira de $x$.

Esta fórmula é muito bonita, porém é inútil, devido a quantidade de operações envolvidas, no entanto, ela nos fornece o $n$-ésimo número primo.

**Exemplo:**

$$p_{10} = 1 + \sum_{m=1}^{2^{10}} \left[ \sqrt[10]{\frac{10}{1+\pi(m)}} \right] = 29.$$

**Fórmula apresentada por Honsbenger (1976), citada por Watanabe (1998).**

Sejam $x$ e $y$ números naturais, $y \neq 0$ e

$$a = x(y+1) - (y! + 1),$$

temos que a fórmula que nos fornece todos os números primos e somente esses é

$$f(x,\ y) = \frac{y-1}{2}\left[\left|a^2 - 1\right| - (a^2 - 1)\right] + 2.$$

**Exemplos:**

- Se $x = 1$ e $y = 1$, então $a = 1(1+1) - (1! - 1)$, logo $a = 0$ e
  $f(1,\ 1) = \frac{1-1}{2}[|0^2 - 1| - (0^2 - 1)] + 2 \Rightarrow f(1,\ 1) = 2.$

- Se $x = 1$ e $y = 2$, então $a = 1(2+1) - (2! + 1) = 3 - 3 \Rightarrow a = 0$
  $f(1,\ 2) = \frac{2-1}{2}[|0^2 - 1| - (0^2 - 1)] + 2 = \frac{1}{2}(1+1) + 2 \Rightarrow f(1,\ 2) = 3.$

- Se $x = 2$ e $y = 2$, então $a = 2(2+1) - (2! + 1) = 6 - 3 \Rightarrow a = 3$
  $f(2,\ 2) = \frac{2-1}{2}[|3^2 - 1| - (3^2 - 1)] + 2 \Rightarrow f(2,\ 2) = 2.$

Temos ainda que $f(5,\ 4) = 5$, $f(103,\ 6) = 7$, $f(329891,\ 10) = 11$ e $f(36846277,\ 12) = 13$.

Para acharmos os pares $(x,\ y)$, correspondentes a cada número primo correspondente, basta fazermos

$$x = \frac{(p-1)! + 1}{p} \quad \text{e} \quad y = p - 1.$$

Assim, por exemplo, para obter 13, fazemos
$x = \dfrac{(13-1)!+1}{13} = 36846277$ e $y = 13 - 1 = 12$. Para maiores detalhes da demonstração, ver Watanabe (1998).

### 4.3.2 Testes de primalidade

**Teorema 4.10.** *Se um número inteiro positivo $n > 1$ não é primo, ou seja, é composto, então $n$ possui necessariamente um fator primo $p \leq \sqrt{n}$.*

**Demonstração**

Com efeito, se o inteiro positivo $n > 1$ é composto, então

$$n = a \cdot b, \quad 1 < a < n \quad \text{e} \quad 1 < b < n,$$

portanto, sem perda de generalidade vamos supor que $a \leq b$ e, portanto, $a^2 \leq a \cdot b$. Então, $a^2 \leq n \Rightarrow a \leq \sqrt{n}$. Por ser $a > 1$, o teorema fundamental da aritmética garante que $a$ tem pelo menos um divisor primo $p$, de modo que $p \leq a \leq \sqrt{n}$ e como $p \mid a$ e $a \mid n$, segue-se que $p \mid n$, isto é, o inteiro primo $p \leq \sqrt{n}$ é um divisor de $n$.

**Método das divisões sucessivas**

O teorema anterior nos fornece um método de reconhecer se um dado número inteiro $n > 1$ é primo ou composto. O método consiste em dividirmos $n$ sucessivamente pelos primos que não excedem $\sqrt{n}$. Caso alguma das divisões seja exata (resto igual a zero), concluímos que $n$ é composto; caso contrário concluímos que $n$ é primo.

**Exemplos:**

a) Verificar se 533 é primo ou composto.

- $\sqrt{533} \cong 23,09$. Primeiramente, dividimos 533 sucessivamente por 2, 3, 5, 7, 11, 13, 17, 19, 23 que são todos os primos menores do que ou iguais a 23.
- $533 \div 2 = 266$ e resto $= 1$
- $533 \div 3 = 177$ e resto $= 2$

- $533 \div 5 = 106$ e resto = 3
- $533 \div 7 = 76$ e resto = 1
- $533 \div 11 = 48$ e resto = 5
- $533 \div 13 = 41$ e resto = 0. Portanto, $533 = 13 \cdot 41$, ou seja, 533 é composto.

b) Verifique se 353 é primo ou composto.

- $\sqrt{353} \cong 18,79$. Primeiramente, dividimos 353 sucessivamente por 2, 3, 5, 7, 11, 13, 17 que são todos os primos menores do que ou iguais a 18.
- $353 \div 2 = 176$ e resto = 1
- $353 \div 3 = 117$ e resto = 2
- $353 \div 5 = 70$ e resto = 3
- $353 \div 7 = 50$ e resto = 3
- $353 \div 11 = 32$ e resto = 1
- $353 \div 13 = 27$ e resto = 2
- $353 \div 17 = 20$ e resto = 13.

  Como nenhuma das divisões é exata, podemos garantir que 353 é primo.

O método apresentado é ineficaz quando o número a ser testado é muito grande, pois além de termos que fazer todas as divisões, temos ainda que conhecer a lista de primos menores do que ou iguais a $\sqrt{n}$.

### Crivo de Eratóstenes

O crivo de Eratóstenes (matemático grego, nascido por volta de 284 a.C) é o mais antigo dos métodos para achar números primos, e assim como o método anterior, não envolve nenhuma fórmula explícita.

**O método consiste em:**

Seja um número natural $n$, deseja-se determinar os números primos menores do que ou iguais a $n$. Para isto, listamos os números $2, 3, 4, 5, 6, \ldots, n$ e, em seguida, eliminam-se todos os inteiros compostos que são múltiplos dos primos $p$, tais que $p \leq \sqrt{n}$, isto é, $2p,\ 3p,\ 4p, \ldots$ e então os números que sobram são os números primos menores do que $n$.

**Exemplo:** Listar todos os números primos que são menores do que 80.

1. Lista-se todos os números de 2 a 80

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 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 |

2. Os primos $p$, tais que $p \leq \sqrt{80}$ ou $p \leq 8,9$ são: $2, 3, 5, 7$.

3. Elimina-se os inteiros compostos múltiplos de 2, isto é, $4, 6, 8, 10, 12, \ldots, 80$.

4. Elimina-se os inteiros compostos múltiplo de 3, isto é, $6, 9, 12, 15, \ldots, 78$.

5. Elimina-se os inteiros compostos múltiplo de 5, isto é, $10, 15, 20, \ldots, 80$.

6. Elimina-se os números inteiros compostos que são múltiplo 7, isto é, $14, 21, 28, 42, 49, 56, 63, 70, 77$.

7. Todos os números inteiros que não foram eliminados na lista, são todos os primos menores do que 80. São eles:
   $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79$.

O crivo de Eratóstenes também torna-se inútil, quando o número em questão é um número grande.

### Teste de Wilson

O Teorema de Wilson e o seu recíproco, isto é, um inteiro $p$ é primo se, e somente se, $(p-1)! \equiv -1(\text{mod } p)$, teoremas 4.4 e 4.5, nos fornece mais um teste de primalidade.

Podemos verificar se 11 é primo, utilizando o Teorema de Wilson, para isso basta fazer $p = 11$. Se satisfazer o Teorema de Wilson é primo, caso contrário, é composto.

$$(11-1)! \equiv -1(\text{mod } 11) \Rightarrow 10! \equiv -1(\text{mod } 11) \Rightarrow 3628800 \equiv -1(\text{mod } 11),$$

isto é, dividindo 3628801 por 11, obtemos resto igual a zero, portanto, concluímos que 11 é primo.

Vamos testar agora um número um pouco maior e verificar o que acontece.

Vamos verificar se 29 é primo.

$$(29-1)! \equiv -1(\text{mod } 29) \Rightarrow 304888344611713860501504000000 \equiv -1(\text{mod } 29)$$

e, portanto, dividindo 304888344611713860501504000001 por 29 encontramos resto zero e, portanto, concluímos que 29 é primo, pois 29 satisfaz o Teorema de Wilson.

Como podemos observar, no exemplo anterior, se aumentarmos muito o número $p$, o Teste de Wilson é impraticável, pois teríamos que calcular $(p-1)!$, porém não podemos deixar de descartar a sua importância teórica.

**Observação 4.2.** *Podemos também usar congruência para diminuírmos bastante o trabalho. Vejamos:*

$$28! \equiv 1 \cdot 2 \cdot 3 \cdot 4 \ldots 14 \cdot (-14) \cdot (-13) \cdot (-12) \ldots (-1)(\text{mod } 29) \Rightarrow (28)! \equiv (14!)^2(\text{mod } 29).$$

*Temos ainda:*

$$\begin{aligned} & (2 \cdot 14) \cdot (4 \cdot 7) \equiv (-1)(-1) \equiv 1(\text{mod } 29) \\ \Rightarrow\ & (5 \cdot 6) \cdot (3 \cdot 10) \equiv 1 \cdot 1 \equiv 1(\text{mod } 29) \\ \Rightarrow\ & 9 \cdot 13 \equiv 117 = 29 \cdot 4 + 1 \equiv 1(\text{mod } 29) \\ \Rightarrow\ & 8 \cdot 11 = 88 = 87 + 1 = 3 \cdot 29 + 1 \equiv (\text{mod } 29) \\ \Rightarrow\ & 14! \equiv 12(\text{mod } 29) \\ \Rightarrow\ & (14)^2 \equiv 144(\text{mod } 29), \end{aligned}$$

*mas* $5 \cdot 29 = 145 \Rightarrow (14!)^2 \equiv -1(\text{mod } 29)$*, portanto,* $28! \equiv -1(\text{mod } 29)$*. Logo, 29 é primo.*

### Teste de Fermat

Uma das versões do Teorema de Fermat diz que se $p$ é primo e $a$ um inteiro positivo, então $a^p \equiv a(\text{mod } p)$, portanto, para descobrirmos que um inteiro é composto, basta verificarmos que existe um inteiro $b$ tal que $b^n \not\equiv b(\text{mod } n)$.

Convém observar que, só precisamos considerar os inteiros $1 < b < n-1$, pois qualquer inteiro é congruente a um inteiro no intervalo de 0 a $n-1$, além disso, a equação $b^n \equiv b(\text{mod } n)$ é sempre satisfeita quando $b$ é 0, 1 ou $n-1$.

**Teste:** Se $n > 0$ e $1 < b < n-1$ são números inteiros e $b^{n-1} \not\equiv 1(\text{mod } n)$ ou $b^n \not\equiv b(\text{mod } n)$, então $n$ é um número composto. O número $b$ é conhecido como uma testemunha do fato de $n$ ser composto (Coutinho, 2007).

**Exemplo:** Verificar se o número 117 é composto.

Devemos encontrar um inteiro $b$, tal que $b^{117} \not\equiv b(\text{mod } 117)$. Fazendo $b = 2$, temos

$$2^{117} = 2^{7\cdot 16+5} = (2^7)^{16} \cdot 2^5.$$

Sabemos que

$2^7 = 128 \equiv 11(\text{mod } 117) \Rightarrow 2^{117} \equiv 11^{16} \cdot 2^5 \equiv (11^2)^8 \cdot 2^5 \equiv (121)^8 \cdot 2^5 \equiv 4^8 \cdot 2^5 \equiv 2^{21}(\text{mod } 117)$.
Como $2^{21} = (2^7)^3$, temos

$$2^{21} \equiv 11^3 \equiv 121 \cdot 11 \equiv 4 \cdot 11 \equiv 44(\text{mod } 117),$$

o que implica, então, $2^{117} \equiv 44(\text{mod } 117)$, ou seja, $2^{117} \not\equiv 2(\text{mod } 117)$. Portanto, 117 é composto.

### Teste de Leibniz

Ainda considerando o Teorema de Fermat, Leibniz achava que se invertêssemos o Teorema de Fermat teríamos um teste de primalidade, isto é, considerando um número $n$ ímpar que satisfaz $b^{n-1} \equiv 1(\text{mod } n)$, para algum $1 < b < n-1$, poderíamos afirmar que $n$ era primo, o que não é verdade pois, por Leibniz, 341 seria um número primo, considerando que $2^{340-1} \equiv 1(\text{mod } 341)$, o que não é verdade também, pois $341 = 11 \cdot 31$. Estes "falsos primos" são conhecidos como pseudoprimos, isto é, um inteiro positivo $n$, ímpar e composto, é um pseudoprimo para a base $b$ (onde $1 < b < n-1$) se $b^{n-1} \equiv 1(\text{mod } n)$. Assim ,341 é um pseudoprimo para a base 2.

É importante ressaltar que o Teste de Leibniz não pode ser totalmente descartado, pois, por exemplo, entre 1 e $10^9$ existem 50847524 primos e apenas 5597 pseudoprimos para a base 2. Portanto, um número menor do que $10^9$ que passar no teste de Leibniz tem uma alta probabilidade de ser primo e ainda se fizermos o teste para mais de uma base, o teste ficará ainda mais eficiente. E como estamos limitando as bases de 1 a $n-1$, poderíamos considerar a possibilidade de testarmos se $n$ é pseudoprimo para todas as bases, o que seria impraticável quando temos o número $n$ muito grande.

**Definição 4.3** (Números de Carmichael)**.** *Chama-se número de Carmichael, todo número composto ímpar $n$ ($n > 0$) tal que $b^n \equiv b (\text{mod } n)$ para todo $1 < b < n-1$.*

**Observação 4.3.** *Convém observar que para ser um número de Carmichael, temos que ter n composto, pois um número primo p também satisfaz a equação $b^p \equiv b (\text{mod } p)$, mas não é um número de Carmichael.*

**Exemplo 4.1.** *O menor número de Carmichael é 561.*

### Teste de Miller

O Teste de Leibniz, através do Teorema de Fermat, consegue detectar se um número é composto com uma eficiência razoável, porém, o nosso interesse é descobrir se dado um número $n$, este é primo. Apesar da probabilidade disso acontecer ser alta pelo Teste de Leibniz, quando aumentarmos o número $n$, verificamos que o Teste de Leibniz se torna impraticável. O Teste de Miller, introduzido por G. L. Miller em 1976, vem melhorar muito o Teste de Leibniz, pois consegue encontrar números compostos mesmo entre os pseudoprimos.

**O teste:**

Seja $n$ um número inteiro positivo ímpar para o qual queremos testar a sua primalidade e a base inteira $b$, tal que $1 < b < n-1$. Como $n$ é ímpar, pode-se garantir que $n-1$ é par e, portanto, podemos fatorá-lo (dividindo $n-1$ por 2 sucessivamente) até encontrarmos $n-1 = 2^k \cdot q$, onde $q$ é um inteiro ímpar e $k \geq 1$.

O teste consiste em calcularmos a seguinte sequência de potência módulo $n$:

$$b^q,\ b^{2q},\ b^{2^2\cdot q},\ldots,b^{2^{k-1}\cdot q},\ b^{2^k\cdot q}.$$

Pelo Teste de Fermat, se $n$ for primo, temos que pelo menos uma destas potências tem que ser congruente a 1 módulo $n$, pois

$$b^{2^k\cdot q}\equiv b^{n-1}\equiv 1(\text{mod } n).$$

Seja $j$ o menor expoente tal que $b^{2^j\cdot q}\equiv 1(\text{mod } n)$. Se $j\geq 1$, podemos escrever

$$b^{2^j\cdot q}-1=\left(b^{2^{j-1}\cdot q}\right)^2-1^2=\left(b^{2^{j-1}\cdot q}-1\right)\cdot\left(b^{2^{j-1}\cdot q}+1\right).$$

Se $n$ é primo e divide $b^{2^j\cdot q}-1$, então $n$ divide $b^{2^{j-1}}-1$ ou $n$ divide $b^{2^{j-1}\cdot q}+1$. Pela minimalidade de $j$, $b^{2^{j-1}\cdot q}-1$ não pode ser divisível por $n$, logo temos que $b^{2^{j-1}\cdot q}+1$ é divisível por $n$, isto é,

$$b^{2^{j-1}\cdot q}\equiv -1(\text{mod } n).$$

Com os cálculos apresentados, concluímos que se $n$ é primo, então uma das potências $b^q,\ b^{2q},\ b^{2^2\cdot q},\ldots,b^{2^{k-1}\cdot q}$ tem que ser congruente a $-1$ módulo $n$, isto para $j\geq 1$. Se $j=0$, temos que $b^q\equiv 1(\text{mod } n)$, porém, essa congruência não nos permite aplicar o produto notável, considerando que $q$ é ímpar. Baseado nesses fatos, concluímos que, se $n$ é primo, então uma das sequências é congruente a $-1$ ou $b^q\equiv 1(\text{mod } n)$ e se nada disso ocorrer, então $n$ é composto.

**Algoritmo do teste de Miller**

Entrada: Inteiro ímpar $n$ que se quer verificar e a base $b$ inteira com $1<b<n-1$.

Saída: Uma mensagem que $n$ é composto ou teste inconclusivo.

**1º passo** Fatore $n-1$ até encontrar $q$ ímpar e $k$ inteiro, tais que $n-1=2^k\cdot q$.

**2º passo** Na sequência de potência $b^{2^j\cdot q}$, comece fazendo $j=0$ e $r=$ resto da divisão euclidiana de $b^q$ por $n$.

**3º passo** Se $j=0$ e $r=1$ ou se $j\geq 0$ e $r=n-1$ a saída é teste inconclusivo.

**4º passo** Faça $j=j+1$ e $r=r_2$, onde $r_2$ é o resto da divisão de $r^2$ por $n$.

**5º passo** Se $j<k$, volte ao 3º passo, senão a saída é $n$ é composto.

**Exemplo 1:** $n = 341$ (É bom lembrar que pelo Teste de Leibniz não concluímos que 341 é composto).

Entrada: $n = 341$ e $b = 2$ $(1 < b < n - 1)$, isto é, $1 < 2 < 340$.

**1º passo** $n - 1 = 2^k \cdot q$, assim $340 = 2^2 \cdot 85$. Logo, $k = 2$ e $q = 85$.

**2º passo** Na sequência de potência $b^{2^j \cdot q}$, para $j = 0$, temos $2^{2^0 \cdot 85} = 2^{85}$ e $r$ é igual ao resto de $2^{85}$ por 341. Calculamos o resto de $2^{85}$ por 341 e obtivemos 32, isto é, $2^{85} \equiv 32 (\text{mod } 341)$.

**3º passo** Como para $j = 0$, obtivemos resto diferente de 1 e de 340, passamos ao 4º passo.

**4º passo** Fazendo agora $j = 0 + 1 \Rightarrow j = 1$, isto é, $b^{2q} = 2^{2 \cdot 85} = 2^{170}$. Agora, calculamos o resto da divisão de $32^2$ por 341, isto é, $2^{85} \equiv 32 (\text{mod } 341)$

$(2^{85})^2 \equiv 32^2 (\text{mod } 341) \equiv 1 (\text{mod } 341)$ ou $2^{170} \equiv 1 (\text{mod } 341)$. Pelo algoritmo de Miller, concluímos que 341 é composto.

**Exemplo 2:** $n = 561$ e $b = 2$.

Entrada: $n = 561$ e base $b = 2$ $(1 < 2 < 560)$.

**1º passo** $560 = 2^4 \cdot 35$, logo $k = 4$ e $q = 35$.

**2º passo** Na sequência de potência $b^{2^j \cdot q}$, para $j = 0$, temos $2^{2^0 \cdot 35} = 2^{35}$ e $r$ é igual ao resto da divisão de $2^{35}$ por 561. Calculando o resto da divisão de $2^{35}$ por 561 obtivemos 263, isto é, $2^{35} \equiv 263 (\text{mod } 561)$.

**3º passo** Como para $j = 0$, obtivemos resto diferente de 1 e de 560, passamos ao 4º passo.

**4º passo** Fazendo agora $j = 0 + 1 \Rightarrow j = 1$, isto é, $b^{2q} = 2^{2 \cdot 35} = 2^{70}$. Agora, calculando o resto da divisão de $263^2$ por 561, encontramos 166, isto é, $2^{35} \equiv 263 (\text{mod } 561)$

$$2^{70} \equiv 263^2 (\text{mod } 561) \equiv 166 (\text{mod } 561).$$

Agora, para $j = 2$, temos $b^{2^2 \cdot q} = 2^{2^2 \cdot 35} = 2^{140}$ e como $2^{70} \equiv 166 (\text{mod } 561)$ implica que $2^{140} \equiv 166 (\text{mod } 561)$. Calculando o resto da divisão de $166^2$ por 561, obtivemos 67 e, portanto, $2^{140} \equiv 166^2 \equiv 67 (\text{mod } 561)$ ou $2^{140} \equiv 67 (\text{mod } 561)$.

E por último, para $j = 3$, temos que $b^{2^3 \cdot q} = 2^{8 \cdot 35} = 2^{280}$, então temos

$2^{140} \equiv 67 (\text{mod } 561)$, então $(2^{140})^2 \equiv 67^2 (\text{mod } 561) \Rightarrow 2^{280} \equiv 67^2 (\text{mod } 561)$. Calculando o resto da divisão de $67^2$ por 561, obtivemos 1, isto é, $2^{280} \equiv 67^2 \equiv 1 (\text{mod } 561)$ ou $2^{280} \equiv 1 (\text{mod } 561)$ e como calculamos todos os valores possíveis para $j (j < 4)$ e não encontramos resto que satisfazem o 3º passo do algoritmo, concluímos que 561 é composto.

Veremos agora um exemplo simples, para o qual temos que a saída do Teste de Miller é inconclusiva.

**Exemplo 3:** $n = 25$ e $b = 7$.

Entrada: $n = 25$ e base $b = 7$ $(1 < 7 < 24)$

**1º passo** $24 = 2^3 \cdot 3$, logo $k = 3$ e $q = 3$.

**2º passo** Na sequência de potência $b^{2^j \cdot q}$, para $j = 0$, temos $7^{2^0 \cdot 3} = 7^3$ e $r$ é o resto da divisão de $7^3$ por 25. Calculando o resto da divisão de $7^3$ por 25, obtivemos 18, isto é, $7^3 \equiv 18 (\text{mod } 25)$.

**3º passo** Como para $j = 0$, obtivemos resto diferente de 1 e de 24, passamos para 4º passo.

**4º passo** Fazendo agora $j = 0 + 1 \Rightarrow j = 1$, isto é, $b^{2q} = 7^{2 \cdot 3} = 7^6$ e agora calculando o resto da divisão de $18^2$ por 25 encontramos 24, isto é, $7^3 \equiv 18 (\text{mod } 25) \Rightarrow (7^3)^2 \equiv 18^2 (\text{mod } 25) \Rightarrow 7^6 \equiv 18^2 \equiv 24 (\text{mod } 25)$.

Observe então que o resto $r = n - 1$ ou $r = 25 - 1 \Rightarrow r = 24$ e pelo passo 3 temos que o teste é inconclusivo, apesar de sabermos que 25 é composto. Se aplicássemos o mesmo teste para base 2, iríamos chegar facilmente que 25 é composto.

**Definição 4.4** (Pseudoprimo Forte)**.** *É todo número inteiro r composto que tem resultado inconclusivo para o Teste de Miller com respeito a uma base b, dizemos neste caso que n é um pseudoprimo forte para a base b.*

Assim, por exemplo, 25 é um pseudoprimo forte para a base 7. É importante lembrar que 25 não é pseudoprimo forte para a base 2 e que se um número inteiro é pseudoprimo forte para uma determinada base, ele também será pseudoprimo para esta mesma base.

Uma prova da utilidade do Teste de Miller é que existem apenas 1282 pseudoprimos fortes entre 1 e 1 bilhão ($10^9$). É claro que o Teste de Miller só aumenta a sua eficácia à medida que

aplicamos o teste para várias bases. Se o Teste de Miller tem saída inconclusivo quando aplicado para mais de $n/4$ base entre 1 e $n-1$, então podemos garantir que $n$ é primo. Essa demonstração pode ser encontrada em Lemos (1989).

### Fatoração por Fermat

Fermat criou um método (algoritmo) de fatoração muito eficiente quando o número $n$, a ser fatorado, tem um fator primo que não é muito menor que sua raiz quadrada ( $\sqrt{n}$).

A ideia do algoritmo criado por Fermat é a seguinte:

Seja $n$ um número inteiro $n$ ímpar, então tenta-se achar números inteiros positivos $x$ e $y$, tais que $n = x^2 - y^2$, ou seja, $n = (x+y)(x-y)$, então temos que $x+y$ e $x-y$ são os fatores de $n$.

Observe que se $y > 0$, então $n = x^2 - y^2$ ou $x^2 = n + y^2$ ou ainda $x = \sqrt{n+y^2} \geq \sqrt{n}$.

**Observação 4.4.** *Se r é um número real, denotamos sua parte inteira por* $[r]$.

**Exemplos:** $[2,63] = 2,\ [\sqrt{45}] = 6,\ [8] = 8.$

**Algoritmo de Fermat**

Entrada: inteiro positivo ímpar $n$.

Saída: uma mensagem que $n$ é primo ou um fator de $n$.

**1º passo** Comecemos com $x = [\sqrt{n}]$ (parte inteira de $\sqrt{n}$); se $n = x^2$, então $x$ é um fator de $n$ e, portanto, concluímos que $n$ é composto.

**2º passo** Caso contrário, some uma unidade a $x$ e calcule $y = \sqrt{x^2 - n}$.

**3º passo** Repetimos o 2º passo até encontrarmos um valor inteiro para $y$, caso isto ocorra, $n$ tem fatores $x+y$ e $x-y$, porém, se não encontramos nenhum valor inteiro para $y$ até que $x$ seja igual a $\dfrac{n+1}{2}$, concluímos que $n$ é primo.

**Exemplo:** Seja $n = 10217593$.

**1º passo** Façamos $x = [\sqrt{10217593}] = 3196$. Devemos observar que $3196^2 = 10214416 < 10217593$.

**2º passo** Somando-se uma unidade a $x = 3196$, encontramos $x = 3197$ e então $y = \sqrt{x^2 - n} = \sqrt{3197^2 - 10217593} = 56,709\ldots$

**3º passo** Repetindo o processo,teremos

| x | $y = \sqrt{x^2 - 10217593}$ |
|---|---|
| 3197 | $56,709\ldots$ |
| 3198 | $98,035\ldots$ |
| 3199 | $126,522\ldots$ |
| 3200 | $149,689\ldots$ |
| 3201 | $169,729\ldots$ |
| 3202 | $187,645\ldots$ |
| 3203 | 204 |

Obtivemos, então, o inteiro 204 para a 7ª etapa e, portanto, $x = 3203$ e $y = 204$. Então< os fatores de $n$ são $x + y = 3407$ e $x - y = 2999$. Logo, concluímos que $n = (x + y)(x - y)$, ou seja, $10217593 = 3407 \cdot 2999$.

**Exemplo:** Seja $n = 23$, temos então:

**1º passo:** $x = [\sqrt{23}] = 4,\ 4^2 = 16 < 23.$

**2º passo / 3ºpasso:**

| x | $y - \sqrt{x^2 - 23}$ |
|---|---|
| 5 | $1,414\cdots$ |
| 6 | $3,605\cdots$ |
| 7 | $5,099\cdots$ |
| 8 | $6,403\cdots$ |
| 9 | $7,615\cdots$ |
| 10 | $8,774\cdots$ |
| 11 | $9,899\cdots$ |
| 12 | 11 |

Como só achamos o inteiro $y$ para $x = \dfrac{n+1}{2}$ ou $\dfrac{23+1}{2} = 12$, concluímos que 23 é primo.

A demonstração do algoritmo de Fermat pode ser encontrada em Coutinho (2007).

**Teste de Agrawal-Kayal-Saxena (AKS)**

Recentemente, os algoritmos para testar a primalidade de um número $n$ ou eram determinísticos, porém, com difícil implantação, quando $n$ crescia muito, ou probabilísticos, isto é, não forneciam com absoluta certeza se $n$ era primo ou não. Somente em 2002, o professor Manindra Agrawal e seus dois alunos de doutorado, Neeraj Kayal e Nitin Saxena, do Departamento de Ciência da Computação e Engenharia do Instituto Indiano de Tecnologia em Kampur, construíram um teste de primalidade determinístico em tempo polinomial, bastante eficaz sem ter que considerar conjecturas.

Hoje em dia esse algoritmo é conhecido como AKS, em homenagem aos seus criadores, considerando as iniciais dos respectivos nomes. Tal fato histórico foi visto pelos especialistas como muito simples.

Para maiores detalhes, consultar Coutinho (2004).

# Referências Bibliográficas


[1] AGRAWAL, M., KAYAL, N., SAXENA, N. **Primes is in P. Indian Institute of Tecnology Kanpur**. Disponível em: http://www.cse.utk.ac.in/news/primality.pdf / . Acesso em 14.jan.2009.

[2] ALENCAR FILHO E. **Teoria elementar dos números.** 3.ed. São Paulo: Nobel, 1985. 386p.

[3] ALENCAR FILHO E. **Teoria das congruências.** São Paulo: Nobel, 1986. 220p.

[4] ARGOLO, P. Divisores, múltiplos e decomposição em fatores primos: algumas considerações pedagógicas. **Revista do Professor de Matemática,** n.20, p. 31-32, jan./abr. 1992.

[5] ÁVILA, G. **A distribuição dos números primos.** Revista do Professor de Matemática, n.19, jul./dez. 1991.

[6] CARDOSO, M.L., GONÇALVES, O.A. Uma interpretação geométrica do MMC. **Revista do Professor de Matemática,** n.32, p. 27-28, set./dez. 1996.

[7] COUTINHO, S.C. **Números inteiros e criptografia RSA.** 2.ed. 4.imp. Rio de Janeiro: IMPA, 2005. 226p.

[8] COUTINHO, S.C. **Primalidade em tempo polinomial**: uma introdução ao algoritmo AKS. Rio de Janeiro: SBM, 2004. 105p.

[9] COSTA, G.C. **Um estudo sobre a complexidade computacional do problema de decidir a primalidade de um número.** 2007. Monografia (Graduação em Matemática Licenciatura) - Faculdade Jesus Maria José, Taguatinga - DF, 2007.

[10] DOMINGUES, H.H., IEZZI, G. **Álgebra moderna.** 4.ed. reform. São Paulo: Atual, 2003. 368p.

[11] DOMINGUES, H.H. **Fundamentos de aritmética.** São Paulo: Atual, 1991.

[12] FONSECA, R.V. Números perfeitos, amigos e sociáveis. **Revista do Professor de Matemática,** n.41, p. 34-37, set./dez. 1999.

[13] GONÇALVES, A. **Introdução à álgebra.** 5.ed. 3.imp. Rio de Janeiro: IMPA, 2005. 194p.

[14] GOMES, O.R., SILVA, J.C. **Estruturas algébricas para licenciatura**: introdução à teoria dos números. Brasília, 2008. 208p.

[15] GUEDES, M.G.P. Outros critérios de divisibilidade. **Revista do Professor de Matemática,** n.12, p. 24-27, jan./jun. 1988.

[16] HEFEZ, A. **Elementos de aritmética.** 2.ed. Rio de Janeiro: SBM, 2006. 169p.

[17] LEMOS, M. **Criptografia, números primos e algoritmos.** Rio de Janeiro: IMPA, 2005. 72p.

[18] LANDAU, E.G.H. **Teoria elementar dos números.** Rio de Janeiro: Ciência Moderna, 2002. 292p.

[19] MILIES, C.P., COELHO, S.P. **Números**: uma introdução à matemática. 3.ed. 2.reimp. São Paulo: USP, 2006. 240p.

[20] MOREIRA, C.G., SALDANHA, N. **Primos de Mersenne (e outros primos muito grandes).** 3.ed. Rio de Janeiro: IMPA, 2008. 87p.

[21] MAIER, R.R. **Teoria dos números.** Brasília: UnB - Departamento de Matemática, 2003. (Texto de aula).

[22] NEVES,V. **Introdução à teoria dos números.** [s.l.]: Universidade de Aveiro, 2001. (Texto de aula).

[23] NERY, C., POSSANI, C. Os primos esquecidos. **Revista do Professor de Matemática,** n.47, p. 16-20, set./dez. 2001.

[24] OLIVEIRA, Z.C. Uma interpretação geométrica do MDC. **Revista do Professor de Matemática,** n.29, set./dez. 1995.

[25] PATERLINI, R.R. Um método para o cálculo do MDC e do MMC. **Revista do Professor de Matemática,** n.13, p. 34-37, jul./dez. 1988.

[26] POLEZZI, M. Como obter o MDC e o MMC sem fazer contas? **Revista do Professor de Matemática**, n.51, jan./abr. 2003.

[27] SAMPAIO, J.C.V., CAETANO, P.A.S. **Introdução à teoria dos números**: um curso breve. São Carlos: EDUFSCAR, 2008. 109p.

[28] SANTOS, J.P.O. **Introdução à teoria dos números.** 3.ed. Rio de Janeiro: IMPA, 2006. 198p.

[29] SHOKRANIAN, S. **Uma introdução à teoria dos números.** Rio de Janeiro: Ciência Moderna Ltda, 2008. 233p.

[30] SHOKRANIAN, S., SOARES, M., GODINHO, H. **Teoria dos números.** 2.ed. Brasília: UnB, 1999. 325p.

[31] SOUZA, B.A. **Teoria dos números e o RSA.** 2004. Dissertação (Mestrado em Matemática Aplicada) - Universidade Estadual de Campinas, Campinas, 2004.

[32] TÁBOAS, C.M.G., RIBEIRO, H.S. Sobre critério de divisibilidade. **Revista do Professor de Matemática**, n.6, p. 21-24, jan./jun. 1985.

[33] TORRES, G.Z. Divisibilidade por 3, 7, 9, 11, 13, 17, ... **Revista do Professor de Matemática,** n.58, p. 13-17, set./dez. 2005.

[34] UMBELINO JUNIOR, A. Divisibilidade por 7. **Revista do Professor de Matemática,** n.43, p. 38-39, maio/ago. 2000.

[35] VIDIGAL, A., AVRITZER, D., FARIAS e SOARES, E. et al. **Fundamentos de álgebra.** Belo Horizonte: UFMG, 2005. 199p.

[36] WATANABE, R.G. Uma fórmula para números primos. **Revista do Professor de Matemática,** n.37, maio/ago. 1998.