

UNIVERSIDADE DE BRASÍLIA  
DEPARTAMENTO DE MATEMÁTICA -IE

# TEORIA DOS NÚMEROS

Texto de aula

PROFESSOR RUDOLF R. MAIER

Versão atualizada

2005

Estas notas são o resultado da experiência nas aulas do curso  
do mesmo título, proferido regularmente pelo autor neste  
Departamento de Matemática.

Durante o curso e na elaboração destas notas fizemos livre uso e seguimos com  
modificações e complementações à linha do livro

## ELEMENTARY NUMBER THEORY

de David M. Burton

Revised Printing

University of New Hampshire

Allyn and Bacon, Inc.

Boston·London·Sydney·Toronto

©1980

# Índice

§ 1	<b>Resultados Preliminares</b> .....	1
	O princípio da indução	
	O teorema binomial	
	As fórmulas para $S_n(m) = \sum_{k=1}^n k^m$	
	Os números triangulares	
	Algumas observações sobre lógica elementar	
	Diferença de dois quadrados	
§ 2	<b>Teoria de divisibilidade nos números inteiros</b> ...	21
	O algoritmo geral de divisão	
	Máximo divisor comum de dois números	
	Números relativamente primos	
	O algoritmo EUCLIDIANO	
	O mínimo múltiplo comum	
	Equações DIOFANTINAS	
§ 3	<b>Números primos e sua distribuição</b> .....	34
	O teorema fundamental da aritmética	
	A quantidade dos divisores de um número $n$	
	A decomposição primária de $n!$	
	Estimativas sobre quantidades de primos	
	A função $\pi$ dos números primos	
	Decomposição de números e o crivo do ERATÓSTENES	
	A conjectura de GOLDBACH	
	Progressões aritméticas e primos	
	Polinômios e primos	
§ 4	<b>Triplos PITAGÓRICOS e a conjectura de FERMAT</b> ...	53
	Triplos PITAGÓRICOS	
	A conjectura de FERMAT	

§ 5	<b>Números deficientes-abundantes-perfeitos e de MERSENNE</b> .....	61
	Números deficientes, abundantes e perfeitos	
	O teorema de EUCLIDES/EULER	
	Números de MERSENNE	
§ 6	<b>A teoria das congruências</b> .....	69
	Divisibilidade e congruências	
	Congruências lineares	
	Congruências simultâneas e o teorema do resto chinês	
§ 7	<b>Os Teoremas de FERMAT e de WILSON</b> .....	78
	O pequeno teorema de FERMAT	
	O teorema de WILSON	
§ 8	<b>Congruências quadráticas e a lei da reciprocidade quadrática de EULER/GAUSS</b> .....	85
	Restos quadráticos	
	Um Lema de EULER	
	O símbolo de LEGENDRE	
	Um Lema de GAUSS	
	O símbolo de LEGENDRE $\left(\frac{2}{p}\right)$	
	A lei da reciprocidade quadrática	
	Mais alguns símbolos de LEGENDRE especiais	
§ 9	<b>Representação de inteiros como soma de quadrados</b> .....	105
	Soma de dois quadrados	
	Soma de três quadrados	
	Soma de quatro quadrados (o teorema de LAGRANGE)	
§ 10	<b>A função <math>\varphi</math> de EULER</b> .....	114
	Restos relativamente primos e a função $\varphi$	
	O teorema de EULER	
	Mais algumas propriedades da função $\varphi$	
§ 11	<b>Raízes primitivas</b> .....	123
	Ordens módulo $n$ e raízes primitivas	
	Existência de raízes primitivas.	

# TEORIA DOS NÚMEROS

Notas de aula - Versão atualizada 2005

PROF. RUDOLF R. MAIER

## § 1 Resultados Preliminares

A Teoria dos Números, a mais pura disciplina dentro da mais pura das Ciências - da Matemática - tem uma longa história, originando-se nas antigas civilizações da humanidade. Listamos primeiro alguns nomes famosos de matemáticos que voltarão a aparecer no contexto do nosso curso:

<b>Pitagoras</b>	(569-500 a. C.)
<b>Euclides</b>	( $\approx$ 350 a. C.)
<b>Eratóstenes</b>	(276-196 a. C.)
<b>Diofantos</b>	( $\approx$ 250 d. C.)
<b>Plutarco</b>	( $\approx$ 100 d. C.)
<b>Marin Mersenne</b>	(1588-1648)
<b>Pierre de Fermat</b>	(1601-1665)
<b>Blaise Pascal</b>	(1623-1662)
<b>Christian Goldbach</b>	(1690-1764)
<b>Leonhard Euler</b>	(1707-1783)
<b>Joseph Louis Lagrange</b>	(1736-1813)
<b>John Wilson</b>	(1741-1793)
<b>Adrien Marie Legendre</b>	(1752-1833)
<b>Carl Friedrich Gauss</b>	(1777-1855)
<b>Augustin Louis Cauchy</b>	(1789-1857)
<b>Peter Gustav Dirichlet</b>	(1805-1859)
<b>P. L. Tchebychef</b>	(1821-1894)
<b>Frederick Nelson Cole</b>	(1861-1927)
<b>Axel Thue</b>	(1863-1922)
<b>Jacques Salomon Hadamard</b>	(1865-1963)
<b>Charles de la Vallée Poussin</b>	(1866-1962)

Dedicaremos os nossos estudos durante este curso às propriedades dos  
*números inteiros racionais.*

Lidaremos então com o conjunto

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

dos números inteiros e seus subconjuntos, particularmente com os subconjuntos

$$\mathbb{N}_0 = \{ 0, 1, 2, 3, \dots \} \quad \text{e} \quad \mathbb{N} = \{ 1, 2, 3, \dots \}$$

dos números *inteiros não-negativos* e dos *números naturais*.

Iniciamos, lembrando exemplos de algumas seqüências importantes no conjunto  $\mathbb{N}$  dos números naturais:

### 1.1 Exemplo.

*Seqüências importantes em  $\mathbb{N}$  são: A seqüência*

- a)  $(n)_{n \in \mathbb{N}} = (1, 2, 3, \dots, n, \dots)$  *de todos os números naturais,*
- b)  $(2n)_{n \in \mathbb{N}} = (2, 4, 6, \dots, 2n, \dots)$  *dos números naturais pares,*
- c)  $(2n-1)_{n \in \mathbb{N}} = (1, 3, 5, \dots, 2n-1, \dots)$  *dos números ímpares,*
- d)  $(n^2)_{n \in \mathbb{N}} = (1, 4, 9, \dots, n^2, \dots)$  *dos quadrados perfeitos,*
- e)  $(n^3)_{n \in \mathbb{N}} = (1, 8, 27, \dots, n^3, \dots)$  *dos cubos perfeitos,*
- f)  $(2^n)_{n \in \mathbb{N}} = (2, 4, 8, \dots, 2^n, \dots)$  *das potências de 2*
- g)  $(p_n)_{n \in \mathbb{N}} = (2, 3, 5, \dots, p_n, \dots)$  *dos números primos,*
- h) *etc.*

Dizemos também:  $n$  é o  $n$ -ésimo número natural,  $2n$  é o  $n$ -ésimo número par,  $2n - 1$  é o  $n$ -ésimo número ímpar,  $n^2$  é o  $n$ -ésimo quadrado perfeito, etc.

Temos *duas operações internas* em  $\mathbb{N}_0$  e também em  $\mathbb{Z}$  a *adição*  $+$  e a *multiplicação*  $\cdot$  as quais queremos admitir sem mais explicações.

A *ordem natural* em  $\mathbb{Z}$  é dada por:  $\forall n, m \in \mathbb{Z}$  temos

$$m \leq n \iff \text{a equação } m + x = n \text{ possui uma solução } x \in \mathbb{N}_0.$$

Uma fundamental propriedade do conjunto  $\mathbb{N}$  dos números naturais é:

## O PRINCÍPIO DA INDUÇÃO.

*Todo conjunto não vazio  $S$  de números naturais possui um elemento mínimo.  
Em símbolos:*

$$\forall S \subseteq \mathbb{N}, S \neq \emptyset, \exists m \in S \text{ tal que } m \leq n \forall n \in S.$$

Deste princípio segue a importante

### 1.2 Proposição.

*Seja  $T$  um conjunto de números naturais (i.e.  $T \subseteq \mathbb{N}$ ) satisfazendo às propriedades:*

- a)  $1 \in T$
- b) *Sempre se  $n \in T$ , então também  $n+1 \in T$ .*

*Então  $T = \mathbb{N}$  é o conjunto de todos os números naturais.*

**Demonstração:** Suponhamos  $T \neq \mathbb{N}$ . Para o conjunto complementar  $S = \mathbb{N} \setminus T$  temos então  $\emptyset \neq S \subseteq \mathbb{N}$ . Pelo princípio da indução existe  $m \in S$  tal que  $m \leq n$  para todos os  $n \in S$ . Como  $1 \in T$  pela propriedade a), temos  $1 \notin S$ , particularmente  $m > 1$ . Daí concluímos  $n = m-1 \in T$ . Pela propriedade b) temos porém  $m = n+1 \in T$ , de onde sai o absurdo  $m \in S \cap T = \emptyset$ . Isto mostra que  $S \neq \emptyset$  é impossível. Temos que ter  $S = \emptyset$  e daí  $T = \mathbb{N}$ . ■

Proposição 1.2 aplica-se para verificar a validade geral de fórmulas as quais envolvem números naturais, como mostra o seguinte

### 1.3 Exemplo.

*Para todos os números naturais  $n$  vale*

$$1 + 3 + 5 + \dots + (2n-3) + (2n-1) = n^2 \quad (*).$$

Em palavras: A soma dos  $n$  primeiros números naturais ímpares é o  $n$ -ésimo quadrado perfeito.

**Demonstração:** Seja  $T = \left\{ n \in \mathbb{N} \mid \sum_{k=1}^n (2k-1) = n^2 \right\}$  o conjunto dos números naturais para os quais a fórmula (\*) é verdadeira (o "conjunto verdade" ou o "conjunto de validade" de (\*)). Para mostrar que  $T = \mathbb{N}$ , só é preciso verificar a) e b)

da Proposição 1.2 para este  $T$ :

Para  $n = 1$  (\*) simplesmente afirma que  $1 = 1^2$ , o que certamente é verdade, ou seja,  $1 \in T$ .

Suponhamos  $n \in T$  para algum número natural  $n$ , isto é,

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

Somando-se  $2n+1$  a ambos os lados, obtemos

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

de onde segue

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

Isto por sua vez significa  $n+1 \in T$ . Pela proposição concluímos que o conjunto verdade da fórmula (\*) é o conjunto  $T = \mathbb{N}$  de todos os números naturais. ■

#### 1.4 Exemplo.

Para todos os números naturais  $n$  e todo real  $a \neq 1$  vale

$$1 + a + a^2 + a^3 + \dots + a^{n-1} + a^n = \frac{a^{n+1} - 1}{a - 1} .$$

Particularmente (quando  $a = 2$ ) obtemos

$$1 + 2 + 4 + \dots + 2^{n-1} + 2^n = 2^{n+1} - 1 .$$

**Demonstração:** Mais uma vez temos que verificar a asserção para  $n = 1$  e para  $n+1$  sob a hipótese que ela já é válida para algum  $n$ :

Para  $n = 1$  simplesmente afirma-se que  $1+a = \frac{a^2-1}{a-1}$ , o que é verdade (porquê?).

Suponhamos, para algum número natural  $n$  já esteja provado

$$1 + a + a^2 + a^3 + \dots + a^{n-1} + a^n = \frac{a^{n+1} - 1}{a - 1} .$$

Somando-se  $a^{n+1}$  a ambos os lados, obtemos

$$1 + a + a^2 + \dots + a^{n-1} + a^n + a^{n+1} = \frac{a^{n+1} - 1}{a - 1} + a^{n+1} ,$$



de onde segue

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

Isto diz que a fórmula continua válida para  $n+1$ . Concluímos que ela vale para todo  $n \in \mathbb{N}$ .

■

Mencionamos que, às vezes é conveniente trabalhar com a seguinte generalização de 1.2:

### 1.2' Proposição.

Seja  $n_0 \in \mathbb{Z}$  um inteiro fixo e seja  $T'$  um conjunto de (alguns) números inteiros maiores ou iguais a  $n_0$  (i.e.  $T' \subseteq \{n \mid n_0 \leq n \in \mathbb{Z}\}$ ), satisfazendo às propriedades:

- a)  $n_0 \in T'$
- b) Sempre se  $n_0 \leq n \in T'$ , então também  $n+1 \in T'$ .

Então  $T' = \{n \mid n_0 \leq n \in \mathbb{Z}\}$  é o conjunto de todos os números inteiros maiores ou iguais a  $n_0$ .

Isto é facilmente verificado pela aplicação de 1.2 ao conjunto

$$T = \{n - n_0 + 1 \mid n \in T'\} .$$

Observamos que para este  $T$  temos  $T \subseteq \mathbb{N}$  e  $n_0 \in T'$  é equivalente a  $1 \in T$ . (1.2 é obtido de volta a partir de 1.2' fazendo-se  $n_0 = 1$ ).

A título de ilustração mencionamos o seguinte exemplo. A afirmação (correta) que o leitor queira verificar:

$$2^n > n^2 \quad \text{para todos os } n \geq 5$$

podemos substituir pela afirmação equivalente

$$2^{n+4} > (n + 4)^2 \quad \text{para todos os } n \in \mathbb{N}$$

(ou também por

$$2^{n+783} > (n + 783)^2$$

para todos os  $n \in \mathbb{Z}$  com  $n \geq -778$ , se quisermos).

## O TEOREMA BINOMIAL

Se  $n \in \mathbb{N}_0$  entendemos por  $n!$  o produto

$$n! = \prod_{k=1}^n k = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n, \quad \text{se } n \in \mathbb{N}$$

e acrescentamos

$$0! = 1, \quad \text{se } n = 0 \quad (\text{produto vazio}).$$

$n!$  lê-se:  $n$  fatorial.

É imediato que se tem  $0! = 1! = 1$ ,  $2! = 2$ ,  $3! = 2! \cdot 3 = 6$ ,  $4! = 3! \cdot 4 = 24$ ,  $\dots$ ,  $n! = (n-1)! \cdot n$ ,  $(n+1)! = n! \cdot (n+1)$ ,  $\dots$ .

**1.5 Definição.** Para todo  $n \in \mathbb{N}$  e todos os  $k \in \mathbb{N}_0$  com  $0 \leq k \leq n$  colocamos

$$\binom{n}{k} = \frac{n!}{k!(n-k)!},$$

número este que se chama o *coeficiente binomial*  $n$  sobre  $k$ .

Temos as seguintes propriedades dos coeficientes binomiais:

### 1.6 Observação.

Para todo  $n \in \mathbb{N}$  e todos os  $k \in \mathbb{N}_0$  com  $0 \leq k \leq n$  valem

- $\binom{n}{k} = \frac{n(n-1) \cdot \dots \cdot (n-k+1)}{k!}$ .
- $\binom{n}{k} = \binom{n}{n-k}$ .
- $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$  se  $k \geq 1$ .

**Demonstração:** a)  $\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1) \cdot \dots \cdot (n-k+1) \cdot (n-k) \cdot \dots \cdot 2 \cdot 1}{k!(n-k)!} = \frac{n(n-1) \cdot \dots \cdot (n-k+1)}{k!}$ .

b) Observamos primeiro que com  $0 \leq k \leq n$  temos também  $0 \leq n-k \leq n$ . Pela definição temos de imediato

$$\binom{n}{n-k} = \frac{n!}{(n-k)![n-(n-k)]!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}.$$

c) Se  $k \geq 1$  calculamos

$$\begin{aligned} \binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)![n-(k-1)]!} = \frac{n!(n-k+1) + n!k}{k!(n-k+1)!} = \\ &= \frac{n!(n+1)}{k!(n-k+1)!} = \frac{(n+1)!}{k![(n+1)-k]!} = \binom{n+1}{k}. \end{aligned}$$

■

Eis alguns valores específicos de coeficientes binomiais:

$$\binom{n}{0} = \binom{n}{n} = 1, \quad \binom{n}{1} = \binom{n}{n-1} = n, \quad \binom{n}{2} = \binom{n}{n-2} = \frac{n(n-1)}{2}.$$

Podemos enunciar e provar agora o fundamental

*teorema do desenvolvimento binomial:*

### 1.7 Teorema.

Para todo  $n \in \mathbb{N}$  e todos os números reais  $a, b$  temos

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k,$$

por extenso:

$$\begin{aligned} &(a+b)^n = \\ &= \binom{n}{0} a^n b^0 + \binom{n}{1} a^{n-1} b^1 + \binom{n}{2} a^{n-2} b^2 + \dots + \binom{n}{k} a^{n-k} b^k + \dots + \binom{n}{n-1} a^1 b^{n-1} + \binom{n}{n} a^0 b^n. \end{aligned}$$

**Demonstração:** Demonstraremos isto por indução sobre o expoente  $n$ , isto é, provaremos  $1 \in T$  e a implicação " $n \in T \Rightarrow n+1 \in T$ ", quando  $T$  é o conjunto de validade da fórmula.

Para  $n = 1$  afirma-se que  $(a+b)^1 = \sum_{k=0}^1 \binom{1}{k} a^{1-k} b^k = \binom{1}{0} a^{1-0} b^0 + \binom{1}{1} a^{1-1} b^1$ , sendo

igual a  $a+b$  de ambos os lados, i.e.  $1 \in T$ .

Suponhamos então que, para algum  $n \in \mathbb{N}$ , já esteja provado

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k \quad (*)$$

e provamos a validade para  $n+1$ . Para isto multiplicamos os dois lados de (\*) por  $(a + b)$  e obtemos, usando-se a observação 1.6 c):

$$\begin{aligned}
 (a + b)^{n+1} &= \left( \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k \right) (a + b) = \\
 & \sum_{k=0}^n \binom{n}{k} a^{n-k+1} b^k + \sum_{k=0}^n \binom{n}{k} a^{n-k} b^{k+1} = \\
 &= a^{n+1} + \sum_{k=1}^n \binom{n}{k} a^{n-k+1} b^k + \sum_{k=0}^{n-1} \binom{n}{k} a^{n-k} b^{k+1} + b^{n+1} = \\
 &= a^{n+1} + b^{n+1} + \sum_{k=1}^n \binom{n}{k} a^{n-k+1} b^k + \sum_{k=1}^n \binom{n}{k-1} a^{n-k+1} b^k = \\
 &= a^{n+1} + b^{n+1} + \sum_{k=1}^n \left[ \binom{n}{k} + \binom{n}{k-1} \right] a^{n+1-k} b^k = a^{n+1} + b^{n+1} + \sum_{k=1}^n \binom{n+1}{k} a^{n+1-k} b^k = \\
 &= \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k,
 \end{aligned}$$

isto é,

$$(a + b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k .$$

Isto significa que, a partir da suposta validade da fórmula (\*) para algum  $n$ , conseguimos provar a sua validade para  $n+1$  (i.e.  $n \in T \Rightarrow n+1 \in T$ ). Concluimos que (\*) tem validade para todo  $n \in \mathbb{N}$ . ■

É usual, escrever-se os coeficientes binomiais  $\binom{n}{k}$  (acrescentando-se ainda  $\binom{0}{0} = 1$ ), ordenados no chamado *Triângulo de PASCAL*, cuja  $n$ -ésima linha fornece então os coeficientes no desenvolvimento de  $(a + b)^n$  para  $n = 0, 1, 2, 3, \dots$

$$\begin{array}{ccccccc}
 & & & & & & \binom{0}{0} \\
 & & & & & & \binom{1}{0} & \binom{1}{1} \\
 & & & & & & \binom{2}{0} & \binom{2}{1} & \binom{2}{2} \\
 & & & & & & \binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} \\
 & & & & & & \dots & \dots & \dots & \dots \\
 & & & & & & \binom{n}{0} & \binom{n}{1} & \dots & \binom{n}{k-1} & \binom{n}{k} & \dots & \binom{n}{n-1} & \binom{n}{n} \\
 & & & & & & \binom{n+1}{0} & \binom{n+1}{1} & \dots & \binom{n+1}{k} & \dots & \binom{n+1}{n} & \binom{n+1}{n+1} \\
 & & & & & & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots
 \end{array}$$

Vemos ainda a visualização da fórmula 1.6 c), a qual diz como o termo  $\binom{n+1}{k}$  da  $(n+1)$ -ésima linha no triângulo de Pascal é obtido como soma dos termos vizinhos  $\binom{n}{k-1}$  e  $\binom{n}{k}$  da linha anterior.

Disto conclui-se facilmente por indução sobre  $n$  a

## 1.8 Conseqüência.

*Os coeficientes binomiais são números inteiros.*

AS FÓRMULAS PARA  $S_n(m) = \sum_{k=1}^n k^m$

**1.9 Definição.** Para todo  $n \in \mathbb{N}$  e todo  $m \in \mathbb{N}_0$  colocamos

$$S_n(m) = \sum_{k=1}^n k^m = 1^m + 2^m + 3^m + \dots + n^m,$$

isto é,  $S_n(m)$  é a soma das  $n$  primeiras  $m$ -ésimas potências.

Por exemplo,

$$S_n(0) = 1^0 + 2^0 + 3^0 + \dots + n^0 = n,$$

$$S_n(1) = 1^1 + 2^1 + 3^1 + \dots + n^1 = 1 + 2 + 3 + \dots + n$$

é a soma dos primeiros  $n$  números naturais,

$$S_n(2) = 1^2 + 2^2 + 3^2 + \dots + n^2 = 1 + 4 + 9 + \dots + n^2$$

é a soma dos primeiros  $n$  quadrados perfeitos,

$$S_n(3) = 1^3 + 2^3 + 3^3 + \dots + n^3 = 1 + 8 + 27 + \dots + n^3$$

é a soma dos primeiros  $n$  cubos perfeitos, etc.

Como podemos obter fórmulas fechadas para  $S_n(m)$ ?

A seguinte *fórmula recursiva* permite calcular  $S_n(m)$  a partir das fórmulas anteriores  $S_n(0) = n$ ,  $S_n(1)$ ,  $S_n(2)$ ,  $\dots$ ,  $S_n(m-1)$ :

### 1.10 Teorema.

Para todos os  $n, m \in \mathbb{N}$  vale

$$(m+1) \cdot S_n(m) = (n+1)^{m+1} - 1 - \sum_{k=0}^{m-1} \binom{m+1}{k} S_n(k).$$

Por extenso:

$$\begin{aligned} & (m+1) \cdot S_n(m) = \\ & = (n+1)^{m+1} - 1 - \binom{m+1}{0} S_n(0) - \binom{m+1}{1} S_n(1) - \binom{m+1}{k} S_n(k) - \dots - \binom{m+1}{m-1} S_n(m-1). \end{aligned}$$

**Demonstração:** Desenvolvemos primeiro a expressão  $(1+x)^{m+1}$  pelo teorema binomial:

$$(1+x)^{m+1} = \sum_{k=0}^{m+1} \binom{m+1}{k} x^k,$$

por extenso,

$$(1+x)^{m+1} = 1 + \binom{m+1}{1} x^1 + \binom{m+1}{2} x^2 + \dots + \binom{m+1}{k} x^k + \dots + \binom{m+1}{m-1} x^{m-1} + \binom{m+1}{m} x^m + x^{m+1}.$$

Colocando-se  $x = 1, 2, \dots, \ell, \dots, n$ , obtemos

$$2^{m+1} = 1 + \binom{m+1}{1} 1^1 + \binom{m+1}{2} 1^2 + \dots + \binom{m+1}{k} 1^k + \dots + \binom{m+1}{m-1} 1^{m-1} + \binom{m+1}{m} 1^m + 1^{m+1}$$

$$3^{m+1} = 1 + \binom{m+1}{1} 2^1 + \binom{m+1}{2} 2^2 + \dots + \binom{m+1}{k} 2^k + \dots + \binom{m+1}{m-1} 2^{m-1} + \binom{m+1}{m} 2^m + 2^{m+1}$$

.....

$$(\ell+1)^{m+1} = 1 + \binom{m+1}{1} \ell^1 + \binom{m+1}{2} \ell^2 + \dots + \binom{m+1}{k} \ell^k + \dots + \binom{m+1}{m-1} \ell^{m-1} + \binom{m+1}{m} \ell^m + \ell^{m+1}$$

.....

$$(n+1)^{m+1} = 1 + \binom{m+1}{1} n^1 + \binom{m+1}{2} n^2 + \dots + \binom{m+1}{k} n^k + \dots + \binom{m+1}{m-1} n^{m-1} + \binom{m+1}{m} n^m + n^{m+1}.$$

Somando-se estas  $n$  equações verticalmente, cancelando-se de ambos os lados os números  $2^{m+1}, \dots, n^{m+1}$  e observando-se a definição de  $S_n(k)$ , obtemos

$$(n+1)^{m+1} = n + \sum_{k=1}^{m-1} \binom{m+1}{k} S_n(k) + (m+1) S_n(m) + 1.$$

Lembrando ainda  $n = S_n(0)$ , isto dá a nossa fórmula afirmada

$$(m+1) \cdot S_n(m) = (n+1)^{m+1} - 1 - \sum_{k=0}^{m-1} \binom{m+1}{k} S_n(k).$$

■

Veamos os primeiros casos desta fórmula.

$$\text{a) } m = 1 : (1 + 1) \cdot S_n(1) = (n + 1)^{1+1} - 1 - \sum_{k=0}^{1-1} \binom{1+1}{k} S_n(k)$$

$$\text{ou seja, } 2 \cdot S_n(1) = (n + 1)^2 - 1 - S_n(0)$$

$$\text{ou ainda } 2 \cdot S_n(1) = n^2 + 2n + 1 - 1 - n = n(n + 1)$$

o que dá para a soma dos  $n$  primeiros números naturais:

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

$$\text{b) } m = 2 : (2 + 1) \cdot S_n(2) = (n + 1)^{2+1} - 1 - \sum_{k=0}^{2-1} \binom{2+1}{k} S_n(k)$$

$$\text{ou seja, } 3 \cdot S_n(2) = (n + 1)^3 - 1 - S_n(0) - 3 \cdot S_n(1)$$

$$\begin{aligned} \text{ou ainda } 3 \cdot S_n(2) &= (n + 1)^3 - (1 + n) - 3 \cdot \frac{n(n + 1)}{2} = \\ &= (n + 1) \left[ (n + 1)^2 - 1 - \frac{3}{2}n \right] = \frac{(n + 1)(2n^2 + n)}{2} , \end{aligned}$$

o que dá para a soma dos  $n$  primeiros quadrados perfeitos:

$$S_n(2) = \frac{n(n + 1)(2n + 1)}{6} .$$

$$\text{c) } m = 3 : (3 + 1) \cdot S_n(3) = (n + 1)^{3+1} - 1 - \sum_{k=0}^{3-1} \binom{3+1}{k} S_n(k)$$

$$\text{ou seja, } 4 \cdot S_n(3) = (n + 1)^4 - 1 - S_n(0) - 4 \cdot S_n(1) - 6 \cdot S_n(2)$$

$$\begin{aligned} \text{ou ainda } 4 \cdot S_n(3) &= (n + 1)^4 - (1 + n) - 4 \cdot \frac{n(n + 1)}{2} - 6 \cdot \frac{n(n + 1)(2n + 1)}{6} = \\ &= (n + 1) \left[ (n + 1)^3 - 1 - 2n - n(2n + 1) \right] = (n + 1) \left[ n^3 + n^2 \right] = n^2(n + 1)^2 \end{aligned}$$

o que dá para a soma dos  $n$  primeiros cubos perfeitos:

$$S_n(3) = \frac{n^2(n + 1)^2}{4} .$$

Comparando-se os casos  $m = 1$  e  $m = 3$  vemos que  $S_n(3) = (S_n(1))^2$  o que dá ainda a relação interessante

$$(1 + 2 + 3 + \dots + n)^2 = 1^3 + 2^3 + 3^3 + \dots + n^3 ,$$

válida para todos os  $n \in \mathbb{N}$ .

Uma fórmula fechada para  $S_n(m)$  sem uso das anteriores podemos estabelecer em forma de um  $(m+1) \times (m+1)$ -determinante:

### 1.11 Teorema.

Para todo  $n \in \mathbb{N}$  e  $m \in \mathbb{N}_0$  temos

$$S_n(m) = \frac{1}{(m+1)!} \cdot \begin{vmatrix} \binom{1}{0} & 0 & 0 & \dots & 0 & 0 & (n+1)^1 - 1 \\ \binom{2}{0} & \binom{2}{1} & 0 & \dots & 0 & 0 & (n+1)^2 - 1 \\ \binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \dots & 0 & 0 & (n+1)^3 - 1 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots \\ \binom{m}{0} & \binom{m}{1} & \binom{m}{2} & \dots & \binom{m}{m-2} & \binom{m}{m-1} & (n+1)^m - 1 \\ \binom{m+1}{0} & \binom{m+1}{1} & \binom{m+1}{2} & \dots & \binom{m+1}{m-2} & \binom{m+1}{m-1} & (n+1)^{m+1} - 1 \end{vmatrix}.$$

**Demonstração:** Nossa fórmula de recursão

$$(m+1) \cdot S_n(m) = (n+1)^{m+1} - 1 - \sum_{k=0}^{m-1} \binom{m+1}{k} S_n(k)$$

podemos reescrever, substituindo-se  $m = \ell$ , como

$$\sum_{k=0}^{\ell} \binom{\ell+1}{k} S_n(k) = (n+1)^{\ell+1} - 1.$$

Explicitando-se esta para  $\ell = 0, 1, 2, \dots, m$ , obtemos um sistema de  $m+1$  equações lineares nas  $m+1$  incógnitas  $S_n(0), S_n(1), S_n(2), \dots, S_n(m)$ :

$$\begin{aligned} \binom{1}{0} S_n(0) &= (n+1)^1 - 1 \\ \binom{2}{0} S_n(0) + \binom{2}{1} S_n(1) &= (n+1)^2 - 1 \\ \binom{3}{0} S_n(0) + \binom{3}{1} S_n(1) + \binom{3}{2} S_n(2) &= (n+1)^3 - 1 \\ &\dots\dots\dots \\ \binom{m}{0} S_n(0) + \binom{m}{1} S_n(1) + \dots + \binom{m}{m-1} S_n(m-1) &= (n+1)^m - 1 \\ \binom{m+1}{0} S_n(0) + \binom{m+1}{1} S_n(1) + \dots + \binom{m+1}{m-1} S_n(m-1) + \binom{m+1}{m} S_n(m) &= (n+1)^{m+1} - 1 \end{aligned}$$

O determinante dos coeficientes deste sistema (o produto dos coeficientes da diagonal neste caso) é



$$\binom{1}{0} \binom{2}{1} \binom{3}{2} \cdots \binom{m}{m-1} \binom{m+1}{m} = (m+1)! .$$

A aplicação da regra de Cramer fornece para a incógnita  $S_n(m)$ , como afirmado:

$$S_n(m) = \frac{1}{(m+1)!} \cdot \begin{vmatrix} \binom{1}{0} & 0 & 0 & \cdots & 0 & 0 & (n+1)^1 - 1 \\ \binom{2}{0} & \binom{2}{1} & 0 & \cdots & 0 & 0 & (n+1)^2 - 1 \\ \binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \cdots & 0 & 0 & (n+1)^3 - 1 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ \binom{m}{0} & \binom{m}{1} & \binom{m}{2} & \cdots & \binom{m}{m-2} & \binom{m}{m-1} & (n+1)^m - 1 \\ \binom{m+1}{0} & \binom{m+1}{1} & \binom{m+1}{2} & \cdots & \binom{m+1}{m-2} & \binom{m+1}{m-1} & (n+1)^{m+1} - 1 \end{vmatrix} .$$

■

## OS NÚMEROS TRIANGULARES

**1.12 Definição.** Para todo  $m \in \mathbb{N}$  indicamos por

$$t_m = \frac{m(m+1)}{2} .$$

$t_m$  chama-se o  $m$ -ésimo número triangular.

Desta definição decorre imediatamente:

**1.13 Observação.**

Para todo  $m \in \mathbb{N}$  temos

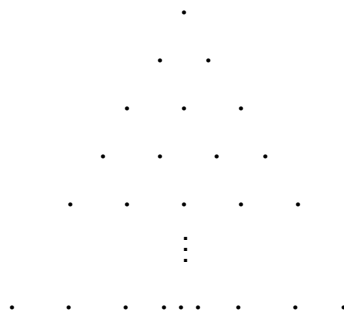
$$t_m = S_m(1) = 1 + 2 + 3 + \cdots + m = \binom{m+1}{2} \text{ tal como}$$

$$t_{m+1} = t_m + (m+1) .$$

A seqüência dos números triangulares é

$$(t_m)_{m \in \mathbb{N}} = \left( 1, 3, 6, 10, \dots, \frac{m(m+1)}{2}, \dots \right) .$$

A denominação "número triangular" para os números desta seqüência explica-se pelo seguinte *triângulo equilátero* de lados  $m$  o qual contém exatamente  $t_m$  pontos:



A seguinte caracterização dos números triangulares entre os números naturais é um resultado clássico devido a PLUTARCO (ca. 100 d. C.)

### 1.14 Proposição.

Para todo número natural  $n$  temos:

$n$  é um número triangular, se e somente se,  $8n + 1$  é um quadrado perfeito.

**Demonstração:** Nesta proposição duas coisas estão sendo afirmadas e têm que ser provadas:

- 1) Sempre quando  $n$  é um número triangular,  $8n + 1$  será um quadrado perfeito.
- 2) Sempre quando  $8n + 1$  é um quadrado perfeito,  $n$  será um número triangular.

Seja primeiro  $n$  um número triangular, i.e.  $n = t_m$  para algum  $m \in \mathbb{N}$ . Segue que

$$8n + 1 = 8t_m + 1 = 8 \cdot \frac{m(m+1)}{2} + 1 = 4m^2 + 4m + 1 = (2m + 1)^2$$

é um quadrado perfeito.

Seja agora  $n \in \mathbb{N}$  tal que  $8n + 1 = k^2$  é um quadrado perfeito. Como  $k$  é ímpar  $\geq 3$  concluímos que  $\frac{k-1}{2} \in \mathbb{N}$ . Coloquemos  $m = \frac{k-1}{2}$  e segue com esta escolha de  $m$ :

$$t_m = t_{\frac{k-1}{2}} = \frac{\frac{k-1}{2} \left( \frac{k-1}{2} + 1 \right)}{2} = \frac{k^2 - 1}{8} = n ,$$

mostrando que  $n$  é um número triangular (mais exatamente:  $n$  é o  $\frac{k-1}{2}$ -ésimo termo na seqüência dos números triangulares).



## ALGUMAS OBSERVAÇÕES SOBRE LÓGICA ELEMENTAR

Suponhamos,  $\mathcal{A}$  e  $\mathcal{B}$  são "asserções" (ou "propriedades") - as quais podem ser verdadeiras ou falsas e cuja veracidade ou falsidade pode ser constatada de forma única. Quando escrevemos

$$\mathcal{A} \implies \mathcal{B}$$

queremos dizer que

$$\mathcal{A} \text{ implica em } \mathcal{B},$$

ou seja, sempre quando  $\mathcal{A}$  for verdadeira, também  $\mathcal{B}$  será verdadeira. Outra maneira de dizer isto é:

(A validade de)  $\mathcal{A}$  é *condição suficiente* para (a validade de)  $\mathcal{B}$ ,  
ou  $\mathcal{B}$  é *condição necessária* para  $\mathcal{A}$ ,  
ou  $\mathcal{A}$  vale *somente se*  $\mathcal{B}$  vale,  
ou  $\mathcal{B}$  vale *se*  $\mathcal{A}$  vale,  
ou ainda *Se*  $\mathcal{A}$ , *então*  $\mathcal{B}$ .

É claro que

$$\mathcal{B} \iff \mathcal{A} \text{ significa o mesmo quanto } \mathcal{A} \implies \mathcal{B}.$$

Vejamos exemplos.

Seja  $\mathcal{A}$  a asserção: "um certo número natural  $n$  é múltiplo de 4"  
(isto pode ser verdadeiro ou falso),

$\mathcal{B}$  a asserção: " $n$  é par".

Claramente temos neste caso

$$\mathcal{A} \implies \mathcal{B},$$

pois sempre se  $n$  é múltiplo de 4, concluímos que  $n$  é par. Assim, podemos dizer:

" $n$  ser múltiplo de 4 *implica que*  $n$  é par",

" $n$  ser múltiplo de 4 é *condição suficiente para*  $n$  ser par",

" $n$  ser par é *condição necessária para*  $n$  ser múltiplo de 4"

" $n$  é múltiplo de 4 *somente se*  $n$  é par",

" $n$  é par, *se*  $n$  é múltiplo de 4"

"*se*  $n$  é múltiplo de 4, *então*  $n$  é par".

Um outro exemplo. Seja

$\mathcal{A}$  a asserção: " *está chovendo* ",

(também isto pode ser verdadeiro ou falso aqui e agora),

$\mathcal{B}$  a asserção: " *a praça está molhada* ".

Também neste caso temos

$$\mathcal{A} \implies \mathcal{B},$$

pois, se realmente está chovendo, temos certeza que a praça está molhada. Assim, podemos dizer:

" estar chovendo *implica que* a praça está molhada ",

" estar chovendo *é condição suficiente para* termos uma praça molhada ",

" uma praça molhada *é condição necessária para* estar chovendo ",

" está chovendo *somente se* a praça está molhada ",

" a praça está molhada *se* está chovendo ",

" *se* está chovendo, *então* a praça está molhada ".

### Exercício:

Pensando-se num certo quadrângulo  $Q$ , façam o mesmo com as asserções

$\mathcal{A}$ : "  $Q$  é um quadrado ",

$\mathcal{B}$ : "  $Q$  é um losângo ".

É claro que a seta numa implicação  $\mathcal{A} \implies \mathcal{B}$  não pode ser simplesmente invertida: Se  $\mathcal{A}$  é condição suficiente para  $\mathcal{B}$ , isto significa que  $\mathcal{B}$  é condição necessária para  $\mathcal{A}$ , mas não que  $\mathcal{B}$  é condição suficiente para  $\mathcal{A}$ :

O fato de "  $n$  ser par " é condição necessária mas não suficiente para "  $n$  ser múltiplo de 4 ". O fato de "  $n$  ser múltiplo de 4 " é condição suficiente mas não necessária para "  $n$  ser par ": Também 6 é par sem ser múltiplo de 4.

O fato de termos " uma praça molhada " é condição necessária mas não suficiente para " estar chovendo ". O fato de " estar chovendo " é condição suficiente mas não necessária para termos " uma praça molhada ": A praça pode estar molhada sem que esteja chovendo (por exemplo devido a uma operação dos bombeiros).

Existem asserções  $\mathcal{A}$  e  $\mathcal{B}$  que ambas implicam na outra, ou seja, as quais satisfazem simultaneamente

$$\mathcal{A} \implies \mathcal{B} \quad \text{e} \quad \mathcal{B} \implies \mathcal{A}.$$

Nesta situação temos então que  $\mathcal{A}$  é suficiente para  $\mathcal{B}$  e também  $\mathcal{A}$  é necessário para  $\mathcal{B}$ . Dizemos que  $\mathcal{A}$  é (condição) *necessário(a) e suficiente* para  $\mathcal{B}$ , ou também  $\mathcal{A}$  vale *se e somente se* vale  $\mathcal{B}$ .

Este fato indicamos por

$$\mathcal{A} \iff \mathcal{B}.$$

Dizemos também que  $\mathcal{A}$  e  $\mathcal{B}$  são *asserções equivalentes*, ou ainda que  $\mathcal{A}$  constitui uma *propriedade característica* para  $\mathcal{B}$  (e vice versa).

Por exemplo: Seja

$\mathcal{A}$  a asserção: " $n$  é múltiplo de 6",

$\mathcal{B}$  a asserção: " $n$  é um número par que é múltiplo de 3".

Cada uma destas duas propriedades, as quais um número  $n$  pode ter ou não, é suficiente para a outra. Cada uma é necessária para a outra. Cada uma é necessária e suficiente para a outra. Cada uma vale se e somente se a outra vale.

**Exercício:**

Pensar sobre as asserções equivalentes, quando  $Q$  é um certo quadrângulo:

$\mathcal{A}$ : " $Q$  é um quadrado"

$\mathcal{B}$ : " $Q$  é um losângulo que é um retângulo".

Se  $\mathcal{A}$  é uma asserção, indicamos por  $\bar{\mathcal{A}}$  a asserção "*não- $\mathcal{A}$* ", a qual é verdadeira se e somente se  $\mathcal{A}$  é falsa. Sejam  $\mathcal{A}$  e  $\mathcal{B}$  duas asserções e suponha

$$\mathcal{A} \implies \mathcal{B}.$$

O que acontece com esta implicação se negarmos as duas asserções? A resposta é que devemos também *inverter a seta da implicação*, ou seja, teremos

$$\bar{\mathcal{A}} \iff \bar{\mathcal{B}}.$$

Em outras palavras: Se  $\mathcal{A}$  é suficiente para  $\mathcal{B}$ , então  $\bar{\mathcal{B}}$  é suficiente para  $\bar{\mathcal{A}}$ .

Ou também: Se  $\mathcal{A}$  é suficiente para  $\mathcal{B}$ , então  $\bar{\mathcal{A}}$  é necessário para  $\bar{\mathcal{B}}$ .

Por exemplo, se negarmos a implicação

"ser múltiplo de 4 é suficiente para ser par",  
 ("ser um quadrado é suficiente para ser um retângulo"),

a implicação negada é:

" não ser múltiplo de 4 é necessário para ser ímpar",  
(" não ser um quadrado é necessário para não ser retângulo")

mas, não ser múltiplo de 4 (não ser quadrado) não é suficiente para ser ímpar (não ser retângulo).

Claro que numa equivalência podemos negar as asserções dos dois lados, ou seja, não importa se escrevemos

$$\mathcal{A} \iff \mathcal{B} \text{ ou } \overline{\mathcal{A}} \iff \overline{\mathcal{B}}.$$

Na Proposição 1.14 já conhecemos mais um exemplo de duas propriedades equivalentes, a saber, uma caracterização de um número natural  $n$  ser triangular: Necessário e suficiente para  $n$  ser triangular é a propriedade de  $8n + 1$  ser um quadrado perfeito.

Existem teoremas que afirmam simplesmente *implicações*, de modo que na sua demonstração deve ser verificado que uma certa propriedade  $\mathcal{B}$  é consequência de uma propriedade  $\mathcal{A}$  (a hipótese).

outros teoremas matemáticos afirmam *equivalências* de certas propriedades. Eles tem a forma:

*Sob certas condições são equivalentes:*

- a) Vale a propriedade  $\mathcal{A}$
- b) Vale a propriedade  $\mathcal{B}$ .

A demonstração de um tal teorema sempre se divide em duas partes:

"a)  $\Rightarrow$  b)": ..... Aqui deve ser mostrado que  $\mathcal{A}$  é suficiente para  $\mathcal{B}$ .

Isto pode ser mostrado diretamente, mostrando-se que  $\mathcal{B}$  é verdade, supondo-se a veracidade de  $\mathcal{A}$ . Ou indiretamente, supondo-se a veracidade de  $\overline{\mathcal{B}}$  e concluindo-se que  $\overline{\mathcal{A}}$  é verdade.

"b)  $\Rightarrow$  a)": ..... Aqui deve ser mostrado que  $\mathcal{A}$  é necessário para  $\mathcal{B}$  (que  $\mathcal{B}$  é suficiente para  $\mathcal{A}$ ).

Isto pode ser mostrado, verificando-se que  $\mathcal{A}$  é verdade, supondo-se a veracidade de  $\mathcal{B}$ . Ou indiretamente, supondo-se que  $\mathcal{A}$  é falso e concluindo-se que  $\mathcal{B}$  é falso.

### 1.15 Observação.

Se  $n \in \mathbb{N}$  é um quadrado perfeito, então valem:

- a) Se  $n$  for par, então  $n$  é divisível por 4.
- b) Se  $n$  for ímpar, então  $n$  é da forma  $8k + 1$  com  $k \in \mathbb{N}_0$ , isto é,  $n$  deixa o resto 1 quando dividido por 8.

(ver §2)

**Demonstração:** Seja  $n = m^2$  com  $m \in \mathbb{N}$ .

- a) Se  $m = 2k$  é par, então  $n = 4k^2$  é divisível por 4.
- b) Se  $m = 2\ell - 1$  é ímpar, então  $n = (2\ell - 1)^2 = 4\ell^2 - 4\ell + 1 = 4(\ell - 1)\ell + 1$ . Como o produto  $(\ell - 1)\ell$  de dois números naturais consecutivos é par, digamos  $(\ell - 1)\ell = 2k$ , concluímos  $n = 8k + 1$ .

■

Convém frisar que, as afirmações de 1.15 não são equivalências. Trata-se de duas implicações: A condição de um número  $n$  ser quadrado perfeito par (ímpar) é *suficiente* para  $n$  ser divisível por 4 (ser da forma  $8k + 1$ ). Estas propriedades porém *não são necessárias*:  $n = 12$  ( $n = 17$ ) é divisível por 4 (é da forma  $8k + 1$ ) sem que  $n$  seja quadrado perfeito.

### 1.16 Exemplo.

Na seqüência dos números 11, 111, 1111, ..., 111...1111, ... não aparece nenhum quadrado perfeito.

**Demonstração:** Temos  $11 = 8 + 3$  e  $n = 111...1111 = 111...1000 + 111 = 8\ell + 8 \cdot 13 + 7 = 8k + 7$  para  $n \geq 111$ . Isto quer dizer que nenhum dos números na seqüência é da forma  $8k + 1$ , condição necessária para ser um quadrado perfeito.

■

### DIFERENÇA DE DOIS QUADRADOS

Além dos próprios quadrados perfeitos existem muitos números naturais os quais podem ser escritos como *diferença*  $n = x^2 - y^2$  de dois quadrados perfeitos onde  $x \in \mathbb{N}$  e  $y \in \mathbb{N}_0$ . Por outro lado, os números 2 e 6 por exemplo não gozam desta propriedade (porquê?). Os números que são diferença de dois quadrados são facilmente caracterizados:

### 1.17 Proposição.

Seja  $n \in \mathbb{N}$ . Equivalentes são :

a)  $n = x^2 - y^2$  para certos  $x, y \in \mathbb{N}_0$ .

b)  $n \notin \{2, 6, 10, 14, \dots, 4k + 2, \dots\}$

Em outras palavras:  $n$  é diferença de dois quadrados se e somente se  $n$  é ímpar ou divisível por 4 (i.e.  $n$  não deixa resto 2 quando dividido por 4).

**Demonstração:** "a)  $\Rightarrow$  b)": Suponha  $n = x^2 - y^2$ . Para provar que  $n \notin \{2, 6, 10, \dots\}$  podemos supor que  $n$  é par. Isto quer dizer que  $x$  e  $y$  ambos são pares ou ambos ímpares: Se  $x = 2k$  e  $y = 2\ell$ , temos  $n = x^2 - y^2 = (2k)^2 - (2\ell)^2 = 4(k^2 - \ell^2) \notin \{2, 6, 10, \dots\}$ . Se  $x = 2k - 1$  e  $y = 2\ell - 1$  temos também  $n = x^2 - y^2 = (2k - 1)^2 - (2\ell - 1)^2 = 4(k^2 - \ell^2 - k + \ell) \notin \{2, 6, 10, \dots\}$ .

"b)  $\Rightarrow$  a)": Suponhamos, reciprocamente,  $n \notin \{2, 6, 10, \dots\}$ . Isto significa que  $n$  é ímpar ou divisível por 4.

Se  $n$  é ímpar,  $n \pm 1$  é par e portanto  $\frac{n \pm 1}{2} \in \mathbb{N}_0$ . Como ainda  $\left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2 = \frac{(n+1)^2 - (n-1)^2}{4} = \frac{4n}{4} = n$ , concluímos que

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

é uma possível decomposição de  $n$  como diferença de dois quadrados.

Se  $n = 4k$ , decompomos  $n = (k+1)^2 - (k-1)^2$ , ou seja,

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

Pensando-se ainda na subdivisão do conjunto  $\mathbb{N}$  nos 4 subconjuntos

$$\mathbb{N} = \{4, 8, 12, \dots\} \cup \{1, 5, 9, 13, \dots\} \cup \{2, 6, 10, 14, \dots\} \cup \{3, 7, 11, 15, \dots\}$$

(ver 2.5 e § 6), vemos que entre estes somente os números de  $\{2, 6, 10, 14, \dots\}$  não são diferença de dois quadrados. Simplificando podemos dizer:

*75% dos números naturais são diferença de dois quadrados.*

(Para mais detalhes, comparar 3.24 e 3.25.)



## § 2 Teoria de divisibilidade nos números inteiros

### O ALGORITMO GERAL DE DIVISÃO

#### 2.1 Proposição. (O algoritmo de divisão)

Sejam  $a, b$  dois números inteiros com  $b > 0$ . Então existem únicos números inteiros  $q, r$  tais que

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

$q$  chama-se o *quociente*,  $r$  o *menor resto não-negativo* na divisão de  $a$  por  $b$ .

**Demonstração:** A existência de  $q$  e  $r$ :

Dados  $a, b \in \mathbb{Z}$  com  $b > 0$  consideremos o conjunto

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

Temos obviamente  $S \subseteq \mathbb{N}_0$ . Para  $x = -|a|$  obtemos  $a - bx = a - b(-|a|) = a + b|a| \geq a + |a| \geq 0$  pois  $b \geq 1$ . Isto mostra que  $S \neq \emptyset$ . Pelo princípio da indução temos que existe um  $r \in S$  mínimo, i.e.  $r \leq y \quad \forall y \in S$ . Como  $r \in S$  existe um  $x = q \in \mathbb{Z}$  com  $r = a - bq$ . Segue então  $a = bq + r$ . Falta provar que  $0 \leq r < b$ . Como  $r \in S$  certamente  $r \geq 0$ . Supondo-se  $r \geq b$  segue  $a - bq - b = r - b \geq 0$ , ou seja,  $r > a - (q+1)b \in S$  contradizendo a minimalidade do  $r \in S$ . Isto mostra que  $r \geq b$  é impossível. Temos que ter  $r < b$ .

A unicidade de  $q$  e  $r$ :

Suponhamos que  $q, r$  e  $q', r'$  são inteiros tais que

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

Então  $r' - r = bq - bq' = b(q - q')$  e segue  $|r' - r| = |b(q - q')| = b|q - q'|$ .

Agora, adicionando-se as desigualdades  $\begin{cases} 0 \leq r' < b \\ -b < -r \leq 0 \end{cases}$  segue  $-b < r' - r < b$ ,

ou seja,  $|r' - r| < b$ . Daí temos a contradição

$$b > |r' - r| = b|q - q'| \geq b, \quad \text{no caso } q \neq q'.$$

Concluimos  $q = q'$  e então  $r = r'$ .

■

## 2.2 Exemplo.

Para  $a = 100$  e  $b = 7$  temos  $q = 14$  e  $r = 2$  pois  $100 = 7 \cdot 14 + 2$ .

Para  $a = -100$  e  $b = 7$  temos  $q = -15$  e  $r = 5$  pois  $-100 = 7 \cdot (-15) + 5$ .

## 2.3 Teorema. (Algoritmo de divisão geral)

Para quaisquer números  $a, b \in \mathbb{Z}$  com  $b \neq 0$  existem únicos  $q, r \in \mathbb{Z}$  tais que

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

**Demonstração:** Temos  $|b| > 0$ . Por 2.1, existem únicos  $q', r \in \mathbb{Z}$  com  $a = |b|q' + r$  com  $0 \leq r < |b|$ .

Se  $b > 0$  então  $|b| = b$  e podemos considerar  $q = q'$  junto com  $r$ .

Se  $b < 0$  então  $|b| = -b$  e podemos considerar  $q = -q'$  junto com  $r$  obtendo  $a = |b|q' + r = (-b)q' + r = b(-q') + r = bq + r$ .

■

## 2.4 Exemplo.

Para  $a = 100$  e  $b = -7$  temos  $q = -14$  e  $r = 2$  pois  $100 = (-7) \cdot (-14) + 2$ .

Para  $a = -100$  e  $b = -7$  temos  $q = 15$  e  $r = 5$  pois  $-100 = (-7) \cdot 15 + 5$ .

## 2.5 Conseqüência.

- a) Considerando-se  $b = 2$  temos para qualquer  $a \in \mathbb{Z}$  um  $q \in \mathbb{Z}$  com  $a = 2q$  ou  $a = 2q + 1$  e conseqüentemente

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

tal que

$$\{2q \mid q \in \mathbb{Z}\} \cap \{2q+1 \mid q \in \mathbb{Z}\} = \emptyset ,$$

isto é, temos uma decomposição do conjunto  $\mathbb{Z}$  dos inteiros em dois subconjuntos disjuntos - os inteiros *pares* e os inteiros *ímpares*.

- b) De forma semelhante, considerando-se  $b = 3$  temos para qualquer  $a \in \mathbb{Z}$  um  $q \in \mathbb{Z}$  com  $a = 3q$  ou  $a = 3q + 1$  ou  $a = 3q + 2$  e conseqüentemente

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

uma decomposição de  $\mathbb{Z}$  em três subconjuntos disjuntos.

- c) Para  $b = 4$  obtemos

$$\mathbb{Z} = \{4q \mid q \in \mathbb{Z}\} \dot{\cup} \{4q+1 \mid q \in \mathbb{Z}\} \dot{\cup} \{4q+2 \mid q \in \mathbb{Z}\} \dot{\cup} \{4q+3 \mid q \in \mathbb{Z}\}$$

d) Em geral, para  $b = n \in \mathbb{N}$  obtemos

$$\mathbb{Z} = \{nq \mid q \in \mathbb{Z}\} \dot{\cup} \{nq+1 \mid q \in \mathbb{Z}\} \dot{\cup} \dots \dot{\cup} \{nq+(n-1) \mid q \in \mathbb{Z}\}$$

Observação: Os  $n$  conjuntos

$$\{nq \mid q \in \mathbb{Z}\}, \{nq+1 \mid q \in \mathbb{Z}\}, \{nq+2 \mid q \in \mathbb{Z}\}, \dots, \{nq+(n-1) \mid q \in \mathbb{Z}\}$$

chamam-se as *classes de resto* módulo  $n$  (ver §6).

## 2.6 Definição.

Dizemos que um inteiro  $b$  é *divisível* por um inteiro  $a$  (também:  $a$  *divide*  $b$  ou  $b$  é *múltiplo* de  $a$ ) se existe  $q \in \mathbb{Z}$  com  $b = aq$ .

Notação: Escrevemos  $a \mid b$  se  $a$  divide  $b$  e  $a \nmid b$  se isto não ocorre.

Por exemplo:  $3 \mid -12$ ,  $5 \mid 15$ ,  $-7 \mid 21$ . Vale  $1 \mid b$  para todo  $b \in \mathbb{Z}$  e  $a \mid 0$  para todo  $a \in \mathbb{Z}$ .

Porém:  $\pm 4 \nmid \pm 10$ ,  $\pm 49 \nmid \pm 77$ .

## 2.7 Proposição. (Regras)

Para todos os números  $a, b, c, d \in \mathbb{Z}$  valem

- $a \mid 0$ ,  $1 \mid b$ ,  $a \mid a$ .
- $a \mid 1 \iff a = \pm 1$ ;  $0 \mid b \iff b = 0$ .
- Se  $a \mid b$  e  $c \mid d$  então  $ac \mid bd$ .
- Se  $a \mid b$  e  $b \mid c$  então  $a \mid c$ .
- $a \mid b$  e  $b \mid a \iff a = \pm b$ .
- Se  $a \mid b$  e  $b \neq 0$  então  $|a| \leq |b|$ .
- Se  $a \mid b$  e  $a \mid c$  então  $a \mid bx + cy \ \forall x, y \in \mathbb{Z}$ .

Estas propriedades são conseqüências fáceis da definição e deixamos a sua demonstração como exercício. Provemos, por exemplo, o item g):

$a \mid b$  e  $a \mid c$  significa que existem  $q_1, q_2 \in \mathbb{Z}$  tais que  $aq_1 = b$  e  $aq_2 = c$ . Segue então  $bx + cy = (aq_1)x + (aq_2)y = a(q_1x + q_2y)$  com  $q_1x + q_2y \in \mathbb{Z}$ , mostrando

assim  $a \mid (bx + cy)$ .

## MÁXIMO DIVISOR COMUM DE DOIS NÚMEROS

### 2.8 Definição.

Sejam  $a, b \in \mathbb{Z}$  dois números, pelo menos um deles diferente de zero. O *máximo divisor comum* entre  $a$  e  $b$  é o número natural

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

definido pelas duas propriedades:

- a)  $d \mid a$  e  $d \mid b$  (i. e.  $d$  é divisor comum de  $a$  e  $b$ .)
- b) Se algum  $c \in \mathbb{N}$  dividir ambos  $a$  e  $b$  então temos também  $c \mid d$ .

### 2.9 Teorema.

Sejam  $a, b \in \mathbb{Z}$  não ambos zero e seja  $d = \text{mdc}(a, b)$ . Então existem  $x_1, y_1 \in \mathbb{Z}$  tais que

$$ax_1 + by_1 = d.$$

**Demonstração:** Consideremos o conjunto

$$S = \{ ax + by \mid x, y \in \mathbb{Z}, ax + by > 0 \}.$$

Seja primeiro  $a \neq 0$ . Fazendo-se  $y = 0$  e  $x = 1$  se  $a > 0$   $x = -1$  se  $a < 0$  vemos que  $ax + by = a(\pm 1) + b \cdot 0 = |a| > 0$  o que mostra que  $S \neq \emptyset$ . Se  $a = 0$  então  $|b| > 0$  e uma escolha análoga de  $x$  e  $y$  mostra  $S \neq \emptyset$  também neste caso.

Pelo princípio da indução, existe um  $d \in S$  minimal. Como  $d \in S$  temos  $d > 0$  e existem  $x_1, y_1 \in \mathbb{Z}$  tais que  $d = ax_1 + by_1$ .

Afirmamos que este  $d$  é o  $\text{mdc}(a, b)$ :

Dividamos  $a$  por  $d$  com resto:  $\exists q, r \in \mathbb{Z}$  tais que  $a = qd + r$  e  $0 \leq r \leq d-1$ . Então  $r = a - qd = a - q(ax_1 + by_1) = a(1 - qx_1) + b(-qy_1)$ . Se fosse  $r > 0$  poderíamos concluir que  $r \in S$ , o que claramente é um absurdo já que  $r < d$  e  $d$  é o elemento mínimo de  $S$ . Logo  $r = 0$  e  $a = qd$  o que significa  $d \mid a$ .

Da mesma forma mostra-se que  $d \mid b$ . Logo,  $d$  é divisor comum de  $a$  e  $b$ .

Seja  $c \in \mathbb{N}$  tal que  $c \mid a$  e  $c \mid b$ . Por 2.7 g) concluímos que  $c \mid ax_1 + by_1 = d$ . Logo

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

■

## 2.10 Conseqüência.

Sejam  $a, b \in \mathbb{Z}$ , não ambos nulos e seja  $d = \text{mdc}(a, b)$ . Então

$$\{ax + by \mid x, y \in \mathbb{Z}\} = \{dz \mid z \in \mathbb{Z}\}.$$

Em palavras: As combinações lineares inteiras de  $a$  e  $b$  são exatamente os múltiplos do  $\text{mdc}(a, b)$ .

**Demonstração:** Abreviemos  $T = \{ax + by \mid x, y \in \mathbb{Z}\}$  e  $R = \{dz \mid z \in \mathbb{Z}\}$ . Pelo teorema 2.9 existem  $x_1, y_1 \in \mathbb{Z}$  com  $d = ax_1 + by_1$ . Para todo  $z \in \mathbb{Z}$  segue  $dz = a(x_1z) + b(y_1z) \in T$ . Logo  $R \subseteq T$ . Como  $d \mid (ax + by)$  para qualquer  $ax + by \in T$ , segue também  $T \subseteq R$ . Logo,  $T = R$ .

■

## NÚMEROS RELATIVAMENTE PRIMOS

### 2.11 Definição.

Dois números  $a, b \in \mathbb{Z}$  chamam-se *relativamente primos* (ou *primos entre si*) se  $\text{mdc}(a, b) = 1$ .

Por exemplo,  $\text{mdc}(-12, 35) = 1$  i.e.  $-12$  e  $35$  são primos entre si.

### 2.12 Proposição.

Dois números  $a, b \in \mathbb{Z}$  não ambos nulos, são relativamente primos, se e somente se existem  $x_1, y_1 \in \mathbb{Z}$  tais que

$$ax_1 + by_1 = 1.$$

**Demonstração:** Seja  $d = \text{mdc}(a, b)$ .

Se  $d = 1$ , existem os  $x_1, y_1 \in \mathbb{Z}$  com  $ax_1 + by_1 = 1$  por 2.9.

Reciprocamente, seja  $ax + by = 1$  possível com  $x, y \in \mathbb{Z}$ . De  $d \mid a$  e  $d \mid b$  concluímos  $d \mid 1$ . Isto dá  $d = 1$ .

■

Mencionamos algumas conseqüências desta caracterização dos números relativamente primos.

### 2.13 Conseqüência.

Sejam  $a, b \in \mathbb{Z}$ , não ambos nulos e  $d = \text{mdc}(a, b)$ . Então

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

(Observamos que  $\frac{a}{d}$  e  $\frac{b}{d}$  são números inteiros!)

**Demonstração:** De  $ax + by = d$  para certos  $x, y \in \mathbb{Z}$ , segue  $\frac{a}{d}x + \frac{b}{d}y = 1$ . Por 2.12 concluímos a afirmação. ■

### 2.14 Conseqüência.

Sejam  $a, b, c \in \mathbb{Z}$  tais que  $a|c$  e  $b|c$ .

Se  $\text{mdc}(a, b) = 1$ , então temos também  $ab|c$ .

**Demonstração:** Existem  $r, s, x, y \in \mathbb{Z}$  tais que  $ar = c = bs$  e  $ax + by = 1$ . Daí concluímos

$$c = c \cdot 1 = c(ax + by) = cax + cby = (bs)ax + (ar)by = ab(sx + ry),$$

com  $sx + ry \in \mathbb{Z}$ . Segue  $ab|c$ . ■

### 2.15 Conseqüência. (O Lema de EUCLIDES)

Sejam  $a, b, c \in \mathbb{Z}$  tais que  $a|bc$  e  $\text{mdc}(a, b) = 1$ . Então  $a|c$ .

**Demonstração:** Temos  $r, x, y \in \mathbb{Z}$  tais que  $ar = bc$  e  $ax + by = 1$ . Daí concluímos

$$c = c \cdot 1 = c(ax + by) = cax + cby = cax + ary = a(cx + ry).$$

Segue  $a|c$ . ■

### 2.16 Conseqüência.

Sejam  $a, b, c \in \mathbb{Z}$  tais que  $\text{mdc}(a, b) = \text{mdc}(a, c) = 1$ . Então temos também  $\text{mdc}(a, bc) = 1$ ,

**Demonstração:** Temos  $x, y, u, v \in \mathbb{Z}$  tais que  $ax + by = 1 = au + cv$ . Daí concluímos

$$1 = 1 \cdot 1 = (ax + by)(au + cv) = a^2xu + axcv + byau + bycv = \\ = a(axu + xcv + byu) + bc(yv),$$

onde  $axu + xcv + byu, yv \in \mathbb{Z}$ . Concluímos  $\text{mdc}(a, bc) = 1$ . ■

### O ALGORITMO EUCLIDIANO

Para dois números  $a, b \in \mathbb{Z}$  com  $b \neq 0$  consideremos o seguinte processo:

Colocamos  $r_0 = |b|$ . Existem  $q_1, r_1 \in \mathbb{Z}$  tais que

$$a = bq_1 + r_1 \quad \text{com } 0 \leq r_1 < r_0.$$

Se  $r_1 = 0$ , o processo pára. Se  $r_1 \neq 0$  existem  $q_2, r_2 \in \mathbb{Z}$  tais que

$$r_0 = r_1q_2 + r_2 \quad \text{com } 0 \leq r_2 < r_1.$$

Se  $r_2 = 0$ , o processo pára. Se  $r_2 \neq 0$  existem  $q_3, r_3 \in \mathbb{Z}$  tais que

$$r_1 = r_2q_3 + r_3 \quad \text{com } 0 \leq r_3 < r_2.$$

.....

Se o processo já chegou em

$$r_{k-2} = r_{k-1}q_k + r_k \quad \text{com } 0 \leq r_k < r_{k-1},$$

o próximo passo é:

Se  $r_k = 0$ , o processo pára. Se  $r_k \neq 0$  existem  $q_{k+1}, r_{k+1} \in \mathbb{Z}$  tais que

$$r_{k-1} = r_kq_{k+1} + r_{k+1} \quad \text{com } 0 \leq r_{k+1} < r_k$$

.....

Obtemos assim uma cadeia decrescente

$$|b| = r_0 > r_1 > r_2 > \dots > r_k > r_{k+1} > \dots \geq 0$$

de inteiros não-negativos. Existe portanto um determinado  $n \in \mathbb{N}_0$  tal que

$$r_n \neq 0 \quad \text{porém} \quad r_{n+1} = 0 .$$

Assim, este processo termina como

$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1} \quad \text{com} \quad 0 < r_{n-1} < r_{n-2}$$

$$r_{n-2} = r_{n-1}q_n + r_n \quad \text{com} \quad 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_nq_{n+1} .$$

O processo o qual acabamos de descrever, chama-se o *algoritmo EUCLIDiano* para  $a$  e  $b$ . Temos o seguinte

### 2.17 Teorema.

No algoritmo EUCLIDiano para  $a$  e  $b$  temos que

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

Em palavras: O último resto não nulo no algoritmo EUCLIDiano é o máximo divisor comum de  $a$  e  $b$ .

**Demonstração:** Considerando-se a cadeia das equações estabelecidas a partir da última ( $r_{n-1} = r_nq_{n+1}$ ), vemos que  $r_n$  divide todos os restos anteriores. Finalmente,  $r_n$  divide  $r_1$  e  $r_0 = |b|$  e  $a$ . Isto torna  $r_n$  um divisor comum de  $a$  e  $b$ .

Partindo da primeira das equações com um qualquer divisor comum  $c$  de  $a$  e  $b$  vemos que  $c$  divide todos os restos, particularmente  $c|r_n$ . Isto mostra a afirmação. ■

### 2.18 Exemplo.

Determinar

$$\text{mdc}(\pm 7519, \pm 8249) .$$

Podemos nos restringir a valores positivos e encarar  $a = 7519$  e  $b = 8249$ . O algoritmo EUCLIDiano dá



$$\begin{aligned}
7519 &= 0 \cdot 8249 + 7519 \\
8249 &= 1 \cdot 7519 + 730 \\
7519 &= 10 \cdot 730 + 219 \\
730 &= 3 \cdot 219 + 73 \\
219 &= 3 \cdot 73
\end{aligned}$$

Conclusão:  $\text{mdc}(\pm 7519, \pm 8249) = 73$ .

Ilustramos ainda neste exemplo como o algoritmo EUCLIDIANO é útil para se conseguir soluções  $x, y \in \mathbb{Z}$  com  $ax + by = \text{mdc}(a, b)$ : Subindo a partir da penúltima equação do algoritmo, vemos:

$$\begin{aligned}
73 &= 730 - 3 \cdot 219 = 730 - 3 \cdot (7519 - 10 \cdot 730) = 31 \cdot 730 - 3 \cdot 7519 = \\
&= 31 \cdot (8249 - 7519) - 3 \cdot 7519 = -34 \cdot 7519 + 31 \cdot 8249.
\end{aligned}$$

## O MÍNIMO MÚLTIPLO COMUM

### 2.19 Definição.

Sejam  $a, b \in \mathbb{Z}$  dois números, ambos não nulos.

O *mínimo múltiplo comum* entre  $a$  e  $b$  é o número natural

$$m = \text{mmc}(a, b)$$

definido pelas duas propriedades:

- a)  $a|m$  e  $b|m$  (i. e.  $m$  é múltiplo comum de  $a$  e  $b$ .)
- b) Se  $a|c$  e  $b|c$  para algum  $c \in \mathbb{N}$  então temos também  $m|c$ .

### 2.20 Exemplo.

$a = 6$  e  $b = -8$ .

Os múltiplos comuns destes  $a$  e  $b$  são  $\{\pm 24, \pm 48, \pm 72, \dots\}$ . Entretanto

$$m = \text{mmc}(6, -8) = 24.$$

### 2.21 Proposição.

Sejam  $0 \neq a, b \in \mathbb{Z}$ ,  $d = \text{mdc}(a, b)$  e  $m = \text{mmc}(a, b)$ . Então vale a relação

$$md = |ab|.$$

**Demonstração:** Coloquemos  $m' = \frac{|ab|}{d}$ .

Existem  $r, t \in \mathbb{Z}$  tais que  $dr = a$  e  $dt = b$ . Temos  $m' = \frac{|a|}{d} |b| = \pm rb$  e também  $m' = |a| \frac{|b|}{d} = \pm at$ . Isto mostra que  $m'$  é múltiplo comum de  $a$  e  $b$ .

Seja  $c \in \mathbb{N}$  tal que  $a|c$  e  $b|c$ . Existem então  $u, v \in \mathbb{Z}$  tais que  $au = c = bv$ . Por 2.9 existem  $x_1, y_1 \in \mathbb{Z}$  com  $ax_1 + by_1 = d$ . Segue

$$\frac{c}{m'} = \frac{cd}{|ab|} = \frac{c}{|ab|} (ax_1 + by_1) = \frac{c}{|b|} \frac{ax_1}{|a|} + \frac{c}{|a|} \frac{by_1}{|b|} = \pm \frac{c}{b} x_1 \pm \frac{c}{a} y_1 = \pm vx_1 \pm uy_1 \in \mathbb{Z}.$$

Mostramos que  $\frac{c}{m'} \in \mathbb{Z}$  o que significa  $m'|c$ . Assim  $m' = m$ . ■

## 2.22 Exemplo.

Sabemos  $\text{mdc}(\pm 7519, \pm 8249) = 73$ . Conseqüentemente

$$\text{mmc}(\pm 7519, \pm 8249) = \frac{7519 \cdot 8249}{73} = 849647.$$

## EQUAÇÕES DIOFANTINAS

Uma relação em  $n$  incógnitas  $x_1, x_2, \dots, x_n$  da forma

$$f(x_1, x_2, \dots, x_n) = 0$$

é considerada uma *equação DIOFANTINA*, quando o interesse é dirigido às soluções inteiras  $x_1, \dots, x_n \in \mathbb{Z}$  dela. Por exemplo, a relação  $x_1^2 + x_2^2 + \dots + x_n^2 = 100$  a equação da hiper-esfera de raio 10 no espaço  $n$  dimensional, pode ser considerada uma equação DIOFANTINA, quando as  $n$ -uplas de coordenadas *inteiras*  $x_1, \dots, x_n$  são procuradas.

Uma equação DIOFANTINA é *linear* se ela tiver a forma

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = c.$$

Em particular, queremos tratar agora as equações DIOFANTINAS lineares de grau 2 ou seja,

$$ax + by = c \quad \text{com } a, b, c \in \mathbb{Z}.$$

## 2.23 Teorema.

Sejam  $a, b, c \in \mathbb{Z}$ ,  $a, b$  não ambos zero.

a) A equação DIOFANTINA

$$ax + by = c \quad (*)$$

admite pelo menos uma solução  $x, y \in \mathbb{Z}$  se e somente se  $d = \text{mdc}(a, b) \mid c$ .

b) Suponha  $d \mid c$  e seja  $(x_0, y_0)$  uma solução (particular) de (\*). Então a solução geral (i. e. o conjunto de **todas** as soluções) de (\*) é dada por

$$\begin{cases} x = x_0 + \frac{b}{d}t \\ y = y_0 - \frac{a}{d}t \end{cases} \quad (t \in \mathbb{Z}).$$

**Demonstração:** a) Como  $d \mid a$  e  $d \mid b$  temos também  $d \mid c$  para qualquer possível solução  $(x, y)$  de (\*). Logo,  $d \mid c$  é uma condição necessária para a solubilidade de (\*).

Reciprocamente, seja  $d \mid c$ , digamos  $d\ell = c$  para algum  $\ell \in \mathbb{Z}$ . Por 2.9 sabemos que existem  $x_1, y_1 \in \mathbb{Z}$  com  $d = ax_1 + by_1$ . Segue  $c = a(\ell x_1) + b(\ell y_1)$  e vemos que  $(\ell x_1, \ell y_1)$  é uma solução particular de (\*).

b) Seja  $(x_0, y_0)$  uma solução particular e  $t \in \mathbb{Z}$ . Provamos primeiro que qualquer

par de números  $\begin{cases} x = x_0 + \frac{b}{d}t \\ y = y_0 - \frac{a}{d}t \end{cases} \quad (t \in \mathbb{Z})$  satisfaz a equação também:

$$ax + by = a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) = ax_0 + \frac{ab}{d}t + by_0 - \frac{ba}{d}t = ax_0 + by_0 = c.$$

Seja reciprocamente  $(x, y)$  uma qualquer solução de (\*). Temos então  $ax_0 + by_0 = c = ax + by$  e daí

$$a(x - x_0) = b(y_0 - y).$$

Existem  $r, s \in \mathbb{Z}$  tais que  $a = rd$  e  $b = ds$  e vale  $\text{mdc}(r, s) = \text{mdc}(\frac{a}{d}, \frac{b}{d}) = 1$ . Segue  $dr(x - x_0) = ds(y_0 - y)$  e daí

$$r(x - x_0) = s(y_0 - y),$$

pois  $d \neq 0$ .

Podemos supor  $a \neq 0$ . Concluimos  $r \mid s(y_0 - y)$  e daí  $r \mid y_0 - y$  pois  $\text{mdc}(r, s) = 1$ . Logo existe  $t \in \mathbb{Z}$  tal que  $rt = y_0 - y$  de onde vem  $y = y_0 - rt = y_0 - \frac{a}{d}t$ .

Segue  $r(x - x_0) = s(y_0 - y) = srt$  e então  $x - x_0 = st$ , pois  $r \neq 0$ . Isto dá  $x = x_0 + st = x_0 + \frac{b}{d}t$ . Logo temos

$$\begin{cases} x = x_0 + \frac{b}{d}t \\ y = y_0 - \frac{a}{d}t \end{cases}$$

para algum  $t \in \mathbb{Z}$ , como afirmado. ■

## 2.24 Exemplo.

Determinar a solução geral de

$$54x + 21y = 906 .$$

Solução: Temos  $\text{mdc}(54, 21) = 3 \mid 906$ . Logo a equação é solúvel e simplifica para

$$18x + 7y = 302 \quad (*) \quad \text{com } \text{mdc}(18, 7) = 1 .$$

Temos que  $(2, -5)$  é uma solução de  $18x + 7y = 1$  o que dá  $302 \cdot (2, -5) = (604, -1510)$  como solução particular de  $(*)$ . Isto dá como solução geral

$$\begin{cases} x = 604 + 7t \\ y = -1510 - 18t \end{cases} \quad (t \in \mathbb{Z}).$$

■

## 2.25 Exemplo.

Um teatro vende ingressos e cobra RS 18.— por adulto e RS 7,50 por criança. Numa noite, arrecada-se RS 900.—. Quantos adultos e crianças assistiram ao espetáculo, sabendo-se que eram mais adultos do que crianças?

**Solução.** Seja  $x$  o número de crianças,  $y$  o número de adultos que assistiram. Temos que resolver então a equação DIOFANTINA

$$7,5x + 18y = 900 \quad \text{sob a condição adicional } y > x \geq 0 .$$

ou seja

$$15x + 36y = 1800 .$$

Observando-se ainda  $\text{mdc}(15, 36) = 3 \mid 1800$ , esta equivale a

$$5x + 12y = 600 \quad (*).$$

Como  $(120, 0)$  é obviamente uma solução de  $(*)$ , vemos que a solução geral de  $(*)$  é dada por

$$\begin{cases} x = 120 + 12t \\ y = -5t \end{cases} \quad (t \in \mathbb{Z}).$$

De  $y > x \geq 0$  decorre  $-5t > 120 + 12t \geq 0$  e daí

$$-7,05\dots = -\frac{120}{17} > t \geq -\frac{120}{12} = -10,$$

ou seja,

$$-10 \leq t < -7,05\dots,$$

o que dá

$$t \in \{-10, -9, -8\}.$$

As 3 possíveis soluções são então:

$$\begin{cases} x = 0 \\ y = 50 \end{cases} \quad \begin{cases} x = 12 \\ y = 45 \end{cases} \quad \begin{cases} x = 24 \\ y = 40 \end{cases}.$$

■

## § 3 Números primos e sua distribuição

O TEOREMA FUNDAMENTAL DA ARITMÉTICA

### 3.1 Definição.

Um número  $p \in \mathbb{N}$  é denominado *primo*, se  $p > 1$  e se seus únicos divisores são  $p$  e 1. Indicamos por

$$\mathbb{P} = \{p \in \mathbb{N} \mid p \text{ é primo}\}$$

o conjunto de todos os números primos.

Podemos dizer então

$$p \in \mathbb{P} \iff (\forall a, b \in \mathbb{N} : p = ab \implies a = p \text{ e } b = 1 \text{ ou } a = 1 \text{ e } b = p,)$$

Um número  $n > 1$  é dito *composto* se ele não é primo. Assim,  $n$  é composto, se existem  $r, s \in \mathbb{N}$ ,  $1 < s \leq r < n$  com  $n = rs$ .

Os primeiros números primos são

2, 3, 5, 7, 11, 13, 17, ... . Entretanto

4, 6, 8, 9, 10, 12, 14, 15, ...

são os primeiros números compostos.

O Lema de EUCLIDES (Cons. 2.15) dá a seguinte propriedade fundamental dos números primos:

### 3.2 Proposição.

Seja  $p \in \mathbb{P}$ . Então

$$\forall a, b \in \mathbb{N} : p \mid ab \implies p \mid a \text{ ou } p \mid b$$

Em palavras: um primo divide um produto, somente se ele divide um dos fatores.

**Demonstração:** Suponhamos  $p \mid ab$  e  $p \nmid a$ . Agora,  $p \nmid a$  significa  $\text{mdc}(p, a) = 1$ . Segue  $p \mid b$  por 2.15.

■

Observamos que esta propriedade necessária dos números primos é também suficiente para que um  $n \in \mathbb{N}$  seja primo: Pois, se  $n = rs$  é composto ( $1 < s \leq r < n$ ), temos  $n|rs$  porém tanto  $n \nmid r$  quanto  $n \nmid s$ .

Por exemplo: Se  $5|ab$  então temos certeza que um dos fatores  $a$  ou  $b$  (ou ambos) é múltiplo de 5. Mas, temos  $6|12 = 3 \cdot 4$ , porém tanto  $6 \nmid 3$  quanto  $6 \nmid 4$ .

### 3.3 O teorema fundamental da aritmética.

a) *Todo número  $1 < n \in \mathbb{N}$  é produto de números primos, quer dizer, existem  $p_1, p_2, \dots, p_r \in \mathbb{P}$  tais que*

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_r.$$

b) *Se  $p_1 \cdot p_2 \cdot \dots \cdot p_r = q_1 \cdot q_2 \cdot \dots \cdot q_s$  com  $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s \in \mathbb{P}$  e se  $p_1 \leq p_2 \leq \dots \leq p_r$  tal como  $q_1 \leq q_2 \leq \dots \leq q_s$ , então*

$$r = s \text{ e } p_1 = q_1, p_2 = q_2, \dots, p_r = q_r.$$

**Demonstração:** a) Se  $n = p$  é um número primo, a afirmação fica clara ( $r = 1$ ). Mostramos a afirmação para  $n$  composto, supondo-se sua veracidade para todo  $m \in \mathbb{N}$  com  $1 < m < n$ .

Seja  $S = \{t \in \mathbb{N} \mid 1 < t|n\}$ . Como  $n > 1$  sabemos  $n \in S$ , i.e.  $S \neq \emptyset$ . Pelo princípio da indução existe um  $p_1 \in S$  minimal. É claro (provar isto!) que  $p_1$  é primo e temos  $m \in \mathbb{N}$  com  $n = p_1 \cdot m$ . Como  $p_1 > 1$  e  $n$  não é primo, segue  $1 < m < n$ . Como a afirmação já é válida para este  $m$ , existem  $p_2, p_3, \dots, p_r \in \mathbb{P}$  tais que  $m = p_2 \cdot p_3 \cdot \dots \cdot p_r$ . Segue, como afirmado:

$$n = p_1 \cdot m = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_r.$$

b) Suponha  $p_1 \cdot p_2 \cdot \dots \cdot p_r = q_1 \cdot q_2 \cdot \dots \cdot q_s$  com  $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s \in \mathbb{P}$  e  $p_1 \leq p_2 \leq \dots \leq p_r$  tal como  $q_1 \leq q_2 \leq \dots \leq q_s$

Temos  $p_1|q_1 \cdot q_2 \cdot \dots \cdot q_s$  de onde concluímos, aplicando-se repetidas vezes a Proposição 3.2, que  $p_1$  tem que dividir algum dos fatores  $q_1, q_2, \dots, q_s$ . Logo existe  $k$  ( $1 \leq k \leq s$ ) com  $p_1|q_k$ . Como  $p_1$  e  $q_k$  são primos, temos  $p_1 = q_k \geq q_1$ . Da mesma forma,  $q_1|p_\ell$  para algum  $\ell$  ( $1 \leq \ell \leq r$ ) e segue  $q_1 = p_\ell \geq p_1$ . Assim  $p_1 = q_1$ . Agora, de  $p_1 \cdot p_2 \cdot \dots \cdot p_r = p_1 \cdot q_2 \cdot \dots \cdot q_s$  segue

$$p_2 \cdot \dots \cdot p_r = q_2 \cdot \dots \cdot q_s.$$

Por indução concluímos  $r-1 = s-1$  (i.e.  $r = s$ ) e  $p_2 = q_2, p_3 = q_3, \dots, p_r = q_r$ .  
 Junto com  $p_1 = q_1$  isto dá a afirmação. ■

É comum, formular o teorema fundamental da aritmética da seguinte forma:

### 3.3' O teorema da decomposição primária.

Para todo número  $1 < n \in \mathbb{N}$  existem únicos primos **distintos**  $p_1, p_2, \dots, p_r$  (os quais podemos supor em ordem natural  $p_1 < \dots < p_r$ ) e únicos números  $a_1, a_2, \dots, a_r \in \mathbb{N}$  de tal maneira que

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_r^{a_r} = \prod_{k=1}^r p_k^{a_k}$$

O produto  $\prod_{k=1}^r p_k^{a_k}$  chama-se a *decomposição primária* de  $n$ .

#### A QUANTIDADE DOS DIVISORES DE UM NÚMERO $n$

Como o conjunto dos divisores de um número  $n \in \mathbb{N}$  é finito, podemos nos interessar pelo tamanho deste conjunto, isto é, pela quantidade dos divisores de  $n$ . Dado  $n \in \mathbb{N}$ , vamos indicar por

$$\tau(n) = |\{t \in \mathbb{N} \mid t \text{ divide } n\}|$$

a *quantidade dos divisores naturais* de  $n$ .

Por exemplo, temos  $\tau(n) = 1 \iff n = 1$ ,  $\tau(n) = 2 \iff n = p$  é primo.

Lembrando-se que  $t \mid n \iff \exists, s = \frac{n}{t} \in \mathbb{N}$  tal que  $n = st$  vemos que também  $\frac{n}{t}$  divide  $n$ . Como ainda  $\frac{n}{\frac{n}{t}} = t$ , temos que

$$\{t \mid t \text{ divide } n\} = \left\{ \frac{n}{t} \mid t \text{ divide } n \right\} .$$

Por exemplo, para os divisores de 12 temos

$$\{1, 2, 3, 4, 6, 12\} = \left\{ \frac{12}{1}, \frac{12}{2}, \frac{12}{3}, \frac{12}{4}, \frac{12}{6}, \frac{12}{12} \right\} .$$

É fácil verificar a seguinte observação interessante:



### 3.4 Proposição.

Para todo  $n \in \mathbb{N}$  temos

$$\prod_{t|n} t = n^{\tau(n)/2} \quad \left( = \sqrt{n^{\tau(n)}} \right).$$

Em palavras: O produto formado sobre todos os divisores positivos de  $n$  é a potência  $\tau(n)/2$ -ésima de  $n$ .

**Demonstração:** Temos

$$\left( \prod_{t|n} t \right)^2 = \left( \prod_{t|n} t \right) \cdot \left( \prod_{t|n} \frac{n}{t} \right) = \prod_{t|n} t \cdot \frac{n}{t} = \prod_{t|n} n = n^{\tau(n)},$$

pois  $\tau(n)$  é a quantidade dos fatores  $n$  deste último produto. Extraindo-se ainda a raiz quadrada de ambos os lados, vemos a afirmação. ■

Podemos determinar  $\tau(n)$  também a partir da decomposição primária de  $n$ .

### 3.5 Observação.

Seja  $1 < n \in \mathbb{N}$  escrito na decomposição primária

$$n = \prod_{k=1}^r p_k^{a_k}$$

com  $p_1, \dots, p_r$  primos distintos,  $r, a_1, \dots, a_r \in \mathbb{N}$ . Um número  $t \in \mathbb{N}$  é divisor de  $n$  se e somente se

$$t = \prod_{k=1}^r p_k^{\ell_k} \quad \text{com} \quad 0 \leq \ell_1 \leq a_1, \dots, 0 \leq \ell_r \leq a_r.$$

**Demonstração:** Seja  $t = \prod_{k=1}^r p_k^{\ell_k}$  com  $0 \leq \ell_1 \leq a_1, \dots, 0 \leq \ell_r \leq a_r$ . Temos

$$t \cdot \prod_{k=1}^r p_k^{a_k - \ell_k} = \prod_{k=1}^r p_k^{\ell_k} \cdot \prod_{k=1}^r p_k^{a_k - \ell_k} = \prod_{k=1}^r p_k^{a_k} = n,$$

onde  $\prod_{k=1}^r p_k^{a_k - \ell_k} \in \mathbb{N}$ , pois  $a_k - \ell_k \geq 0$ . Logo,  $t$  é divisor de  $n$ .

Reciprocamente, qualquer divisor  $t$  de  $n$  tem que ter esta forma, pela unicidade da decomposição primária de  $t$  e  $n$ . Logo, a afirmação vale. ■

### 3.6 Conseqüência.

Seja  $n \in \mathbb{N}$  escrito como

$$n = \prod_{k=1}^r p_k^{a_k}$$

com  $p_1, p_2, \dots, p_r$  primos distintos e  $a_1, a_2, \dots, a_r \in \mathbb{N}$ . Então

$$\tau(n) = \prod_{k=1}^r (a_k + 1).$$

**Demonstração:** Pela observação 3.5 temos que os divisores  $t \in \mathbb{N}$  de  $n$  correspondem, biunivocamente, às  $r$ -uplas  $(\ell_1, \ell_2, \dots, \ell_r)$  com  $0 \leq \ell_1 \leq a_1, \dots, 0 \leq \ell_r \leq a_r$ . Portanto  $\tau(n)$  é a quantidade destas  $r$ -uplas. Mas, na  $k$ -ésima coordenada temos as  $a_k + 1$  possibilidades  $0, 1, 2, \dots, a_k$  para escolhermos  $\ell_k$  ( $1 \leq k \leq r$ ). Isto dá um total de  $(a_1 + 1)(a_2 + 1) \cdot \dots \cdot (a_r + 1)$  escolhas e fornece a afirmação. ■

### 3.7 Conseqüência.

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

$n$  é um quadrado perfeito  $\iff \tau(n)$  é ímpar.

**Demonstração:** Seja  $n = \prod_{k=1}^r p_k^{a_k}$  a decomposição primária de  $n$ . Temos que  $n$  é um quadrado perfeito  $\iff$  todos os expoentes  $a_1, a_2, \dots, a_r$  são pares  $\iff$  todos os  $a_1 + 1, a_2 + 1, \dots, a_r + 1$  são ímpares  $\iff$  o produto  $(a_1 + 1)(a_2 + 1) \dots (a_r + 1) = \tau(n)$  é ímpar. ■

A decomposição primária é útil para determinar o mdce o mmcde dois números:

Dados dois números  $n, m \in \mathbb{N}$ , existem primos distintos  $p_1, \dots, p_r$  (os primos que dividem em pelo menos um de  $n$  ou  $m$ ) e expoentes não-negativos  $a_1, \dots, a_r, b_1, \dots, b_r \in \mathbb{N}_0$  tais que, simultaneamente,

$$n = \prod_{k=1}^r p_k^{a_k} \quad \text{e} \quad m = \prod_{k=1}^r p_k^{b_k}.$$

■

### 3.8 Proposição.

Sejam  $n, m \in \mathbb{N}$ , escritos simultâneamente na forma indicada. Então

$$\text{mdc}(m, n) = \prod_{k=1}^r p_k^{\min(a_k, b_k)}$$

tal como

$$\text{mmc}(m, n) = \prod_{k=1}^r p_k^{\max(a_k, b_k)} .$$

**Demonstração:** Para o mdc:

Como  $\min(a_k, b_k) \leq a_k$  e também  $\leq b_k$ , temos por 3.5, que o produto  $\prod_{k=1}^r p_k^{\min(a_k, b_k)}$  certamente é divisor comum de  $n$  e  $m$ . Por outro lado, um qualquer divisor comum  $t$  de  $n$  e  $m$ , é da forma  $t = \prod_{k=1}^r p_k^{\ell_k}$  com  $0 \leq \ell_k \leq a_k$  e  $0 \leq \ell_k \leq b_k$  e então  $0 \leq \ell_k \leq \min(a_k, b_k)$ . Logo,  $t \mid \prod_{k=1}^r p_k^{\min(a_k, b_k)}$ . Isto mostra  $\text{mdc}(m, n) = \prod_{k=1}^r p_k^{\min(a_k, b_k)}$ .

Da mesma forma trata-se o mmc. Fazer isto como exercício!

■

### A DECOMPOSIÇÃO PRIMÁRIA DE $n!$

Estudamos em seguida qual é a decomposição primária do número  $n!$  para qualquer  $n \in \mathbb{N}$ . Agora, se  $p \mid n! = 1 \cdot 2 \cdot \dots \cdot n$  para algum prim  $p$ , uma aplicação repetida de 3.2 mostra que  $p$  tem que dividir um dos fatores  $2, 3, \dots, n$  deste produto. Em particular,  $n!$  não pode ser divisível por nenhum primo  $> n$ . Por outro lado, qualquer primo  $p$  com  $p \leq n$  aparece em  $n!$  e podemos afirmar de antemão que a decomposição primária de  $n!$  é da forma

$$n! = \prod_{k=1}^r p_k^{a_k} ,$$

onde  $p_1 = 2, p_2 = 3, p_3 = 5, \dots, p_r \leq n < p_{r+1}$ , i. e.  $p_1, \dots, p_r$  são exatamente todos os primos que são  $\leq n$  e os expoentes  $a_1, a_2, \dots, a_r$  são números naturais os quais devemos determinar.

Uma maneira mais elegante de escrever isto é

$$n! = \prod_{p \in \mathcal{P}} p^{a_p(n)} .$$

Aqui  $p$  é considerado seu próprio índice e o índice dos expoentes  $a_p(n) \in \mathbb{N}_0$ , sendo que  $p$  varia sobre  $\mathbb{P}$  com a condição  $a_p(n) = 0$  se  $p > n$ .

A pergunta é

$$a_p(n) = ? \quad \text{se } p \leq n ?$$

Vejamos um exemplo (escrevemos  $a_p = a_p(40)$  para simplificar a notação):

$$40! = 2^{a_2} \cdot 3^{a_3} \cdot 5^{a_5} \cdot 7^{a_7} \cdot 11^{a_{11}} \cdot 13^{a_{13}} \cdot 17^{a_{17}} \cdot 19^{a_{19}} \cdot 23^{a_{23}} \cdot 29^{a_{29}} \cdot 31^{a_{31}} \cdot 37^{a_{37}}$$

$$a_2, a_3, \dots, a_{37} = ?$$

É imediato que  $a_{37} = a_{31} = a_{29} = a_{23} = 1$ .

Agora, 19 divide 19 e 38. Logo,  $a_{19} = 2$ , ocorrendo o mesmo com  $a_{17}$ .

Temos  $a_{13} = 3$ , devido aos fatores 13, 26 e 39.

De forma semelhante:  $a_{11} = 3$  e  $a_7 = 5$ .

Agora temos  $8 = \frac{40}{5}$  fatores 5 em  $40!$ , devido aos divisores 5, 10, 15, 20, 25, 30, 35, 40. Mas vem mais um fator 5, ainda não contado, devido a  $25 = 5^2$ . Logo  $a_5 = 9$ .

O número 3 aparece 13 vezes nos divisores 3, 6, 9, ..., 39, mais 4 vezes nos divisores 9, 18, 27, 36 e mais uma terceira vez em 27. Isto dá um total de 18 fatores 3 em  $40!$ . Logo  $a_3 = 18$ .

Finalmente contamos  $a_2 = 38$ , devido a  $20 = \frac{40}{2}$  fatores 2 em 2, 4, 6, 8, 10, ..., 40, mais 10 fatores 2, ainda não contados em 4, 8, 12, 16, ..., 40, mais 5 fatores ainda não contados em 8, 16, 24, 32, 40, mais 2 fatores 2, ainda não contados, em 16, 32, mais um fator 2 devido a 32.

Logo temos

$$40! = 2^{38} \cdot 3^{18} \cdot 5^9 \cdot 7^5 \cdot 11^3 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23 \cdot 29 \cdot 31 \cdot 37.$$

Como fica o caso geral?

### 3.9 Definição.

Para cada número real  $x$  indicamos por

$$[x] = \text{o maior inteiro contido em } x$$

(i.e. escrevemos  $x = [x] + r$  onde  $[x] \in \mathbb{Z}$  e  $r \in \mathbb{R}$  com  $0 \leq r < 1$ ).

Por exemplo temos  $\left[\frac{17}{4}\right] = \left[\frac{19}{4}\right] = 4$ ,  $[\sqrt{5}] = 2$ ,  $[\pi] = 3$ ,  $[-\pi] = -4$ . Quando  $x \geq 0$  tem a forma decimal  $x = n, \dots$  com  $n \in \mathbb{N}_0$ , temos claramente  $[n, \dots] = n$ .

### 3.10 Teorema.

Para cada  $n \in \mathbb{N}$  a decomposição primária de  $n!$  é dada por

$$n! = \prod_{p \in P} p^{a_p(n)},$$

onde os expoentes  $a_p(n)$  são calculados por

$$a_p(n) = \sum_{k=1}^{\infty} \left[ \frac{n}{p^k} \right].$$

Observamos que esta soma  $\sum_{k=1}^{\infty} \left[ \frac{n}{p^k} \right]$  a qual é formalmente uma soma infinita, na verdade contém somente finitos somandos não-nulos, já que  $\left[ \frac{n}{p^k} \right] = 0$ , sempre quando  $p^k > n$ . Particularmente,  $a_p(n) = 0$ , se  $p > n$ . Isto significa que no produto (formalmente infinito) para  $n!$  na verdade aparecem automaticamente só os primos  $p \leq n$ .

**Demonstração:** Seja  $p$  um primo qualquer.

Existe um único  $\ell_1 \in \mathbb{N}_0$  tal que

$$\ell_1 p \leq n < (\ell_1 + 1)p.$$

Da mesma forma, existe um único  $\ell_2 \in \mathbb{N}_0$  tal que

$$\ell_2 p^2 \leq n < (\ell_2 + 1)p^2,$$

.....

em geral, para todo  $k \in \mathbb{N}$  existe um único  $\ell_k \in \mathbb{N}_0$  tal que

$$\ell_k p^k \leq n < (\ell_k + 1)p^k.$$

.....

Agora, em  $n!$  aparecem

$\ell_1$  fatores  $p$  devido os fatores

$$p, 2p, 3p, \dots, \ell_1 p,$$

mais  $\ell_2$  fatores  $p$ , ainda não contados, devidos a

$$p^2, 2p^2, 3p^2, \dots, \ell_2 p^2,$$

.....

mais  $\ell_k$  fatores  $p$ , ainda não contados, devido a

$$p^k, 2p^k, 3p^k, \dots, \ell_k p^k$$

.....

Isto dá um total de  $a_p(n) = \ell_1 + \ell_2 + \dots + \ell_k + \dots$  fatores  $p$  contidos em  $n!$ . Mas, de  $\ell_k p^k \leq n < (\ell_k + 1)p^k$  segue  $\ell_k \leq \frac{n}{p^k} < (\ell_k + 1)$ , ou seja,

$$\ell_k = \left[ \frac{n}{p^k} \right].$$

Logo temos como afirmado

$$a_p(n) = \sum_{k=1}^{\infty} \left[ \frac{n}{p^k} \right].$$

■

Observa-se que sempre

$$a_2(n) \geq a_3(n) \geq a_5(n) \geq \dots \geq a_p(n) \geq a_q(n) \geq \dots \text{ se } p < q.$$

Uma consequência disto é, por exemplo, que  $n!$  termina em  $a_5(n)$  zeros.

### 3.11 Exemplo.

- Em quantos zeros termina  $357!$  ?
- Qual é a maior potência de  $165$  que divide em  $2000!$  ?

Respostas:

a) Em  $a_5(357) = \sum_{k=1}^{\infty} \left[ \frac{357}{5^k} \right] = \left[ \frac{357}{5} \right] + \left[ \frac{357}{25} \right] + \left[ \frac{357}{125} \right] = 71 + 14 + 2 = 87$  zeros.

b) Temos  $165 = 3 \cdot 5 \cdot 11$  e vale  $a_{11}(2000) = \sum_{k=1}^{\infty} \left[ \frac{2000}{11^k} \right] = \left[ \frac{2000}{11} \right] + \left[ \frac{2000}{121} \right] + \left[ \frac{2000}{1331} \right] = 181 + 16 + 1 = 198$ . Logo é a 198-ésima a maior potência de  $165$  - e também a maior de  $11$  - que divide  $2000!$ .

■

**3.12 Teorema.** (EUCLIDES)

*O conjunto  $\mathbb{P}$  dos números primos é infinito.*

**Demonstração:** Suponhamos  $\mathbb{P} = \{p_1, p_2, \dots, p_r\}$  fosse um conjunto finito. Consideremos o número natural  $n = p_1 \cdot p_2 \cdot \dots \cdot p_r + 1$ . Pelo Teorema fundamental da aritmética, este  $n > 1$  é divisível por algum primo  $q$ . Pela suposição,  $q = p_k$  para algum  $k \in \{1, 2, \dots, r\}$ . Daí segue o absurdo que  $q|1$ . Logo, nenhum conjunto finito pode abranger todos os primos. ■

**3.13 Proposição.**

*Para o  $n$ -ésimo número primo  $p_n$  vale a estimativa*

$$p_n \leq 2^{2^{n-1}}.$$

**Demonstração:** Para  $n = 1$  afirma-se  $2 = p_1 \leq 2^{2^{1-1}} = 2^1 = 2$  o que certamente é verdade. Suponhamos já provadas as desigualdades

$$\begin{aligned} p_1 &\leq 2^{2^0} \\ p_2 &\leq 2^{2^1} \\ p_3 &\leq 2^{2^2} \\ &\dots\dots\dots \\ p_n &\leq 2^{2^{n-1}}. \end{aligned}$$

Se  $\mathbb{P} \ni q | p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$ , então  $q > p_n$ , particularmente,  $p_{n+1} \leq q$ .

Segue

$$p_{n+1} \leq p_1 \cdot p_2 \cdot \dots \cdot p_n + 1 \leq 2^{1+2+2^2+\dots+2^{n-1}} + 1 = 2^{2^n-1} + 1 \leq 2^{2^n-1} + 2^{2^n-1} = 2^{2^n}.$$

■

Convém observar que esta cota superior para o tamanho de  $p_n$  não é muito boa. Uma cota melhor obtem-se, admitindo-se (sem demonstração) o seguinte mais profundo

### 3.14 Teorema. (TCHEBYCHEF).

Para  $2 \leq m \in \mathbb{N}$  temos que sempre existe um primo  $p$  com  $m < p < 2m$ .

### 3.15 Conseqüência.

Para o  $n$ -ésimo número primo  $p_n$  vale a estimativa

$$p_n \leq 2^n.$$

**Demonstração:** Temos  $2 = p_1 \leq 2^1$  e por 3.14:  $\forall n = 1, 2, 3, \dots$  tem-se  $p_n < p_{n+1} < 2 \cdot p_n$ . De  $p_n \leq 2^n$  segue então  $p_{n+1} \leq 2 \cdot 2^n = 2^{n+1}$ . ■

### 3.16 Definição.

Um par de números  $(p, p + 2)$  é denominado um *gêmeo de primos* se ambos,  $p$  e  $p + 2$  são primos.

### 3.17 Exemplo.

$$(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73)$$

são os *gêmeos de primos* com  $p \leq 97$ .

Enquanto existem infinitos primos, é interessante fazer a seguinte

### 3.18 Observação.

*É desconhecido se existe uma quantidade infinita de gêmeos de primos.*

A FUNÇÃO  $\pi$  DOS NÚMEROS PRIMOS

### 3.19 Definição.

Para todo  $0 \leq x \in \mathbb{R}$  define-se a função  $\pi(x)$  por

$$\pi(x) = |\{p \in \mathbb{P} \mid p \leq x\}|$$

isto é,  $\pi(x)$  é a quantidade dos números primos menores ou iguais a  $x$ .

Por exemplo temos  $\pi(x) = 0$  se  $0 \leq x < 2$ ,  $\pi(x) = 1$  se  $2 \leq x < 3$ ,  $\pi(x) = 2$  se



$3 \leq x < 5$ . Em geral:

Se  $p_1 = 2, p_2 = 3, p_3 = 5, p_4, p_5, \dots, p_{25} = 97, \dots$  é a seqüência dos números primos em ordem natural, então

$$\pi(x) = r \text{ se } p_r \leq x < p_{r+1} \quad (r = 1, 2, 3, \dots).$$

Uma das grandes descobertas do final do século passado (1896), a qual citamos aqui sem apresentar sua mais profunda demonstração, é o chamado *Teorema dos números primos* e que leva os nomes dos matemáticos CAUCHY/HADAMARD/DE LA VALÉE POUSSIN). Ele descreve o comportamento assintótico da função  $\pi(x)$ .

### 3.20 Teorema.

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$

Isto quer dizer que, se  $x$  é grande, a quantidade dos números primos  $\leq x$  é dada, com aproximação cada vez melhor, por  $\frac{x}{\ln x}$ .

## DECOMPOSIÇÃO DE NÚMEROS E O CRIVO DO ERATÓSTENES

### 3.21 Observação.

Sejam  $n, r, s \in \mathbb{N}$  tais que  $n = rs$  com  $1 \leq s \leq r \leq n$ .

a) Temos  $s \leq \sqrt{n} \leq r$ .

b) Se  $n$  for composto, então existem  $r, s \in \mathbb{N}$  tais que  $1 < s \leq \sqrt{n} \leq r < n$  e  $n = rs$ .

**Demonstração:** a) De  $s \leq r < \sqrt{n}$  segue a contradição

$$n = sr < \sqrt{n}\sqrt{n} = n.$$

Da mesma forma, de  $\sqrt{n} < s \leq r$  segue a contradição

$$n = \sqrt{n}\sqrt{n} < sr = n.$$

Logo devemos ter  $s \leq \sqrt{n} \leq r$ .

b) é uma consequência de a). ■

### 3.22 Conseqüência.

Se  $n \in \mathbb{N}$  é composto, então  $n$  é divisível por algum primo  $p \leq \sqrt{n}$ .

**Demonstração:** Podemos escolher em 3.21 b) um divisor primo  $p$  de  $s$ . ■

Esta última observação tem importância prática na procura de números primos e é a base do chamado

*crivo do ERATÓSTENES:*

Desejamos determinar os primos  $\leq n$  para um dado  $2 \leq n \in \mathbb{N}$ . Para isto escrevemos os números

$$2, 3, 4, 5, 6, \dots, n.$$

Guardamos o 2 como primo e riscamos todos os números pares  $4 \leq 2k \leq n$ .

Depois guardamos o 3 e riscamos todos os múltiplos de 3 com  $6 \leq 3k \leq n$ . O próximo número não riscado é o primo 5. Riscamos seus múltiplos

$10 \leq 5k \leq n$  e continuamos desta maneira.

Vemos que, depois de riscar os múltiplos de todos os primos até o maior primo  $p \leq \sqrt{n}$ , sobram somente os números primos até  $n$ .

Por exemplo, para  $n = 100$ : Depois de riscar entre os números  $2, 3, 4, 5, 6, \dots, 100$  os múltiplos (próprios) de 2, 3, 5 e 7, sobram os 25 primos 2, 3, 5, 7, 11, 13,  $\dots$ , 83, 89, 97. Isto é claro por 3.22, pois qualquer  $n \leq 100$  composto é múltiplo de um dos primos  $2, 3, 5, 7 \leq 10 = \sqrt{100}$ .

Também podemos pensar assim: Para se verificar se um dado número  $n$  é primo ou composto, só é preciso testar como possíveis divisores os primos  $p \leq \sqrt{n}$ . Se nenhum deles divide,  $n$  será primo.

Portanto, para ver se um  $n \leq 100$  é primo ou não, os quatro testes

$$2|n(?), \quad 3|n(?), \quad 5|n(?), \quad 7|n(?)$$

são suficientes, dos quais  $2|n(?)$  e  $5|n(?)$  têm resposta óbvia.

Da mesma maneira, somente os testes com (no máximo) os primos  $p \leq 13$

são suficientes para conseguir uma possível decomposição de um qualquer  $n \leq 200$ .  $p \leq 31$  para qualquer  $n \leq 1000$ ,  $p \leq 97$  para  $n \leq 10000$ .

### 3.23 Proposição.

Seja  $n \in \mathbb{N}$  ímpar.

Entre os pares de inteiros  $(x, y)$  com

$$0 \leq y < x \leq n = x^2 - y^2$$

e os pares  $(r, s)$  com

$$1 \leq s \leq r \leq n = rs$$

existe uma correspondência biunívoca natural.

**Demonstração:** Se  $n = x^2 - y^2$  com  $0 \leq y < x \leq n$ , façamos  $r = x + y$  e  $s = x - y$  e segue  $n = rs$  e  $1 \leq s \leq r \leq n$ .

Seja, reciprocamente,  $n = rs$  com  $1 \leq s \leq r \leq n$ . Como  $n$  é ímpar, temos que  $r$  e  $s$  são ímpares e  $\frac{r \pm s}{2}$  são inteiros. Façamos  $x = \frac{r+s}{2}$  e  $y = \frac{r-s}{2}$ . Temos  $x, y \in \mathbb{N}_0$  e  $0 \leq y < x \leq n$ . Além disso vale  $x^2 - y^2 = \frac{(r+s)^2 - (r-s)^2}{4} = rs = n$ .

■

### 3.24 Conseqüência.

Seja  $n \in \mathbb{N}$  ímpar.

- $n$  possui tantas decomposições distintas  $n = x^2 - y^2$  como diferença de dois quadrados quantas decomposições multiplicativas distintas  $n = rs$  ele admite.
- $n$  é primo, se e somente se

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

é a única decomposição de  $n$  como diferença de dois quadrados.

### 3.25 Exemplos.

- Para  $n = 33 = 33 \cdot 1 = 11 \cdot 3$  temos as decomposições correspondentes como diferença de dois quadrados:

$$33 = 17^2 - 16^2 = 7^2 - 4^2.$$

- Para  $n = 9 = 9 \cdot 1 = 3 \cdot 3$  temos

$$9 = 5^2 - 4^2 = 3^2 - 0^2.$$

c) Em geral, para  $n = pq = pq \cdot 1 = p \cdot q$  onde  $p \geq q$  são primos, temos as decomposições correspondentes como diferença de dois quadrados:

$$pq = \left(\frac{pq+1}{2}\right)^2 - \left(\frac{pq-1}{2}\right)^2 = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2 .$$

d) Para  $n = 105 = 105 \cdot 1 = 35 \cdot 3 = 21 \cdot 5 = 15 \cdot 7$  temos

$$105 = 63^2 - 62^2 = 19^2 - 16^2 = 13^2 - 8^2 = 11^2 - 4^2 .$$

A descoberta de uma decomposição de um número ímpar  $n$  como diferença de dois quadrados pode ser favorável quando  $n$  é "quase um quadrado perfeito", i.e. quando  $n = rs$  com  $y = r - s$  "pequeno". Isto pode servir para descobrir a decomposição primária de um tal número.

Vejamos alguns exemplos:

Queremos descobrir se o número  $n = 2438323$  é primo ou não. Temos  $\sqrt{n} = 1561,51\dots$  e as tentativas se este  $n$  é divisível por algum primo  $p \leq 1561$ , é decepcionante, experimentando-se com  $p = 3, 7, 11, 13, \dots$ . Escrevendo-se porém  $y^2 = x^2 - n$ , começando com  $x = 1562$ , vemos na hora que  $x^2 - n$  é de fato um quadrado perfeito  $y^2$  com  $y = 39$ . Isto nos dá a decomposição  $n = (1562 + 39)(1562 - 39) = 1601 \cdot 1523$ . Esta é a decomposição completa de  $n$ , pois 1523 e 1601 são realmente primos (senão  $n$  já teria sido divisível por algum  $p \leq 37$ ).

Para ganhar a decomposição de  $n = 17473$ , calculamos  $\sqrt{n} = 132,18\dots$  e as colocações  $x = 133, 134, 135 \dots$  mostram na quinta tentativa para  $x = 137$  que realmente  $137^2 - n = 36^2$ . Mais uma vez descobrimos a decomposição  $n = (137 + 36)(137 - 36) = 173 \cdot 101$ .

Se  $n = p(p+2)$  é por exemplo (sem que se tenha conhecimento antecipado disso!) o produto dos primos de um gêmeo, este método - observando-se  $p < \sqrt{n} = \sqrt{p(p+2)} < \sqrt{p^2 + 2p + 1} = p + 1$  - fornece logo no primeiro passo para  $x = p + 1$ :

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

ou seja, a decomposição  $n = [(p+1) + 1] \cdot [(p+1) - 1]$ .

Mais algumas observações com respeito a números primos.

## A CONJETURA DE GOLDBACH

CHRISTIAN GOLDBACH (1690-1754) estabeleceu a seguinte pergunta que até hoje não pôde ser decidida:

### 3.26 Conjetura.

*Todo número par  $n > 4$  é soma de dois primos ímpares.*

### 3.27 Exemplo.

$6 = 3 + 3$ ,  $8 = 3 + 5$ ,  $10 = 7 + 3 = 5 + 5$ ,  $12 = 7 + 5$ , ...,  
 $100 = 97 + 3 = 89 + 11 = 83 + 17 = 71 + 29 = 59 + 41 = 53 + 47$   
.....

Pelo teorema de Tchebychef existe sempre um primo entre qualquer número e seu dobro. Por outro lado, é uma observação simples que existem intervalos de comprimento arbitrário  $n$ , livre de números primos, como mostra

### 3.28 Proposição.

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

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

*são todos compostos.*

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

$$\begin{aligned} 2 \mid (n+1)! + 2 &= k_n + 1, \\ 3 \mid (n+1)! + 3 &= k_n + 2, \\ &\vdots \quad \vdots \quad \vdots \\ n \mid (n+1)! + n &= k_n + (n-1), \\ (n+1) \mid (n+1)! + (n+1) &= k_n + n, \end{aligned}$$

mostrando que estes números são compostos. ■

## PROGRESSÕES ARITMÉTICAS E PRIMOS

Dados  $a, b \in \mathbb{N}_0$  com  $b > 0$ , podemos considerar a progressão aritmética

$$(a + bn)_{n \in \mathbb{N}_0} = (a, a + b, a + 2b, a + 3b, \dots)$$

e podemos perguntar sobre números primos possivelmente aparecendo nela. Para que um dos  $a + bn$  com  $n \geq 2$  possa ser primo, é claramente necessário que  $\text{mdc}(a, b) = 1$ , pois  $\text{mdc}(a, b)$  divide cada  $a + bn$ . No caso  $a = 0, b = 1$  temos a seqüência dos números naturais, a qual contém infinitos primos por EUCLIDES. Também, se  $a = 1$  e  $b = 2$ , a seqüência dos números ímpares contém infinitos primos.

É mais um resultado clássico e profundo do século passado, devido a DIRICHLET (1837) que queremos citar aqui sem demonstração:

### 3.29 Teorema.

*Se  $a, b \in \mathbb{N}_0$  são dois números com  $b > 0$  e  $\text{mdc}(a, b) = 1$ , então, na progressão aritmética*

$$(a + bn)_{n \in \mathbb{N}_0}$$

*aparecem infinitos números primos.*

Como mais um caso particular deste teorema de Dirichlet queremos provar o

### 3.30 Exemplo.

*Para  $b = 4$  e  $a = 3$  temos:*

*Existem infinitos primos da forma  $4n + 3$   $n = 0, 1, 2, 3, \dots$*

### 3.31 Observação.

*Sejam  $k_1, k_2, \dots, k_r \in \mathbb{N}$ . Então o produto*

$$(4k_1 + 1) \cdot (4k_2 + 1) \cdot \dots \cdot (4k_r + 1)$$

*tem a forma  $4\ell + 1$  com  $\ell \in \mathbb{N}$ .*

*(i.e. um produto de números que deixam resto 1 quando divididos por 4 é um número do mesmo tipo [ver § 6]).*

**Demonstração:** É suficiente, verificar isto para dois fatores:

$$(4k_1 + 1) \cdot (4k_2 + 1) = 16k_1k_2 + 4k_1 + 4k_2 + 1 = 4(4k_1k_2 + k_1 + k_2) + 1.$$

**Demonstração** do Exemplo 3.30: Suponhamos  $\overline{\mathbb{P}} = \mathbb{P} \cap \{4n+3 \mid n = 0, 1, 2, 3, \dots\}$  é finito, digamos

$$\overline{\mathbb{P}} = \{p_1=3, p_2=7, \dots, p_r\} .$$

Consideremos o número  $N = 4p_1p_2\dots p_r - 1 = 4(p_1p_2\dots p_r - 1) + 3 > 1$  e seja  $N = q_1 \cdot q_2 \cdot \dots \cdot q_s$  com primos  $q_1, \dots, q_s \in \mathbb{P}$ . Todo número ímpar é da forma  $4k+1$  ou  $4k+3$ . Como  $N$  é da forma  $4\ell+3$ , por 3.31, nem todo  $q_i$  pode ter a forma  $4k_i+1$ , ou seja, existe um  $q_i \in \overline{\mathbb{P}}$ , digamos  $q_i = p_j$ . Mas então segue  $q_i \mid 4p_1\dots p_r - N = 1$ , um absurdo. Logo,  $\overline{\mathbb{P}}$  não pode ser finito. ■

## POLINÔMIOS E PRIMOS

Queremos encerrar este parágrafo, pensando sobre o natural desejo de escrever o  $n$ -ésimo número primo  $p_n$  como uma função transparente de  $n$ . Será que existe alguma expressão polinomial  $f(n) = a_s n^s + a_{s-1} n^{s-1} + \dots + a_1 n + a_0$  com coeficientes inteiros, que forneça a seqüência dos números primos - ou pelo menos - forneça somente primos?

O seguinte exemplo é interessante neste contexto.

### 3.32 Exemplo.

Para  $f(n) = n^2 + n + 41$  temos

$$f(n) \in \mathbb{P} \quad \text{para todo } n = 1, 2, 3, \dots, 39 .$$

Entretanto,  $f(40) = 41^2$  e  $f(41) = 41 \cdot 43$ .

A resposta geral é decepcionante: Nenhum polinômio (não constante) pode assumir somente números primos, como mostra

### 3.33 Proposição.

*Seja  $f(n) = a_s n^s + a_{s-1} n^{s-1} + \dots + a_1 n + a_0$  uma expressão polinomial com coeficientes  $a_0, a_1, \dots, a_s \in \mathbb{Z}$  e  $a_s > 0, s \geq 1$ . Então a seqüência  $(f(n))_{n \in \mathbb{N}}$  assume infinitos valores naturais compostos.*

**Demonstração:** Claro que  $f(n)$  pode assumir somente finitos valores negativos, pois  $a_s > 0$ . Se  $f(n)$  sempre é composto, não há nada para provar. Podemos supor

então que exista  $n_0 \in \mathbb{N}$  tal que  $f(n_0) = p$  é primo e  $f(n) > 0$  para  $n \geq n_0$ . Para todo  $t \in \mathbb{N}$  temos

$$\begin{aligned} f(n_0 + tp) &= a_s(n_0 + tp)^s + \dots + a_1(n_0 + tp) + a_0 = \\ &= a_s n_0^s + \dots + a_1 n_0 + a_0 + k_t p = p(1 + k_t) \end{aligned}$$

com  $k_t \in \mathbb{N}$  apropriado. Segue que os valores

$$f(n_0 + tp) = p(1 + k_t) \quad \text{com } t \in \mathbb{N}$$

são números compostos. Como  $k_t = a_s p^s t^s \pm \dots$  assume infinitos valores naturais distintos quando  $t \in \mathbb{N}$ , concluímos a afirmação. ■



## § 4 Triplos PITAGÓRICOS e a conjectura de FERMAT

### TRIPLOS PITAGÓRICOS

#### 4.1 Definição.

Um triplo de números naturais  $(x, y, z)$  chama-se um *triplo Pitagórico* se

$$x^2 + y^2 = z^2 .$$

O triplo  $(x, y, z)$  chama-se *primitivo* se  $\text{mdc}(x, y, z) = 1$

(é claro como o mdc de mais de dois números deve ser entendido).

#### 4.2 Exemplo.

$(4, 3, 5), (8, 6, 10), \dots, (4n, 3n, 5n), \dots$

$(12, 5, 13), (24, 10, 26), \dots, (12n, 5n, 13n), \dots$

são triplos PITAGÓRICOS, sendo que  $(4, 3, 5)$  e  $(12, 5, 13)$  são primitivos.

É imediata a seguinte

#### 4.3 Observação.

Com qualquer triplo PITAGÓRICO  $(x_1, y_1, z_1)$  (*primitivo*) e qualquer  $n \in \mathbb{N}$ , também  $(nx_1, ny_1, nz_1)$  é um triplo PITAGÓRICO. Para  $n > 1$  estes últimos não são primitivos.

Também reciprocamente temos

#### 4.4 Observação.

Seja  $(x, y, z)$  um qualquer triplo PITAGÓRICO,  $d = \text{mdc}(x, y, z)$  e ponhamos  $x_1 = \frac{x}{d}$ ,  $y_1 = \frac{y}{d}$ ,  $z_1 = \frac{z}{d}$ . Então  $(x_1, y_1, z_1)$  é um triplo PITAGÓRICO primitivo e vale  $(x, y, z) = (dx_1, dy_1, dz_1)$ .

**Demonstração:** É claro que  $\text{mdc}(x_1, y_1, z_1) = 1$  e vale  $(x, y, z) = (dx_1, dy_1, dz_1)$ .

Além disso,  $x_1^2 + y_1^2 = \left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2 = \frac{x^2 + y^2}{d^2} = \left(\frac{z}{d}\right)^2 = z_1^2$ , mostrando que  $(x_1, y_1, z_1)$  é triplo PITAGÓRICO primitivo.

■

Portanto, para se classificar os triplos PITAGÓRICOS, é suficiente a restrição aos primitivos.

#### 4.5 Observação.

Seja  $(x, y, z)$  um triplo PITAGÓRICO primitivo. Então exatamente um dos números  $x$  ou  $y$  é par, o outro é ímpar -  $z$  é ímpar.

**Demonstração:** Suponhamos  $x$  e  $y$  ambos pares. Então  $z^2 = x^2 + y^2$  e também  $z$  é par. Segue a contradição  $2 \leq \text{mdc}(x, y, z) = 1$ .

Suponhamos  $x$  e  $y$  ambos ímpares, digamos  $x^2 = 4k + 1$  e  $y^2 = 4\ell + 1$ . Segue  $z^2 = x^2 + y^2 = 4(k + \ell) + 2$ , o que é impossível para um quadrado par (ver 1.15 a)). Logo,  $x$  e  $y$  têm paridades distintas e  $z$  é ímpar. ■

**Combinamos que, daqui em diante,  $x$  é par,  $y$  é ímpar quando  $(x, y, z)$  é um triplo PITAGÓRICO primitivo.**

#### 4.6 Observação.

Seja  $(x, y, z)$  um triplo PITAGÓRICO primitivo. Então

$$\text{mdc}(x, y) = \text{mdc}(y, z) = \text{mdc}(x, z) = 1 ,$$

i.e. os  $x, y, z$  são relativamente primos dois a dois.

**Demonstração:** Se  $d = \text{mdc}(x, y) > 1$ , então existe um divisor primo  $p$  de  $d$ . Logo,  $p|x$  e  $p|y$ , segue  $p|x^2 + y^2 = z^2$  e também  $p|z$ . Assim temos a contradição  $p \leq \text{mdc}(x, y, z) = 1$ .

Os dois outros casos são mostrados da mesma forma. ■

#### 4.7 Observação.

Sejam  $n, m, c \in \mathbb{N}$  com  $nm = c^2$  e  $\text{mdc}(m, n) = 1$ .

Então existem  $N, M \in \mathbb{N}$  tais que  $n = N^2$  e  $m = M^2$ , i. e.  $n$  e  $m$  são quadrados perfeitos individualmente.

**Demonstração:** Sejam  $n = \prod_{k=1}^r p_k^{a_k}$  e  $m = \prod_{k=1}^s q_k^{b_k}$  as decomposições primárias de  $n$  e  $m$ . Então os  $q_k$  são diferentes dos  $p_\ell$  pois  $\text{mdc}(m, n) = 1$ . Segue que

$nm = p_1^{a_1} \cdot \dots \cdot p_r^{a_r} \cdot q_1^{b_1} \cdot \dots \cdot q_s^{b_s}$  é a decomposição primária de  $nm$ . Como  $nm = c^2$  é quadrado perfeito, segue que todos os  $a_1, \dots, a_r, b_1, \dots, b_s$  são pares. Logo  $n = N^2$  e  $m = B^2$  para  $N = \prod_{k=1}^r p_k^{a_k/2}$  e  $M = \prod_{k=1}^s q_k^{b_k/2}$ . ■

Estamos agora em condições de provar o teorema de classificação dos triplos PITAGÓRICOS.

#### 4.8 Teorema.

- a) *Escolhendo-se números  $s, t \in \mathbb{N}$  com  $s > t \geq 1$  e  $\text{mdc}(s, t) = 1$ ,  $s - t$  ímpar (i.e.  $s$  e  $t$  possuem paridades distintas), e colocando-se*

$$x = 2st, \quad y = s^2 - t^2, \quad z = s^2 + t^2,$$

*$(x, y, z)$  será um triplo PITAGÓRICO primitivo.*

- b) *Qualquer triplo PITAGÓRICO primitivo é obtido pelo método de a).*

Particularmente, existem infinitos triplos PITAGÓRICOS primitivos. Eis o início de uma tabela dos triplos PITAGÓRICOS primitivos:

$s$	$t$	$x = 2st$	$y = s^2 - t^2$	$z = s^2 + t^2$
2	1	4	3	5
3	2	12	5	13
4	1	8	15	17
4	3	24	7	25
5	2	20	21	29
5	4	40	9	41
6	1	12	35	37
6	5	60	11	61
7	2	28	45	53
7	4	56	33	65
7	6	84	13	85
⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮

**Demonstração:** a) Temos  $x^2 + y^2 = (2st)^2 + (s^2 - t^2)^2 = 4s^2t^2 + s^4 + t^4 - 2s^2t^2 = s^4 + 2s^2t^2 + t^4 = (s^2 + t^2)^2 = z^2$ , mostrando que  $(x, y, z)$  é um triplo PITAGÓRICO. Suponha  $p \mid \text{mdc}(x, y, z)$  para algum primo  $p$ . Então  $p$  é ímpar e de  $p \mid 2st$  segue que  $p \mid s$  ou  $p \mid t$ . De  $z = s^2 + t^2$  (ou de  $y = s^2 - t^2$ ) segue então que  $p \mid s$  e  $p \mid t$ , dando o absurdo  $p \leq \text{mdc}(s, t) = 1$ .

Assim,  $(x, y, z)$  é um triplo primitivo.

b) Seja  $(x, y, z)$  um qualquer triplo PITAGÓRICO primitivo com  $x$  par,  $y$  ímpar. Temos  $x^2 = z^2 - y^2 = (z + y)(z - y)$  e daí  $\mathbb{N} \ni \frac{x^2}{4} = \frac{z + y}{2} \cdot \frac{z - y}{2}$ . Então

$$\left(\frac{x}{2}\right)^2 = uv \quad \text{com} \quad u = \frac{z + y}{2} \quad \text{e} \quad v = \frac{z - y}{2}.$$

Se  $d = \text{mdc}(u, v)$ , então  $d \mid u \pm v$ . Mas,  $u + v = \frac{z + y}{2} + \frac{z - y}{2} = z$  e  $u - v = \frac{z + y}{2} - \frac{z - y}{2} = y$ , dando  $d \mid \text{mdc}(y, z)$ . Por 4.6 sabemos  $\text{mdc}(y, z) = 1$  pois  $(x, y, z)$  é primitivo. Logo  $\text{mdc}(u, v) = 1$ .

Concluimos por 4.7 que  $u$  e  $v$  são individualmente quadrados perfeitos. Coloquemos  $u = s^2$  e  $v = t^2$  com  $s, t \in \mathbb{N}$ . Temos então  $\text{mdc}(s, t) = \text{mdc}(u, v) = 1$  e  $s - t$  é ímpar. Além disso,  $s^2 - t^2 = u - v = y$  e  $s^2 + t^2 = v + u = z$ . De  $\frac{x^2}{4} = uv = t^2s^2$  segue  $x = \sqrt{4t^2s^2} = 2st$ . ■

#### 4.9 Conseqüência.

*Os triplos PITAGÓRICOS, primitivos e não-primitivos, são obtidos por*

$$(2nst, n(s^2 - t^2), n(s^2 + t^2))$$

*onde  $n, s, t \in \mathbb{N}$  com  $s > t \geq 1$ ,  $\text{mdc}(s, t) = 1$ ,  $s - t$  ímpar.*

Num qualquer triplo PITAGÓRICO primitivo  $(x, y, z)$ ,  $x$  é múltiplo de 4 e  $y$  é ímpar  $> 1$ . Os triplos PITAGÓRICOS primitivos são numerosos, como mostra

#### 4.10 Proposição.

- Qualquer número ímpar  $> 1$  é o  $y$  de pelo menos um triplo PITAGÓRICO primitivo.*
- Todo número natural divisível por 4 é o  $x$  de pelo menos um triplo PITAGÓRICO primitivo.*

**Demonstração:** a) Se  $y = 2k - 1 = s^2 - t^2 > 1$  é dado, podemos resolver  $s + t = 2k - 1$  e  $s - t = 1$ , obtendo que  $s = k$  e  $t = k - 1$ . Assim,

$$(2k(k - 1), 2k - 1, 2k(k - 1) + 1)$$

é um exemplo para um triplo primitivo com  $y$  dado.

b) Se  $x = 4k = 2st$  é dado, podemos considerar  $s = 2k$  e  $t = 1$  e obtemos

$$(4k, 4k^2 - 1, 4k^2 + 1)$$

como triplo primitivo com  $x$  dado. ■

Para  $y > 1$  ímpar obtemos tantos triplos primitivos  $(\cdot, y, \cdot)$  quantas existem *decomposições multiplicativas*  $y = k\ell$  com  $\text{mdc}(k, \ell) = 1$  (compare 3.24). Particularmente temos

#### 4.11 Exemplo.

Para qualquer primo  $p > 2$ , o **único** triplo PITAGÓRICO da forma  $(\cdot, p, \cdot)$  é

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

Ele necessariamente é primitivo.

#### 4.12 Exemplo.

a) Para qualquer primo  $p > 2$  dado, os triplos PITAGÓRICOS da forma  $(\cdot, p^2, \cdot)$  são:

Um **único** não-primitivo

$$p \cdot \left(\frac{p^2 - 1}{2}, p, \frac{p^2 + 1}{2}\right),$$

e um **único** primitivo

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

e em geral:

b) Para qualquer primo  $p > 2$  e  $n \in \mathbb{N}$  dados, os triplos PITAGÓRICOS da forma  $(\cdot, p^n, \cdot)$  são:

Um **único** primitivo

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

e  $n - 1$  não-primitivos

$$p^{n-k} \cdot \left( \frac{p^{2k} - 1}{2}, p^k, \frac{p^{2k} + 1}{2} \right),$$

obtidos para  $k = 1, 2, \dots, n-1$ .

#### 4.13 Exemplo.

Para quaisquer dois primos  $2 < q < p$ , os triplos da forma  $(\cdot, pq, \cdot)$  são:  
Dois não-primitivos

$$p \cdot \left( \frac{q^2 - 1}{2}, q, \frac{q^2 + 1}{2} \right) \quad e \quad q \cdot \left( \frac{p^2 - 1}{2}, p, \frac{p^2 + 1}{2} \right)$$

e dois primitivos

$$\left( \frac{p^2 q^2 - 1}{2}, pq, \frac{p^2 q^2 + 1}{2} \right) \quad e \quad \left( \frac{p^2 - q^2}{2}, pq, \frac{p^2 + q^2}{2} \right).$$

**Demonstrações:** Exercício. ■

#### A CONJETURA DE FERMAT

A conjectura de FERMAT (também: o "último Teorema" de FERMAT) afirma que a equação DIOFANTINA

$$x^n + y^n = z^n$$

não é solúvel por nenhum triplo  $(x, y, z)$  com  $x, y, z \in \mathbb{N}$  se  $n \geq 3$ .

Demonstraremos esta afirmação no caso  $4 \mid n$ , já provado pelo próprio PIERRE DE FERMAT (1601-1665).

Mencionamos que, o enigma desta conjectura de FERMAT, entretanto e finalmente em 1994/95, depois de ocupar as mentes matemáticas mais capacitadas por mais de 350 anos, tem sido provado pelo matemático ANDREW WILES.

Ver na revista *Annals of Mathematics*, **142** (1995), os artigos:

*Modular elliptic curves and Fermat's Last Theorem*, pgs. 443-551,  
de A. WILES e

*Ring-theoretic properties of certain Hecke algebras*, pgs. 553-572,  
de RICHARD TAYLOR e A. WILES.

#### 4.14 Observação.

Sejam  $n, a, b, c \in \mathbb{N}$  tais que  $a|n, b|n, c|n$ . Se existirem números  $x, y, z \in \mathbb{N}$  tais que  $x^n + y^n = z^n$ , então existem também  $x', y', z' \in \mathbb{N}$  tais que

$$x'^a + y'^b = z'^c.$$

**Demonstração:** Sejam  $r, s, t \in \mathbb{N}$  com  $n = ar = bs = ct$ . Fazendo-se  $x' = x^r, y' = y^s, z' = z^t$ , segue

$$x'^a + y'^b = x^{ra} + y^{sb} = x^n + y^n = z^n = z^{tc} = z'^c$$

■

Equivalentemente podemos formular

#### 4.15 Observação.

Seja  $n \in \mathbb{N}$ . Se existirem números  $a, b, c \in \mathbb{N}$  com  $a|n, b|n, c|n$  tais que  $x^a + y^b = z^c$  é impossível para  $x, y, z \in \mathbb{N}$ , então também  $x^n + y^n = z^n$  é impossível com  $x, y, z \in \mathbb{N}$ .

Esta observação reduz o problema da conjectura de FERMAT para seu tratamento somente com os expoentes primos: Porquê

$$x^p + y^p = z^p \quad \text{é impossível para todos os primos } p > 2?$$

#### 4.16 Conseqüência.

Seja  $n \in \mathbb{N}$  com  $4|n$ . Se  $x^4 + y^4 = z^2$  é impossível para  $x, y, z \in \mathbb{N}$ , então também  $x^n + y^n = z^n$  é impossível com  $x, y, z \in \mathbb{N}$ .

■

#### 4.17 Teorema. (FERMAT).

A equação  $x^4 + y^4 = z^2$

não possui solução  $x, y, z \in \mathbb{N}$ .

(Conseqüentemente a conjectura de FERMAT estará provada quando  $4|n$ .)

**Demonstração:** Consideremos o conjunto

$$S = \{z \in \mathbb{N} \mid \exists x, y \in \mathbb{N} \text{ com } x^4 + y^4 = z^2\}.$$

Suponhamos,  $x^4 + y^4 = z^2$  fosse solúvel com  $x, y, z \in \mathbb{N}$ . Isto significa  $S \neq \emptyset$ . Seja  $z_0 \in S$  o elemento mínimo. Logo, existem  $x_0, y_0 \in \mathbb{N}$  com  $z_0^2 = x_0^4 + y_0^4$ . Porém, se  $z_0 > z_1 \in \mathbb{N}$ , então não existem  $x_1, y_1 \in \mathbb{N}$  com  $z_1^2 = x_1^4 + y_1^4$ . Portanto, o método desta demonstração vai ser, construir a partir de  $(x_0, y_0, z_0)$

um triplo  $x_1, y_1, z_1 \in \mathbb{N}$  com  $z_1^2 = x_1^4 + y_1^4$  e  $z_1 < z_0$ . Se conseguirmos isto, teremos a contradição desejada que terminará a demonstração.

Mostramos primeiro  $\text{mdc}(x_0, y_0) = 1$  :

Se  $d = \text{mdc}(x_0, y_0)$ , colocamos  $x_1 = \frac{x_0}{d}$  e  $y_1 = \frac{y_0}{d}$  e obtemos

$$x_1^4 + y_1^4 = \left(\frac{x_0}{d}\right)^4 + \left(\frac{y_0}{d}\right)^4 = \frac{x_0^4 + y_0^4}{d^4} = \frac{z_0^2}{d^4} = \left(\frac{z_0}{d^2}\right)^2 = z_1^2$$

abreviando-se  $z_1 = \frac{z_0}{d^2}$ . Como  $z_1 < z_0$  se  $d > 1$ , concluímos  $d = 1$ .

Como  $(x_0^2)^2 + (y_0^2)^2 = z_0^2$  com  $\text{mdc}(x_0^2, y_0^2) = 1$ , temos que  $(x_0^2, y_0^2, z_0)$  é um triplo PITAGÓRICO primitivo. Por 4.8 existem  $s, t \in \mathbb{N}$  com  $s > t$ ,  $\text{mdc}(s, t) = 1$  e  $s - t$  ímpar, tais que

$$x_0^2 = 2st, \quad y_0^2 = s^2 - t^2 \quad \text{e} \quad z_0 = s^2 + t^2 .$$

Afirmamos que  $t$  é par: Se  $s$  fosse par, teríamos  $s = 2s'$  e  $t = 2t' + 1$  e segue

$$y_0^2 = (2s')^2 - (2t' + 1)^2 = 4s'^2 - 4t'^2 - 4t' - 1 = 4(s'^2 - t'^2 - t') - 1 = 4\ell - 1 ,$$

o que é impossível para um quadrado perfeito (um quadrado perfeito ímpar deveria ter a forma  $4k + 1$ !). Logo de fato  $t$  é par e  $s$  é ímpar. Coloquemos  $t = 2r$  com  $r \in \mathbb{N}$  e obtemos  $x_0^2 = 2st = 4sr$  e daí

$$\left(\frac{x_0}{2}\right)^2 = sr .$$

Temos  $\text{mdc}(r, s) = 1$ , pois  $\text{mdc}(s, t) = 1$ . Logo,  $r$  e  $s$  ambos são quadrados perfeitos, digamos  $s = z_1^2$ ,  $r = w_1^2$  com  $z_1, w_1 \in \mathbb{N}$ .

De  $y_0^2 = s^2 - t^2$  segue que

$$t^2 + y_0^2 = s^2$$

e como  $\text{mdc}(s, t) = 1$ , vemos que  $(t, y_0, s)$  é um triplo PITAGÓRICO primitivo. Existem então  $u, v \in \mathbb{N}$  com  $u > v$ ,  $u - v$  ímpar,  $\text{mdc}(u, v) = 1$ , tais que

$$t = 2uv, \quad y_0 = u^2 - v^2 \quad \text{e} \quad s = u^2 + v^2 .$$

Agora,  $uv = \frac{t}{2} = r = w_1^2$ . Mais uma vez concluímos que  $u$  e  $v$  são individualmente quadrados perfeitos, digamos  $u = x_1^2$  e  $v = y_1^2$  com  $x_1, y_1 \in \mathbb{N}$ . Calculamos

$$x_1^4 + y_1^4 = u^2 + v^2 = s = z_1^2 ,$$

o que significa  $z_1 \in S$ . Mas como  $0 < z_1 < z_1^2 = s < s^2 < s^2 + t^2 = z_0$ , isto é impossível devido à minimalidade de  $z_0 \in S$ .

Isto mostra que  $S$  é vazio e portanto,  $x^4 + y^4 = z^2$  não pode ser solúvel em  $\mathbb{N}$ .

■



## § 5 Números deficientes - abundantes - perfeitos e de MERSENNE

### NÚMEROS DEFICIENTES, ABUNDANTES E PERFEITOS

Além da função  $\tau(n)$ , da quantidade dos divisores de  $n$ , introduzimos agora

#### 5.1 Definição.

Para todo  $n \in \mathbb{N}$  indicamos por

$$\sigma(n) = \sum_{t|n} t$$

a soma de todos os divisores naturais de  $n$ .

#### 5.2 Exemplo.

$$\sigma(1) = 1,$$

$$\sigma(p) = p + 1, \text{ se } p \text{ é primo,}$$

$$\sigma(6) = 1 + 2 + 3 + 6 = 12, \quad \sigma(12) = 1 + 2 + 4 + 3 + 6 + 12 = 28.$$

#### 5.3 Proposição.

Seja  $n = p^a$  para algum primo  $p$  e  $a \in \mathbb{N}_0$ . Então

$$\sigma(p^a) = \frac{p^{a+1} - 1}{p - 1}.$$

**Demonstração:** Temos que  $\{1, p, p^2, \dots, p^a\}$  são os divisores deste  $n$ . Logo, por 1.4

$$\sigma(p^a) = \sum_{t|n} t = \sum_{k=0}^a p^k = \frac{p^{a+1} - 1}{p - 1}.$$

■

É claro que  $\sigma(n) = 1 + n + \dots \geq n + 1 > n$  para todo  $n \geq 2$ .

Também:  $\sigma(n) = n + 1 \iff n = p$  é primo.

Procuramos classificar os números naturais agora sob o aspecto de comparar  $\sigma(n)$  com  $n$ , pela seguinte

## 5.4 Definição.

Um número  $n \in \mathbb{N}$  chama-se

- a) *deficiente*, se  $\sigma(n) < 2n$
- b) *abundante*, se  $\sigma(n) > 2n$
- c) *perfeito*, se  $\sigma(n) = 2n$ .

## 5.5 Exemplos.

$n = 15$  :  $\sigma(15) = 24$   $2n = 30$   $\sigma(15) < 2 \cdot 15$ . Portanto, 15 é deficiente.

$n = 12$  :  $\sigma(12) = 28$   $2n = 24$   $\sigma(12) > 2 \cdot 12$ . Portanto, 12 é abundante.

$n = 6$  :  $\sigma(6) = 12$   $2n = 12$   $\sigma(6) = 2 \cdot 6$ . Portanto, 6 é perfeito.

De verificação imediata é (fazer o gráfico da função !):

## 5.6 Observação.

A função real

$$y = \frac{x}{x-1}$$

é decrescente e vale

$$1 < \frac{x}{x-1} \leq 2 \quad \text{para } x \geq 2.$$

## 5.7 Proposição.

- a) Se  $p$  é primo e  $a \in \mathbb{N}$ , então  $p^a$  é deficiente.
- b)  $3 \cdot 2^k$  é abundante para todo  $k \geq 2$ .

**Demonstração:** a) Usando-se 5.3 e 5.6, obtemos

$$\sigma(p^a) = \sum_{t|p^a} t = \frac{p^{a+1} - 1}{p - 1} < \frac{p^{a+1}}{p - 1} = p^a \cdot \frac{p}{p - 1} \leq 2 \cdot p^a.$$

$$\begin{aligned} \text{b) } \sigma(3 \cdot 2^k) &= 1 + 2 + 4 + \dots + 2^{k-1} + 2^k + 3 + 3 \cdot 2 + 3 \cdot 4 + \dots + 3 \cdot 2^k \\ &= (1 + 3) \cdot (1 + 2 + \dots + 2^k) = 4 \cdot (2^{k+1} - 1) \end{aligned}$$

$$= 2 \cdot 2^k \left(4 - \frac{1}{2^{k-1}}\right) > 2 \cdot (2^k \cdot 3), \quad \text{pois } k \geq 2.$$

■

## 5.8 Proposição.

Sejam  $2 < p < q$  primos. Então, para todos os  $a, b \in \mathbb{N}$ , o número

$$n = p^a \cdot q^b \text{ é deficiente.}$$

**Demonstração:**

$$\begin{aligned} \sigma(n) &= \\ &= 1 + p + \dots + p^a + q(1 + p + \dots + p^a) + \dots + q^b(1 + p + \dots + p^a) = \\ &= (1 + p + \dots + p^a)(1 + q + \dots + q^b) = \frac{p^{a+1} - 1}{p - 1} \cdot \frac{q^{b+1} - 1}{q - 1} < \frac{p^{a+1}q^{b+1}}{(p - 1)(q - 1)} = \\ &= p^a q^b \cdot \frac{pq}{(p - 1)(q - 1)} = n \cdot \frac{p}{p - 1} \cdot \frac{q}{q - 1} \leq n \cdot \frac{3}{3 - 1} \cdot \frac{5}{5 - 1} = \frac{15}{8}n < 2n, \end{aligned}$$

usando-se que a função  $\frac{x}{x-1}$  é decrescente (5.6) e  $p \geq 3, q \geq 5$ . ■

## 5.9 Observação.

Sejam  $n, m \in \mathbb{N}$  com  $\text{mdc}(m, n) = 1$ . Então

- $d | mn \iff d = st$  com  $s | n$  e  $t | m$ .
- Se  $s_1, s_2 | n$  e  $t_1, t_2 | m$  e se  $s_1 t_1 = s_2 t_2$ , então  $s_1 = s_2$  e  $t_1 = t_2$ .

(i.e. os divisores de  $mn$  são obtidos de forma única, por combinação dos divisores de  $n$  com os de  $m$ .)

**Demonstração:** a) "  $\Leftarrow$  " é claro.

"  $\Rightarrow$  " : Sejam  $n = \prod_{k=1}^r p_k^{a_k}$  e  $m = \prod_{k=1}^{r'} q_k^{b_k}$  as decomposições primárias de  $n$  e  $m$ . Como  $\text{mdc}(m, n) = 1$ , temos que  $mn = p_1^{a_1} \cdot \dots \cdot p_r^{a_r} \cdot q_1^{b_1} \cdot \dots \cdot q_{r'}^{b_{r'}}$  é a decomposição primária de  $mn$ . Portanto, se  $d | mn$ , então  $d = p_1^{\ell_1} \cdot \dots \cdot p_r^{\ell_r} q_1^{u_1} \cdot \dots \cdot q_{r'}^{u_{r'}}$  com  $0 \leq \ell_1 \leq a_1, \dots, 0 \leq \ell_r \leq a_r, 0 \leq u_1 \leq b_1, \dots, 0 \leq u_{r'} \leq b_{r'}$ . Com  $s = p_1^{\ell_1} \cdot \dots \cdot p_r^{\ell_r}$  e  $t = q_1^{u_1} \cdot \dots \cdot q_{r'}^{u_{r'}}$  temos assim  $d = st, s | n$  e  $t | m$ .

b) Também este item é facilmente verificado pela comparação das decomposições primárias de  $s_1 t_1$  e  $s_2 t_2$ . ■

### 5.10 Proposição.

Sejam  $n, m \in \mathbb{N}$  com  $\text{mdc}(m, n) = 1$ . Então

- a)  $\tau(nm) = \tau(n)\tau(m)$
- b)  $\sigma(nm) = \sigma(n)\sigma(m)$ .

**Demonstração:** a)  $\tau(nm) = |\{d \mid d \mid mn\}| = |\{st \mid s \mid n, t \mid m\}| =$   
 $= |\{s \mid s \mid n\}| \cdot |\{t \mid t \mid m\}| = \tau(n)\tau(m)$ .

b)  $\sigma(nm) = \sum_{d \mid nm} d = \sum_{s \mid n} \sum_{t \mid m} st = \left( \sum_{s \mid n} s \right) \cdot \left( \sum_{t \mid m} t \right) = \sigma(n)\sigma(m)$ .

■

### 5.11 Conseqüência.

Seja  $n = p_1^{a_1} \cdot \dots \cdot p_r^{a_r} \in \mathbb{N}$  com  $p_1, \dots, p_r$  primos distintos e  $a_1, \dots, a_r \in \mathbb{N}$ .  
 Então

- a)  $\tau(n) = \prod_{k=1}^r (a_k + 1)$
- b)  $\sigma(n) = \prod_{k=1}^r \frac{p_k^{a_k+1} - 1}{p_k - 1}$ .

**Demonstração:** Temos  $\text{mdc}\left(p_1^{a_1}, \prod_{k=2}^r p_k^{a_k}\right) = 1$ .

a) (Isto já vimos em 3.6 e segue agora mais uma vez por indução assim):

$\tau(n) = \tau\left(p_1^{a_1} \cdot \prod_{k=2}^r p_k^{a_k}\right) = \tau(p_1^{a_1}) \tau\left(\prod_{k=2}^r p_k^{a_k}\right)$ . Por indução temos

$$\tau\left(\prod_{k=2}^r p_k^{a_k}\right) = (a_2 + 1) \cdot \dots \cdot (a_r + 1)$$

e como  $\tau(p_1^{a_1}) = |\{1, p_1, \dots, p_1^{a_1}\}| = a_1 + 1$ , a afirmação segue.

b)  $\sigma(n) = \sigma\left(p_1^{a_1} \cdot \prod_{k=2}^r p_k^{a_k}\right) = \sigma(p_1^{a_1}) \sigma\left(\prod_{k=2}^r p_k^{a_k}\right)$ . Por indução temos

$$\sigma\left(\prod_{k=2}^r p_k^{a_k}\right) = \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdot \dots \cdot \frac{p_r^{a_r+1} - 1}{p_r - 1}$$

e como (5.3)  $\sigma(p_1^{a_1}) = \frac{p_1^{a_1+1} - 1}{p_1 - 1}$ , a afirmação segue. ■

## O TEOREMA DE EUCLIDES/EULER

Provaremos agora uma classificação dos *números perfeitos pares*, que devemos a EUCLIDES e EULER.

Lembrando:  $n \in \mathbb{N}$  é perfeito, se  $\sigma(n) = 2n$ .

### 5.12 Teorema.

a) (EUCLIDES) Se  $k \geq 2$  é tal que  $p = 2^k - 1$  é primo, então

$$n = 2^{k-1} (2^k - 1) \quad \text{é um número perfeito (par)}$$

b) (EULER) Todo número perfeito **par** é obtido pelo método de a).

**Demonstração:** a) Seja  $k \geq 2$  tal que  $p = 2^k - 1$  é primo.

Como  $\text{mdc}(2^{k-1}, 2^k - 1) = 1$ , calculamos

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

mostrando que  $n = 2^{k-1} (2^k - 1)$  é perfeito.

b) Seja  $n$  um qualquer número perfeito *par*. Podemos escrever  $n = 2^{k-1}m$  com  $k \geq 2$  e  $m$  ímpar. Como  $n$  é perfeito, concluímos

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

Segue então  $2^k - 1 \mid 2^k m$ . Como  $\text{mdc}(2^k - 1, 2^k) = 1$ , concluímos  $2^k - 1 \mid m$ . Logo, existe um  $M \in \mathbb{N}$  com  $(2^k - 1)M = m$ . Além disso, temos  $M \neq m$ , pois  $k \geq 2$ . Assim,  $2^k (2^k - 1)M = 2^k m = (2^k - 1)\sigma(m)$ , ou seja

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

Portanto  $\sigma(m) = M + m$ . Concluímos que  $M$  e  $m$  são os únicos divisores de  $m$ . Particularmente,  $M = 1$  e  $m = 2^k - 1$  é primo. Logo,  $n$  tem a forma afirmada

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

■

Na terceira coluna da seguinte tabela temos os primeiros números perfeitos :

$k$	$2^k - 1$	$2^{k-1} (2^k - 1)$
2	3	6
3	7	28
5	31	496
7	127	8128
13	8191	33550336
17	131071	65536 · 131071
19	524287	262144 · 524287
31	$2^{31} - 1$	$2^{30} (2^{31} - 1)$
⋮	⋮	⋮
44497	$2^{44497} - 1$	$2^{44496} (2^{44497} - 1)$
⋮	⋮	⋮

Ver também Ex. 7.6.

Devemos mencionar aqui que

*é desconhecido se existe algum número perfeito ímpar.*

Para os maiores números perfeitos, hoje explicitamente conhecidos,

ver a **Nota** no final deste parágrafo 5.

## NÚMEROS DE MERSENNE

Para o estudo dos números perfeitos, acabamos de ver que os números da forma  $2^k - 1$  são de fundamental importância.

### 5.13 Definição.

Os números da seqüência  $(2^k - 1)_{k \geq 2}$  chamam-se os *números de MERSENNE*. Colocamos

$$M_k = 2^k - 1 \quad k = 2, 3, 4, \dots$$

Assim, a seqüência dos números de MERSENNE começa como

$$(M_k)_{k \geq 2} = (3, 7, 15, 31, 63, 127, 255, 511, 1023, \dots, 2^k - 1, \dots)$$

Particularmente interessa, quando um  $M_k$  é primo. Uma condição *necessária* para que  $M_k$  possa ser primo, é dada na

#### 5.14 Proposição.

*Se  $M_k$  for primo, então  $k = p$  é primo.*

Esta condição necessária certamente *não é suficiente*, pois

$$M_{11} = 2047 = 23 \cdot 89$$

não é primo, apesar de  $k = 11$  ser primo.

A demonstração de 5.14 é consequência da seguinte

#### 5.15 Observação.

*Sejam  $2 \leq a, k \in \mathbb{N}$ .*

*Se  $a^k - 1$  for primo, então  $a = 2$  e  $k$  é primo.*

**Demonstração:** Temos (fazendo-se  $k - 1 = n$  em 1.4):

$$a^k - 1 = (a - 1)(1 + a + a^2 + \dots + a^{k-1})$$

com  $(1 + a + \dots + a^{k-1}) > 1$ , pois  $k \geq 2$ . Ora, se  $a^k - 1$  for primo, concluímos  $a - 1 = 1$ , ou seja,  $a = 2$ .

Seja  $k = rs$  composto com  $1 < s \leq r < k$ . Temos (com  $a = 2^r$  e  $n + 1 = s$  em 1.4) a decomposição

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

na qual  $2^r - 1 > 1$  e  $1 + 2^r + \dots + 2^{(s-1)r} > 1$ , pois  $s > 1$ . Logo  $2^k - 1$  não é primo quando  $k$  é composto. ■

Assim,

$$\{M_k \mid 2 \leq k \in \mathbb{N}\} \cap \mathbb{P} = \{M_k \mid k \in \mathbb{P}\} \cap \mathbb{P}$$

i. e. ao procurar primos  $M_k$  na seqüência dos números de MERSENNE, somente os *índices*  $k = p$  primos interessam.

### 5.16 Definição.

Um número  $M_p$  com  $p \in \mathbb{P}$  chama-se um *primo de MERSENNE* se  $M_p$  fôr primo.

### 5.17 Exemplo.

Os primeiros primos de MERSENNE para  $p = 2, 3, 5, \dots$  são:

$$M_2 = 3, \quad M_3 = 7, \quad M_5 = 31, \quad M_7 = 127, \quad M_{13} = 8191, \\ M_{17} = 131071, \quad M_{19} = 524287, \quad M_{31} \dots$$

Entretanto,  $23 \mid M_{11}$ ,  $47 \mid M_{23}$ ,  $233 \mid M_{29}$ ,  $223 \mid M_{37}, \dots$

Ainda mencionamos o resultado de COLE (1902):

$$M_{67} = 193707721 \cdot 761838257287$$

onde 193707721 é o *menor* divisor primo de  $M_{67}$  !

Mais propriedades de divisibilidade dos números de MERSENNE conheceremos nos próximos parágrafos em conexão com os teoremas de FERMAT e de WILSON e as congruências quadráticas.

### Nota:

Mencionamos que, em Maio de 2004, para  $p = 24\,036\,583$ , o 41<sup>o</sup> e por enquanto maior primo de MERSENNE

$$M_p = 2^{24\,036\,583} - 1$$

foi encontrado por JOSH FINDLEY. Ele possui entre 7 e 8 milhões de dígitos (pois  $\log_{10} 2^{24\,036\,583} = 24\,036\,583 \cdot \log_{10} 2 = 24\,036\,583 \cdot 0,3010 \approx 7,235 \cdot 10^6$  !). O *número perfeito correspondente* - com mais de 14 milhões de dígitos - é

$$P = 2^{24\,036\,582} \cdot (2^{24\,036\,583} - 1).$$

O penúltimo (40<sup>o</sup>) primo de MERSENNE foi encontrado em Novembro de 2003 por MICHAEL SHAFER para  $p = 20\,996\,011$ :

$$M_{20\,996\,011} = 2^{20\,996\,011} - 1.$$



## § 6 A teoria das congruências

### DIVISIBILIDADE E CONGRUÊNCIAS

#### 6.1 Definição.

Seja  $n \in \mathbb{N}_0$  um número fixo. Dois números  $a, b \in \mathbb{Z}$  chamam-se *congruentes módulo  $n$* , se  $a - b$  é múltiplo de  $n$ . Em símbolos:  $a \equiv b \pmod{n}$ . Assim,

$$a \equiv b \pmod{n} \iff n \mid a - b.$$

#### 6.2 Exemplos.

- a) Para  $n = 6$ :  $1 \equiv 7 \equiv -5 \equiv -11 \pmod{6}$   $123 \equiv -135 \pmod{6}$ .
- b) Para  $n = 0$ :  $a \equiv b \pmod{0} \iff a = b$ .
- c) Para  $n = 1$ :  $a \equiv b \pmod{1}$  sempre.
- d) Para  $n = 2$ :  $a \equiv b \pmod{2} \iff a$  e  $b$  têm a mesma paridade.

É imediata a seguinte

#### 6.3 Observação.

Dois números **não-negativos**  $a, b \in \mathbb{N}_0$ , escritos no sistema decimal, são congruentes módulo 10, (100, 1000, ...,  $10^m$ )  $\iff$   $a$  e  $b$  coincidem no último dígito (nos últimos 2, 3, ...,  $m$  dígitos).

#### 6.4 Observação.

Seja  $n > 0$ ,  $a, b \in \mathbb{Z}$  escritos na forma

$$a = nq_1 + r_1 \quad e \quad b = nq_2 + r_2$$

com  $q_1, q_2, r_1, r_2 \in \mathbb{Z}$  ( $0 \leq r_1, r_2 < n$ ). Então

$$a \equiv b \pmod{n} \iff r_1 = r_2.$$

**Demonstração:** "  $\Leftarrow$  " : Se  $r_1 = r_2$  temos  $a - b = n(q_1 - q_2) + (r_1 - r_2) = n(q_1 - q_2)$ , i. e.  $n \mid a - b$ . Isto significa  $a \equiv b \pmod{n}$ .

"  $\Rightarrow$  " : Se  $a \equiv b \pmod{n}$ , temos  $n \mid a - b = n(q_1 - q_2) + (r_1 - r_2)$  e daí,  $n \mid r_1 - r_2$ . Mas de  $0 \leq |r_1 - r_2| < n$  concluímos então  $r_1 - r_2 = 0$ , i. e.  $r_1 = r_2$ . ■

## 6.5 Conseqüência.

Todo número  $a \in \mathbb{Z}$  é congruente  $\text{mod } n$  a exatamente um dos números

$$\{0, 1, 2, \dots, n-1\}$$

e estes últimos são incongruentes entre si  $\text{mod } n$ .

O conjunto

$$\{0, 1, 2, \dots, n-1\}$$

chama-se o conjunto dos *menores restos não-negativos* módulo  $n$ .

## 6.6 Definição.

Seja  $n > 0$ .

Um conjunto de  $n$  números  $\{r_1, r_2, \dots, r_n\}$  chama-se um *sistema completo de resíduos (restos)* módulo  $n$  se cada  $a \in \mathbb{Z}$  é congruente a exatamente um dos números  $r_1, r_2, \dots, r_n$ .

Equivalentemente: Os  $r_1, r_2, \dots, r_n$  são congruentes  $\text{mod } n$ , em alguma ordem, aos números  $0, 1, 2, \dots, n-1$ .

## 6.7 Exemplos.

a) Para  $n = 8$  temos:

$$\{0, 1, 2, 3, 4, 5, 6, 7\}$$

é o conjunto dos menores restos não-negativos módulo 8

$$\{-28, -15, -6, 11, 15, 22, 101, 800\}$$

é um sistema completo de resíduos módulo 8, pois  $-28 \equiv 4$ ,  $-15 \equiv 1$ ,  $-6 \equiv 2$ ,  $11 \equiv 3$ ,  $15 \equiv 7$ ,  $22 \equiv 6$ ,  $101 \equiv 5$ ,  $800 \equiv 0 \pmod{8}$ .

b) De fácil verificação é também que

$$\{0, 3, 3^2, 3^3, \dots, 3^{16}\}$$

é um sistema completo de restos módulo 17.

Pelo desenvolvido fica clara a seguinte

## 6.8 Observação.

Sejam  $n \in \mathbb{N}$ ,  $q_0, q_1, \dots, q_{n-1} \in \mathbb{Z}$ . Então

$$\{nq_0, nq_1 + 1, \dots, nq_{n-1} + (n-1)\}$$

é um sistema completo de resíduos mod  $n$ . Além disso, todo sistema completo de restos mod  $n$  é obtido desta forma.

## 6.9 Teorema. (Propriedades fundamentais das congruências)

Sejam  $n \in \mathbb{N}$ ,  $a, b, c, d \in \mathbb{Z}$ . O seguinte vale:

- a)  $a \equiv a \pmod{n}$
- b) Se  $a \equiv b \pmod{n}$ , então  $b \equiv a \pmod{n}$ .
- c) Se  $a \equiv b \pmod{n}$  e  $b \equiv c \pmod{n}$ , então  $a \equiv c \pmod{n}$ .
- d) Se  $a \equiv b \pmod{n}$  e  $c \equiv d \pmod{n}$ , então
$$a + c \equiv b + d \quad \text{e} \quad ac \equiv bd \pmod{n}.$$

**Demonstração:** Estas propriedades são facilmente verificadas a partir da definição e deixaremos os detalhes ao leitor.

Provemos, por exemplo o item d):  $a \equiv b$  e  $c \equiv d \pmod{n}$  significa que existem  $q_1, q_2 \in \mathbb{Z}$  tais que  $nq_1 = a - b$  e  $nq_2 = c - d$ . Segue  $(a + c) - (b + d) = (a - b) + (c - d) = n(q_1 + q_2)$ , i. e.  $a + c \equiv b + d \pmod{n}$ .

Também  $ac - bd = ac - cb + cb - bd = c(a - b) + b(c - d) = n(cq_1 + bq_2)$ , ou seja  $ac \equiv bd \pmod{n}$ .

■

Particularmente, de  $a \equiv b \pmod{n}$  seguem  $a + c \equiv b + c$  e  $ac \equiv bc \pmod{n}$  e também  $a^k \equiv b^k \pmod{n}$  para todo  $k \in \mathbb{N}$ .

Estas regras dizem que congruências mod  $n$  se comportam (mantendo-se um certo cuidado em relação ao cancelamento de fatores comuns [ver 6.16/6.17] e com potências de expoentes negativos), como se fossem igualdades.

Vejamos a utilidade do *cálculo com congruências* em alguns exemplos.

## 6.10 Exemplos.

a)  $233 \mid M_{29} = 2^{29} - 1.$

b)  $107 \mid M_{53} + 2 = 2^{53} + 1.$

**Demonstração:** a) De  $2^8 = 256 \equiv 23 \pmod{233}$  segue  $2^{16} = (2^8)^2 \equiv 23^2 = 529 \equiv 63 \pmod{233}.$

Daí  $2^{24} = 2^8 \cdot 2^{16} \equiv 23 \cdot 63 \equiv 51 \pmod{233}$  e finalmente  $2^{29} = 2^{24} \cdot 2^5 \equiv 51 \cdot 32 \equiv 1 \pmod{233}.$

Mas isto significa exatamente  $233 \mid 2^{29} - 1.$

b) De maneira semelhante concluímos: De  $2^7 = 128 \equiv 21 \pmod{107}$  segue  $2^{14} = (2^7)^2 \equiv 21^2 = 441 \equiv 13 \pmod{107}$  e  $2^{28} = (2^{14})^2 \equiv 13^2 = 169 \equiv 62 \pmod{107}.$

Daí  $2^{42} = 2^{14} \cdot 2^{28} \equiv 13 \cdot 62 \equiv 57 \pmod{107}$  e finalmente  $2^{53} = 2^7 \cdot 2^4 \cdot 2^{42} \equiv 21 \cdot 16 \cdot 57 \equiv 15 \cdot (-50) \equiv -1 \pmod{107}.$  Assim  $107 \mid 2^{53} + 1.$

■

Algumas congruências módulo 10, 100, 1000, ...

## 6.11 Proposição.

Para  $k \geq 2$  coloquemos

$$R_k = 2^{k-1}(2^k - 1).$$

a) Se  $k \equiv 1 \pmod{4}$ , então  $R_k$  termina em 6.

b) Se  $k \equiv 3 \pmod{4}$ , então  $R_k$  termina em 28.

**Demonstração:** a) Afirma-se  $R_k \equiv 6 \pmod{10}$  desde que  $k \equiv 1 \pmod{4}$ : Temos então  $k = 4\ell + 1$  para algum  $\ell \geq 1$  e segue  $R_k = 2^{4\ell}(2^{4\ell+1} - 1) = 16^\ell(2 \cdot 16^\ell - 1) \equiv 6^\ell(2 \cdot 6^\ell - 1) \equiv 6(12 - 1) \equiv 6 \cdot 1 = 6 \pmod{10}.$

b) Afirma-se  $R_k \equiv 28 \pmod{100}$  desde que  $k \equiv 3 \pmod{4}$ : Temos então  $k = 4\ell + 3$  para algum  $\ell \geq 0$ . Escrevemos ainda  $\ell = 5t + r$  com  $r \in \{0, 1, 2, 3, 4\}$ . Observando-se  $16^5 \equiv 76 \equiv 76^t \pmod{100}$  para todo  $t \geq 1$ , obtemos  $\pmod{100}$ :

$$R_k = 2^{4\ell+2}(2^{4\ell+3} - 1) = 4 \cdot 16^\ell(8 \cdot 16^\ell - 1) = 4 \cdot 16^{5t+r}(8 \cdot 16^{5t+r} - 1) \equiv$$

$$\equiv 4 \cdot 76 \cdot 16^r (8 \cdot 76 \cdot 16^r - 1) \equiv 4 \cdot 16^r (8 \cdot 16^r - 1) \equiv \begin{cases} 4 \cdot 7 = 28 & \text{se } r = 0 \\ 64 \cdot 27 \equiv 28 & \text{se } r = 1 \\ 24 \cdot 47 \equiv 28 & \text{se } r = 2 \\ 84 \cdot 67 \equiv 28 & \text{se } r = 3 \\ 44 \cdot 87 \equiv 28 & \text{se } r = 4 \end{cases} .$$

Assim,  $R_k \equiv 28 \pmod{100}$  em todos os 5 casos de  $r$ .

■

Observamos que, por 5.12, particularmente os números perfeitos pares têm a forma dos  $R_k$  em 6.11. Portanto temos:

### 6.12 Conseqüência.

*Todo número perfeito par termina em 6 ou 28.*

### 6.13 Exemplo.

*Quais são os últimos 1, 2, 3, 4, ... dígitos de*

$$n = 1! + 2! + 3! + 4! + \dots + 100! ?$$

**Solução:** Como  $10 \mid k!$  para  $k \geq 5$ , o último dígito de  $n$  é o mesmo de  $1! + 2! + 3! + 4! \equiv 3 \pmod{10}$ .

Os últimos 2 dígitos de  $n$  são os de  $1! + 2! + 3! + \dots + 9!$ , pois  $100 \mid k!$  para  $k \geq 10$ . Mas,  $1! + 2! + \dots + 9! \equiv 33 + 20 + 20 + 40 + 20 + 80 \equiv 13 \pmod{100}$ .

$$1! + 2! + \dots + 100! \equiv 1! + 2! + \dots + 14! \equiv 313 \pmod{1000}$$

etc.

## CONGRUÊNCIAS LINEARES

### 6.14 Definição.

Dado  $n \in \mathbb{N}$ . Uma *congruência linear* é uma congruência da forma

$$ax \equiv b \pmod{n}$$

onde  $a, b \in \mathbb{Z}$  são dados e as soluções  $x \in \mathbb{Z}$  são procuradas.

Por exemplo:  $2x \equiv 5 \pmod{6}$ : Não tem solução, enquanto

$4x \equiv 2 \pmod{6}$ : Possui duas soluções incongruentes  $x \equiv 2$  e  $x \equiv 5 \pmod{6}$ .

Sobre as soluções das congruências lineares vale

## 6.15 Teorema.

Sejam  $n \in \mathbb{N}$  e  $a, b \in \mathbb{Z}$ .

- a) A congruência  $ax \equiv b \pmod{n}$  admite uma solução, se e somente se,  $d = \text{mdc}(a, n) \mid b$ .
- b) Se  $d \mid b$ , então  $ax \equiv b \pmod{n}$  possui exatamente  $d$  soluções incongruentes entre si  $\pmod{n}$ . Se  $x_0 \in \mathbb{Z}$  é uma solução particular, então  $d$  soluções incongruentes são obtidas por

$$x_0, x_0 + \frac{n}{d}, x_0 + 2 \cdot \frac{n}{d}, \dots, x_0 + (d-1) \cdot \frac{n}{d}.$$

**Demonstração:** a) é claro, pois a congruência  $ax \equiv b \pmod{n}$  equivale à equação DIOFANTINA linear  $ax + ny = b$  a qual é solúvel se e somente se,  $d = \text{mdc}(a, n) \mid b$  (comparar 2.23).

b) Seja  $d \mid b$  e seja  $x_0 \in \mathbb{Z}$  com  $ax_0 \equiv b \pmod{n}$ , i. e.  $ax_0 + ny_0 = b$  para algum  $y_0 \in \mathbb{Z}$ . Por 2.23 toda solução de  $ax \equiv b \pmod{n}$  é então da forma  $x = x_0 + \frac{n}{d}t$  com  $t \in \mathbb{Z}$ . Escrevendo-se  $t = qd + k$  com  $q, k \in \mathbb{Z}$  com  $0 \leq k \leq d-1$  vemos  $x = x_0 + \frac{n}{d}t = x_0 + \frac{n}{d}(qd + k) = x_0 + qn + k \cdot \frac{n}{d} \equiv x_0 + k \cdot \frac{n}{d} \pmod{n}$ . Mostramos portanto que toda solução é congruente módulo  $n$  a um dos  $d$  números indicados. Mais ainda, de  $x_0 + j \cdot \frac{n}{d} \equiv x_0 + k \cdot \frac{n}{d} \pmod{n}$  com  $0 \leq j, k \leq d-1$  segue  $j \cdot \frac{n}{d} \equiv k \cdot \frac{n}{d} \pmod{n}$  e daí  $j \cdot \frac{n}{d} = k \cdot \frac{n}{d} + \ell n$  com  $\ell \in \mathbb{Z}$ . Dividindo-se por  $\frac{n}{d}$ , segue  $j = k + \ell d \equiv k \pmod{d}$ . De  $0 \leq |j - k| \leq d-1$  concluímos  $\ell = 0$  e  $j = k$ . Isto mostra que as  $d$  soluções indicadas são incongruentes  $\pmod{n}$ . ■

O teorema mostra ainda que as  $d$  soluções incongruentes módulo  $n$  de  $ax \equiv b \pmod{n}$ , são todas congruentes módulo  $\frac{n}{d}$ . Podemos concluir portanto:

## 6.16 Conseqüência.

Sejam  $n \in \mathbb{N}$  e  $a, x, y \in \mathbb{Z}$  com  $d = \text{mdc}(a, n)$ . Então

$$ax \equiv ay \pmod{n} \implies x \equiv y \pmod{\frac{n}{d}}.$$

Isto quer dizer, um fator comum numa congruência módulo  $n$  pode ser cancelado, desde que se observe que a nova congruência só é válida módulo  $\frac{n}{d}$ .

(Mesmo quando  $a \equiv 0 \pmod{n}$  esta conclusão é verdadeira, pois neste caso  $d = n$  e  $\frac{n}{d} = 1$  e tanto a congruência  $0x \equiv 0y \pmod{n}$  quanto a  $x \equiv y \pmod{1}$

são afirmações vazias, válidas para todos os  $x, y$ !)

### 6.17 Conseqüência.

Sejam  $n \in \mathbb{N}$  e  $a, x, y \in \mathbb{Z}$  com  $\text{mdc}(a, n) = 1$ . Então as duas congruências

$$ax \equiv ay \pmod{n} \quad e \quad x \equiv y \pmod{n}$$

são equivalentes.

Isto significa, numa congruência módulo  $n$  um fator comum *relativamente primo* com  $n$  pode ser cancelado.

### CONGRUÊNCIAS SIMULTÂNEAS E O TEOREMA DO RESTO CHINÊS

Quais são os números naturais que deixam simultaneamente o resto 4 quando divididos por 5 e o resto 3 quando divididos por 4? A resposta é: São os números

$$19 + 20k \quad k = 0, 1, 2, 3, \dots$$

Pergunta geral: Sejam  $n_1, n_2, \dots, n_r \in \mathbb{N}$ ,  $a_1, a_2, \dots, a_r \in \mathbb{Z}$ . Quais são os números  $x \in \mathbb{Z}$  que deixam os restos  $a_1, a_2, \dots, a_r$  quando divididos, respectivamente, por  $n_1, n_2, \dots, n_r$ ?

Nem quaisquer exigências simultâneas poderão ser cumpridas. Por exemplo  $x \equiv 1 \pmod{2}$  não é compatível com  $x \equiv 2 \pmod{4}$ .

Uma contradição entre as exigências não ocorre porém, se os módulos  $n_1, n_2, \dots, n_r$  são relativamente primos em pares, como mostra o

### 6.18 Teorema do resto chinês.

Sejam  $n_1, n_2, \dots, n_r \in \mathbb{N}$  tais que  $\text{mdc}(n_i, n_j) = 1$  para  $1 \leq i \neq j \leq r$ , i.e. os  $n_1, \dots, n_r$  são relativamente primos, dois a dois. Sejam  $a_1, a_2, \dots, a_r \in \mathbb{Z}$ . Então as congruências

$$\begin{aligned}
x &\equiv a_1 \pmod{n_1} \\
x &\equiv a_2 \pmod{n_2} \\
x &\equiv a_3 \pmod{n_3} \\
&\vdots \quad \vdots \quad \vdots \\
x &\equiv a_r \pmod{n_r}
\end{aligned}$$

possuem uma solução simultânea. Além disso, quaisquer duas soluções são congruentes módulo o produto  $n_1 \cdot n_2 \cdot \dots \cdot n_r$ .

**Demonstração:** Coloquemos  $N = n_1 n_2 \dots n_r$  e para todo  $k = 1, 2, \dots, r$ :

$$N_k = \prod_{j \neq k} n_j = n_1 \dots n_{k-1} n_{k+1} \dots n_r \quad (1 \leq k \leq r),$$

isto é,

$$N_1 = \frac{N}{n_1}, \quad N_2 = \frac{N}{n_2}, \quad \dots, \quad N_r = \frac{N}{n_r}.$$

Para todo  $k = 1, 2, \dots, r$  temos  $\text{mdc}(N_k, n_k) = 1$ , pois os  $n_1, \dots, n_r$  são relativamente primos em pares ( $\mathbb{P} \ni p \mid N_k = n_1 \dots n_{k-1} n_{k+1} \dots n_r \implies p \mid n_j$  para algum  $j \neq k \implies p \nmid n_k$ ). Logo, a congruência  $N_k x \equiv 1 \pmod{n_k}$  possui uma solução. Seja  $x_k \in \mathbb{Z}$ , tal que  $N_k x_k \equiv 1 \pmod{n_k}$  ( $1 \leq k \leq r$ ).

Afirmamos que

$$x = N_1 x_1 a_1 + N_2 x_2 a_2 + \dots + N_r x_r a_r$$

é uma solução simultânea das congruências. De fato: Para todo  $k = 1, 2, 3, \dots, r$  temos: Como  $n_k$  divide  $N_1, N_2, \dots, N_{k-1}, N_{k+1}, \dots, N_r$  segue

$$x \equiv 0 + \dots + 0 + N_k x_k a_k + 0 + \dots + 0 \equiv 1 \cdot a_k = a_k \pmod{n_k}.$$

Como  $N \equiv 0 \pmod{n_1}$ ,  $N \equiv 0 \pmod{n_2}$ ,  $\dots$ ,  $N \equiv 0 \pmod{n_r}$ , qualquer número que difere de  $x$  por um múltiplo de  $N$  é solução simultânea das congruências também.

Reciprocamente, se  $\bar{x} \in \mathbb{Z}$  é uma qualquer solução das congruências, então  $\bar{x} \equiv a_k \pmod{n_k}$  e assim  $n_k \mid \bar{x} - x$  para todo  $k = 1, 2, \dots, r$ . Concluimos  $\bar{x} \equiv x \pmod{n_1 n_2 \dots n_r}$ , pois os  $n_1, n_2, \dots, n_r$  são relativamente primos em pares e portanto, seu mínimo múltiplo comum é seu produto.

■



### 6.19 Exemplo.

Determinar os números  $n \in \mathbb{Z}$  com  $|n| \leq 12,4 \times 10^6$ , que deixam simultaneamente os restos 37, 54, 17 e 100 quando divididos respectivamente, por 40, 63, 23 e 143.

Solução: Temos  $r = 4$ ,  $a_1 = 37$ ,  $a_2 = 54$ ,  $a_3 = 17$ ,  $a_4 = 100$ ,  $n_1 = 40$ ,  $n_2 = 63$ ,  $n_3 = 23$ ,  $n_4 = 143$  e devemos resolver as congruências simultâneas

$$\begin{aligned} x &\equiv 37 \pmod{40} \\ x &\equiv 54 \pmod{63} \\ x &\equiv 17 \pmod{23} \\ x &\equiv 100 \pmod{143}. \end{aligned}$$

Como os  $n_1, n_2, n_3, n_4$  são relativamente primos, dois a dois, existe uma solução a qual é determinada módulo  $N = 40 \cdot 63 \cdot 23 \cdot 143 = 8288280$ . Calculamos

$$\left\{ \begin{array}{l} N_1 = \frac{N}{40} = 207207 \\ N_2 = \frac{N}{63} = 131560 \\ N_3 = \frac{N}{23} = 360360 \\ N_4 = \frac{N}{143} = 57960 \end{array} \right. \cdot \text{As congruências} \left\{ \begin{array}{l} N_1 x \equiv 1 \pmod{n_1} \\ N_2 x \equiv 1 \pmod{n_2} \\ N_3 x \equiv 1 \pmod{n_3} \\ N_4 x \equiv 1 \pmod{n_4} \end{array} \right. \text{são}$$

$$\left\{ \begin{array}{l} 207207x \equiv 1 \pmod{40} \\ 131560x \equiv 1 \pmod{63} \\ 360360x \equiv 1 \pmod{23} \\ 57960x \equiv 1 \pmod{143} \end{array} \right. \text{as quais se reduzem para} \left\{ \begin{array}{l} 7x \equiv 1 \pmod{40} \\ 16x \equiv 1 \pmod{63} \\ 19x \equiv 1 \pmod{23} \\ 45x \equiv 1 \pmod{143} \end{array} \right. .$$

$$\text{Suas soluções são} \left\{ \begin{array}{l} x_1 \equiv 23 \pmod{40} \\ x_2 \equiv 4 \pmod{63} \\ x_3 \equiv 17 \pmod{23} \\ x_4 \equiv 89 \pmod{143} \end{array} \right. .$$

Uma solução simultânea é então  $x = N_1 x_1 a_1 + N_2 x_2 a_2 + N_3 x_3 a_3 + N_4 x_4 a_4 = 207207 \cdot 23 \cdot 37 + 131560 \cdot 4 \cdot 54 + 360360 \cdot 17 \cdot 17 + 57960 \cdot 89 \cdot 100$

$$\equiv 4198437 \equiv 12486717 \equiv -4089843 \equiv -12378123 \pmod{8288280}.$$

Os números procurados  $n$  com  $|n| \leq 12,4 \times 10^6$  são portanto:

$$n = 4198437, \quad n = -4089843 \quad \text{e} \quad n = -12378123 .$$

## § 7 Os Teoremas de FERMAT e de WILSON

Queremos tratar neste parágrafo algumas propriedades referentes a congruências módulo números primos.

### O PEQUENO TEOREMA DE FERMAT

O primeiro resultado neste contexto é:

#### 7.1 Teorema. (O "pequeno teorema" de FERMAT)

Seja  $p \in \mathbb{P}$  e  $a \in \mathbb{Z}$  de tal maneira que  $p \nmid a$ . Então

$$a^{p-1} \equiv 1 \pmod{p}.$$

**Demonstração:** Dados  $p$  e  $a$  com  $p \nmid a$ , consideremos os conjuntos

$$\{1, 2, 3, \dots, p-1\} \text{ e } \{a, 2a, 3a, \dots, (p-1)a\}.$$

Temos  $a, 2a, \dots, (p-1)a \not\equiv 0 \pmod{p}$ .

Se  $i, j \in \{1, 2, \dots, p-1\}$  e  $ia \equiv ja \pmod{p}$ , concluímos  $i \equiv j \pmod{p}$ , já que  $\text{mdc}(a, p) = 1$ . Então  $i = j$ , pois  $0 \leq |i - j| < p$ . Isto significa que os números  $a, 2a, \dots, (p-1)a$  são incongruentes entre si  $\pmod{p}$ . Logo, os  $a, 2a, \dots, (p-1)a$  são congruentes, em alguma ordem, aos  $1, 2, \dots, p-1$ . Podemos concluir então que

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \equiv a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1)a, \text{ ou seja}$$

$$(p-1)! \equiv a^{p-1} \cdot (p-1)! \pmod{p}.$$

Como  $\text{mdc}(p, (p-1)!) = 1$ , por 6.17 podemos cancelar nesta congruência o fator  $(p-1)!$  e obtemos, como afirmado,

$$a^{p-1} \equiv 1 \pmod{p}.$$

■

#### 7.1' Teorema de FERMAT (2ª formulação).

Para qualquer primo  $p$  e qualquer  $a \in \mathbb{Z}$  temos

$$a^p \equiv a \pmod{p}$$

(i.e.  $a$  e  $a^p$  sempre deixam o mesmo resto quando divididos por  $p$  - qualquer que seja  $a \in \mathbb{Z}$ ).

Observação: Se  $p \nmid a$  e sabendo-se 7.1, a congruência de 7.1' é obtida de  $a^{p-1} \equiv 1 \pmod p$  multiplicando-se por  $a$ . Para  $a \equiv 0 \pmod p$ , 7.1' é trivial.

Reciprocamente, se  $a^p \equiv a \pmod p$ , ou seja,  $a \cdot a^{p-1} \equiv a \cdot 1 \pmod p$  e se  $p \nmid a$ , obtém-se 7.1 por cancelamento do fator  $a$  desta congruência (comparar 6.17). Logo, as duas formulações do teorema de FERMAT são equivalentes.

Queremos dar uma prova independente para 7.1':

Provaremos primeiro que 7.1' é verdade quando  $a \geq 0$  por indução sobre  $a$ . De fato, para  $a = 0$  (e também para  $a = 1$ ) não há nada para provar. Supondo já provado  $a^p \equiv a \pmod p$  para algum  $a$ , segue pelo teorema do desenvolvimento binomial

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

Mas, para  $1 \leq k \leq p-1$ , os coeficientes binomiais

$$\binom{p}{k} = \frac{p(p-1)\dots(p-k+1)}{k!},$$

são números inteiros (ver 1.8) divisíveis por  $p$ , pois o fator  $p$  no numerador não cancela com nenhum fator de  $k!$ . Melhor explicado:

$$\text{De } p \mid p(p-1)\dots(p-k+1) = k! \cdot \binom{p}{k} \text{ e } p \nmid k! \text{ segue } p \mid \binom{p}{k}.$$

Isto significa que  $\binom{p}{1}a^{p-1} + \dots + \binom{p}{p-1}a \equiv 0 \pmod p$ , ou seja,  $(a + 1)^p \equiv a^p + 1$ .

Mas, por hipótese de indução,  $a^p \equiv a \pmod p$ , de onde segue

$$(a + 1)^p \equiv a + 1 \pmod p,$$

a afirmação para  $a + 1$ .

Se  $a < 0$ , escrevemos  $a = -b$  com  $b > 0$ . Pelo mostrado,

$$a^p = (-b)^p = (-1)^p b^p \equiv (-1)^p b = \begin{cases} -b = a \pmod p & \text{se } p > 2 \\ b = -a \equiv a \pmod 2 & \text{se } p = 2 \end{cases}$$

ou seja,  $a^p \equiv a \pmod p$  sempre. ■

Vejamos a utilidade do teorema de FERMAT numa primeira

## 7.2 Conseqüência.

Seja  $q = 2n + 1$  um número primo. Então

$$\text{Ou } q \mid M_n = 2^n - 1 \text{ ou } q \mid M_n + 2 = 2^n + 1 .$$

**Demonstração:** Primeiro observamos que  $q$  não pode dividir ambos  $M_n$  e  $M_n + 2$ , senão  $q$  dividiria  $M_n + 2 - M_n = 2$ , que não é verdade.

Como  $q \nmid a = 2$  e  $q$  é primo, segue pelo teorema de FERMAT:  $2^{q-1} \equiv 1 \pmod{q}$ , ou seja,  $2^{2n} - 1 = 2^{q-1} - 1 \equiv 0 \pmod{q}$ . Logo,  $q \mid 2^{2n} - 1 = (2^n - 1)(2^n + 1) = M_n(M_n + 2)$ , de onde concluímos  $q \mid M_n$  ou  $q \mid M_n + 2$ . ■

Números de MERSENNE  $M_p$  com índice primo nem sempre são primos. Queremos elaborar uma *condição necessária* para que um  $M_p$  com  $p \in \mathbb{P}$  possa ser *composto*. Primeiro provamos

## 7.3 Observação.

Seja  $q \in \mathbb{P}$ ,  $a \in \mathbb{Z}$  tal que  $q \nmid a$ . Seja  $k_0 \in \mathbb{N}$  o **menor** número tal que  $a^{k_0} \equiv 1 \pmod{q}$  e seja  $k \in \mathbb{N}$  com  $a^k \equiv 1 \pmod{q}$  (por exemplo  $k = q - 1$ ).

$$\text{Então } k_0 \mid k.$$

( $k_0$  é a chamada *ordem*  $\mathbf{o}_q(a)$  de  $a \pmod{q}$ . Ver § 11)

**Demonstração:** Existem  $\ell, r \in \mathbb{N}_0$  com  $k = \ell k_0 + r$  onde  $0 \leq r < k_0$ . Segue  $1 \equiv a^k = a^{\ell k_0 + r} = (a^{k_0})^\ell \cdot a^r \equiv 1^\ell \cdot a^r = a^r \pmod{q}$ . Como  $a^r \equiv 1$  e  $0 \leq r < k_0$  e  $k_0$  é o menor expoente natural com  $a^{k_0} \equiv 1 \pmod{q}$ , concluímos  $r = 0$ . Assim  $k_0 \mid k$ . ■

## 7.4 Proposição.

Sejam  $p, q$  números primos ímpares.

$$\text{Se } q \mid M_p \text{ então } q = 2kp + 1 \text{ com } k \in \mathbb{N} .$$

**Demonstração:**  $q \mid M_p = 2^p - 1$  significa  $2^p \equiv 1 \pmod{q}$ . Seja  $k_0$  o menor expoente positivo com  $2^{k_0} \equiv 1 \pmod{q}$ . Por 7.3 sabemos  $k_0 \mid p$ . De  $2 \not\equiv 1 \pmod{q}$  concluímos  $k_0 > 1$  e segue  $k_0 = p$ . Como  $q \nmid 2$  temos por FERMAT:  $2^{q-1} \equiv 1 \pmod{q}$ .

Outra vez, por 7.3:  $p = k_0 | q - 1$ . Logo, existe  $\ell \in \mathbb{N}$  com  $p\ell = q - 1$ , ou seja,  $q = p\ell + 1$ . Como  $p, q$  são ímpares, concluímos que  $\ell = 2k$  é par. Assim,  $q = 2kp + 1$ .

■

## 7.5 Exemplos.

a)  $q | M_{11} \implies q = 22k + 1$ . De fato:

$$M_{11} = 23 \cdot 89 \text{ com } \begin{cases} 23 = 22 \cdot 1 + 1 \\ 89 = 22 \cdot 4 + 1 \end{cases}$$

b)  $q | M_{29} \implies q = 58k + 1$ . De fato:

$$M_{29} = 233 \cdot 1103 \cdot 2089 \text{ com } \begin{cases} 233 = 58 \cdot 4 + 1 \\ 1103 = 58 \cdot 19 + 1 \\ 2089 = 58 \cdot 36 + 1 \end{cases}$$

c) (Ver Ex. 5.15)  $q | M_{67} \implies q = 134k + 1$ . De fato:

$$M_{67} = 193707721 \cdot 761838257287$$

$$\text{com } \begin{cases} 193707721 = 134 \cdot 1445580 + 1 \\ 761838257287 = 134 \cdot 5685360129 + 1 \end{cases}$$

## 7.6 Exemplo.

*Os números de MERSENNE*

$M_{13}, M_{17}$  e  $M_{19}$  são primos.

**Demonstração:** Para  $M_{13}$ : Temos  $\sqrt{M_{13}} = 90,5\dots$ . Um possível divisor primo  $q$  próprio de  $M_{13}$  é  $\leq 89$  e da forma  $26k + 1$ . As únicas possibilidades são  $q = 53$  e  $q = 79$  que ambos não dividem  $M_{13} = 8191$ .

Para  $M_{17}$ : Temos  $\sqrt{M_{17}} = 362,03\dots$ . Um possível divisor primo  $q$  próprio de  $M_{17}$  é  $\leq 359$  e da forma  $34k + 1$ . As únicas possibilidades são  $q \in \{103, 137, 239, 307\}$  que todos não dividem  $M_{17} = 131071$ .

Para  $M_{19}$ : Temos  $\sqrt{M_{19}} = 724,07\dots$ . Um possível divisor primo  $q$  próprio de  $M_{19}$  é  $\leq 724$  e da forma  $38k + 1$ . As únicas possibilidades são  $q \in \{191, 229, 419, 457, 571, 647\}$  que todos não dividem  $M_{19} = 524287$ .

■

## 7.7 Conseqüência.

Qualquer possível divisor  $t$  de  $M_p = 2^p - 1$  (inclusive 1 e o próprio número  $M_p$ ) é da forma  $t = 2kp + 1$  com algum  $k \in \mathbb{N}$ .

**Demonstração:** Produtos de números da forma  $2kp + 1$  (i.e. números ímpares  $\equiv 1 \pmod{p}$ ) continuam da mesma forma. Qualquer  $t \mid M_p$  é produto de primos desta forma.

(Observe que, como  $p \mid 2^p - 2$  temos para o próprio  $M_p$ :

$$2^p - 1 = 2^p - 2 + 1 = 2kp + 1 !)$$

■

## 7.8 Exemplo.

A decomposição completa de  $M_{23}$  é

$$M_{23} = 47 \cdot 178481 ,$$

pois, qualquer possível divisor primo  $q$  próprio de 178481 é da forma  $q = 46k + 1$  e  $q \leq 422, 47, \dots$ . Isto dá  $q \in \{47, 139, 277\}$  que não dividem 178481.

## O TEOREMA DE WILSON

Mais uma congruência básica módulo números primos é dada no

## 7.9 Teorema. (WILSON)

Para todo primo  $p$  vale

$$(p - 1)! \equiv -1 \pmod{p} .$$

## 7.10 Proposição.

Seja  $p > 2$  um primo e  $a, b \in \mathbb{Z}$ .

$$a) \quad a^2 \equiv b^2 \pmod{p} \iff a \equiv \pm b \pmod{p} .$$

$$b) \quad a^2 \equiv 1 \pmod{p} \iff a \equiv \pm 1 \pmod{p} .$$

**Demonstração:** a) " $\Leftarrow$ ": De  $a \equiv \pm b \pmod{p}$  segue  $a^2 \equiv (\pm b)^2 = b^2 \pmod{p}$ .

" $\Rightarrow$ ": De  $a^2 \equiv b^2 \pmod{p}$  segue  $b^2 - a^2 = (b - a)(b + a) \equiv 0 \pmod{p}$ , ou seja,

$p|(b-a)(b+a)$ . Daí  $p|b-a$  ou  $p|b+a$ , pois  $p$  é primo. Isto significa  $a \equiv b$  ou  $a \equiv -b \pmod{p}$ .

b) É o caso particular  $b \equiv 1 \pmod{p}$  de a).

■

(Lembremos que uma tal conclusão não poderia ser feita se o módulo não é primo: módulo 8 temos por exemplo:  $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1$  apesar de  $3, 5 \not\equiv \pm 1 \pmod{8}$ !)

### 7.11 Observação.

Seja  $p > 2$  um primo e seja  $2 \leq a \leq p-2$ . Então existe um único  $b \in \{2, \dots, p-2\}$  tal que  $ab \equiv 1 \pmod{p}$ . Além disso,  $a \neq b$ .

**Demonstração:** A congruência  $ax \equiv 1 \pmod{p}$  possui uma única solução  $x = b \in \{1, 2, \dots, p-1\}$ . Necessariamente,  $b \neq 1$  e  $b \neq p-1$ , pois  $a \not\equiv \pm 1 \pmod{p}$ . Portanto  $2 \leq b \leq p-2$ .

Por 7.10 temos também  $a \not\equiv b \pmod{p}$ , i.e.  $a \neq b$ .

■

Estamos agora em condições para provar o Teorema de WILSON.

**Demonstração de 7.9:** Escrevemos o conjunto  $\{2, \dots, p-2\}$  sob o aspecto de 7.11:  $\forall a \in \{2, \dots, p-2\} \exists$  único  $b \in \{2, \dots, p-2\}$  com  $ab \equiv 1 \pmod{p}$  e  $a \neq b$ . Podemos então reordenar o conjunto  $\{2, \dots, p-2\}$  como

$$\{2, \dots, p-2\} = \left\{ a_1, b_1, a_2, b_2, \dots, a_{\frac{p-3}{2}}, b_{\frac{p-3}{2}} \right\},$$

onde  $a_1 b_1 \equiv a_2 b_2 \equiv \dots \equiv a_{\frac{p-3}{2}} b_{\frac{p-3}{2}} \equiv 1 \pmod{p}$ . Segue

$$\begin{aligned} (p-1)! &= 1 \cdot 2 \cdot \dots \cdot (p-1) = 1 \cdot (a_1 b_1) \cdot (a_2 b_2) \cdot \dots \cdot \left( a_{\frac{p-3}{2}} b_{\frac{p-3}{2}} \right) (p-1) \equiv \\ &\equiv 1 \cdot 1 \cdot 1 \cdot \dots \cdot 1 \cdot (p-1) \equiv -1 \pmod{p}. \end{aligned}$$

■

### 7.12 Exemplo.

Para  $p = 19$  temos

$$18! = 1 \cdot (2 \cdot 10) \cdot (3 \cdot 13) \cdot (4 \cdot 5) \cdot (6 \cdot 16) \cdot (7 \cdot 11) \cdot (8 \cdot 12) \cdot (9 \cdot 17) \cdot (14 \cdot 15) \cdot (-1) \equiv -1 \pmod{19}.$$

Observamos que o teorema de WILSON *caracteriza* os números primos:

### 7.13 Observação.

*Se  $n > 1$  é composto, então temos*

$$\begin{cases} (n-1)! \equiv 0 \not\equiv -1 \pmod{n} & \text{se } n > 4 \\ (4-1)! \equiv 2 \not\equiv -1 \pmod{4}. \end{cases}$$

**Demonstração:** Se  $n$  não é o quadrado de um primo, existe uma decomposição  $n = rs$  com  $2 \leq s < r \leq n-1$  e segue que

$$(n-1)! = 1 \cdot 2 \cdot \dots \cdot s \cdot \dots \cdot r \cdot \dots \cdot (n-1) \text{ é divisível por } n = sr.$$

Se  $n = p^2$  é o quadrado de um primo e  $p > 2$  teremos  $p < 2p \leq n-1$  e segue outra vez

$$(n-1)! = 1 \cdot 2 \cdot \dots \cdot p \cdot \dots \cdot 2p \cdot \dots \cdot (n-1) \equiv 0 \pmod{p^2}.$$

Sobra o caso  $n = 4$  no qual  $(4-1)! = 3! = 6 \equiv 2 \pmod{4}$ .

■



## § 8 Congruências quadráticas e a lei da reciprocidade quadrática de EULER/GAUSS

### RESTOS QUADRÁTICOS

#### 8.1 Definição.

Seja  $p$  um número primo. Um  $a \in \mathbb{Z}$  é dito um

$\left\{ \begin{array}{l} \text{resto quadrático} \\ \text{resto não-quadrático} \end{array} \right. \pmod{p}$ , se a congruência  $x^2 \equiv a \pmod{p}$   $\left\{ \begin{array}{l} \text{admitir} \\ \text{não admitir} \end{array} \right.$

uma solução  $x = b \in \mathbb{Z}$ .

#### 8.2 Exemplos.

a) Para  $p = 5$ :

$$\left. \begin{array}{l} x^2 \equiv 0 \longleftarrow b \equiv 0 \\ x^2 \equiv 1 \longleftarrow b \equiv \pm 1 \\ x^2 \equiv 2 \longleftarrow \nexists b \\ x^2 \equiv 3 \longleftarrow \nexists b \\ x^2 \equiv 4 \longleftarrow b \equiv \pm 2 \end{array} \right\} \pmod{5}.$$

b) Para  $p = 19$ :  $\{1^2, 2^2, \dots, 18^2\} =$   
 $= \{1, 4, 9, 16, 5^2 \equiv 6, 6^2 \equiv 17, 11, 7, 5, 5, 7, 11, 17, 6, 16, 9, 17^2 \equiv 4, 18^2 \equiv 1\} =$   
 $= \{1, 4, 5, 6, 7, 9, 11, 16, 17\}.$

Conseqüentemente,

$$\left\{ \begin{array}{l} \{1, 4, 5, 6, 7, 9, 11, 16, 17\} \\ \{2, 3, 8, 10, 12, 13, 14, 15, 18\} \end{array} \right\} \text{ são os restos } \left\{ \begin{array}{l} \text{quadráticos} \\ \text{não-quadráticos} \end{array} \right. \pmod{19}.$$

O resto  $0 \pmod{p}$  fica usualmente fora da consideração. Para  $p = 2$ , o único resto não nulo é  $1 \pmod{2}$  o qual claramente é seu próprio quadrado. A distinção entre quadrados e não quadrados só é interessante se  $p > 2$ .

Em geral vemos que, se  $p > 2$  é um primo, os restos quadráticos  $\pmod{p}$  entre  $\{1, 2, 3, \dots, p-1\}$  são os números representados por

$$\begin{aligned}
& \{1^2, 2^2, \dots, (p-2)^2, (p-1)^2\} = \\
& = \left\{1^2, 2^2, \dots, \left(\frac{p-3}{2}\right)^2, \left(\frac{p-1}{2}\right)^2, \left(\frac{p+1}{2}\right)^2, \left(\frac{p+3}{2}\right)^2, \dots, (p-2)^2, (p-1)^2\right\} = \\
& \left\{1^2, 2^2, \dots, \left(\frac{p-3}{2}\right)^2, \left(\frac{p-1}{2}\right)^2, \left(p-\frac{p-1}{2}\right)^2, \left(p-\frac{p-3}{2}\right)^2, \dots, (p-2)^2, (p-1)^2\right\} \equiv \\
& \equiv \left\{1^2, 2^2, \dots, \left(\frac{p-3}{2}\right)^2, \left(\frac{p-1}{2}\right)^2, \left(-\frac{p-1}{2}\right)^2, \left(-\frac{p-3}{2}\right)^2, \dots, (-2)^2, (-1)^2\right\} = \\
& = \left\{1^2, 2^2, \dots, \left(\frac{p-3}{2}\right)^2, \left(\frac{p-1}{2}\right)^2\right\}
\end{aligned}$$

Estes últimos  $\frac{p-1}{2}$  números são incongruentes entre si, pois  $x^2 \equiv b^2 \pmod{p}$  possui exatamente as duas soluções incongruentes  $x \equiv \pm b \pmod{p}$ .

Podemos afirmar então que sempre existem  $\frac{p-1}{2}$  restos quadráticos e  $\frac{p-1}{2}$  restos não-quadráticos entre  $\{1, 2, \dots, p-1\}$ . A tarefa é separá-los. Como o exemplo acima (mod 19) mostra, não há nenhuma regularidade visível nisso.

Queremos caracterizar primeiro os primos  $p$  módulo os quais,  $-1$  (i.e.  $p-1$ ) é um resto quadrático.

### 8.3 Proposição.

Seja  $p > 2$  um primo. A congruência

$$x^2 \equiv -1 \pmod{p} \text{ admite uma solução} \iff p \equiv 1 \pmod{4}.$$

**Demonstração:** " $\Rightarrow$ ": Seja  $x^2 \equiv -1 \pmod{p}$  solúvel. Então existe  $b \in \mathbb{Z}$  tal que  $b^2 \equiv -1 \pmod{p}$ . Por FERMAT (7.1) obtemos

$$1 \equiv b^{p-1} = (b^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

e daí  $(-1)^{\frac{p-1}{2}} = +1$ , pois  $1 \not\equiv -1 \pmod{p}$ . Segue que  $\frac{p-1}{2} = 2k$  é par e portanto  $p = 4k + 1 \equiv 1 \pmod{4}$ .

" $\Leftarrow$ ": Seja  $p \equiv 1 \pmod{4}$ . Concluimos por WILSON (7.9)

$$\begin{aligned}
-1 & \equiv (p-1)! = 1 \cdot 2 \cdot \dots \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \dots \cdot (p-2) \cdot (p-1) \equiv \\
& \equiv 1 \cdot 2 \cdot \dots \cdot \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \cdot \dots \cdot (-2) \cdot (-1) \equiv \\
& \equiv (-1)^{\frac{p-1}{2}} \cdot \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p},
\end{aligned}$$

pois  $(-1)^{\frac{p-1}{2}} = +1$ , já que  $p \equiv 1 \pmod{4}$ .

Logo a congruência  $x^2 \equiv -1 \pmod{p}$  é satisfeita por  $b = \left(\frac{p-1}{2}\right)!$ .

■

Eis uma tabela dos primos  $p \leq 97$  que são  $\equiv 1 \pmod{4}$  e as duas soluções incongruentes  $< p$  de  $x^2 \equiv -1 \pmod{p}$ :

$p \equiv 1 \pmod{4}$	sols. $x$ e $p - x$ de $x^2 \equiv -1 \pmod{p}$
5	2, 3
13	5, 8
17	4, 13
29	12, 17
37	6, 31
41	9, 32
53	23, 30
61	11, 50
73	27, 46
89	34, 55
97	22, 75

Estamos agora em condições para provar mais um caso particular ( $b = 4, a = 1$ ) do teorema de Dirichlet (3.29), a saber

#### 8.4 Exemplo.

*Existem infinitos primos da forma  $4n + 1$  com  $n \in \mathbb{N}$ .*

**Demonstração:** Suponhamos  $\{p_1=5, p_2=13, p_3, \dots, p_r\}$  fosse o conjunto de todos os primos  $\equiv 1 \pmod{4}$ . Consideremos  $N = (2p_1p_2\dots p_r)^2 + 1 \in \mathbb{N}$ . Se  $q \in \mathbb{P}$  e  $q|N$ , então  $(2p_1p_2\dots p_r)^2 + 1 \equiv 0 \pmod{q}$ . Isto significa que a congruência  $x^2 \equiv -1 \pmod{q}$  é solúvel por  $x = 2p_1p_2\dots p_r$ . Por 8.3 concluímos  $q \equiv 1 \pmod{4}$ . Assim,  $q \in \{p_1, p_2, \dots, p_r\}$ , o que dá o absurdo  $q|1$ . Logo, o conjunto  $\{p_1, p_2, \dots, p_r\}$  não pode estar completo. ■

## UM LEMA DE EULER

Uma primeira informação sobre restos quadráticos é dada na

### 8.5 Proposição. (Lema de EULER)

Seja  $p > 2$  um primo,  $a \in \mathbb{Z}$ ,  $p \nmid a$ .

- a) Sempre  $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$
- b)  $a^{\frac{p-1}{2}} \equiv +1 \pmod{p} \iff a$  é resto quadrático  $\pmod{p}$ .
- b')  $a^{\frac{p-1}{2}} \equiv -1 \pmod{p} \iff a$  é resto não-quadrático  $\pmod{p}$ .

**Demonstração:** a) Por FERMAT (7.1) temos  $1 \equiv a^{p-1} = \left(a^{\frac{p-1}{2}}\right)^2 \pmod{p}$  e conseqüentemente  $0 \equiv a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \pmod{p}$ .

Isto significa  $p \mid \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right)$ . Como  $p$  é primo, concluímos  $p \mid a^{\frac{p-1}{2}} - 1$  ou  $p \mid a^{\frac{p-1}{2}} + 1$  e daí

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

b) e b') são obviamente as mesmas afirmações. Provemos b):

"  $\Leftarrow$  ": Suponhamos,  $a$  é quadrado módulo  $p$ . Assim, existe  $b \in \mathbb{Z}$  tal que  $a \equiv b^2 \pmod{p}$ . Segue por FERMAT

$$a^{\frac{p-1}{2}} = (b^2)^{\frac{p-1}{2}} = b^{p-1} \equiv 1 \pmod{p}.$$

"  $\Rightarrow$  ": Suponhamos,  $a$  não é quadrado módulo  $p$ . Para todo  $c \in \{1, 2, \dots, p-1\}$ , a congruência  $cx \equiv a \pmod{p}$  possui exatamente uma solução  $c' \in \{1, 2, \dots, p-1\}$ . Além disso,  $c \neq c'$  (senão  $a \equiv cc' = c^2$  seria um quadrado!). Escrevemos o conjunto  $\{1, 2, \dots, p-1\}$  como

$$\{1, 2, \dots, p-1\} = \left\{c_1, c'_1, c_2, c'_2, \dots, c_{\frac{p-1}{2}}, c'_{\frac{p-1}{2}}\right\},$$

tal que  $c_k c'_k \equiv a \pmod{p}$  para  $1 \leq k \leq \frac{p-1}{2}$ . Segue agora por WILSON:

$$\begin{aligned} -1 &\equiv (p-1)! = 1 \cdot 2 \cdot \dots \cdot (p-1) = \\ &= \left(c_1 c'_1\right) \cdot \left(c_2 c'_2\right) \cdot \dots \cdot \left(c_{\frac{p-1}{2}} c'_{\frac{p-1}{2}}\right) \equiv a \cdot a \cdot \dots \cdot a = a^{\frac{p-1}{2}} \pmod{p}. \end{aligned}$$

■

## 8.6 Exemplo.

Para  $p = 13$  temos  $\frac{p-1}{2} = 6$ ,

$\left\{ \begin{array}{l} \{1, 4, 9, 10, 12\} \text{ são os quadrados} \\ \{2, 5, 6, 7, 8, 11\} \text{ os não-quadrados} \end{array} \right.$  módulo 13. Vale

$1^6 \equiv 4^6 \equiv 3^6 \equiv 9^6 \equiv 10^6 \equiv 12^6 \equiv 1 \pmod{13}$ , enquanto

$2^6 \equiv 5^6 \equiv 6^6 \equiv 7^6 \equiv 8^6 \equiv 11^6 \equiv -1 \pmod{13}$ , como é de fácil verificação direta.

## O SIMBOLO DE LEGENDRE

### 8.7 Definição.

Para todo primo  $p > 2$  e todo  $a \in \mathbb{Z}$  com  $p \nmid a$ , colocamos

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } a \text{ é resto quadrático mod } p \\ -1 & \text{se } a \text{ é resto não-quadrático mod } p \end{cases} .$$

$\left(\frac{a}{p}\right)$  chama-se o *símbolo de LEGENDRE* de  $a$  módulo  $p$ .

O símbolo de LEGENDRE então é uma "sim/não-função" para decidir se um número  $a$  é ou não é um resto quadrático módulo  $p$ .

### 8.8 Exemplos.

$$\left(\frac{2}{5}\right) = \left(\frac{2}{13}\right) = \left(\frac{45}{17}\right) = -1 \text{ porém } \left(\frac{2}{7}\right) = \left(\frac{101}{13}\right) = 1 ,$$

pois  $x^2 \equiv 2 \pmod{5}$ ,  $x^2 \equiv 2 \pmod{13}$   $x^2 \equiv 45 \equiv 11 \pmod{17}$  não têm solução.

Mas  $(\pm 3)^2 \equiv 2 \pmod{7}$  e  $(\pm 6)^2 \equiv 10 \equiv 101 \pmod{13}$ .

### 8.9 Proposição.

Para todo primo  $p > 2$  vale

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} .$$

**Demonstração:** Isto é a tradução do conteúdo de 8.3 para o conceito do símbolo

de LEGENDRE:  $-1$  é resto quadrático mod  $p \Leftrightarrow$

$$\Leftrightarrow p \equiv 1 \pmod{4} \Leftrightarrow \frac{p-1}{2} \text{ é par} \Leftrightarrow (-1)^{\frac{p-1}{2}} = +1.$$

■

Propriedades elementares do símbolo de LEGENDRE são:

### 8.10 Proposição.

Seja  $p > 2$  um primo e  $a, b \in \mathbb{Z}$  com  $p \nmid a$  e  $p \nmid b$ . Então valem

a) Se  $a \equiv b \pmod{p}$ , então  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ .

b)  $\left(\frac{a^2}{p}\right) = 1$ , particularmente  $\left(\frac{1}{p}\right) = 1$ .

c)  $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ .

d)  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ .

**Demonstração:** a) e b) são claros.

c) Isto é a tradução de 8.5 para o símbolo de LEGENDRE.

d)  $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \pmod{p}$ . Como ambos os lados desta congruência são  $\pm 1$  e como  $p > 2$  (i.e.  $-1 \not\equiv +1 \pmod{p}$ ), podemos concluir

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

■

Observamos ainda que a propriedade d) diz em palavras:

*O produto de dois restos quadráticos ou de dois não-quadráticos é um resto quadrático.*

Porém,

*o produto de um resto quadrático com um não-quadrático é um resto não-quadrático.*

## UM LEMA DE GAUSS

Um Lema técnico para a determinação de  $\left(\frac{a}{p}\right)$  é dado na seguinte

### 8.11 Proposição. (Lema de GAUSS).

Seja  $p > 2$  um primo e  $a \in \mathbb{Z}$  com  $p \nmid a$ . Consideremos o conjunto

$$S = \left\{ a, 2a, 3a, \dots, \frac{p-1}{2}a \right\}.$$

Dividindo-se estes números por  $p$ , para cada  $k = 1, \dots, \frac{p-1}{2}$  vão existir inteiros  $q_k, t_k$  tais que

$$ka = pq_k + t_k \quad \text{onde } 1 \leq t_k \leq p-1.$$

Sejam  $\begin{cases} r_1, r_2, \dots, r_m & \text{os números em } \left\{ t_1, t_2, \dots, t_{\frac{p-1}{2}} \right\} \text{ com } r_i < \frac{p}{2} \\ s_1, s_2, \dots, s_n & \text{os números em } \left\{ t_1, t_2, \dots, t_{\frac{p-1}{2}} \right\} \text{ com } s_j > \frac{p}{2} \end{cases}$ .

Então vale

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Em palavras: Para saber se um  $a \not\equiv 0 \pmod{p}$  é um resto quadrático ou não, considera-se os menores restos não-negativos  $t_1, t_2, \dots, t_{\frac{p-1}{2}}$  que os  $a, 2a, \dots, \frac{p-1}{2}a$  deixam na divisão por  $p$ . *Decisivo* para o valor de  $\left(\frac{a}{p}\right)$  é se a quantidade  $n$  destes restos que jazem acima de  $\frac{p}{2}$  é par ou ímpar.

**Demonstração:** Observamos primeiro que  $a, 2a, 3a, \dots, \frac{p-1}{2}a$  não são divisíveis por  $p$ . Eles também são incongruentes  $\pmod{p}$  entre si ( $ka \equiv la \pmod{p} \Rightarrow (k-l)a \equiv 0 \pmod{p} \Rightarrow p \mid (k-l)a \Rightarrow p \mid k-l \Rightarrow k \equiv l \pmod{p} \Rightarrow k=l$ , pois  $0 \leq |k-l| < p$ ). Conseqüentemente, os  $t_1, t_2, \dots, t_{\frac{p-1}{2}}$  são distintos e  $t_k \geq 1$ . Temos

$$\left\{ t_1, t_2, \dots, t_{\frac{p-1}{2}} \right\} = \left\{ r_1, r_2, \dots, r_m, s_1, s_2, \dots, s_n \right\}$$

e daí  $m + n = \frac{p-1}{2}$ . Consideremos

$$\left\{ r_1, r_2, \dots, r_m, p-s_1, p-s_2, \dots, p-s_n \right\}.$$

Temos  $1 \leq r_i, p-s_j \leq \frac{p-1}{2} < \frac{p}{2}$ . Os  $r_i$  são distintos entre si, o mesmo acontecendo com os  $p-s_j$ .

Será que  $r_i = p-s_j$  para algum par de índices  $i, j$ ?

Então  $r_i + s_j = p$ . Existem  $k, \ell \in \left\{ 1, 2, \dots, \frac{p-1}{2} \right\}$  tais que  $ka \equiv r_i$  e  $la \equiv$

$s_j \pmod p$ . Segue  $p = r_i + s_j \equiv a(k + \ell) \pmod p$  com  $0 < k + \ell \leq \frac{p-1}{2} + \frac{p-1}{2} = p-1 < p$ . Isto é impossível. Logo  $r_i \neq p - s_j \quad \forall 1 \leq i \leq m; 1 \leq j \leq n$ . Concluimos que

$$\{r_1, \dots, r_m, p-s_1, \dots, p-s_n\} = \{1, 2, \dots, \frac{p-1}{2}\}.$$

Segue então

$$\begin{aligned} \left(\frac{p-1}{2}\right)! &= r_1 \cdot \dots \cdot r_m \cdot (p-s_1) \cdot \dots \cdot (p-s_n) \equiv \\ r_1 \cdot \dots \cdot r_m \cdot s_1 \cdot \dots \cdot s_n \cdot (-1)^n &= t_1 \cdot t_2 \cdot \dots \cdot t_{\frac{p-1}{2}} \cdot (-1)^n \equiv \\ a \cdot 2a \cdot \dots \cdot \frac{p-1}{2}a \cdot (-1)^n &= \left(\frac{p-1}{2}\right)! \cdot a^{\frac{p-1}{2}} \cdot (-1)^n \pmod p. \end{aligned}$$

Como  $\text{mdc}\left(\left(\frac{p-1}{2}\right)!, p\right) = 1$ , concluímos por cancelamento do fator  $\left(\frac{p-1}{2}\right)!$  dos dois lados desta congruência, que  $1 \equiv a^{\frac{p-1}{2}} \cdot (-1)^n \pmod p$  ou também  $a^{\frac{p-1}{2}} \equiv (-1)^n \pmod p$ . Agora, por 8.10 c) vemos  $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$ . Logo temos, como afirmado,

$$\left(\frac{a}{p}\right) = (-1)^n.$$

■

O SÍMBOLO DE LEGENDRE  $\left(\frac{2}{p}\right)$

Como primeira aplicação do Lema de GAUSS vamos determinar quando  $a = 2$  é um resto quadrático módulo  $p$ .

### 8.12 Proposição.

Seja  $p > 2$  um primo. Temos

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1 \text{ ou } 7 \pmod 8 \\ -1 & \text{se } p \equiv 3 \text{ ou } 5 \pmod 8 \end{cases}$$

**Demonstração:** Consideremos no Lema de GAUSS (para  $a = 2$ ) o conjunto  $\{1 \cdot 2, 2 \cdot 2, 3 \cdot 2, \dots, \frac{p-1}{2} \cdot 2\}$ . Estes números são coincidentes com seus menores restos não-negativos na divisão por  $p$  e aparecem em ordem natural, i.e.

$$\begin{aligned} \{1 \cdot 2, 2 \cdot 2, 3 \cdot 2, \dots, \frac{p-1}{2} \cdot 2\} &= \{t_1, t_2, \dots, t_{\frac{p-1}{2}}\} = \\ \{r_1, r_2, \dots, r_m, s_1, s_2, \dots, s_n\} &= \\ = \{2, 4, 6, \dots, \left[\frac{p}{4}\right] \cdot 2, \left(\left[\frac{p}{4}\right] + 1\right) \cdot 2, \dots, \frac{p-1}{2} \cdot 2\}, \end{aligned}$$



onde  $2, 4, 6, \dots, \lfloor \frac{p}{4} \rfloor \cdot 2$  são os restos  $< \frac{p}{2}$  e  $(\lfloor \frac{p}{4} \rfloor + 1) \cdot 2, \dots, \frac{p-1}{2} \cdot 2$  os  $> \frac{p}{2}$ .

Temos então  $n = \frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor$ . O lema de GAUSS (8.11) diz que

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor}.$$

**Caso 1):**

$p \equiv 1 \pmod{8}$ , digamos,  $p = 8\ell + 1$ . Segue  $n = 4\ell - \lfloor 2\ell + \frac{1}{4} \rfloor = 4\ell - 2\ell = 2\ell$ .

Logo  $\left(\frac{2}{p}\right) = (-1)^{2\ell} = 1$ .

**Caso 2):**

$p \equiv 3 \pmod{8}$ , digamos,  $p = 8\ell + 3$ . Segue  $n = 4\ell + 1 - \lfloor 2\ell + \frac{3}{4} \rfloor = 4\ell + 1 - 2\ell = 2\ell + 1$ .

Logo  $\left(\frac{2}{p}\right) = (-1)^{2\ell+1} = -1$ .

**Caso 3):**

$p \equiv 5 \pmod{8}$ , digamos,  $p = 8\ell + 5$ . Segue  $n = (4\ell + 2) - \lfloor 2\ell + \frac{5}{4} \rfloor = (4\ell + 2) - (2\ell + 1) = 2\ell + 1$ .

Logo  $\left(\frac{2}{p}\right) = (-1)^{2\ell+1} = -1$ .

**Caso 4):**

$p \equiv 7 \pmod{8}$ , digamos,  $p = 8\ell + 7$ . Segue  $n = (4\ell + 3) - \lfloor 2\ell + \frac{7}{4} \rfloor = (4\ell + 3) - (2\ell + 1) = 2\ell + 2$ .

Logo  $\left(\frac{2}{p}\right) = (-1)^{2\ell+2} = 1$ .

■

A proposição 8.12 também podemos formular assim:

### 8.12' Proposição.

Seja  $p > 2$  um primo. Temos

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

**Demonstração:** Primeiro observamos que  $p^2 - 1 = (p-1)(p+1)$  é o produto de dois números pares consecutivos e portanto é divisível por 8. Logo  $\frac{p^2-1}{8} \in \mathbb{N}$ . Além disso temos

$$\begin{aligned} \frac{p^2-1}{8} \text{ é ímpar} &\Leftrightarrow \\ 16 \nmid p^2 - 1 &\Leftrightarrow 8 \nmid p-1 \text{ e } 8 \nmid p+1 \Leftrightarrow p \not\equiv \pm 1 \pmod{8} \Leftrightarrow \\ p \not\equiv 1 \text{ ou } 7 \pmod{8} &\Leftrightarrow p \equiv 3 \text{ ou } 5 \pmod{8} \Leftrightarrow \left(\frac{2}{p}\right) = -1. \end{aligned}$$

■

Eis a tabela dos primos  $p \equiv \pm 1 \pmod{8}$  com  $p \leq 97$  e as duas soluções incongruentes  $< p$  da congruência  $x^2 \equiv 2 \pmod{p}$

$p \equiv \pm 1 \pmod{8}$	sols. $x$ e $p - x$ de $x^2 \equiv 2 \pmod{p}$
7	3, 4
17	6, 11
23	5, 18
31	8, 23
41	17, 24
47	7, 40
71	12, 59
73	32, 41
79	9, 70
89	25, 64
97	14, 83

Sabemos (ver Cons. 7.2): Se  $q = 2n + 1$  é primo, então  $q \mid M_n$  ou  $q \mid M_n + 2$ . Estamos agora em condições de especificar isto melhor na seguinte

### 8.13 Proposição.

Seja  $n \in \mathbb{N}$  tal que  $q = 2n + 1$  é primo. Então temos

- Se  $q \equiv 1$  ou  $7 \pmod{8}$ , então  $q \mid M_n$ .
- Se  $q \equiv 3$  ou  $5 \pmod{8}$ , então  $q \mid M_n + 2$ .

**Demonstração:** Usando-se as proposições 8.5 e 8.12, obtemos:

- $q \equiv 1$  ou  $7 \pmod{8} \Rightarrow \left(\frac{2}{q}\right) = 1 \equiv 2^{\frac{q-1}{2}} = 2^n \pmod{q} \Rightarrow q \mid 2^n - 1 = M_n$ .
- $q \equiv 3$  ou  $5 \pmod{8} \Rightarrow \left(\frac{2}{q}\right) = -1 \equiv 2^{\frac{q-1}{2}} = 2^n \pmod{q} \Rightarrow q \mid 2^n + 1 = M_n + 2$ .

■

Em termos de  $n$  obtemos

### 8.14 Proposição.

Seja  $n \in \mathbb{N}$  tal que  $q = 2n + 1$  é primo. Então temos

a) Se  $n \equiv 0$  ou  $3 \pmod{4}$ , então  $q \mid M_n$ .

b) Se  $n \equiv 1$  ou  $2 \pmod{4}$ , então  $q \mid M_n + 2$ .

**Demonstração:** Por 8.13 temos:

a)  $n \equiv 0$  ou  $3 \pmod{4} \Rightarrow q = 2n + 1 \equiv 1$  ou  $7 \pmod{8} \Rightarrow q \mid M_n$ .

b)  $n \equiv 1$  ou  $2 \pmod{4} \Rightarrow q = 2n + 1 \equiv 3$  ou  $5 \pmod{8} \Rightarrow q \mid M_n + 2$ . ■

Quando  $p$  é primo, todo eventual divisor primo  $q$  de  $M_p$  é da forma  $q = 2pk + 1$  (ver Cons. 7.7). Este  $k$  pode ser muito grande (ver Ex. 5.15 no caso  $p = 67$ ). Reciprocamente, porém, para uma série de alguns primos,  $k = 1$  fornece o menor divisor primo de  $M_p$ .

Uma condição *suficiente* que garante que um número de MERSENNE  $M_p$  com índice primo seja *composto*, é

### 8.15 Conseqüência.

Seja  $p \equiv 3 \pmod{4}$  um primo, tal que também  $q = 2p + 1$  é primo. Então

$q \mid M_p$ , particularmente  $M_p$  não é primo, se  $p > 3$ .

(Para  $p = 3$  temos  $M_3 = 7 = 2 \cdot 3 + 1$ .)

**Demonstração:** Isto é o caso de 8.14 no qual  $n = p \equiv 3 \pmod{4}$  é primo. ■

Eis a tabela dos primos  $3 < p \leq 500$  que são  $\equiv 3 \pmod{4}$  tais que também  $q = 2p + 1$  é primo

$p$	$q = 2p + 1$	<i>Obs.</i>	
11	23	23	$M_{11}$
23	47	47	$M_{23}$
83	167	167	$M_{83}$
131	263	263	$M_{131}$
179	359	359	$M_{179}$
191	383	383	$M_{191}$
239	479	479	$M_{239}$
251	503	503	$M_{251}$
359	719	719	$M_{359}$
419	839	839	$M_{419}$
431	863	863	$M_{431}$
443	887	887	$M_{443}$
491	983	983	$M_{491}$

## A LEI DA RECIPROCIDADE QUADRÁTICA

Vamos conhecer um método que permite calcular  $\left(\frac{a}{p}\right)$  para qualquer  $a \in \mathbb{Z}$  com  $p \nmid a$ . Primeiro fazemos a seguinte

### 8.16 Observação.

Seja  $p > 2$  um primo,  $a \in \mathbb{Z}$  decomposto como

$$a = \pm 2^{k_0} \cdot q_1^{k_1} \cdot q_2^{k_2} \cdot \dots \cdot q_r^{k_r}$$

com primos ímpares distintos  $p \neq q_1, q_2, \dots, q_r$  e expoentes  $k_0 \geq 0$ ,  $k_1, k_2, \dots, k_r > 0$ . Então

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right) \cdot \left(\frac{2}{p}\right)^{k_0} \cdot \left(\frac{q_1}{p}\right)^{k_1} \cdot \left(\frac{q_2}{p}\right)^{k_2} \cdot \dots \cdot \left(\frac{q_r}{p}\right)^{k_r}.$$

Neste último produto, somente a paridade dos expoentes  $k_0, \dots, k_r$  influi e podemos riscar os termos com  $k_i$  par.

**Demonstração:** É só preciso aplicar repetidas vezes a regra  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ .

■

Obviamente, 8.16 reduz o conhecimento de qualquer símbolo de LEGENDRE  $\left(\frac{a}{p}\right)$  ao conhecimento de  $\left(\frac{-1}{p}\right)$ , de  $\left(\frac{2}{p}\right)$  e de  $\left(\frac{q}{p}\right)$  para todo primo ímpar  $q \neq p$ . O cálculo de  $\left(\frac{q}{p}\right)$  conseguiremos pelo

**8.17 Teorema.** (Lei da reciprocidade quadrática de EULER/GAUSS).

*Sejam  $p, q > 2$  primos distintos. Então vale*

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Procuremos entender primeiro a asserção da lei da reciprocidade:

Para dois primos ímpares distintos  $p$  e  $q$ , ambos os símbolos de LEGENDRE  $\left(\frac{q}{p}\right)$  e  $\left(\frac{p}{q}\right)$  estão definidos. A questão que surge é, o que acontece, se trocarmos neles os papéis de  $p$  e  $q$ , ou seja: O que tem a ver a questão se  $q$  é um resto quadrático mod  $p$  com a questão se  $p$  é um resto quadrático mod  $q$ ?

Para um número ímpar  $m$  temos que  $\frac{m-1}{2}$  é par se  $m \equiv 1 \pmod{4}$ , enquanto ímpar se  $m \equiv 3 \pmod{4}$ . Assim, o produto  $\frac{p-1}{2} \cdot \frac{q-1}{2}$  é ímpar (par)  $\Leftrightarrow$  ambos  $p$  e  $q$  são  $\equiv 3 \pmod{4}$  (pelo menos um de  $p$  ou  $q$  é  $\equiv 1 \pmod{4}$ ).

Logo, a lei da reciprocidade diz que podemos simplesmente trocar  $p$  e  $q$  se pelo menos um de  $p$  ou  $q$  é  $\equiv 1 \pmod{4}$ . Porém, se  $p \equiv q \equiv 3 \pmod{4}$ , o símbolo invertido troca o sinal.

**8.18 Exemplo.**

$p = 2579$  é um primo  $\equiv 3 \pmod{4}$ . Queremos descobrir se o primo  $q = 991 \equiv 3 \pmod{4}$  é um resto quadrático mod 2579 ou não. Calculamos

$$\begin{aligned} \left(\frac{991}{2579}\right) &= \left(\frac{2579}{991}\right) \cdot (-1)^{\frac{2579-1}{2} \cdot \frac{991-1}{2}} = \left(\frac{2579}{991}\right) \cdot (-1)^{1289 \cdot 495} = \\ &= -\left(\frac{597}{991}\right) = -\left(\frac{3}{991}\right) \cdot \left(\frac{199}{991}\right) = \\ &= \left(-\left(-\left(\frac{991}{3}\right)\right)\right) \cdot \left(-\left(\frac{991}{199}\right)\right) = \left(\frac{1}{3}\right) \cdot \left(-\left(\frac{195}{199}\right)\right) = \end{aligned}$$

$$\begin{aligned}
&= (+1) \cdot \left(-\left(\frac{3}{199}\right)\right) \cdot \left(\frac{5}{199}\right) \cdot \left(\frac{13}{199}\right) = \left(-\left(-\left(\frac{199}{3}\right)\right)\right) \cdot \left(\frac{199}{5}\right) \cdot \left(\frac{199}{13}\right) = \\
&= \left(\frac{1}{3}\right) \cdot \left(\frac{4}{5}\right) \cdot \left(\frac{4}{13}\right) = (+1)(+1)(+1) = +1.
\end{aligned}$$

Assim, a resposta é *sim*. Por tentativa obtem-se de fato

$$(\pm 138)^2 \equiv 991 \pmod{2579}.$$

Preparamos a demonstração da lei da reciprocidade quadrática por

### 8.19 Proposição.

Seja  $p > 2$  um primo,  $a \in \mathbb{Z}$  um número ímpar tal que  $p \nmid a$ . Então

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]}.$$

**Demonstração:** Consideremos  $\{a, 2a, 3a, \dots, \frac{p-1}{2}a\}$ . Para todo  $k = 1, 2, \dots, \frac{p-1}{2}$  existem  $q_k, t_k \in \mathbb{Z}$  com

$$ka = q_k p + t_k \quad \text{e} \quad 1 \leq t_k \leq p-1.$$

Os  $t_1, t_2, \dots, t_{\frac{p-1}{2}}$  são distintos. Seja

$$\{t_1, t_2, \dots, t_{\frac{p-1}{2}}\} = \{r_1, \dots, r_m, s_1, \dots, s_n\},$$

onde  $1 \leq r_i < \frac{p}{2} < s_j \leq p-1$  para  $i = 1, \dots, m; j = 1, \dots, n$ . Pelo Lema de GAUSS (8.11) temos

$$\left(\frac{a}{p}\right) = (-1)^n.$$

A demonstração estará completa, se conseguirmos provar que os números

$\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]$  e  $n$  possuem a mesma paridade, isto é, são congruentes mod 2.

Vamos provar isto:

Temos  $\frac{ka}{p} = q_k + \frac{t_k}{p}$  com  $0 < \frac{t_k}{p} < 1$ . Isto significa  $\left[\frac{ka}{p}\right] = q_k$ . Logo

$$ka = \left[\frac{ka}{p}\right] p + t_k \quad (k = 1, 2, \dots, \frac{p-1}{2}).$$

Somando-se estas equações, obtemos

$$\sum_{k=1}^{\frac{p-1}{2}} ka = \sum_{k=1}^{\frac{p-1}{2}} \left[ \frac{ka}{p} \right] p + \sum_{k=1}^{\frac{p-1}{2}} t_k ,$$

ou seja,

$$a \sum_{k=1}^{\frac{p-1}{2}} k = p \sum_{k=1}^{\frac{p-1}{2}} \left[ \frac{ka}{p} \right] + \sum_{j=1}^n s_j + \sum_{i=1}^m r_i ,$$

ou seja,

$$\begin{aligned} a \sum_{k=1}^{\frac{p-1}{2}} k &= p \sum_{k=1}^{\frac{p-1}{2}} \left[ \frac{ka}{p} \right] + \underbrace{\sum_{i=1}^m r_i + \sum_{j=1}^n (p - s_j)}_{= \sum_{k=1}^{\frac{p-1}{2}} k} + 2 \sum_{j=1}^n s_j - np \\ &= \sum_{k=1}^{\frac{p-1}{2}} k + 2 \sum_{j=1}^n s_j - np \end{aligned}$$

(observe, lembrando a demonstração do Lema de GAUSS (pg. 92) que

$$\{r_1, \dots, r_m, p - s_1, \dots, p - s_n\} = \{1, 2, \dots, \frac{p-1}{2}\} !).$$

Assim obtemos

$$(a - 1) \sum_{k=1}^{\frac{p-1}{2}} k = p \left( \sum_{k=1}^{\frac{p-1}{2}} \left[ \frac{ka}{p} \right] - n \right) + 2 \sum_{j=1}^n s_j .$$

Lendo-se esta última equação mod 2 e observando-se que  $a - 1$  é par e  $p$  é ímpar, obtemos

$$0 \equiv 1 \cdot \left( \sum_{k=1}^{\frac{p-1}{2}} \left[ \frac{ka}{p} \right] - n \right) + 0 \pmod{2} .$$

Concluimos

$$\sum_{k=1}^{\frac{p-1}{2}} \left[ \frac{ka}{p} \right] \equiv n \pmod{2} ,$$

o que queríamos provar. ■

**Demonstração** da lei da reciprocidade:

Consideremos no  $x, y$ -plano o retângulo de vértices

$$(0, 0), \left(\frac{p}{2}, 0\right), \left(0, \frac{q}{2}\right), \left(\frac{p}{2}, \frac{q}{2}\right) .$$

A diagonal deste retângulo pertence à reta  $y = \frac{q}{p}x$ . Quantos pontos  $(x, y)$  de coordenadas inteiras existem dentro deste retângulo?

Vamos calcular esta quantidade de duas maneiras:

A primeira resposta é:

$$\text{São } \frac{p-1}{2} \cdot \frac{q-1}{2} \text{ pontos } (*) .$$

Não existem pontos inteiros na diagonal, pois de  $py = qx$  segue  $p|x$  e portanto  $x \geq p$ .

A quantidade dos pontos no triângulo inferior  $(0, 0)$ ,  $(\frac{p}{2}, 0)$ ,  $(\frac{p}{2}, \frac{q}{2})$  podemos calcular assim: Para a abscissa  $k$  ( $1 \leq k < \frac{p}{2}$ ) são estes os pontos

$$(k, 1), (k, 2), \dots, (k, \left[ \frac{kq}{p} \right]).$$

Então são

$$\sum_{k=1}^{\frac{p-1}{2}} \left[ \frac{kq}{p} \right]$$

pontos no triângulo inferior.

A quantidade dos pontos no triângulo superior  $(0, 0)$ ,  $(\frac{p}{2}, \frac{q}{2})$ ,  $(0, \frac{q}{2})$  calcula-se assim: Para a ordenada  $\ell$  ( $1 \leq \ell < \frac{q}{2}$ ) são estes os pontos

$$(1, \ell), (2, \ell), \dots, \left( \left[ \frac{\ell p}{q} \right], \ell \right).$$

Então são

$$\sum_{\ell=1}^{\frac{q-1}{2}} \left[ \frac{\ell p}{q} \right]$$

pontos no triângulo superior.

Logo temos também um total de

$$\sum_{k=1}^{\frac{p-1}{2}} \left[ \frac{kq}{p} \right] + \sum_{\ell=1}^{\frac{q-1}{2}} \left[ \frac{\ell p}{q} \right] \quad (**)$$

pontos no retângulo.

Igualando-se (\*) e (\*\*) obtemos

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{k=1}^{\frac{p-1}{2}} \left[ \frac{kq}{p} \right] + \sum_{\ell=1}^{\frac{q-1}{2}} \left[ \frac{\ell p}{q} \right] .$$



Colocando-se isto no expoente de  $(-1)$  e observando-se a Proposição 8.19, obtemos como afirmado

$$\begin{aligned} \left(\frac{q}{p}\right) &= (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kq}{p}\right]} = \\ &= (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \cdot (-1)^{\sum_{\ell=1}^{\frac{q-1}{2}} \left[\frac{\ell p}{q}\right]} = \\ &= (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \cdot \left(\frac{p}{q}\right). \end{aligned}$$

■

## MAIS ALGUNS SÍMBOLOS DE LEGENDRE ESPECIAIS

Já sabemos decidir quando  $-1$  e  $2$  são quadrados perfeitos:

$$\left(\frac{-1}{p}\right) = +1 \Leftrightarrow p \equiv 1 \pmod{4} \quad \left(\frac{2}{p}\right) = +1 \Leftrightarrow p \equiv 1, 7 \pmod{8}$$

Queremos acrescentar mais alguns resultados parecidos:

### 8.20 Exemplos.

- a)  $\left(\frac{-2}{p}\right) = +1 \Leftrightarrow p \equiv 1 \text{ ou } 3 \pmod{8}$
- b)  $\left(\frac{3}{p}\right) = +1 \Leftrightarrow p \equiv \pm 1 \pmod{12}$
- c)  $\left(\frac{5}{p}\right) = +1 \Leftrightarrow p \equiv \pm 1 \pmod{10}$
- d)  $\left(\frac{6}{p}\right) = +1 \Leftrightarrow p \equiv \pm 1 \text{ ou } \pm 5 \pmod{24}$
- e)  $\left(\frac{7}{p}\right) = +1 \Leftrightarrow p \equiv \pm 1, \pm 3, \pm 9 \pmod{28}$
- f)  $\left(\frac{10}{p}\right) = +1 \Leftrightarrow p \equiv \pm 1, \pm 3, \pm 9, \pm 13 \pmod{40}$

**Demonstração:** a)  $\left(\frac{-2}{p}\right) = +1 \Leftrightarrow \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = +1 \Leftrightarrow$

$$\begin{aligned} &\Leftrightarrow \left(\frac{-1}{p}\right) = 1 = \left(\frac{2}{p}\right) \text{ ou } \left(\frac{-1}{p}\right) = -1 = \left(\frac{2}{p}\right) \Leftrightarrow \\ &\Leftrightarrow \begin{cases} p \equiv 1 \pmod{4} \\ \text{e} \\ p \equiv \pm 1 \pmod{8} \end{cases} \text{ ou } \begin{cases} p \equiv 3 \pmod{4} \\ \text{e} \\ p \equiv \pm 3 \pmod{8} \end{cases} \Leftrightarrow \\ &\Leftrightarrow p \equiv 1 \text{ ou } 3 \pmod{8}. \end{aligned}$$

b) Temos

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) \text{ se } p \equiv 1 \pmod{4} \\ -\left(\frac{p}{3}\right) \text{ se } p \equiv 3 \pmod{4} \end{cases} . \text{ Assim,}$$

$$\begin{aligned} \left(\frac{3}{p}\right) = 1 &\Leftrightarrow \begin{cases} p \equiv 1 \pmod{4} \\ \text{e} \\ \left(\frac{p}{3}\right) = 1 \end{cases} \text{ ou } \begin{cases} p \equiv 3 \pmod{4} \\ \text{e} \\ \left(\frac{p}{3}\right) = -1 \end{cases} \Leftrightarrow \\ &\Leftrightarrow \begin{cases} p \equiv 1 \pmod{4} \\ \text{e} \\ p \equiv 1 \pmod{3} \end{cases} \text{ ou } \begin{cases} p \equiv 3 \pmod{4} \\ \text{e} \\ p \equiv 2 \pmod{3} \end{cases} \Leftrightarrow \\ &\Leftrightarrow p \equiv 1 \pmod{12} \text{ ou } p \equiv 11 \pmod{12}. \end{aligned}$$

c) Temos

$$\begin{aligned} \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1 &\Leftrightarrow p \equiv \pm 1 \pmod{5} \Leftrightarrow \\ &\Leftrightarrow p \equiv \pm 1 \pmod{10} \text{ pois } p \text{ é ímpar.} \end{aligned}$$

d) Temos

$$\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1 \Leftrightarrow \begin{cases} \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1 \\ \text{ou} \\ \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = -1 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} p \equiv \pm 1 \pmod{8} \text{ e } p \equiv \pm 1 \pmod{12} \\ \text{ou} \\ p \equiv \pm 3 \pmod{8} \text{ e } p \equiv \pm 5 \pmod{12} \end{cases} \Leftrightarrow$$

$$\Leftrightarrow p \equiv \pm 1 \pmod{24} \text{ ou } p \equiv \pm 5 \pmod{24}.$$

As demonstrações de e) e f) são feitas de forma análoga e são deixadas para o leitor. ■

Em seguida vem tabelas dos primos  $p \leq 97$  que satisfazem alguma das condições a) - f) de 8.20 e as duas soluções incongruentes  $< p$  de  $x^2 \equiv a \pmod{p}$ :

$p \equiv 1 \text{ ou } 3 \pmod{8}$	sols. $x$ e $p - x$ de $x^2 \equiv -2 \pmod{p}$
3	1, 2
11	3, 8
17	7, 10
19	6, 13
41	11, 30
43	16, 27
59	23, 36
67	20, 47
73	12, 61
83	9, 74
89	40, 49
97	17, 80

$p \equiv \pm 1 \pmod{12}$	sols. $x$ e $p - x$ de $x^2 \equiv 3 \pmod{p}$
11	5, 6
13	4, 9
23	7, 16
37	15, 22
47	12, 35
59	11, 48
61	8, 53
71	28, 43
73	21, 52
83	13, 70
97	10, 87

$p \equiv \pm 1 \pmod{10}$	sols. $x$ e $p - x$ de $x^2 \equiv 5 \pmod{p}$
11	4, 7
19	9, 10
29	11, 18
31	6, 25
41	13, 28
59	8, 51
61	26, 35
71	17, 54
79	20, 59
89	19, 70

$p \equiv \pm 1 \text{ ou } \pm 5 \pmod{24}$	sols. $x$ e $p - x$ de $x^2 \equiv 6 \pmod{p}$
5	1, 4
19	5, 14
23	11, 12
29	8, 21
43	7, 36
47	10, 37
53	18, 35
67	26, 41
71	19, 52
73	15, 58
97	43, 54

$p \equiv \pm 1, \pm 3, \pm 9 \pmod{28}$	sols. $x$ e $p - x$ de $x^2 \equiv 7 \pmod{p}$
3	1, 2
19	8, 11
29	6, 23
31	10, 21
37	9, 28
47	17, 30
53	22, 31
59	19, 40
83	16, 67

$p \equiv \pm 1, \pm 3, \pm 9, \pm 13 \pmod{40}$	sols. $x$ e $p - x$ de $x^2 \equiv 10 \pmod{p}$
3	1, 2
13	6, 7
31	14, 17
37	11, 26
41	16, 41
43	15, 28
53	13, 40
67	12, 55
71	9, 62
79	22, 57
83	33, 50
89	30, 59

## § 9 Representação de inteiros como soma de quadrados

### SOMA DE DOIS QUADRADOS

#### 9.1 Definição.

Colocamos

$$Q = \{ n \in \mathbb{N} \mid \exists a, b \in \mathbb{N}_0 \text{ com } n = a^2 + b^2 \} ,$$

i.e. queremos considerar o conjunto dos números naturais que são soma de dois quadrados não-negativos.

#### 9.2 Exemplos.

$$1, 2, 4, 5, 8, 9, 10, 13 \in Q \text{ porém } 3, 6, 7, 11, 12 \notin Q.$$

Claramente,  $Q \supseteq \{1, 4, 9, \dots\}$ , i. e.  $Q$  abrange os quadrados perfeitos (pois admitimos  $b \geq 0$ ).

#### 9.3 Proposição.

$Q$  é multiplicativamente fechado, i.e.

$$n, m \in Q \implies nm \in Q .$$

**Demonstração:** Sejam  $n = a^2 + b^2, m = c^2 + d^2$  com  $a, b, c, d \in \mathbb{N}_0$ . Segue

$$nm = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + |ad - bc|^2 .$$

■

Queremos chegar a uma caracterização dos números em  $Q$ . Eis primeiro uma condição necessária:

#### 9.4 Observação.

Se  $n = a^2 + b^2 \equiv 1 \pmod{2}$  com  $a, b \in \mathbb{N}_0$ , então

$$n \equiv 1 \pmod{4} .$$

**Demonstração:**  $a$  e  $b$  têm paridades distintas. Seja, por exemplo,  $a = 2k$ ,  $b = 2\ell - 1$ . Segue  $n = a^2 + b^2 = (2k)^2 + (2\ell - 1)^2 = 4(k^2 + \ell^2 - \ell) + 1 \equiv 1 \pmod{4}$ . ■

A condição  $n \equiv 1 \pmod{4}$  não é suficiente para um número ímpar ser soma de dois quadrados: Temos, por exemplo  $21 \equiv 1 \pmod{4}$ , porém  $21 \notin Q$ . O mesmo ocorre com 33 ou 57.

Queremos provar que os números *primos*  $\equiv 1 \pmod{4}$  de fato são soma de dois quadrados. Mais exatamente temos

### 9.5 Teorema.

Seja  $p \in \mathbb{P}$  com  $p = 2$  ou  $p \equiv 1 \pmod{4}$ . Então

- a) Existem  $a, b \in \mathbb{N}$  tais que  $p = a^2 + b^2$ .
- b) Se  $p = a^2 + b^2 = c^2 + d^2$  com  $a, b, c, d \in \mathbb{N}$  e  $a \leq b$  e  $c \leq d$ , então  $a = c$  e  $b = d$ .

A demonstração deste teorema necessita da

### 9.6 Proposição. (O Lema de THUE)

Seja  $p$  um número primo,  $a \in \mathbb{Z}$ ,  $p \nmid a$ . Então a congruência  $ax \equiv y \pmod{p}$  admite uma solução  $(x_0, y_0)$  tal que

$$\begin{cases} 1 \leq |x_0| < \sqrt{p} \\ 1 \leq |y_0| < \sqrt{p} \end{cases}$$

**Demonstração:** Seja  $k = \lceil \sqrt{p} \rceil + 1$  e consideremos o conjunto  $S = \{ax - y \mid 0 \leq x \leq k-1, 0 \leq y \leq k-1\}$ .  $S$  contém  $k^2$  números (não necessariamente distintos). Temos  $k^2 > \sqrt{p}\sqrt{p} = p$ . Concluimos que  $S$  contém números que são congruentes módulo  $p$ .

Sejam então  $0 \leq x_1, y_1, x_2, y_2 \leq k-1 < \sqrt{p}$  com

$$ax_1 - y_1 \equiv ax_2 - y_2 \pmod{p}$$

e  $x_1 \neq x_2$  ou  $y_1 \neq y_2$ . Logo,  $a(x_1 - x_2) \equiv y_1 - y_2 \pmod{p}$ .

De  $x_1 - x_2 = 0$  segue  $y_1 - y_2 = 0$ . Como  $p \nmid a$ , de  $y_1 - y_2 = 0$  segue também

$x_1 - x_2 = 0$ . Logo temos  $x_1 \neq x_2$  e  $y_1 \neq y_2$ . Coloquemos

$$\begin{cases} x_0 = x_1 - x_2 \\ y_0 = y_1 - y_2 \end{cases} \text{ e obtemos } ax_0 \equiv y_0 \pmod{p} \text{ com } \begin{cases} 1 \leq |x_0| < \sqrt{p} \\ 1 \leq |y_0| < \sqrt{p} \end{cases} .$$

■

**Demonstração** de 9.5: a) Se  $p = 2$ , então  $p = 1^2 + 1^2$ , que é a decomposição única de  $p$  como soma de dois quadrados.

Podemos supor, então  $p \equiv 1 \pmod{4}$ . Temos  $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = +1$ . Isto significa que a congruência  $x^2 \equiv -1 \pmod{p}$  possui uma solução. Seja  $a \in \mathbb{Z}$  tal que  $a^2 \equiv -1 \pmod{p}$ . Certamente  $p \nmid a$ . Pelo Lema de Thue, existem  $x_0, y_0 \in \mathbb{Z}$  tais que  $ax_0 \equiv y_0 \pmod{p}$  e  $1 \leq |x_0|, |y_0| < \sqrt{p}$ . Segue  $-x_0^2 = (-1)x_0^2 \equiv a^2x_0^2 = (ax_0)^2 \equiv y_0^2 \pmod{p}$ . Logo  $x_0^2 + y_0^2 \equiv 0 \pmod{p}$ , ou seja,  $x_0^2 + y_0^2 = kp$  com  $k \in \mathbb{Z}$ . De  $1 \leq |x_0|, |y_0| < \sqrt{p}$  concluímos  $2 \leq x_0^2 + y_0^2 < 2p$ , ou seja,  $k = 1$  e  $x_0^2 + y_0^2 = p$ .

b) A unicidade: Seja  $p = a^2 + b^2 = c^2 + d^2$  com  $a \leq b$  e  $c \leq d$ . Podemos supor  $p \neq 2$ . Assim  $a < b$  e  $c < d$ .

$$\text{De } \begin{cases} p = a^2 + b^2 \\ p = c^2 + d^2 \end{cases} \text{ segue } \begin{cases} pd^2 = a^2d^2 + b^2d^2 \\ pb^2 = b^2c^2 + b^2d^2 \end{cases} \text{ e daí } p(d^2 - b^2) = a^2d^2 - b^2c^2.$$

$$\text{Logo } (ad - bc)(ad + bc) \equiv 0 \pmod{p}. \text{ Daí segue } \begin{cases} ad \equiv bc \\ \text{ou} \\ ad \equiv -bc \end{cases} \pmod{p}.$$

$$\text{De } a, b, c, d < \sqrt{p} \text{ concluímos } \begin{cases} ad = bc \\ \text{ou} \\ ad + bc = p \end{cases}.$$

$$\text{Temos } p^2 = (a^2 + b^2)(c^2 + d^2) = (ad + bc)^2 + (ac - bd)^2.$$

Se tivermos  $ad + bc = p$ , obtemos  $p^2 = p^2 + (ac - bd)^2$  e daí  $ac = bd$ .

$$\text{Logo temos } \begin{cases} ad = bc \\ \text{ou} \\ ac = bd \end{cases} . \text{ A segunda opção não ocorre, pois de } \begin{cases} a < b \\ c < d \end{cases} \text{ segue}$$

$ac < bd$ . Temos então  $ad = bc$ . De  $a|bc$  e  $\text{mdc}(a, b) = 1$  concluímos  $a|c$ , digamos  $c = ka$ . Então  $ad = bc = kab$ , de onde concluímos  $d = kb$ . Agora,  $p = c^2 + d^2 = (ka)^2 + (kb)^2 = k^2(a^2 + b^2) = k^2p$  de onde segue  $k = 1$ . Daí  $a = c$  e  $b = d$ .

■

Advertimos que um número *composto* o qual é soma de dois quadrados pode ser isto de mais de uma maneira: Por exemplo  $65 = 1^2 + 8^2 = 4^2 + 7^2$ .

Podemos caracterizar agora os números naturais que são soma de dois quadrados, olhando-se na sua decomposição primária.

### 9.7 Teorema.

Seja  $n \in \mathbb{N}$  escrito na forma  $n = M^2 \cdot q_1 \cdot q_2 \cdot \dots \cdot q_s$  com  $M \in \mathbb{N}$ ,  $q_1, q_2, \dots, q_s$  primos distintos,  $s \geq 0$  (porquê é possível escrever todo número  $n \in \mathbb{N}$  desta forma? Reflitam a esse respeito!). Então são equivalentes:

- a)  $n$  é soma de dois quadrados.
- b) Cada  $q_1, q_2, \dots, q_s$  é 2 ou  $\equiv 1 \pmod{4}$ .

**Demonstração:** "b)  $\Rightarrow$  a)": Se cada  $q_i$  é 2 ou  $\equiv 1 \pmod{4}$ , temos  $q_i = a_i^2 + b_i^2$  com certos  $a_i, b_i \in \mathbb{N}_0$  ( $1 \leq i \leq s$ ) devido a 9.5. Aplicando-se 9.3 repetidas vezes, concluímos  $q_1 \cdot \dots \cdot q_s = A^2 + B^2$  com  $A, B \in \mathbb{N}_0$ . Daí

$$n = M^2(A^2 + B^2) = (MA)^2 + (MB)^2.$$

"a)  $\Rightarrow$  b)": Seja  $n = M^2 q_1 \cdot \dots \cdot q_s = a^2 + b^2$ . Podemos supor  $s \geq 1$  e seja  $q_i$  ímpar. Seja  $d = \text{mdc}(a, b)$  e  $a = dr$ ,  $b = dt$  com  $r, t \in \mathbb{N}_0$ , Segue

$$d^2(r^2 + t^2) = a^2 + b^2 = M^2 q_1 \cdot \dots \cdot q_s \quad \text{e} \quad \text{mdc}(r, t) = 1.$$

Agora,  $q_i$  divide o lado direito ímpar vezes. Pelo teorema fundamental da aritmética, o mesmo deve acontecer à esquerda. Logo  $r^2 + t^2 \equiv 0 \pmod{q_i}$ . Como  $\text{mdc}(r, t) = 1$ , temos  $q_i \nmid r$  ou  $q_i \nmid t$ , digamos  $q_i \nmid r$ . Existe então  $r' \in \mathbb{Z}$  tal que  $rr' \equiv 1 \pmod{q_i}$ . De  $r^2 + t^2 \equiv 0 \pmod{q_i}$  segue por multiplicação com  $r'^2$ :  $(rr')^2 + (tr')^2 \equiv 0 \pmod{q_i}$  e daí

$$(tr')^2 \equiv -1 \pmod{q_i}.$$

Isto diz que a congruência  $x^2 \equiv -1 \pmod{q_i}$  é solúvel. Isto significa

$$(-1)^{\frac{q_i-1}{2}} = \left( \frac{-1}{q_i} \right) = +1,$$

ou seja,  $q_i \equiv 1 \pmod{4}$  (comparar 8.3/8.9).

■



## 9.8 Exemplos.

- a)  $3373 = 3^2 + 58^2$ ,  $3229 = 27^2 + 50^2$ , são as decomposições únicas de dois primos  $\equiv 1 \pmod{4}$ .
- b)  $4633 = 113 \cdot 41$  e vale que 113 e 41 são  $\equiv 1 \pmod{4}$ . Temos as duas decomposições  $4633 = 3^2 + 68^2 = 12^2 + 67^2$ .
- c)  $n = M^2 \cdot 17 \cdot 2 \cdot 29 \cdot 7 \cdot 11$  não pode ser soma de dois quadrados, pois 7 (e também 11) é  $\equiv 3 \pmod{4}$
- d) Os números  $\leq 100$  que **não** são soma de dois quadrados, apesar de serem  $\equiv 1 \pmod{4}$ , são:

$$21, 33, 57, 69, 93, 77 .$$

Equivalentemente a 9.7 podemos formular:

### 9.7' Teorema.

Seja  $n \in \mathbb{N}$  escrito na forma

$$n = 2^c \cdot p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_r^{a_r} \cdot q_1^{b_1} \cdot q_2^{b_2} \cdot \dots \cdot q_s^{b_s}$$

com  $c \geq 0, a_1, \dots, a_r, b_1, \dots, b_s \in \mathbb{N}$ ,  $p_1, \dots, p_r$  primos distintos  $\equiv 1 \pmod{4}$ ,  $q_1, \dots, q_s$  primos distintos  $\equiv 3 \pmod{4}$ ,  $r, s \geq 0$ .

Então  $n$  é soma de dois quadrados, se e somente se, todos os expoentes  $b_1, b_2, \dots, b_s$  são pares.

## SOMA DE TRÊS QUADRADOS

6 não é soma de dois, mas de três quadrados  $6 = 1^2 + 1^2 + 2^2$ .

7 não é soma de três, mas de quatro quadrados  $7 = 1^2 + 1^2 + 1^2 + 2^2$ .

Acrescentando-se, se necessário, um somando  $0^2$ , todo número  $n \in \mathbb{Q}$  podemos escrever como soma de três quadrados.

Surge a pergunta como podemos caracterizar os  $n \in \mathbb{N}$  que são soma de (no máximo) três quadrados?

Necessário é

### 9.9 Proposição.

Seja  $n \in \mathbb{N}$  da forma  $n = 4^k(8m + 7)$  com  $k, m \geq 0$ . Então  $n$  jamais é soma de três ou menos quadrados.

**Demonstração:** Seja  $k = 0$  e suponhamos  $n = 8m + 7 = a^2 + b^2 + c^2$  com  $a, b, c \in \mathbb{N}_0$ . Temos  $n \equiv 7 \pmod{8}$ , particularmente  $n \equiv 1 \pmod{2}$ . Mas, de  $a^2, b^2, c^2 \equiv 0, 1$  ou  $4 \pmod{8}$  segue que  $a^2 + b^2 + c^2 \equiv 7 \pmod{8}$  é impossível.

Seja  $k \geq 1$  e suponhamos  $n = 4^k(8m + 7) = a^2 + b^2 + c^2$  para certos  $a, b, c \in \mathbb{N}_0$ . Como  $4 \mid n$  concluímos que todos os  $a, b, c$  são pares (a soma de um quadrado par com dois ímpares seria  $\equiv 2 \pmod{4}$ ). Coloquemos  $a = 2a_1, b = 2b_1, c = 2c_1$  e obtemos  $4^k(8m + 7) = (a^2 + b^2 + c^2) = 4(a_1^2 + b_1^2 + c_1^2)$ , de onde segue que  $n' = 4^{k-1}(8m + 7) = a_1^2 + b_1^2 + c_1^2$  é soma de três quadrados. Mas isto é impossível pela hipótese de indução. ■

### 9.10 Exemplo.

*Os primeiros números que não são soma de três quadrados são*

$$7, 15, 23, 31, 39, 47, 55, 63, 71, 79, 87, 95, \dots ; 28, 60, 92, \dots .$$

Mencionamos - sem demonstração - que também vale o recíproco de 9.9

### 9.11 Teorema.

*Um  $n \in \mathbb{N}$  pode ser escrito como soma de três quadrados, se e somente se,  $n$  não é da forma  $n = 4^k(8m + 7)$  com  $k, m \geq 0$ .*

### SOMA DE QUATRO QUADRADOS

Encerramos este parágrafo com a demonstração de um teorema clássico em teoria dos números

### 9.12 Teorema. (LAGRANGE)

*Para todo  $n \in \mathbb{N}$  existem  $a, b, c, d \in \mathbb{N}_0$  tais que*

$$n = a^2 + b^2 + c^2 + d^2 .$$

Em palavras: Todo número natural pode ser escrito como soma de no máximo 4 quadrados.

Cálculo direto fornece:

### 9.13 Proposição.

Sejam  $a, b, c, d, x, y, z, w \in \mathbb{N}_0$ . Então

$$(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + w^2) = (xa+yb+zc+wd)^2 + (xb-ya+zd-wc)^2 + (xc-yd-za+wb)^2 + (xd+yc-zb-wa)^2$$

(i.e. o subconjunto dos números em  $\mathbb{N}$  que são soma de 4 quadrados é multiplicativamente fechado).

### 9.14 Observação.

Seja  $p$  um primo ímpar. Então

- A congruência  $x^2 + y^2 + 1 \equiv 0 \pmod{p}$  admite uma solução  $(x_0, y_0)$  com  $0 \leq x_0, y_0 \leq \frac{p-1}{2}$ .
- Existe  $k \in \mathbb{N}$  com  $k < p$  tal que  $kp$  é soma de 4 quadrados.

**Demonstração:** a) Consideremos os conjuntos

$$S_1 = \left\{ 1 + 0^2, 1 + 1^2, \dots, 1 + \left(\frac{p-1}{2}\right)^2 \right\} \text{ e } S_2 = \left\{ -0^2, -1^2, \dots, -\left(\frac{p-1}{2}\right)^2 \right\}.$$

Os números em  $S_1$  são incongruentes módulo  $p$ , o mesmo acontecendo com os de  $S_2$  :

De  $1 + r^2 \equiv 1 + \ell^2 \pmod{p}$  (ou de  $-r^2 \equiv -\ell^2 \pmod{p}$ ) segue  $r \equiv \pm \ell \pmod{p}$  e daí  $p | r \pm \ell$ . Como  $0 \leq r, \ell \leq \frac{p-1}{2} < \frac{p}{2}$ , concluímos  $0 \leq |r \pm \ell| < p$  e daí  $r = \ell$ .

Como  $|S_1| + |S_2| = p + 1$ , concluímos que existe um número em  $S_1$  congruente mod  $p$  com algum número em  $S_2$ . Assim,  $1 + x_0^2 \equiv -y_0^2 \pmod{p}$  para certos  $x_0, y_0$  com  $0 \leq x_0, y_0 \leq \frac{p-1}{2}$ . Daí  $x_0^2 + y_0^2 + 1 \equiv 0 \pmod{p}$ .

b) Por a) temos  $x_0^2 + y_0^2 + 1 \equiv 0 \pmod{p}$  para certos  $0 \leq x_0, y_0 \leq \frac{p-1}{2}$ , ou seja,  $x_0^2 + y_0^2 + 1^2 + 0^2 = kp$  com  $k \in \mathbb{N}$ . Mas  $1 \leq kp = x_0^2 + y_0^2 + 1 \leq \left(\frac{p-1}{2}\right)^2 + \left(\frac{p-1}{2}\right)^2 + 1 < \frac{p^2}{4} + \frac{p^2}{4} + 1 < p^2$ . Temos então  $k < p$ .

■

**Demonstração** do teorema de LAGRANGE:

Pela observação 9.13 podemos supor que o número a ser decomposto como soma

de 4 quadrados é um primo  $p$  ímpar. Por 9.14 b) existe um  $k$  com  $1 \leq k < p$  tal que  $kp$  é soma de 4 quadrados. Seja  $k_0$  o *menor* tal número e seja, digamos

$$k_0 p = x^2 + y^2 + z^2 + w^2 .$$

O objetivo da demonstração é mostrar que  $k_0 = 1$  da seguinte maneira: Vamos supor  $1 < k_0 < p$  e construiremos nesta situação um  $n$  com  $1 \leq n < k_0$  tal que  $np$  ainda é soma de 4 quadrados. Isto será uma contradição contra a minimalidade de  $k_0$  que mostrará  $k_0 = 1$ .

Vamos provar primeiro que  $k_0$  é ímpar  $\geq 3$ . De fato, se  $k_0$  é par, podemos supor que  $\{x, y\}$  e  $\{z, w\}$  tenham a mesma paridade. Segue que  $x \pm y$  e  $z \pm w$  são pares e daí  $\frac{x \pm y}{2}$  e  $\frac{z \pm w}{2}$  são inteiros. Segue que

$$\left(\frac{x-y}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 = 2 \cdot \frac{x^2+y^2+z^2+w^2}{4} = \frac{k_0}{2} \cdot p$$

com  $1 \leq \frac{k_0}{2} < k_0$ , em desacordo com a minimalidade de  $k_0$ .

Dividamos agora os  $x, y, z, w$  por  $k_0$  com restos  $a, b, c, d$  no intervalo  $\left(-\frac{k_0}{2}, \frac{k_0}{2}\right)$ ,

i. e. escrevemos

$$\begin{cases} x = q_1 k_0 + a \\ y = q_2 k_0 + b \\ z = q_3 k_0 + c \\ w = q_4 k_0 + d \end{cases} \quad \text{com } a, b, c, d \in \left[-\frac{k_0-1}{2}, \frac{k_0-1}{2}\right] .$$

Desta forma,  $|a|, |b|, |c|, |d| < \frac{k_0}{2}$  e  $a \equiv x, b \equiv y, c \equiv z$  e  $d \equiv w \pmod{k_0}$ . Logo,

$$a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + w^2 = k_0 p \equiv 0 \pmod{k_0} .$$

Logo,  $a^2 + b^2 + c^2 + d^2 = nk_0$  com  $n \geq 0$ .

Se  $n = 0$ , então  $a = b = c = d = 0$  e daí  $x \equiv y \equiv z \equiv w \equiv 0 \pmod{k_0}$ . Assim,  $k_0 \mid x, y, z, w$  e  $k_0^2 \mid x^2 + y^2 + z^2 + w^2 = k_0 p$ . Mas isto dá a contradição  $k_0 \mid p$ , pois  $1 < k_0 < p$ . Logo,  $n \geq 1$ .

Mais ainda, de  $1 \leq nk_0 = a^2 + b^2 + c^2 + d^2 < 4 \cdot \left(\frac{k_0}{2}\right)^2 = k_0^2$  segue  $n < k_0$ , ou seja,

$$1 \leq n < k_0 .$$

$np = ?$  Calculamos, usando-se 9.13:

$$k_0^2 np = (k_0 p)(nk_0) = (x^2 + y^2 + z^2 + w^2)(a^2 + b^2 + c^2 + d^2) = r^2 + s^2 + t^2 + u^2$$

$$\text{com } \begin{cases} r = xa + yb + zc + wd \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{k_0} \\ s = xb - ya + zd - wc \equiv ab - ba + cd - dc \equiv 0 \pmod{k_0} \\ t = xc - yd - za + wb \equiv ac - bd - ca + db \equiv 0 \pmod{k_0} \\ u = xd + yc - zb - wa \equiv ad + bc - cb - da \equiv 0 \pmod{k_0} \end{cases}$$

Portanto,  $k_0 \mid r, s, t, u$  e

$$k_0^2 \mid r^2 + s^2 + t^2 + u^2 .$$

Seja  $\ell \in \mathbb{N}$  com  $k_0^2 \ell = r^2 + s^2 + t^2 + u^2$ . De  $k_0^2 np = k_0^2 \ell$  segue

$$np = \ell = \left(\frac{r}{k_0}\right)^2 + \left(\frac{s}{k_0}\right)^2 + \left(\frac{t}{k_0}\right)^2 + \left(\frac{u}{k_0}\right)^2 .$$

com  $\frac{r}{k_0}, \frac{s}{k_0}, \frac{t}{k_0}, \frac{u}{k_0} \in \mathbb{N}_0$ , mostrando que  $np$  ainda é soma de 4 quadrados. Isto termina a demonstração. ■

## § 10 A função $\varphi$ de EULER

RESTOS RELATIVAMENTE PRIMOS E A FUNÇÃO  $\varphi$

### 10.1 Definição.

Seja  $n \in \mathbb{N}$ . O número  $\varphi(n)$  é definido como sendo

$$\varphi(n) = \left| \left\{ k \in \mathbb{N} \mid 1 \leq k \leq n, \text{mdc}(k, n) = 1 \right\} \right| .$$

A função  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  com  $n \rightarrow \varphi(n)$  chama-se a *função de EULER*.

$\varphi(n)$  é então a *quantidade* dos números entre 1 e  $n$  que são relativamente primos com  $n$ .

### 10.2 Exemplos.

$\varphi(1) = 1 = \varphi(2)$ ,  $\varphi(3) = 2 = \varphi(4) = \varphi(6)$ ,  $\varphi(p) = p - 1$ , se  $p$  é primo.  
 $\varphi(8) = 4 = \varphi(12)$ ,  $\varphi(9) = 6$ , etc.

Como  $\text{mdc}(1, n) = \text{mdc}(n-1, n) = 1$ , temos  $\varphi(n) \geq 2$  para todo  $n \geq 3$ .

### 10.3 Proposição.

Seja  $p$  um primo e  $a \in \mathbb{N}$ . Então

$$\varphi(p^a) = p^{a-1}(p-1) = p^a \left(1 - \frac{1}{p}\right) .$$

**Demonstração:** Entre os  $n = p^a$  números  $1, 2, 3, \dots, p^a$  não são relativamente primos com  $p^a$  exatamente os  $p^{a-1}$  números  $p, 2p, 3p, \dots, p^{a-1}p$ , i. e. os múltiplos de  $p$ . Estes tem que ser retirados. Segue que

$$\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1) = p^a \left(1 - \frac{1}{p}\right) .$$

■

A fórmula de 10.3 podemos interpretar assim:

### 10.4 Observação.

$$\varphi(p^a) \text{ é } \frac{p-1}{p} \cdot 100\% \text{ de } p^a .$$

Em particular, temos os

### 10.4' Exemplos.

a)  $\varphi(625) = 625 - 125 = 500 = \frac{4}{5} \cdot 625 = 80\%$  de 625.

b)  $\varphi(5^a) = 5^a - \frac{1}{5} \cdot 5^a = \frac{4}{5} \cdot 5^a = 80\%$  de  $5^a$ .

c)  $\varphi(2^a) = 2^a - 2^{a-1} = 2^{a-1}(2 - 1) = 2^{a-1} = 50\%$  de  $2^a$ .

Isto, pois  $1, 3, 5, 7, \dots, 2^a - 1 = 2 \cdot 2^{a-1} - 1$ , i.e. os primeiros  $2^{a-1}$  números ímpares, são exatamente os números  $\leq 2^a$  que são relativamente primos com  $2^a$ .

d)  $\varphi(3^a) = 66\frac{2}{3}\%$  de  $3^a$ . Em particular:

$$\varphi(9) = 6, \quad \varphi(27) = 18, \quad \varphi(81) = 54, \quad \text{etc.}$$

Para a seguinte observação compara-se 2.16.

### 10.5 Observação.

Sejam  $a, n, m \in \mathbb{N}$ . Então

$$\text{mdc}(a, mn) = 1 \iff \begin{cases} \text{mdc}(a, n) = 1 \\ \text{e} \\ \text{mdc}(a, m) = 1 \end{cases}.$$

### 10.6 Definição.

Seja  $2 \leq n \in \mathbb{N}$  e sejam

$$1 = a_1 < a_2 < a_3 < \dots < a_{\varphi(n)-1} < a_{\varphi(n)} = n-1$$

os números entre 1 e  $n$  que são relativamente primos com  $n$ .

Se  $b_1, b_2, \dots, b_{\varphi(n)} \in \mathbb{Z}$  são números que são congruentes mod  $n$  com  $a_1, a_2, \dots, a_{\varphi(n)}$ , em alguma ordem, dizemos que

$$\{b_1, b_2, \dots, b_{\varphi(n)}\}$$

forma um sistema reduzido de restos (resíduos) módulo  $n$ .

### 10.7 Exemplo.

Para  $n = 12$  temos (observe  $\varphi(12) = 4$ ):

$$\{1, 5, 7, 11\}$$

são os menores restos não-negativos relativamente primos mod 12,

$$\{97, 19, -13, -43\}$$

é um sistema reduzido de restos mod 12, pois

$$97 \equiv 1, 19 \equiv 7, -13 \equiv 11, -43 \equiv 5 \pmod{12}.$$

É também clara a seguinte

### 10.8 Observação.

Seja  $n \in \mathbb{N}$ .  $b_1, b_2, \dots, b_{\varphi(n)} \in \mathbb{Z}$  formam um sistema reduzido de restos mod  $n$

$$\iff \begin{cases} \text{mdc}(b_i, n) = 1 \quad \forall i = 1, 2, \dots, \varphi(n) \\ \text{e } b_i \not\equiv b_j \pmod{n} \quad \forall 1 \leq i \neq j \leq \varphi(n). \end{cases}$$

### 10.9 Teorema.

Sejam  $n, m \in \mathbb{N}$  com  $\text{mdc}(m, n) = 1$ . Então vale

$$\varphi(nm) = \varphi(n)\varphi(m).$$

**Demonstração:** Consideremos os  $mn$  números  $1, 2, 3, \dots, mn$  escritos no quadro

1	2	3	...	$r$	...	$m$
$m+1$	$m+2$	$m+3$	...	$m+r$	...	$2m$
$2m+1$	$2m+2$	$2m+3$	...	$2m+r$	...	$3m$
$\vdots$	$\vdots$	$\vdots$	...	$\vdots$	...	$\vdots$
$sm+1$	$sm+2$	$sm+3$	...	$sm+r$	...	$(s+1)m$
$\vdots$	$\vdots$	$\vdots$	...	$\vdots$	...	$\vdots$
$(n-1)m+1$	$(n-1)m+2$	$(n-1)m+3$	...	$(n-1)m+r$	...	$nm$

Agora,  $\varphi(mn)$  é a quantidade de entradas no quadro, relativamente primos com



$mn$ , i. e. relativamente primos com  $n$  e com  $m$ , simultaneamente.

Os números da  $r$ -ésima coluna são relativamente primos com  $m \Leftrightarrow \text{mdc}(r, m) = 1$ . Logo existem  $\varphi(m)$  tais colunas no quadro.

Consideremos uma das colunas com  $\text{mdc}(r, m) = 1$ . Quantos números desta coluna são também relativamente primos com  $n$ ?

Para provar que são exatamente  $\varphi(n)$ , precisamos mostrar que os  $n$  números

$$\{sm + r \mid 0 \leq s \leq n-1\},$$

i.e. os números desta  $r$ -ésima coluna, formam um sistema *completo* de resíduos mod  $n$ , ou seja, são incongruentes entre si mod  $n$ : De fato, se  $0 \leq i, j \leq n-1$ , e  $im + r \equiv jm + r \pmod{n}$ , temos  $(i - j)m \equiv 0 \pmod{n}$  e daí  $i \equiv j \pmod{n}$ , pois  $\text{mdc}(m, n) = 1$ . Como ainda  $0 \leq i, j \leq n-1$ , concluímos  $i = j$ .

Assim, em cada uma das  $\varphi(m)$  colunas cujas entradas são relativamente primos com  $m$ , temos  $\varphi(n)$  dessas entradas também relativamente primos com  $n$ :

$$\varphi(mn) = \varphi(m)\varphi(n).$$

■

### 10.10 Teorema.

Seja  $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_r^{a_r}$  com primos distintos  $p_1, p_2, \dots, p_r$  e  $a_1, a_2, \dots, a_r \in \mathbb{N}$ . Então

$$\varphi(n) = \prod_{k=1}^r p_k^{a_k-1}(p_k - 1) = n \cdot \prod_{k=1}^r \left(1 - \frac{1}{p_k}\right).$$

**Demonstração:** Temos  $\text{mdc}\left(p_1^{a_1}, \prod_{k=2}^r p_k^{a_k}\right) = 1$ . Por indução sobre  $r$ , levando-se em conta os resultados 10.9 e 10.3, segue

$$\begin{aligned} \varphi(n) &= \varphi\left(\prod_{k=1}^r p_k^{a_k}\right) = \varphi\left(p_1^{a_1}\right) \cdot \varphi\left(\prod_{k=2}^r p_k^{a_k}\right) = p_1^{a_1-1}(p_1 - 1) \cdot \prod_{k=2}^r p_k^{a_k-1}(p_k - 1) = \\ &= \prod_{k=1}^r p_k^{a_k-1}(p_k - 1). \end{aligned}$$

Além disso, de  $p_k^{a_k-1}(p_k - 1) = p_k^{a_k} \left(1 - \frac{1}{p_k}\right)$  e  $n = \prod_{k=1}^r p_k^{a_k}$  segue a segunda igualdade da afirmação.

■

### 10.11 Exemplos.

$$\begin{aligned} \text{a) } \varphi(8026200) &= \varphi(2^3 \cdot 3^2 \cdot 5^2 \cdot 7^3 \cdot 13) = \\ &= 8026200 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{7}\right) \cdot \left(1 - \frac{1}{13}\right) = \\ &= 8026200 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} \cdot \frac{12}{13} = 1693440. \end{aligned}$$

b) Com  $a_p(20) = \sum_{k=1}^{\infty} \left[ \frac{20}{p^k} \right]$  temos

$$\begin{aligned} \varphi(20!) &= \varphi\left(\prod_{p \in \mathbb{P}} p^{a_p(20)}\right) = \prod_{p \in \mathbb{P}} \varphi(p^{a_p(20)}) = \\ &= \varphi(2^{18}) \cdot \varphi(3^8) \cdot \varphi(5^4) \cdot \varphi(7^2) \cdot \varphi(11) \cdot \varphi(13) \cdot \varphi(17) \cdot \varphi(19) = \\ &= 2^{17} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot (3-1) \cdot (5-1) \cdot (7-1) \cdot (11-1) \cdot (13-1) \cdot (17-1) \cdot (19-1) = \\ &= 2^{17} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 2 \cdot 4 \cdot 6 \cdot 10 \cdot 12 \cdot 16 \cdot 18 = 2^{29} \cdot 3^{11} \cdot 5^4 \cdot 7. \end{aligned}$$

■

Enquanto  $\varphi(1) = \varphi(2) = 1$ , temos:

### 10.12 Observação.

Para  $n \geq 3$  vale

$$\varphi(n) \equiv 0 \pmod{2}.$$

**Demonstração:** Se  $n = 2^a$  com  $a \geq 2$ , temos

$$\varphi(n) = 2^{a-1} \equiv 0 \pmod{2}.$$

Se  $n = p^a \cdot k$  com  $a, k \in \mathbb{N}$ ,  $2 < p \in \mathbb{P}$  e  $p \nmid k$ , temos também

$$\varphi(n) = \varphi(p^a)\varphi(k) = p^{a-1}(p-1)\varphi(k) \equiv 0 \pmod{2} \text{ pois } p-1 \text{ é par.}$$

■

$n-1$  é claramente uma cota superior para  $\varphi(n)$ .

Uma cota inferior é dada na seguinte

### 10.13 Proposição.

Seja  $2 \leq n \in \mathbb{N}$ . Então

$$\frac{1}{2}\sqrt{n} \leq \varphi(n) \leq n-1.$$

**Demonstração:** Só é preciso mostrar  $\frac{1}{2}\sqrt{n} \leq \varphi(n)$  :  
 Seja  $n = 2^{a_0} \cdot p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_r^{a_r}$  com primos  $2 < p_1 < p_2 < \dots < p_r$  e inteiros  $a_0 \geq 0, a_1, a_2, \dots, a_r \geq 1$ .

$$\varphi(n) = \varphi(2^{a_0}) \cdot p_1^{a_1-1} \cdot p_2^{a_2-1} \cdot \dots \cdot p_r^{a_r-1} \cdot (p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_r - 1)$$

onde  $\varphi(2^{a_0}) = 1$  se  $a_0 = 0$  ou  $2^{a_0-1}$  se  $a_0 \geq 1$ . Segue \*)

$$\begin{aligned} \varphi(n) &\geq \varphi(2^{a_0}) \cdot p_1^{\frac{a_1-1}{2}} \cdot p_2^{\frac{a_2-1}{2}} \cdot \dots \cdot p_r^{\frac{a_r-1}{2}} \cdot \sqrt{p_1} \sqrt{p_2} \cdot \dots \cdot \sqrt{p_r} = \\ &= \frac{\varphi(2^{a_0})}{2^{\frac{a_0}{2}}} \cdot 2^{\frac{a_0}{2}} \cdot p_1^{\frac{a_1}{2}} \cdot p_2^{\frac{a_2}{2}} \cdot \dots \cdot p_r^{\frac{a_r}{2}} = \frac{\varphi(2^{a_0})}{2^{\frac{a_0}{2}}} \sqrt{n} \geq \frac{1}{2} \sqrt{n} . \end{aligned}$$

\*) Usa-se aqui a desigualdade  $x - 1 \geq \sqrt{x}$  válida para  $x \geq 3$ . Provar isto!  
 Fazer o gráfico das funções reais  $y = x - 1$  e  $y = \sqrt{x}$ . Onde as duas funções se interceptam ?

■

## O TEOREMA DE EULER

### 10.14 Teorema. (EULER)

Seja  $n \in \mathbb{N}$  e  $b \in \mathbb{Z}$  com  $\text{mdc}(b, n) = 1$ . Então

$$b^{\varphi(n)} \equiv 1 \pmod{n} .$$

**Demonstração:** Podemos supor  $n \geq 2$ . Sejam  $1 = a_1 < a_2 < \dots < a_{\varphi(n)} = n-1$  os restos entre  $0, 1, 2, \dots, n-1$  e relativamente primos com  $n$ . Temos que

$$\left\{ b, ba_2, \dots, ba_{\varphi(n)} \right\}$$

é um sistema reduzido de restos mod  $n$ , pois  $\forall i, j = 1, 2, \dots, \varphi(n) :$

$$ba_i \equiv ba_j \pmod{n} \Rightarrow a_i = a_j \Rightarrow i = j .$$

Segue

$$ba_1 \cdot ba_2 \cdot \dots \cdot ba_{\varphi(n)} \equiv a_1 \cdot a_2 \cdot \dots \cdot a_{\varphi(n)} \pmod{n} ,$$

ou seja

$$b^{\varphi(n)} \cdot a_1 a_2 \dots a_{\varphi(n)} \equiv a_1 a_2 \dots a_{\varphi(n)} \pmod{n} .$$

Como  $\text{mdc}(a_1 a_2 \dots a_{\varphi(n)}, n) = 1$ , podemos cancelar este fator da congruência e obtemos

$$b^{\varphi(n)} \equiv 1 \pmod{n} .$$

■

É claro que, para  $n = p = \text{primo}$  ( $\varphi(n) = \varphi(p) = p - 1$ ), o teorema de EULER passa a ser o teorema de FERMAT (7.1).

### 10.15 Exemplo.

Seja  $n \in \mathbb{N}$ ,  $n \equiv 1 \pmod{2}$  e  $n \not\equiv 0 \pmod{5}$ . Então

*n divide algum número da forma 1111...1111.*

**Demonstração:** Temos  $\text{mdc}(n, 10) = 1$  e  $\text{mdc}(9n, 10) = 1$ . Logo, pelo teorema de EULER 10.14:

$$10^{\varphi(9n)} \equiv 1 \pmod{9n}, \text{ ou seja, } 10^{\varphi(9n)} - 1 = 9nk .$$

Segue

$$n \text{ divide } \frac{10^{\varphi(9n)} - 1}{9} = \frac{9999\dots9999}{9} = 1111\dots1111 .$$

■

## MAIS ALGUMAS PROPRIEDADES DA FUNÇÃO $\varphi$

### 10.16 Proposição.

Para todo  $n \in \mathbb{N}$  temos

$$\sum_{d|n} \varphi(d) = n .$$

**Demonstração:** Para todo divisor  $d$  de  $n$  consideremos o conjunto

$$S_d = \{ k \mid 1 \leq k \leq n, \text{mdc}(k, n) = d \} .$$

Temos  $S_d \cap S_{d'} = \emptyset$  se  $d$  e  $d'$  são divisores distintos. Claramente temos

$$\bigcup_{d|n} S_d = \{ 1, 2, 3, \dots, n \}$$

(para cada  $k$  vale  $k \in S_d$  quando  $d = \text{mdc}(k, n)$ ). Concluimos

$$n = |\{1, 2, 3, \dots, n\}| = \left| \bigcup_{d|n} S_d \right| = \sum_{d|n} |S_d| .$$

Resta saber  $|S_d| = ?$ . Temos

$$k \in S_d \Leftrightarrow \text{mdc}(k, n) = d \Leftrightarrow \text{mdc}\left(\frac{k}{d}, \frac{n}{d}\right) = 1 .$$

Segue

$$|S_d| = |\{\ell \mid 1 \leq \ell \leq \frac{n}{d}; \text{mdc}(\ell, \frac{n}{d}) = 1\}|, \text{ isto é,}$$

$$|S_d| = \varphi\left(\frac{n}{d}\right) .$$

Assim,

$$\sum_{d|n} |S_d| = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d) .$$

Portanto obtemos, como afirmado,

$$n = \sum_{d|n} |S_d| = \sum_{d|n} \varphi(d) .$$

■

Uma segunda demonstração desta fórmula interessante podemos ver via decomposição primária de  $n$ :

**2ª demonstração:** Seja primeiro  $n = p^a$  com  $p \in \mathbb{P}$  e  $a \in \mathbb{N}$ . Temos

$$\sum_{d|n} \varphi(d) = \sum_{\ell=0}^a \varphi(p^\ell) = 1 + \sum_{\ell=1}^a p^{\ell-1}(p-1) = 1 + (p-1) \frac{p^a - 1}{p-1} = p^a .$$

Se  $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_r^{a_r}$  é a decomposição primária de  $n$ , obtemos

$$\begin{aligned} \sum_{d|n} \varphi(d) &= \sum_{\ell_1=0}^{a_1} \dots \sum_{\ell_r=0}^{a_r} \varphi(p_1^{\ell_1} \dots p_r^{\ell_r}) = \sum_{\ell_1=0}^{a_1} \dots \sum_{\ell_r=0}^{a_r} \varphi(p_1^{\ell_1}) \dots \varphi(p_r^{\ell_r}) = \\ &= \left( \sum_{\ell_1=0}^{a_1} \varphi(p_1^{\ell_1}) \right) \cdot \dots \cdot \left( \sum_{\ell_r=0}^{a_r} \varphi(p_r^{\ell_r}) \right) = p_1^{a_1} \cdot \dots \cdot p_r^{a_r} = n . \end{aligned}$$

■

### 10.17 Proposição.

Para todo  $n > 1$  temos

$$\sum_{\substack{k=1 \\ \text{mdc}(k,n)=1}}^n k = \frac{1}{2}n\varphi(n).$$

**Demonstração:** Sejam  $1 = a_1 < a_2 < \dots < a_{\varphi(n)-1} < a_{\varphi(n)} = n-1$  os números entre  $\{1, 2, 3, \dots, n\}$  que são relativamente primos com  $n$ . Portanto

$$\sum_{\substack{k=1 \\ \text{mdc}(k,n)=1}}^n k = \sum_{k=1}^{\varphi(n)} a_k.$$

Temos  $\text{mdc}(k, n) = 1 \Leftrightarrow \text{mdc}(n-k, n) = 1$ . Logo

$$n-a_1 = a_{\varphi(n)}, n-a_2 = a_{\varphi(n)-1}, \dots, n-a_{\varphi(n)-1} = a_2, n-a_{\varphi(n)} = a_1.$$

Assim,

$$\{a_1, a_2, \dots, a_{\varphi(n)}\} = \{n-a_1, n-a_2, \dots, n-a_{\varphi(n)}\},$$

de onde concluímos

$$\sum_{k=1}^{\varphi(n)} a_k = \sum_{k=1}^{\varphi(n)} (n-a_k) = \sum_{k=1}^{\varphi(n)} n - \sum_{k=1}^{\varphi(n)} a_k.$$

Segue

$$2 \cdot \sum_{k=1}^{\varphi(n)} a_k = n\varphi(n),$$

ou seja

$$\sum_{k=1}^{\varphi(n)} a_k = \frac{1}{2}n\varphi(n).$$

Daí

$$\sum_{\substack{k=1 \\ \text{mdc}(k,n)=1}}^n k = \sum_{k=1}^{\varphi(n)} a_k = \frac{1}{2}n\varphi(n).$$

■

## § 11 Raízes primitivas

### ORDENS MÓDULO $n$ E RAÍZES PRIMITIVAS

Para  $n \in \mathbb{N}$  e  $a \in \mathbb{Z}$  com  $\text{mdc}(a, n) = 1$  temos  $a^{\varphi(n)} \equiv 1 \pmod{n}$  pelo teorema de EULER. Particularmente, existe um expoente  $k > 0$  (por exemplo  $k = \varphi(n)$ ), tal que  $a^k \equiv 1 \pmod{n}$ .

#### 11.1 Definição.

Seja  $n \in \mathbb{N}$  e  $a \in \mathbb{Z}$  com  $\text{mdc}(a, n) = 1$ .

O menor número  $k_0 \in \mathbb{N}$  tal que  $a^{k_0} \equiv 1 \pmod{n}$ , indicado por

$$k_0 = \mathbf{o}_n(a),$$

chama-se a ordem de  $a$  mod  $n$ .

Observamos que o teorema de EULER garante

$$\mathbf{o}_n(a) \leq \varphi(n).$$

Claro que  $\mathbf{o}_n(a) = 1 \iff a \equiv 1 \pmod{n}$ . Além disso, como  $n-1 \equiv -1 \pmod{n}$ , temos  $\mathbf{o}_n(n-1) = 2$ , se  $n \geq 3$ .

Destacamos que o símbolo  $\mathbf{o}_n(a)$  não está definido, se  $\text{mdc}(a, n) > 1$ ! Por exemplo,  $\mathbf{o}_9(6)$  ou  $\mathbf{o}_{10}(5)$  não fazem sentido.

#### 11.2 Exemplos.

Eis para alguns valores de  $n$ , as tabelas dos menores restos não-negativos  $a$ , relativamente primos com  $n$ , e suas ordens  $\mathbf{o}_n(a)$ .

a)  $n = 3$   $\varphi(3) = 2$  :

$a$	1	2
$\mathbf{o}_3(a)$	1	2

b)  $n = 4$   $\varphi(4) = 2$  :

$a$	1	3
$\mathbf{o}_4(a)$	1	2

c)  $n = 5$   $\varphi(5) = 4$ :

$a$	1	2	3	4
$\mathbf{o}_5(a)$	1	4	4	2

d)  $n = 6$   $\varphi(6) = 2$  :

$a$	1	5
$\mathbf{o}_6(a)$	1	2

e)  $n = 7$   $\varphi(7) = 6$ :

$a$	1	2	3	4	5	6
$\mathbf{o}_7(a)$	1	3	6	3	6	2

f)  $n = 8$   $\varphi(8) = 4$ :

$a$	1	3	5	7
$\mathbf{o}_8(a)$	1	2	2	2

g)  $n = 9$   $\varphi(9) = 6$ :

$a$	1	2	4	5	7	8
$\mathbf{o}_9(a)$	1	6	3	6	3	2

h)  $n = 12$   $\varphi(12) = 4$ :

$a$	1	5	7	11
$\mathbf{o}_{12}(a)$	1	2	2	2

### 11.3 Observação.

Seja  $n \in \mathbb{N}$ ,  $a \in \mathbb{Z}$  com  $\text{mdc}(a, n) = 1$  e suponhamos  $a^k \equiv 1 \pmod{n}$  para algum  $k \in \mathbb{N}$ . Então

$$\mathbf{o}_n(a) \mid k, \text{ particularmente } \mathbf{o}_n(a) \mid \varphi(n).$$

**Demonstração:** Divisão de  $k$  por  $\mathbf{o}_n(a)$  dá:  $k = \ell \cdot \mathbf{o}_n(a) + r$  com  $0 \leq r \leq \mathbf{o}_n(a) - 1$ . Segue

$$1 \equiv a^k = a^{\ell \mathbf{o}_n(a) + r} = (a^{\mathbf{o}_n(a)})^\ell \cdot a^r \equiv 1^\ell \cdot a^r \equiv a^r \pmod{n}.$$

Concluimos  $r = 0$  pela minimalidade de  $\mathbf{o}_n(a)$ . Logo  $\mathbf{o}_n(a) \mid k$ . ■

### 11.4 Observação.

Seja  $n \in \mathbb{N}$ ,  $a \in \mathbb{Z}$  com  $\text{mdc}(a, n) = 1$  e sejam  $i, j \in \mathbb{N}_0$ . Temos

$$a^i \equiv a^j \pmod{n} \iff i \equiv j \pmod{\mathbf{o}_n(a)}.$$

**Demonstração:** "  $\Leftarrow$  ":  $i \equiv j \pmod{\mathbf{o}_n(a)}$  significa  $i = j + \ell \mathbf{o}_n(a)$  com  $\ell \in \mathbb{N}_0$  quando  $i \geq j$ . Segue

$$a^i = a^{j + \ell \mathbf{o}_n(a)} = (a^{\mathbf{o}_n(a)})^\ell \cdot a^j \equiv 1^\ell \cdot a^j = a^j \pmod{n}.$$

"  $\Rightarrow$  ": Suponhamos  $a^i \equiv a^j \pmod{n}$  com  $i \geq j$ . Assim,  $a^{i-j} \equiv 1 \pmod{n}$ . Por 11.3 concluímos  $\mathbf{o}_n(a) \mid i - j$ , ou seja,  $i \equiv j \pmod{\mathbf{o}_n(a)}$ . ■



## 11.5 Conseqüência.

Os números

$$\{1, a, a^2, a^3, \dots, a^{\mathbf{o}_n(a)-1}\} \quad \text{são incongruentes módulo } n.$$

**Demonstração:** De  $a^i \equiv a^j \pmod n$ , com  $0 \leq i, j \leq \mathbf{o}_n(a) - 1$ , segue  $i \equiv j \pmod{\mathbf{o}_n(a)}$  por 11.4 e então  $i = j$ . ■

## 11.6 Conseqüência.

Seja  $\mathbf{o}_n(a) = \varphi(n)$ . Então

$$\{a, a^2, a^3, \dots, a^{\varphi(n)-1}, a^{\varphi(n)} \equiv 1\}$$

é um sistema reduzido de restos módulo  $n$ .

## 11.7 Exemplo.

Para  $n = 7$  temos  $\mathbf{o}_7(3) = 6 = \varphi(7)$  (ver tabela do Ex. 11.2 b)), conseqüentemente

$$\{3, 3^2, 3^3, 3^4, 3^5, 3^6\}$$

é um sistema reduzido de restos mod 7. De fato:

$$3 \equiv 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5, 3^6 \equiv 1 \pmod 7.$$

O mesmo valendo para

$$\{5, 5^2, 5^3, 5^4, 5^5, 5^6\}.$$

Assim, se encontrarmos um resto  $a$  relativamente primo com  $n$ , de ordem máxima possível, a saber,  $\mathbf{o}_n(a) = \varphi(n)$ , conseguiremos um sistema reduzido de resíduos, o qual consiste das potências deste  $a$ .

## 11.8 Definição.

Seja  $n \in \mathbb{N}$ . Um número  $a \in \mathbb{Z}$  (caso exista!) chama-se

uma raiz primitiva mod  $n$ , se

$$\mathbf{o}_n(a) = \varphi(n).$$

## 11.9 Exemplos.

As tabelas em 11.2 mostram

- a) 2 é uma raiz primitiva mod 3      c) 2 e 3 são raízes primitivas mod 5  
b) 3 é uma raiz primitiva mod 4      d) 5 é uma raiz primitiva mod 6  
e) 5 e 3 são raízes primitivas mod 7    g) 2 e 5 são raízes primitivas mod 9  
f) Não há raiz primitiva mod 8          h) Não há raiz primitiva mod 12.

## 11.10 Proposição.

Sejam  $n \in \mathbb{N}$ ,  $a \in \mathbb{Z}$  com  $\text{mdc}(a, n) = 1$  e seja  $h \in \mathbb{N}$ . Então

$$\mathbf{o}_n(a^h) = \frac{\mathbf{o}_n(a)}{\text{mdc}(h, \mathbf{o}_n(a))}.$$

**Demonstração:** Seja  $r = \mathbf{o}_n(a^h)$  e  $k_0 = \mathbf{o}_n(a)$  e seja  $d = \text{mdc}(h, k_0)$ . Escrevemos  $h = h_1 d$  e  $k_0 = k_1 d$  com  $\text{mdc}(h_1, k_1) = 1$ . De

$$(a^h)^{k_1} = (a^{h_1 d})^{\frac{k_0}{d}} = a^{h_1 k_0} = (a^{k_0})^{h_1} \equiv 1^{h_1} = 1 \pmod{n}$$

concluimos  $r = \mathbf{o}_n(a^h) \mid k_1$ . Particularmente,  $r \leq k_1$ .

De  $(a^h)^r \equiv 1 \pmod{n}$  segue  $a^{hr} \equiv 1 \pmod{n}$  e daí  $k_0 = \mathbf{o}_n(a) \mid hr$ . Concluimos  $k_1 d \mid h_1 dr$ ,  $k_1 \mid h_1 r$  e então  $k_1 \mid r$ . Logo  $k_1 \leq r$ . Assim

$$\mathbf{o}_n(a^h) = r = k_1 = \frac{k_0}{d} = \frac{\mathbf{o}_n(a)}{\text{mdc}(h, \mathbf{o}_n(a))}.$$

■

## 11.11 Conseqüência.

$$\mathbf{o}_n(a^h) = \mathbf{o}_n(a) \iff \text{mdc}(h, \mathbf{o}_n(a)) = 1.$$

## 11.12 Conseqüência.

Seja  $a$  uma raiz primitiva mod  $n$ . Então existem exatamente  $\varphi(\varphi(n))$  raízes primitivas incongruentes mod  $n$ .

**Demonstração:**  $\{a, a^2, a^3, \dots, a^{\varphi(n)-1}, a^{\varphi(n)} \equiv 1\}$  é um sistema reduzido de

restos módulo  $n$  com  $\mathbf{o}_n(a) = \varphi(n)$ . Para  $h \in \{1, 2, \dots, \varphi(n)\}$  temos que  $a^h$  é raiz primitiva, se e somente se  $\mathbf{o}_n(a^h) = \mathbf{o}_n(a)$ , se e somente se  $\text{mdc}(h, \varphi(n)) = 1$ . Existem  $\varphi(\varphi(n))$  tais  $h$  entre os  $1, 2, \dots, \varphi(n)$ . ■

### 11.13 Exemplo.

Para  $n = 22$  temos  $\varphi(22) = \varphi(2)\varphi(11) = 1 \cdot 10 = 10$ . Os menores restos não-negativos e relativamente primos com 22 e suas ordens são

$a$	1	3	5	7	9	13	15	17	19	21
$\mathbf{o}_{22}(a)$	1	5	5	10	5	10	5	10	10	2

A ordem de qualquer um destes números  $a$  é divisor de 10, ou seja,

$$\mathbf{o}_{22}(a) \in \{1, 2, 5, 10\} \quad \forall a \in \{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}.$$

As raízes primitivas mod 22 são  $\{7, 13, 17, 19\}$ . Assim, por exemplo

$$\{7, 7^2, 7^3, \dots, 7^9, 7^{10} \equiv 1\}$$

é um sistema reduzido de restos mod 22 também.

Temos  $\varphi(\varphi(22)) = \varphi(10) = 4$  e os 4 números relativamente primos com 10 são  $h = 1, 3, 7, 9$ . Segue que

$$\{7, 7^3, 7^7, 7^9\}$$

são raízes primitivas módulo 22 que são incongruentes. Elas claramente são congruentes a

$$\{7, 13, 17, 19\}.$$

## EXISTÊNCIA DE RAÍZES PRIMITIVAS

### 11.14 Observação.

Para todo  $k \geq 3$  e todo  $a \in \mathbb{Z}$  ímpar vale

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

**Demonstração:** Esta afirmação é verdadeira para  $k = 3$ , pois sempre  $a^2 \equiv$

1 mod 8 (ver exemplo 11.9 b)). Provaremos a afirmação por indução sobre  $k$  :

Suponhamos  $a^{2^{k-2}} \equiv 1 \pmod{2^k}$  já provado para algum  $k \geq 3$ . Então  $a^{2^{k-2}} = 1 + \ell \cdot 2^k$  para algum  $\ell \in \mathbb{Z}$  e segue

$$\begin{aligned} a^{2^{k-1}} &= \left(a^{2^{k-2}}\right)^2 = (1 + \ell \cdot 2^k)^2 = 1 + 2\ell \cdot 2^k + \ell^2 \cdot 2^{2k} = \\ &= 1 + \ell(1 + \ell 2^{k-1}) 2^{k+1} \equiv 1 \pmod{2^{k+1}}. \end{aligned}$$

Portanto vale  $a^{2^{k-2}} \equiv 1 \pmod{2^k}$  par todo  $k \geq 3$  e todo  $a$  ímpar. ■

Vimos que nem sempre podemos garantir a existência de uma raiz primitiva módulo  $n$  (ver os exemplos 11.2).

*Quais são os números  $n$ , módulo os quais existe raiz primitiva?*

A existência de uma raiz primitiva mod  $n$  é mais a exceção do que a regra, como mostra

### 11.15 Proposição.

- a) Se  $n \in \mathbb{N}$  é decomponível como  $n = rs$  com  $r, s \geq 3$  e  $\text{mdc}(r, s) = 1$ , então **não** existe raiz primitiva mod  $n$ .
- b) Se  $n = 2^k$  com  $k \geq 3$ , então **não** existe raiz primitiva mod  $n$ .

**Demonstração:** a) Se  $a \in \mathbb{Z}$  com  $\text{mdc}(a, n) = 1$ , segue  $\text{mdc}(a, r) = \text{mdc}(a, s) = 1$ . Por 10.12 sabemos  $\varphi(n) \equiv \varphi(r) \equiv \varphi(s) \equiv 0 \pmod{2}$ , pois  $r, s \geq 3$ . Usando-se 10.9 e o teorema de EULER, vemos

$$a^{\frac{\varphi(n)}{2}} = a^{\frac{\varphi(rs)}{2}} = a^{\frac{\varphi(r)\varphi(s)}{2}} = \begin{cases} (a^{\varphi(r)})^{\frac{\varphi(s)}{2}} \equiv 1^{\frac{\varphi(s)}{2}} \equiv 1 \pmod{r} \\ (a^{\varphi(s)})^{\frac{\varphi(r)}{2}} \equiv 1^{\frac{\varphi(r)}{2}} \equiv 1 \pmod{s} \end{cases}$$

Logo,  $a^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{r}$  e  $a^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{s}$ . Segue

$$a^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{n},$$

pois  $\text{mdc}(r, s) = 1$ . Isto significa  $\mathbf{o}_n(a) \leq \frac{\varphi(n)}{2}$  para qualquer  $a$ : Não pode existir raiz primitiva mod  $n$ .

b) Temos  $\varphi(2^k) = 2^{k-1}$ . A Observação 11.14 diz que sempre

$$a^{\frac{\varphi(2^k)}{2}} = a^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

Logo  $\mathfrak{o}_{2^k}(a) \leq \frac{\varphi(2^k)}{2}$  para qualquer  $a$  ímpar: Também não pode existir raiz primitiva mod  $2^k$  para  $k \geq 3$ . ■

Os números que restam e que não se enquadram nos tipos de números descritos em 11.15, são os

$$n \in \{1, 2, 4, p^k, 2p^k\} \quad \text{onde } p \text{ é um primo ímpar e } k \in \mathbb{N}.$$

Nosso objetivo é mostrar que módulo todos estes números de fato existem raízes primitivas. Preparamos a demonstração disso pela

### 11.16 Observação.

Seja  $p$  um número primo,  $r \in \mathbb{N}$ . Uma congruência polinomial

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{r-1}x^{r-1} + a_rx^r \equiv 0 \pmod{p} \quad (*)$$

com  $a_r \not\equiv 0 \pmod{p}$  possui no máximo  $r$  soluções incongruentes mod  $p$ .

Antes de verificar isto, observamos que tal afirmação não continua válida se o módulo não é primo. Por exemplo, a congruência de grau 2:  $x^2 - 1 \equiv 0 \pmod{8}$  possui as 4 soluções incongruentes  $x \equiv 1, 3, 5, 7 \pmod{8}$ .

**Demonstração:** Para  $r = 1$  isto sabemos: A congruência linear  $a_1x + a_0 \equiv 0 \pmod{p}$  com  $a_1 \not\equiv 0 \pmod{p}$  possui solução única em  $\{0, 1, 2, \dots, p-1\}$ . Se  $r > 1$  e se  $b \in \mathbb{Z}$  é uma solução de (\*), então temos  $f(b) \equiv 0 \pmod{p}$ . Podemos escrever

$$f(x) \equiv (x - b) \cdot g(x) + s \pmod{p}$$

com certo polinômio  $g(x)$  de grau  $\leq r - 1$  e uma constante  $s \in \mathbb{Z}$ . De  $0 \equiv f(b) \equiv (b - b)g(b) + s \pmod{p}$  concluímos  $s \equiv 0 \pmod{p}$  e assim

$$f(x) \equiv (x - b)g(x) \pmod{p}.$$

Seja  $c \not\equiv b \pmod{p}$  mais uma raiz de  $f(x)$ . Então  $0 \equiv f(c) \equiv (c - b)g(c) \pmod{p}$ . De  $p \nmid (c - b)$  segue  $p \mid g(c)$  e daí  $g(c) \equiv 0 \pmod{p}$ . Assim,  $c$  é uma raiz de  $g(x)$ . Por hipótese de indução sabemos que  $g(x)$  possui no máximo  $r - 1$  raízes incongruentes mod  $p$ . Segue que  $f(x)$  possui no máximo  $r$  raízes incongruentes mod  $p$ , a saber,  $b$  junto com as raízes de  $g(x)$ . ■

A existência de raízes primitivas módulo números primos é garantida pela

### 11.17 Proposição.

*Seja  $p$  um número primo. Então existe uma raiz primitiva módulo  $p$ .*

Afirma-se então a existência de um  $a \in \mathbb{Z}$  com  $p \nmid a$  e  $\mathfrak{o}_p(a) = p - 1 = \varphi(p)$ , ou seja, um  $a \not\equiv 0 \pmod{p}$  tal que  $a^\ell \not\equiv 1 \pmod{p}$  para todo  $\ell < p - 1$ .

Para que possamos entender melhor o que acontecerá na demonstração de 11.17, pensamos primeiro em dois exemplos: Porquê tem que existir uma raiz primitiva mod 5 e mod 37?

**Primeiro** mod 5:

Temos  $\varphi(5) = 4$ . As possíveis ordens dos restos  $a \not\equiv 0 \pmod{5}$  são os divisores de 4, ou seja,  $\mathfrak{o}_5(a) \in \{1, 2, 4\}$ .

Porquê algum dos restos  $d \in \{1, 2, 3, 4\}$  possui a ordem máxima

$$\mathfrak{o}_5(d) = \varphi(5) = 4 ?$$

(sem simplesmente verificar isto por tentativa!):

Por FERMAT temos  $z^4 \equiv 1 \pmod{5}$  para todo  $z$ . Se nenhum tivesse ordem igual a 4, todos teriam ordem  $\leq 2$  e teríamos  $z^2 \equiv 1 \pmod{5}$  para 4 valores  $z$  incongruentes. Isto é impossível para uma congruência polinomial de grau 2 módulo o primo 5. Logo tem que existir um  $d$  de ordem 4.

(Para comparar, lembremos mais uma vez aqui que os 4 restos 1, 3, 5, 7 mod 8 *todos* possuem ordem 2 e não existe raiz primitiva mod 8!)

**Agora** mod 37:

Temos  $\varphi(37) = 36$ . As possíveis ordens dos restos  $a \not\equiv 0 \pmod{37}$  são os divisores de 36, ou seja,  $\mathfrak{o}_{37}(a) \in \{1, 2, 4, 3, 6, 12, 9, 18, 36\}$ .

Porquê algum dos restos  $a \in \{1, 2, 3, \dots, 36\}$  possui a ordem máxima

$$\mathfrak{o}_{37}(a) = \varphi(37) = 36 ?$$

1) Se conseguirmos um  $d_1 \in \{1, 2, \dots, 36\}$  de ordem  $\mathfrak{o}_{37}(d_1) = 4$  e um  $d_2$  de ordem  $\mathfrak{o}_{37}(d_2) = 9$ , fazemos  $a = d_1 d_2$  e afirmamos que  $\mathfrak{o}_{37}(a) = 36$ :

Se  $\mathfrak{o}_{37}(a) < 36$ , esta ordem seria um dos números 1, 2, 4, 3, 6, 12, 9, 18, ou seja teria que dividir  $18 = \frac{36}{2}$  ou  $12 = \frac{36}{3}$ . Mas  $a^{18} = d_1^{18} d_2^{18} = d_1^{18} \not\equiv 1$ , pois  $4 \nmid 18$ .

Da mesma forma,  $a^{12} = d_1^{12} d_2^{12} = d_2^{12} \not\equiv 1$ , pois  $9 \nmid 12$ . Assim  $\mathfrak{o}_{37}(a) = 36$  se conseguirmos  $d_1, d_2$  com  $\mathfrak{o}_{37}(d_1) = 4$  e  $\mathfrak{o}_{37}(d_2) = 9$ .

2) Porquê existem  $d_1$  e  $d_2$ ?

Por FERMAT temos  $z^{36} \equiv 1 \pmod{37}$  para todo  $z$ . Segue que os elementos em  $\{z^9 \mid z \in \{1, 2, \dots, 36\}\}$  possuem ordens que dividem 4. Se nenhum tivesse ordem igual a 4, todas elas dividiriam 2 e teríamos  $z^{18} = (z^9)^2 \equiv 1 \pmod{37}$  para 36 valores  $z$  incongruentes. Isto é impossível para uma congruência polinomial de grau 18 módulo o primo 37. Logo tem que existir  $d_1$  de ordem 4.

Da mesma forma, os elementos em  $\{z^4 \mid z \in \{1, 2, \dots, 36\}\}$  possuem ordens que dividem 9. Se nenhum deles tivesse ordem igual a 9, todas elas dividiriam 3 e teríamos  $z^{12} = (z^4)^3 \equiv 1 \pmod{37}$  para 36 valores incongruentes. Isto é impossível. Logo também tem que existir  $d_2$  de ordem 9.

As mesmas idéias conduzem a prova geral de 11.17.

**Demonstração** de 11.17: Podemos supor  $p > 2$ . Seja

$$p - 1 = q_1^{b_1} \cdot q_2^{b_2} \cdot \dots \cdot q_r^{b_r}$$

com primos distintos  $q_1, q_2, \dots, q_r$  e  $b_1, b_2, \dots, b_r \in \mathbb{N}$ . Para todo  $i \in \{1, 2, \dots, r\}$  coloquemos

$$m_i = \prod_{\substack{k=1 \\ k \neq i}}^r q_k^{b_k} = q_1^{b_1} \cdot \dots \cdot q_{i-1}^{b_{i-1}} \cdot q_{i+1}^{b_{i+1}} \cdot \dots \cdot q_r^{b_r} = \frac{p-1}{q_i^{b_i}}.$$

Assim  $p - 1 = m_i \cdot q_i^{b_i}$  e  $\text{mdc}(m_i, q_i^{b_i}) = 1$  para todo  $i = 1, 2, \dots, r$ .

Para todo  $z \in \{1, 2, \dots, p-1\}$  consideremos  $d = z^{m_i}$ . Temos pelo teorema de FERMAT (7.1)

$$d^{q_i^{b_i}} = (z^{m_i})^{q_i^{b_i}} = z^{p-1} \equiv 1 \pmod{p},$$

de onde segue  $\mathfrak{o}_p(d) \mid q_i^{b_i}$ . Assim,  $\mathfrak{o}_p(d) = q_i^{\ell_i}$  para algum  $\ell_i$  com  $0 \leq \ell_i \leq b_i$ .

Suponhamos,  $\mathfrak{o}_p(d) < q_i^{b_i}$  para todo  $z \in \{1, 2, \dots, p-1\}$ . Então  $\mathfrak{o}_p(d) \mid q_i^{b_i-1}$  para todo  $z \in \{1, 2, \dots, p-1\}$ . Teríamos

$$z^{\frac{p-1}{q_i}} = z^{m_i \cdot q_i^{b_i-1}} \equiv 1 \pmod{p} \quad \text{para todo } z \in \{1, 2, \dots, p-1\}.$$

Isto é impossível, pois a congruência polinomial  $x^{\frac{p-1}{q_i}} - 1 \equiv 0 \pmod{p}$  de grau  $< p-1$  não pode ter  $p-1$  soluções incongruentes  $\pmod{p}$ , por 11.16.

Concluimos que existe  $z = c_i \in \{1, 2, \dots, p-1\}$  tal que  $c_i^{m_i q_i^{b_i-1}} \not\equiv 1 \pmod{p}$ , ou seja,

$$\mathbf{o}_p(c_i^{m_i}) = q_i^{b_i}.$$

Coloquemos  $d_1 = c_1^{m_1}$ ,  $d_2 = c_2^{m_2}$ ,  $\dots$ ,  $d_r = c_r^{m_r}$ , de sorte que  $\mathbf{o}_p(d_i) = q_i^{b_i}$ . Ponhamos

$$a = d_1 \cdot d_2 \cdot \dots \cdot d_r.$$

Qual é a ordem  $\mathbf{o}_p(a)$  ?

Claro que  $\mathbf{o}_p(a) \mid p-1$ . Se  $\mathbf{o}_p(a) < p-1$ , teríamos  $\mathbf{o}_p(a) \mid \frac{p-1}{q_i} = m_i q_i^{b_i-1}$  para algum  $i \in \{1, 2, \dots, r\}$ . Seguiria, observando-se que  $d_j^{m_j} \equiv 1 \pmod{p}$  para todo  $j \neq i$ :

$$\begin{aligned} 1 &\equiv a^{m_i q_i^{b_i-1}} \equiv d_1^{m_i q_i^{b_i-1}} \cdot \dots \cdot d_{i-1}^{m_i q_i^{b_i-1}} \cdot d_i^{m_i q_i^{b_i-1}} \cdot d_{i+1}^{m_i q_i^{b_i-1}} \cdot \dots \cdot d_r^{m_i q_i^{b_i-1}} \equiv \\ &\equiv d_i^{m_i q_i^{b_i-1}} \pmod{p}, \end{aligned}$$

ou seja,

$$d_i^{m_i q_i^{b_i-1}} \equiv 1 \pmod{p},$$

Mas, como  $\text{mdc}(m_i, q_i^{b_i}) = 1$ , e  $\mathbf{o}_p(d_i) = q_i^{b_i}$ , concluimos por 11.11 que

$$\mathbf{o}_p(d_i^{m_i}) = q_i^{b_i}.$$

Isto dá a contradição

$$d_i^{m_i q_i^{b_i-1}} \not\equiv 1 \pmod{p}.$$

Portanto,  $a^\ell \not\equiv 1 \pmod{p}$  para todo  $\ell < p-1$ . Isto significa

$$\mathbf{o}_p(a) = p-1.$$

■

### 11.18 Proposição.

Seja  $2 < p \in \mathbb{P}$  e  $k \in \mathbb{N}$ . Então existe uma raiz primitiva  $\pmod{p^k}$ , i. e. existe  $b \in \mathbb{Z}$  tal que  $\text{mdc}(b, p^k) = 1$  e  $\mathbf{o}_{p^k}(b) = p^{k-1}(p-1) = \varphi(p^k)$ .

A demonstração desta proposição é feita pela



### 11.19 Observação.

Seja  $p > 2$  um primo. Então

- Existe raiz primitiva  $r \pmod p$  tal que  $r^{p-1} \not\equiv 1 \pmod{p^2}$ .
- Para todo  $r$  de a) vale  $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$  para todo  $k \geq 2$ .
- Todo  $r$  de a) é uma raiz primitiva  $\pmod{p^k}$  para todo  $k \geq 1$ .

Antes de demonstrarmos esta observação, vejamos um

### 11.20 Exemplo.

Para  $p = 5$  temos que 2 e 3 são raízes primitivas  $\pmod 5$ , ambas satisfazendo  $2^{5-1} = 2^4 = 16 \not\equiv 1 \pmod{25}$  e  $3^{5-1} = 3^4 = 81 \equiv 6 \not\equiv 1 \pmod{25}$ . Conseqüentemente 2 e 3 são raízes primitivas  $\pmod{5^k}$  para todo  $k$ .

Módulo 25 temos por exemplo  $\varphi(\varphi(25)) = \varphi(20) = 8$  raízes primitivas, a saber,

$$\{2, 2^3, 2^7, 2^9, 2^{11}, 2^{13}, 2^{17}, 2^{19}\} \equiv \{3, 3^3, 3^7, 3^9, 3^{11}, 3^{13}, 3^{17}, 3^{19}\} \equiv \\ \{2, 8, 3, 12, 23, 17, 22, 13\} \pmod{25}.$$

**Demonstração** de 11.19: a) Seja  $a \in \mathbb{Z}$  raiz primitiva  $\pmod p$  (cuja existência é garantida por 11.17).

Se  $a^{p-1} \not\equiv 1 \pmod{p^2}$ , consideremos  $r = a$ . Se  $a^{p-1} \equiv 1 \pmod{p^2}$ , consideremos  $r = a + p$  que também é raiz primitiva  $\pmod p$ . Vale

$$r^{p-1} = (a + p)^{p-1} = a^{p-1} + (p-1)pa^{p-2} + p^2[\dots] \equiv \\ \equiv 1 + (p-1)pa^{p-2} \not\equiv 1 \pmod{p^2}$$

pois  $(p-1)pa^{p-2} \not\equiv 0 \pmod{p^2}$ .

b) Seja  $r$  uma raiz primitiva  $\pmod p$  com  $r^{p-1} \not\equiv 1 \pmod{p^2}$ . Provemos por indução sobre  $k$  que  $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$  para todo  $k \geq 2$ . A afirmação está correta para  $k = 2$ . Suponhamos, já provado

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k} \quad \text{para algum } k \geq 2.$$

Pelo teorema de EULER temos  $r^{p^{k-2}(p-1)} = r^{\varphi(p^{k-1})} \equiv 1 \pmod{p^{k-1}}$ , ou seja,

$$r^{p^{k-2}(p-1)} = 1 + cp^{k-1} \quad \text{com } p \nmid c.$$

Segue

$$\begin{aligned} r^{p^{k-1}(p-1)} &= \left[ r^{p^{k-2}(p-1)} \right]^p = (1 + cp^{k-1})^p = 1 + pcp^{k-1} + p^{k+1} [\dots] \equiv \\ &\equiv 1 + pcp^{k-1} \not\equiv 1 \pmod{p^{k+1}}, \text{ pois } p \nmid c. \end{aligned}$$

c) Seja  $r$  uma raiz primitiva  $\pmod{p}$  com  $r^{p-1} \not\equiv 1 \pmod{p^2}$ .

Por b) temos  $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$  para todo  $k \geq 2$ . Temos por 11.3

$$\mathfrak{o}_{p^k}(r) \mid \varphi(p^k) = p^{k-1}(p-1).$$

De  $r^{\mathfrak{o}_{p^k}(r)} \equiv 1 \pmod{p^k}$  segue  $r^{\mathfrak{o}_{p^k}(r)} \equiv 1 \pmod{p}$  e daí por 11.3

$$\mathfrak{o}_p(r) = p-1 \mid \mathfrak{o}_{p^k}(r).$$

Segue então  $\mathfrak{o}_{p^k}(r) = (p-1)p^m$  com  $0 \leq m \leq k-1$ .

Como  $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$  concluímos  $m = k-1$ , ou seja,

$$\mathfrak{o}_{p^k}(r) = (p-1)p^{k-1} = \varphi(p^k).$$

Isto significa que  $r$  é raiz primitiva  $\pmod{p^k}$ . ■

### 11.21 Observação.

Seja  $p > 2$  um primo e  $k \in \mathbb{N}$ . Então existe raiz primitiva  $\pmod{2p^k}$ .

**Demonstração:** Temos  $\varphi(2p^k) = \varphi(2)\varphi(p^k) = p^{k-1}(p-1) = \varphi(p^k)$ . Por 11.18 existe raiz primitiva  $r \pmod{p^k}$ . Também  $r + p^k$  é raiz primitiva  $\pmod{p^k}$ . Consideremos  $r'$  o ímpar dos dois números  $r$  e  $r + p^k$ , de sorte que  $\text{mdc}(r', 2p^k) = 1$ . Claramente  $\mathfrak{o}_{2p^k}(r') = p^{k-1}(p-1) = \varphi(2p^k)$ . ■

### 11.22 Exemplo.

Módulo  $p = 5$  temos as raízes primitivas 2 e 3. Como 3 é ímpar, 3 é também raiz primitiva  $\pmod{10}$ . 2 não serve como raiz primitiva  $\pmod{10}$ , pois não tem ordem  $\pmod{10}$ . Mas  $2 + 5 = 7$  é raiz primitiva  $\pmod{10}$ .

Como o exemplo 11.20 mostra, as 8 raízes primitivas  $\pmod{25}$  são

$$\{2, 8, 3, 12, 23, 17, 22, 13\}.$$

As 4 raízes primitivas *ímpares* mod 25, a saber  $\{3, 23, 17, 13\}$  são também raízes primitivas mod 50. Somando-se ainda 25 às 4 pares  $\{2, 8, 12, 22\}$ , vemos que

$$\{3, 23, 17, 13\} \cup \{27, 33, 37, 47\}$$

são todas as 8 raízes primitivas mod 50.

Encerramos esta introdução à Teoria dos Números, resumindo os nossos conhecimentos sobre as raízes primitivas no

### 11.23 Teorema.

Para  $2 \leq n \in \mathbb{N}$ , as seguintes afirmações são equivalentes:

- a) *Existe raiz primitiva mod n.*
- b)  $n \in \{2, 4, p^k, 2p^k \mid 2 < p \in \mathbb{P}, k \in \mathbb{N}\}$ .

### 11.24 Exemplo.

Os números  $n \leq 100$ , módulo os quais existe raiz primitiva são **além dos números primos**  $\{2, 3, 5, \dots, 89, 97\}$ :

$\{4, 6, 9, 10, 14, 18, 22, 25, 26, 27, 34, 38, 46, 49, 50, 54, 58, 62, 74, 81, 82, 86, 94, 98\}$ .